[12] 1) a) Soit R un anneau commutatif. Définir les notions d'un

(i) idéal premier

(ii) idéal maximal.

b) Donner un exemple d'un idéal premier qui n'est pas maximal (sans justification)

c) Trouver tous les idéaux dans $R = \mathbb{Z}_8 = \mathbb{Z}/8\mathbb{Z}$ et identifier ceux qui sont premiers ou maximaux

Solution: (a) Un idéal I est

[2] (i) premier si $I \neq R$ et si $ab \in I \Rightarrow a \in I$ ou $b \in I$ quels que soient $a, b \in R$

[2] (ii) maximal si $I \neq R$ et si $I \subset J \subseteq R \Rightarrow I = J$ ou $J = R$

[2] (b) Dans $R = \mathbb{Z}$, $I = \{0\}$ est un idéal premier qui n'est pas maximal.

[6] (c) (Devoir 3) Vu que $R = \mathbb{Z}/8\mathbb{Z}$ et $8\mathbb{Z} \triangleq \mathbb{Z}$, les idéaux de R sont tous de la forme $n\mathbb{Z}/8\mathbb{Z}$ où $8\mathbb{Z} \subseteq n\mathbb{Z}$, donc $n \mid 8$. Donc $n = 1, 2, 4$ ou 8

$n = 1$: $\mathbb{Z}/8\mathbb{Z} = R = I$: I n'est pas maximal, ni premier

$n = 2$: $2\mathbb{Z}/8\mathbb{Z} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\} = \langle \bar{2} \rangle \subsetneq R$

$n = 4$: $4\mathbb{Z}/8\mathbb{Z} = \{\bar{0}, \bar{4}\} = \langle \bar{4} \rangle \subsetneq \langle \bar{2} \rangle$

$n = 8$: $8\mathbb{Z}/8\mathbb{Z} = \{\bar{0}\}$

$I = \langle \bar{2} \rangle$ est maximal, les autres idéaux ne le sont pas car ils sont tous contenus dans $\langle \bar{2} \rangle$

$\langle \bar{2} \rangle$ est le seul idéal premier (maximal $\Rightarrow$ premier)

$\langle \bar{4} \rangle \ni \bar{4} = \bar{2} \cdot \bar{2}$ mais $\bar{2} \notin \langle \bar{4} \rangle$ etc.

[8] 2) Prouver que le polynômes f est irréductible dans $F[x]$

(a) $F = \mathbb{Q}$, $f = 3x^3 + 5x^2 + x + 2$

(b) $F = \mathbb{Q}$, $f = x^5 + 6x^4 + 12x + 15$

[4] Solution: (a) Vu que $\deg(f) = 3$, f est irréductible si et seulement si f n'a pas des racines dans $\mathbb{Q}$. Mais d'après le critère de la racine rationelle, les seuls possibilités pour une racine rationelle sont

$$\pm 1, \pm 2, \pm \tfrac{1}{3}, \pm \tfrac{2}{3}$$

Il est claire que $f(x) \geq 2$ pour $x > 0$. Donc il suffit de vérifier $f(x)$ pour $x = -1, -2, -\frac{1}{3}, -\frac{2}{3}$. On trouve

$f(-1) = -3 + 5 - 1 + 2 = 3$

$f(-2) = -24 + 20 - 2 + 2 = -4$

$f(-\frac{1}{3}) = -\frac{1}{9} + \frac{5}{9} - \frac{1}{3} + 2 > 0$

$f(-\frac{2}{3}) = \quad > 0$

Autre solution: On réduit modulo 5, et l'on obtient le polynôme $f = 3x^3 + x + 2 = 3(x^3 + 2x - 1)$ et l'on vérifit que $x^3 + 2x - 1$ n'a pas de racines dans $\mathbb{Z}_5$

[4] (b) On applique le critère d'Eisenstein avec $p = 3$

[12] 3) Soit F un corps, et soit $0 \neq I \trianglelefteq F[x]$ un idéal de $F[x]$.
Prouver qu'il y a un polynôme unitaire h tel que
$I = \langle h \rangle$

Solution: D'abord, I contient des polynômes unitaires car $I \neq 0 \Rightarrow 0 \neq f \in I \Rightarrow a^{-1} f \in I$, où a = coefficient dominant de f, et $a^{-1} f$ est un polynômes unitaire. Soit $h \in I$ un polynôme unitaire de degré minimal. On a $\langle h \rangle \subset I$. Pour l'autre inclusion, soit $f \in I$. La division avec reste nous donne $q, r \in F[x]$ telle que $f = qh + r$ avec $r = 0$ ou $\deg r < \deg h$. Si $r \neq 0$ alors $r = f - qh \in I$ car f et $qh \in I$. Si b = coeff dominant de r, le polynôme $b^{-1} r \in I$ est unitaire et $\deg(b^{-1} r) < \deg(h)$, contradiction. Alors, $r = 0$ et $f = qh \in \langle h \rangle$. □

[12] 4) Soit R un anneau intègre.

(a) Donner la définition d'un élément premier dans R et la définition d'un élém. irréd.

(b) Montrer : Un élément premier est un élément irréductible

[4] Solution (a) On dit q'un élément de R est irréductible si ... (voir en bas)

On dit que $p \in R$ est premier si

(i) $p \neq 0$ et $p \notin R^\times$

et (ii) si $p \mid ab$, alors $p \mid a$ et $p \mid b$

[8] (b) Par définition, un élément $p \in R$ est irréductible si

(i) $p \neq 0$ et $p \notin R$, et

(ii) si $p = ab$, alors $a \in R$ ou $b \in R$.

Vu que la condition (i) de deux définitions est la même, il suffit de prouver que (ii) est remplie, ie.

$$p = ab \overset{!}{\Rightarrow} a \in R \text{ ou } b \in R.$$

Mais $p = ab \Rightarrow p \mid ab \Rightarrow p \mid a$ ou $p \mid b$ (car p est premier)

Dans le premier cas on a $pc = a$ pour un $c \in R$, donc $p = ab = pcb$. Ceci implique que $cb = 1$, ie $b \in R^\times$ (car R est un anneau intègre). Dans le deuxième cas, ie $p \mid b$, on conclut de même que $a \in R^\times$.

[9] 5) Soit $R = \mathbb{Z}[\sqrt{-3}] = \{m + n\sqrt{-3} : m, n \in \mathbb{Z}\}$; c'est un sous-anneau de $\mathbb{C}$, donc un anneau intègre (il n'est pas nécessaire de prouver ça). Montrer

(i) $R^\times = \{\pm 1\} = \{r \in R : N(r) = 1\}$ (indice : $N : R \to \mathbb{N}$, $N(m+n\sqrt{-3}) = (m+n\sqrt{-3})(m-n\sqrt{-3}) = m^2 + 3n^2$)

(ii) $1 + \sqrt{-3}$ est irréductible, mais pas premier.

[3] Solution : (i) Si $u \in R^\times$, $u = m + n\sqrt{-3}$, et $v = u^{-1}$, alors on a $1 = N(1_R) = N(uv) = N(u)N(v)$, donc $N(u) = N(v) = 1$, alors $u = \pm 1$. L'autre direction est évident.

[3] (ii) Clairement, $p = 1 + \sqrt{-3} \neq 0$ et $p \notin R^\times$ d'après (i). Si $p = ab$, alors $4 = N(p) = N(a)N(b)$. Mais $N(a) \neq 2$, donc soit $N(a) = 1$, i.e. $a \in R^\times$, ou $N(b) = 1$, i.e. $b \in R^\times$. Alors p est irréductible.

[3] p n'est pas premier : $(1+\sqrt{-3})(1-\sqrt{-3}) = 1 + 3 = 4 = 2 \cdot 2$ et $p \nmid 2$: $pc = 2 \Rightarrow 4 = N(2) = N(p)N(c) = 4N(c)$ $\Rightarrow N(c) = 1$, $c = \pm 1$, ↯ !