Algèbre

Corrigé examen partiel

I - Exemples

1. $\bar{a}$ est inversible dans $\mathbb{Z}/8\mathbb{Z}$ si et seulement si a est premier avec 8, on trouve 4 inversibles (qui sont en fait leur propre inverse) $\bar{1}$, $\overline{-1}$, $\bar{3}$, $\overline{-3}$.

2. On constate que les 4 classes restantes sont des diviseurs de zéro : $\bar{0}$ (qui est toujours un diviseur de zéro !), $\bar{2}$, $\bar{4}$, $\bar{6}$. On vérifie que chacune de ces classes multipliée par $\bar{4}$ donne la classe nulle.

3. Soit K un corps, et $I \subset K$ un idéal. Ou bien $I = (0)$, ou bien I contient un élément non nul a, et alors I contient tout $b \in K$ car $b = (ba^{-1})a$. Ainsi K et (0) sont les deux seuls idéaux de K.

4. Premier exemple standard : $A = \mathbb{Z}$ est un anneau principal, et $a = 2$ est non nul et non inversible dans $\mathbb{Z}$.

   Deuxième exemple standard: $A = \mathbb{R}[X]$ est un anneau principal, et $a = X$ est non nul et non inversible dans $\mathbb{R}[X]$.

5. Premier exemple standard : $\mathbb{Z}[X]$ est un anneau factoriel, et $I = (2, X)$ est un idéal non principal de $\mathbb{Z}[X]$.

   Deuxième exemple standard : $\mathbb{R}[X,Y]$ est un anneau factoriel, et $I = (X,Y)$ est un idéal non principal de $\mathbb{R}[X,Y]$.

6. Pour tout nombre premier p, $\mathbb{Z}/p\mathbb{Z}$ est un corps fini donc ne contient aucun sous-anneau infini, et en particulier pas de sous-anneau isomorphe à $\mathbb{Z}$.

7. Si $P(X) = (X+1)(X-1)$ alors le quotient $\mathbb{R}[X]/(P)$ n'est pas intègre, et donc non isomorphe au corps $\mathbb{C}$: on peut invoquer le résultat du cours (P n'est pas irréductible, ce qui équivaut à pas premier dans $\mathbb{R}[X]$), ou le constater directement : $\overline{(X+1)}\,\overline{(X-1)} = \bar{0}$ dans le quotient. (On pouvait faire un argument similaire avec $P(X) = X^2$).

8. Dans l'anneau $\mathbb{Z}/6\mathbb{Z}$, on a $\bar{3} \cdot \bar{3} = \bar{3}$, ainsi $\bar{3}$ est un idempotent distinct de $\bar{0}$ et $\bar{1}$.

II - Applications du cours

1. Considérons dans $\mathbb{C}[X]$ le système de congruence $\begin{cases} P(X) \equiv & X & \mod (X^2-1) \\ P(X) \equiv & -2 & \mod (X+2) \end{cases}$

   On constate que $P(X) = X$ est une solution particulière évidente (!). Par ailleurs, X^2-1 et $X+2$ sont premiers entre eux, donc (en écrivant une relation de Bézout dans l'anneau principal $\mathbb{C}[X]$), les idéaux (X^2-1) et $(X+2)$ sont comaximaux. On applique le théorème des restes chinois, qui affirme que les solutions du système sont de la forme $P(X) = X + (X^2-1)(X+2)Q(X)$, avec $Q(X) \in \mathbb{C}[X]$ arbitraire.

2. Soit $a \geq 0$ et $n \geq 2$ des entiers. On va utiliser le fait suivant : a et n sont premiers entre eux si et seulement si il existe une relation de Bézout $au + nv = 1$, avec $u, v \in \mathbb{Z}$.

   (a) Supposons a et n premiers entre eux, écrivons une relation de Bézout et réduisons là modulo n, pour obtenir $\bar{a}\bar{u} + \bar{n}\bar{v} = \bar{1}$. Comme $\bar{n} = \bar{0}$, on obtient que $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, d'inverse $\bar{u}$.

(b) Réciproquement, supposons que $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, d'inverse $\bar{u}$. Alors on a $\bar{a}\bar{u} = \bar{1}$, et donc il existe $v \in \mathbb{Z}$ tel que $au = 1 - nv$, autrement dit on a une relation de Bézout $au + bv = 1$ et a et n sont donc premiers entre eux.

3. (a) On applique l'algorithme d'Euclide :

$$X^3 + 7X^2 + 8X - 16 = (X^3 + 6X^2 + 5X - 12) + X^2 + 3X - 4$$
$$X^3 + 6X^2 + 5X - 12 = (X^2 + 3X - 4)(X + 3) + 0$$

Ainsi le PGCD des polynômes $X^3 + 7X^2 + 8X - 16$ et $X^3 + 6X^2 + 5X - 12$ dans l'anneau $\mathbb{Q}[X]$ est égal à $X^2 + 3X - 4$.

(b) Le quotient $\mathbb{Q}[X]/(P(X))$ est bien un espace vectoriel sur $\mathbb{Q}$, de dimension 2, admettant pour base $\bar{1}$, $\bar{X}$. (En général, si $P(X)$ est un polynôme de degré n sur un corps K, le quotient $K[X]/(P)$ est un espace vectoriel de dimension n et une base est $\bar{1}, \bar{X}, \ldots, \bar{X}^{n-1}$).

4. Soit A un anneau intègre, K son corps des fractions, et $P_1, P_2 \in A[X]$. Si P_2 est unitaire, alors le quotient Q obtenu en effectuant la division euclidienne de P_1 par P_2 est un polynôme à coefficient dans A. En effet le quotient Q se construit par récurrence comme une somme de $\frac{c_i}{b}X^i$ où les c_i sont dans A et b est le coefficient dominant de P_2. (Remarque: en fait demander que b soit inversible dans A suffit).

III - Quizz.

1. Vrai, car ils sont tous deux isomorphes à $\mathbb{R}$. Pour tout $a \in \mathbb{R}$, on montre que $\mathbb{R}[X]/(X - a) \simeq \mathbb{R}$ en appliquant le théorème d'isomorphisme au morphisme surjectif $\varphi\colon P(X) \in \mathbb{R}[X] \mapsto P(a) \in \mathbb{R}$, dont le noyau est $(X - a)$.

2. Faux, l'anneau quotient $\mathbb{Z}[X]/(X^2 - 1)$ n'est pas intègre, car $\overline{(X+1)}\,\overline{(X-1)} = \bar{0}$ dans ce quotient.

3. Faux, dans l'anneau quotient $\mathbb{R}[X,Y]/(X)$, $\bar{Y} \neq \bar{0}$ (car Y n'est pas un multiple de X) mais $\overline{YX} = \bar{0}$.

4. Vrai, si $a \wedge n = 1$ alors $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible, et si $a \wedge n = d > 1$ alors en posant $b = n/d \in \mathbb{N}$, on a $\bar{a}\bar{b} = \bar{0}$.

5. Faux, dans l'anneau $\mathbb{Z}[i]$ on a $1 + i = i(1 - i)$ et i est inversible, ainsi $\mathrm{PGCD}(1 + i, 1 - i) = 1 + i$.

6. Vrai, on montre que $\mathbb{R}[X]/(X^2 + X + 1)$ est isomorphe à $\mathbb{C}$ en appliquant le théorème d'isomorphisme au morphisme $\varphi\colon P(X) \in \mathbb{R}[X] \mapsto P(j) \in \mathbb{C}$ où $j = e^{2i\pi/3}$ est une racine cubique de l'unité. En effet φ est surjectif (c'est déjà vrai en restriction aux polynômes de degré 1) et $\ker\varphi = (X^2 + X + 1)$ car si $P(j) = 0$, alors $P(\bar{j}) = 0$ et donc P est multiple de $(X - j)(X - \bar{j}) = X^2 + X + 1$.