[10] 1) (a) Donner la définition d'un idéal maximal, et d'un anneau simple.

(b) Soit R un anneau (pas nécessairement commutatif), et soit $I \trianglelefteq R$ un idéal de R. Prouver : I est un idéal maximal ssi R/I est un anneau simple

Solution : (a) Un idéal I d'un anneau R est <u>maximal</u> si

[2] (i) $I \neq R$ et (ii) si pour $I \subseteq J \subseteq R$, $J \trianglelefteq R$ on a $I = J$ ou $J = R$.
Un anneau R est un anneau simple si (i) $R \neq \{0\}$ et si (ii) pour chaque idéal $I \trianglelefteq R$ on a $I = \{0\}$ ou $I = R$.

[6] (b) "$\Rightarrow$" Si I est maximal, alors $R/I \neq \{0\}$ car $I \neq R$.
Chaque idéal $A \trianglelefteq R/I$ est de la forme $A = J/I$ où $J \trianglelefteq R$ tel que $I \subseteq J$. Vu que I est maximal, on a soit $I = J$, soit $J = R$, donc soit $A = 0$, soit $A = R/I$

"$\Leftarrow$" Vu que $R/I \neq \{0\}$, on a $I \neq R$.
Soit $J \trianglelefteq R$ tel que $I \subseteq J \subseteq R$. Alors $A = J/I \trianglelefteq R/I$.
Donc soit $A = \{0\}$, soit $A = R/I$. Dans le premier cas, $I = J$, dans le deuxième cas $J = R$. Alors, I est maximale.

[2] (c) Donner tous les idéaux maximaux dans $R = \mathbb{Z}$ (sans preuve)

Solution : Chaque idéal $I \trianglelefteq R$ est de la forme $I = n\mathbb{Z}$, $n \in \mathbb{N}$; il est maximal ssi n est un nombre premier

[10] 2) Soit F un corps, et soient $f, g \in F[x]$ des éléments non nuls.

(a) Donner la définition d'un pgcd de f et g

(b) Prouver qu'un pgcd de f et g existe.

[2] Solution (a) On appelle $d \in F[x]$ un pgcd(f,g) si

(i) $d \mid f$ et $d \mid g$, et

(ii) si $h \mid f$ et $h \mid g$, alors $h \mid d$

(iii) d est unitaire (ceci n'est nécessaire)

[8] (b) On pose $X = \{uf + vg : u, v \in F[x]\}$. Alors $X \trianglelefteq F[x]$ (en effet, c'est l'idéal engendré par f et g). On a $X \neq 0$ car $0 \neq f \in X$. Donc, $X = \langle d \rangle$ où $d \in F[x]$ est un polynôme unitaire. On utilise l'algorithme de division pour écrire

$$f = qd + r, \quad q, r \in F[x], \quad r = 0 \text{ ou } \deg r < \deg d$$

En plus, on a $u, v \in F[x]$ tel que $d = uf + vg$. Alors

$$r = f - qd = f - q(uf + vg) = (1 - qu)f + (-qv)g \in X = \langle d \rangle$$

Donc $r = wd$ pour un $w \in F[x]$. Si $r \neq 0$, on a $\deg(r) \geq \deg(d) > \deg(r)$, $\lightning$! Alors $r = 0$, et $d \mid f$. De même, $d \mid g$. Donc (a.i) est vrai.

Soit $h \in F[x]$ t.q. $h \mid f$ et $h \mid g$. De $d = uf + vg$ on voit que $h \mid d$. Donc (a.ii) est vrai aussi.

3) Trouver toutes les racines rationnelles de $f = x^4 - x^3 - x^2 - x - 2$ et écrire f comme un produit des polynômes irréductibles dans $\mathbb{Q}[x]$.

[8] Solution: D'après le critère de la racine rationnelle, les racines de f dans $\mathbb{Q}$ sont des diviseurs de 2. On calcule

$$f(2) = 16 - 8 - 4 - 2 - 2 = 0$$
$$f(-2) = 16 + 8 - 4 + 2 - 2 = 20$$
$$f(1) = 1 - 1 - 1 - 1 - 2 = -4$$
$$f(-1) = 1 + 1 - 1 + 1 - 2 = 0$$

Donc on peut écrire $f = (x-2)(x+1)g = (x^2 - x - 2)q$

où $q \in \mathbb{Q}[x]$ est un polynôme irréductible, car $\deg q = 2$ et q n'a pas des racines dans $\mathbb{Q}$. On trouve q par division:

$$x^4 - x^3 - x^2 - x - 2 \;:\; x^2 - x - 2 = x^2 + 1$$
$$x^4 - x^3 - 2x^2$$
$$\overline{\qquad\qquad - x^2 - x - 2}$$

Alors $f = (x-2)(x+1)(x^2+1)$

est une factorisation de f en facteurs irréductibles.

Référence: §4.1, Exc 25c

[10] 4) Soit F un corps, et soit $h = p_1^{e_1} \cdots p_s^{e_s} \in F[x]$, où $s, e_1, \dots, e_s \geq 1$ et les $p_1, \dots, p_s \in F[x]$ sont irréductibles. On pose $R = F[x]/\langle h \rangle$.

Prouver :

écarté

(a) Si $e_i \geq 2$ pour un i, alors R contient un élément nilpotent non nul.

[4] Solution Soit $e_i \geq 2$. Donc on peut écrire $h = p_i^2 g$ avec $g \in F[x]$. Soit $r = p_i g + \langle h \rangle \in R$. Alors, $r \neq 0$ car $r = 0 \Rightarrow p_i g \in \langle h \rangle$, $p_i g = fh$ $\not\downarrow$ car $\deg p_i g < \deg h$. Aussi $r^2 = p_i^2 g^2 + \langle h \rangle = 0$ car $p_i^2 g^2 = p_i (p_i^2 g) = p_i h \in \langle h \rangle$. Donc r satisfait aux conditions imposées.

(b) Soit $s = 1$, donc $h = p^e$, et soit I l'image canonique de $\langle p \rangle$ dans R (donc $I = \{ f + \langle h \rangle : f \in \langle p \rangle \}$).

Montrer : $R \setminus I = R^\times$ et $I = \{ r \in R : r \text{ nilpotent} \}$

[10] Solution : Soit $r \in I$, par exemple $r = f + \langle h \rangle$, $f = gp$ pour un $g \in F[x]$. Alors $r^e + \langle h \rangle = g^e h + \langle h \rangle = 0_R$. Donc

$$I \subset \{ r \in R : r \text{ nilpotent} \} =: \mathcal{N} \qquad (*)$$

Soit $r = f + \langle h \rangle \notin I$. Donc $p \nmid f$, et a fortiori $p^e \nmid f$. Donc $\operatorname{pgcd}(h, f) \sim 1$, et il y a $u, v \in F[x]$ tels que $1 = uh + vf$. Alors $(f + \langle h \rangle)(v + \langle h \rangle) = 1 + \langle h \rangle$ montre

$$R \setminus I \subset R^\times := \{ x \in R : x \text{ inversible} \} \qquad (**)$$

Maintenant, les égalités $R \setminus I = R^\times$ et $\mathcal{N} = I$ découle de (*) et (**)

(Exercices de devoir 6 et devoir 6 - suppl)

5) Soit R un anneau intègre avec une fonction $\delta : R \to \mathbb{N}$ telle que pour $a, b \in R$ et $b \neq 0$ il y a $q, r \in R$ tels que

$$a = qb + r, \quad r = 0 \text{ ou } \delta(r) < \delta(q)$$

[8] Prouver que R est un anneau principal.

Preuve: Soit $I \trianglelefteq R$. Il faut prouver que $I = \langle b \rangle$ pour un $b \in R$, où $\langle b \rangle = \{ br : r \in R \}$. Si $I = \{0\}$, alors $I = \langle 0 \rangle$. Donc on peut supposer $I \neq 0$. On peut alors choisir $0 \neq b \in I$ tel que

$$\delta(b) = \min\{\delta(a) : 0 \neq a \in I\}$$

Alors, $\langle b \rangle \subseteq I$ car $b \in I$. Pour l'autre direction, soit $a \in I$. D'après la hypothèse on peut écrire

$$a = qb + r, \quad r = 0 \text{ ou } \delta(r) < \delta(b)$$

pour certains $q, r \in R$. En effet, $r = a - qb \in I$ car $a, b \in I$. Vu que $\delta(r) < \delta(b) = \min\{\delta(a) : 0 \neq a \in I\}$, on ne peut pas avoir $r \neq 0$. Donc $r = 0$, i.e. $a \in \langle b \rangle$. Donc $I = \langle b \rangle$.

[8] 6) Sat E/F une extension.

(a) Donner les définitions suivantes:

(i) $u \in E$ est un élément algébrique sur F,

(ii) E/F est une extension finie,

(iii) E/F est une extension algébrique.

(5) Prouver: Si E/F est une extension finie, alors E/F est une extension finie.

[3] Solution (a) (i) $u \in E$ est un élément algébrique s'il y a $0 \neq f \in F[x]$ tel que $f(e) = 0$.

(ii) E/F est une extension finie si la dimension de l'espace vectoriel E sur F est finie

(iii) E/F est une extension algébrique si chaque $e \in E$ est un élément algébrique.

[5] (5) Supposons $\dim_F E = n < \infty$. Il faut prouver que chaque $e \in E$ est algébrique sur F. Alors, les $n+1$ éléments (pas nécessairement distincts)

$$1, e, e^2, \dots, e^n$$

sont linéairement dépendants. Donc, il y a $a_0, \dots, a_n \in F$, pas tous nuls, tels que

$$0 = a_0 + a_1 e + \dots + a_n e^n = f(e) \text{ pour}$$

$$0 \neq f = a_0 + a_1 x + \dots + a_n x^n \in F[x].$$

[10] 7) Trouver un corps de décomposition E de $f = x^4 - x^2 - 2 \in \mathbb{Q}[x]$ et déterminer $[E:\mathbb{Q}]$.

Solution Vu que f est un polynôme paire, on a $f(\pm i) = 0$.

Donc $x^2+1 = (x+i)(x-i)$ divise f. On calcule

$$\begin{array}{r} x^4 - x^2 - 2 \;:\; (x^2+1) = x^2 - 2 \\ \underline{x^4 + x^2} \\ -2x^2 - 2 \\ \underline{2x^2 + 2} \\ 0 \end{array}$$

Alors $f = (x^2+1)(x^2-2)$. Donc les racines de f dans $\mathbb{C}$ sont $\pm\sqrt{2}, \pm i$. Alors $E = \mathbb{Q}(i, \sqrt{2})$ est un corps de décomposition de f. On a un tour des corps de décomposition :

$$\begin{array}{l} E = \mathbb{Q}(i,\sqrt{2}) \\ \quad | \\ K = \mathbb{Q}(\sqrt{2}) \\ \quad | \\ \mathbb{Q} \end{array}$$

Donc $[E:\mathbb{Q}] = [E:K][K:\mathbb{Q}]$.

On sait $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ car x^2-2 est irréductible sur $\mathbb{Q}$ ($\pm\sqrt{2} \notin \mathbb{Q}$)

Pour $[E:K]$ on a $[E:K] \geq 2$ car $E \not\subset \mathbb{R}$ mais $K \subset \mathbb{R}$. D'autre côté, $g(i) = 0$ pour $g = x^2+1 \in \mathbb{Q}[x] < K[x]$, donc $[E:K] \leq 2$. Alors $[E:K] = 2$ et en total on l'obtient $[E:\mathbb{Q}] = 4$.

(Similaire à l'exercice 1 de §6.3)

Autre solution: On utilise le critère de la racine rationelle pour trouver que $f(\pm 2) = 0$, donc $x^2 - 2 \mid f$. Après division on obtient $f = (x^2+1)(x^2-2)$, et l'on procède comme avant.

[12]8 (a) Déterminer tous les idéaux $I \trianglelefteq \mathbb{F}_2[x]$ tels que $\mathbb{F}_2[x]/I \cong \mathbb{F}_8$. Vous devez justifier votre réponse.

[8] Solution : (Exercice suggéré, §6.4 #1c)

(pour $f \in \mathbb{F}_2[x]$ unitaire)

$\mathbb{F}_2[x]$ est un anneau principal, donc $I = \langle f \rangle$! Aussi $\mathbb{F}_8$ est un corps, donc f est irréductible. Finalement $[\mathbb{F}_8 : \mathbb{F}_2] = 3$ $= \dim_{\mathbb{F}_2} (\mathbb{F}_2[x]/\langle f \rangle) = \deg f$. Alors :

$$f = a_0 + a_1 x + a_2 x^2 + x^3 \quad , \quad a_i \in \mathbb{F}_2 = \{0,1\}$$

Si $a_0 = 0$ alors $x \mid f$, donc f n'est pas irréductible. Alors :

$$f = 1 + a_1 x + a_2 x^2 + x^3 \ .$$

Vu que $\deg f = 3$, on sait f irréductible $\Leftrightarrow$ f n'a pas des racines dans $\mathbb{F}_2$ $\Leftrightarrow$ $f(0) \neq 0 \neq f(1)$

$\Leftrightarrow$ $1 \neq 1 + 0$ et $1 = 1 + a_1 + a_2 + 1$ $\Leftrightarrow$ $1 = a_1 + a_2$

$\Leftrightarrow$ $(a_1, a_2) = (1,0)$ ou $(a_1, a_2) = (0,1)$.

Alors, $\mathbb{F}_2[x]/I \cong \mathbb{F}_8$ $\Leftrightarrow$ $I = \langle 1 + x + x^3 \rangle$ ou $I = \langle 1 + x + x^2 + x^3 \rangle$.

[4] (b) Pour votre choix de I trouver un élément primitif de $\mathbb{F}_8$.

Solution : $(\mathbb{F}_8 \setminus \{0\}, \cdot)$ est un groupe d'ordre 7. Donc chaque élément $u \in \mathbb{F}_8$, $u \neq 0$ et $u \neq 1$, est un élément primitif.

[5 points bonus]

9) Vrai ou faux? Vous devez justifier vos réponses

[1] (a) Dans $\mathbb{Z}[i]$ l'élément $1+i$ est un élément premier, qui n'est pas irréductible.

Réponse: Faux, car un élément premier est toujours irréductible.

[2] (b) $\mathbb{C}$ est la clôture algébrique de $\mathbb{Q}$

Réponse: Faux, car chaque élément d'une clôture algébrique est un élément algébrique sur $\mathbb{Q}$, mais π (ou e) ne sont pas algébrique sur $\mathbb{Q}$

[2] (c) $\mathbb{Z}[x]$ est un anneau factoriel

Réponse: Vrai, car R factoriel $\Rightarrow R[x]$ factoriel d'après le Thm