M1 Année 2016/2017

ELEMENTS DE CORRECTION

Question du cours :

1. Donner le critère d'Eisenstein pour qu'un polynôme à coefficients dans un anneau A factoriel soit irréductible.

   donner une démonstration du critère d'Eisenstein pour $A = \mathbb{Z}$ et p un nombre premier en considèrant le morphisme de réduction modulo p, $\mathbb{Z}[X] \to (\mathbb{Z}/(p))[X]$,

> Cours

2. Soit p un nombre premier montrer que

$$X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X],$$

   est irreductible. [Indication : on pourra poser $X = Y + 1$]

> En utilisant la substitution $X = Y + 1$ on obtient un polynôme dont :
>
> - tous les coeffs sont divisible par p sauf le dominant
> - le terme constant qui vaut p.

3. Montrer que $X^4 + 1$ est irreductible dans $\mathbb{Z}[X]$.

> En utilisant la substitution $X = Y + 1$ on obtient le polynôme $Y^4 + 4Y^3 + 6Y^2 + 6Y + 2$. Puis on applique Eisenstein avec $p = 2$

Exercice 1

1. (a) Donner un exemple d'un anneau intègre qui n'est pas factoriel.

> $\mathbb{Z}[i\sqrt{3}] \subset \mathbb{C}$ est intègre car $\mathbb{C}$ est intègre. Mais
>
> $$2 \times 2 = 4 = (\sqrt{3} + i)(\sqrt{3} - i),$$
>
> et $2, (\sqrt{3} + i)$ sont irreductible non associés.

(b) Donner un exemple d'un anneau factoriel qui n'est pas principal.

$A[X]$ est factoriel ssi A est factoriel
mais $A[X]$ est principal ssi A est un corps :

- $\mathbb{Z}[X]$ est factoriel car $\mathbb{Z}$ factoriel mais pas principal car $\mathbb{Z}$ n'est pas un corps.

2. Donner un exemple d'un anneau A avec un idéal premier $I \subset A$ qui n'est pas maximal.

L'idéal $(X) \subset \mathbb{R}[X, Y]$ est premier car

$$X|fg \Rightarrow X|f \text{ ou } X|g$$

mais (X) n'est pas maximal car contenu dans l'idéal des polynômes qui s'annulent en $(0, 0)$.

3. (a) Soient A, B des anneaux commutatifs et $\phi : A \to B$ un morphisme d'anneaux commutatifs (tel que $\phi(1_A) = 1_B$). Montrer que si $I \subset B$ est un idéal premier alors $\phi^{-1}(I) \subset A$ est un idéal premier.

- $I \neq \{0_B\}$ premier ssi B/I intègre et il suffit de montrer que $A/\phi^{-1}(I)$ est intègre
- Le morphisme $\phi : A \to B$ induit un morphisme

$$\phi : A/\phi^{-1}(I) \to B/I,$$

injectif car son nouyau $= \phi^{-1}(I)$.
On voit ainsi que $A/\phi^{-1}(I)$ est intègre car isomorphe à un sous anneau d'un anneau intègre

(b) Determiner les idéaux maximaux de $\mathbb{R}[X]/(X^2)$.

Soit $I \subset \mathbb{R}[X]/(X^2)$ un idéal et $\mathbb{R}[X]$ est principal, car $\mathbb{R}$ est un corps, donc $\exists f$, $\phi^{-1}(I) = (f)$
Par hyp. $(X^2) = \ker \phi \subset (f)$ donc $f|X^2$

- f = 1 et $(f) = \mathbb{R}[X] \Rightarrow I = \mathbb{R}[X]/(X^2)$
- f = X
- $f = X^2$ et $(f) = \ker \phi = 0_{\mathbb{R}[X]/(X^2)}$

BILAN : il existe un unique idéal maximal $\phi((X))$.

4. (a) Montrer que $X^2 + X + 1$ est irréductible dans $\mathbb{R}[X]$.

- $X^2 + X + 1$ est de degré 2 donc irreductible $\Leftrightarrow$ il n'a pas de racine dans $\mathbb{R}$.
- Son discriminant = -3.

(b) Determiner les idéaux maximaux de $\mathbb{R}[X]/(X^2 + X + 1)$.

X^2+X+1 irred donc premier car $\mathbb{R}[X]$ principal $\Rightarrow \mathbb{R}[X]/(X^2+X+1)$ un corps
$\Rightarrow$ 2 idéaux et aucun n'est maximal.

Exercice 2

1. Soient K un corps, L une extension finie de K et M, $K \subset M \subset L$ un corps intermediare. Décrire la relation entre les degrés $[L : K], [M, K]$ et $[L : M]$.

$$[M : K] = [L : M][L : K].$$

2. Soient L un corps, $K \subset L$ un sous corps et $\alpha \in L$. Montrer que $K(\alpha)$, l'intersection de tous les sous corps de L qui contiennent K et α, est un corps.

(a) Un sous corps est un sous anneau et l'intersection de sous anneaux est sous anneau.

(b) Il suffit de verifier que si x appartient à l'intersection alors x^{-1} aussi (facile).

3. On suppose que $[L : K]$ est fini.

(a) Montrer que le morphisme d'évaluation

$$\mathrm{spe}_\alpha : K[X] \to L$$

n'est pas injectif.

Le morphisme spe_α est un morphisme de K-e.v. et son image est un sous e.v. L'espace de départ $K[X]$ est un K-e.v. de dimension infinie et l'espace d'arrivée est de dimension finie.
Tout sous espace d'une espace de dimension finie est finie $\Rightarrow$ spe_α n'est pas injectif.

(b) Donner la définition :

i. du degré de α sur K.

C'est le degré du poly. minimal P_α qui est generateur du $\ker \text{spe}_\alpha$.

ii. du degré de $K(\alpha)$ sur K.

C'est la dimension de $K(\alpha)$ comme K-e.v.

(c) Montrer que $K(\alpha) = K[\alpha]$ et en déduire que le degré de α sur K est égal au degré de $K(\alpha)$ sur K.

Evidement $K[\alpha] \subset K(\alpha)$ et il suffit de montrer que $K(\alpha) \subset K[\alpha]$. J'ai fait en cours.

(d) Soient $\alpha, \beta \in L$ avec le degré de α sur K égal à m et le degré de β sur K égal à n. Montrer que $\alpha + \beta$ est algebrique sur K de degré au plus mn.

$\alpha\beta \in K(\alpha, \beta) \Rightarrow K(\alpha\beta) \subset K(\alpha, \beta) = K(\alpha)(\beta)$ et d'après les question precedentes il suffit de majorer $[K(\alpha, \beta) : K]$. On a que :

- $K(\alpha) : K] = m$
- $K(\alpha, \beta) : K(\alpha)] \leq K(\beta) : K] = n$

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K] \leq n \times m.$$

4. (a) Soient K un corps et $f \in K[X]$ un polynôme unitaire de degré 3. Montrer que le degré du corps de décomposition de f sur K est un diviseur de 6.

Le degré de f est strictement inferieur à 4 donc f est irréductible ssi f n'a pas de racine dans K.

- Si f a une racine $\alpha \in K$ alors $f = (X - \alpha)g$ pour $g \in K[X]$ de degré 2. Le corps de rupture est soit K si g admet une racine soi une extension quadratique de K.
- Si f n'a pas de racine on note L le corps de decomposition et on choisit une corps de rupture M qui est forcement de degré 3. Si on note $\alpha \in M$ l'argument precedent montre que $[L : M] = 1, 2$.

(b) Soit $\mathbb{F}_3$ le corps de cardinal 3 et $f = X^3 + X^2 + 1 \in \mathbb{F}_3[X]$.

i. Est-ce que le polynôme f est irréductible sur $\mathbb{F}_3$?

Non car f a une racine $X = 1$

ii. Determiner le corps de décomposition de f.

- f n'a pas de racine multiple car f et $f' = 2X$ sont premiers entre eux.
- f ne s'annule pas en $0, 2 \in \mathbb{F}_3$ donc le corps de decomposition n'est pas $\mathbb{F}_3$ et il est donc une extension quadratique de $\mathbb{F}_3$. Or un corps fini $\mathbb{F}_q$ admet une unique extension quadratique à savoir $\mathbb{F}_{q^2}$.

Réponse : $\mathbb{F}_9$.

Exercice 3

On considère la matrice

$$M = \begin{pmatrix} 9 & 15 & 21 \\ 15 & 9 & 6 \\ 21 & 6 & 9 \end{pmatrix}$$

1. Calculer :

(a) le PGCD des coefficients de M.

PGCD = 3

(b) le déterminant de M.

$-1809 = -27 \times 67$

(c) le produit

$$\begin{pmatrix} 1 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 9 & 15 & 21 \\ 15 & 9 & 6 \\ 21 & 6 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 18 & 18 \\ 15 & 9 & 6 \\ 21 & 6 & 9 \end{pmatrix} \tag{1}$$

2. (a) Trouver une matrice équivalente à M de la forme

$$M = \begin{pmatrix} 3 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$

où $a, b, c, d \in \mathbb{Z}$ sont à determiner.

A partir de la matrice dans (1) j'ai trouvé

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -81 & -120 \\ -84 & -117 \end{pmatrix}$$

L'important est le PGCD = 3 et le det = -603

(b) Préciser le PGCD de quatre entiers a, b, c, d.

PGCD = 3

3. Trouver la matrice réduite équivalente à M :

$$\begin{pmatrix} a_1 & 0 & 0 \\ 0 & a_2 & b \\ 0 & c & a_3 \end{pmatrix}$$

avec $a_i \in \mathbb{Z}$.

$a_1 = |a_2| = 3$, $|a_3| = 201$

4. Soit N le sous-module de $\mathbb{Z}^3$ engendré par les vecteurs colonne de la matrice M. Trouver une base de $\mathbb{Z}^3$ adaptée à N.

Pas necessaire pour faire la suite et pas de solution unique.

5. Décrire la classe d'isomorphisme du groupe $\mathbb{Z}^3/N$.

$\mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/201$