TD1 : Généralités sur les anneaux

Diego Izquierdo

Les exercices 1, 3, 7 et 10 ont été traités pendant la séance. L'exercice 15 sera traité pendant la 2è séance de TD.

Exercice 2 : Autour de $\mathbb{Z}/n\mathbb{Z}$

Soit $n > 0$ un entier.

1. (a) Quels sont les diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$? Quels sont les éléments réguliers de $\mathbb{Z}/n\mathbb{Z}$?

> **Indications :** Les diviseurs de 0 sont les classes d'entiers qui ne sont pas premiers avec n et ne sont pas multiples de n. Les éléments réguliers sont les classes d'entiers qui sont premiers avec n.

(b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ?

> **Indications :** L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si, et seulement si, il n'a pas de diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$. D'après la question 1.(a), cela revient à dire que n est premier.

2. (a) Quel est le nilradical de $\mathbb{Z}/n\mathbb{Z}$?

> **Indications :** Si $a \in \mathbb{Z}$ est tel que a^k est multiple de n pour un certain n, alors tout diviseur premier de n divise a. Réciproquement, si tout diviseur premier de n divise a, alors n divise a^k pour k assez grand. Donc, si $p_1, ...p_r$ sont les diviseurs premiers de n, le nilradical de $\mathbb{Z}/n\mathbb{Z}$ est $p_1...p_r\mathbb{Z}/n\mathbb{Z}$.

(b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il réduit ?

> **Indications :** L'anneau $\mathbb{Z}/n\mathbb{Z}$ est réduit si, et seulement si, son nilradical est réduit à (0). D'après la question 2.(a), cela équivaut à dire que, pour tout premier p, la valuation p-adique de n vaut 0 ou 1.

3. (a) Combien d'idempotents possède l'anneau $\mathbb{Z}/n\mathbb{Z}$?

> **Indications :** Écrivons $n = p_1^{\alpha_1}...p_r^{\alpha_r}$ (décomposition en produit de facteurs premiers de n). Le lemme chinois donne un isomorphisme :
>
> $$\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$
>
> Les idempotents de $\mathbb{Z}/p_i^{\alpha_i}$ sont 0 et 1. Donc les idempotents de $\prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ sont les $(x_1, ..., x_r)$ avec $x_i \in \{0, 1\}$. On en déduit que $\mathbb{Z}/n\mathbb{Z}$ a 2^n idempotents.

(b) À quelle condition sur n existe-t'il des anneaux non nuls A et B tels que $\mathbb{Z}/n\mathbb{Z} = A \times B$?

> **Indications :** Il existe des anneaux non nuls A et B tels que $\mathbb{Z}/n\mathbb{Z} = A \times B$ si, et seulement si, $\mathbb{Z}/n\mathbb{Z}$ possède des idempotents différents de 0 et 1. D'après la question 3.(a), cela équivaut à dire que n possède au moins 2 diviseurs premiers distincts.

3. Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$? Sont-ils principaux ?

Indications : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, pour d diviseur de n. Ce sont aussi des idéaux. Donc les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$. Ils sont tous principaux.

4. Quels sont les idéaux premiers de $\mathbb{Z}/n\mathbb{Z}$?

Indications : Considérons l'idéal $I = d\mathbb{Z}/n\mathbb{Z}$, avec d diviseur de n. Si d n'est pas premier, on écrit $d = ab$ avec a et b des entiers naturels différents de 1, et alors $\overline{a}\overline{b} \in I$ mais $\overline{a} \notin I$ et $\overline{b} \notin I$, donc I n'est pas premier. Réciproquement, si d est premier et on considère a et b des entiers tels que $\overline{a}\overline{b} \in I$, alors il existe des entiers u et v tels que $ab = du + nv$: on en déduit que d divise ab, et donc d divise a ou b (l'entier d étant premier). Cela prouve que $\overline{a} \in I$ ou $\overline{b} \in I$.

En résumant, les idéaux premiers de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$, avec d diviseur premier de n.

5. Soit $m > 0$ un entier. Quels sont les morphismes d'anneaux :

(a) de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

Indications : Il n'y a que la projection naturelle.

(b) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$?

Indications : Il n'y en a pas.

(c) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$?

Indications : Si m divise n, il y a uniquement la projection naturelle. Sinon, il n'y a pas de morphismes.

(d) de $\mathbb{Q}$ dans $\mathbb{Z}/n\mathbb{Z}$?

Indications : Il n'y en a pas.

Exercice 4 : Anneau des entiers algébriques

1. En exhibant un polynôme annulateur, montrer que le nombre $\sqrt{2}+\sqrt[3]{11}$ est un entier algébrique.

Indications : Soit $x = \sqrt{2} + \sqrt[3]{11}$. Alors $(x - \sqrt{2})^3 = 11$, et donc $x^3 + 6x - 11 = \sqrt{2}(3x^2 + 2)$. Cela montre que :

$$(x^3 + 6x - 11)^2 = 2(3x^2 + 2)^2,$$

et donc x est un entier algébrique.

2. Soient $a = \sqrt[3]{2} + \sqrt[3]{3}$ et $A = \mathbb{Z}[a]$. Montrer qu'en tant que groupe, A est libre de type fini. En déduire que a est un entier algébrique.

Indications : L'anneau A est contenu dans $B = \mathbb{Z}[\sqrt[3]{2}, \sqrt[3]{3}]$. Le groupe abélien B est de type fini puisqu'il est engendré par :

$$1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[3]{3}, \sqrt[3]{9}, \sqrt[3]{6}, \sqrt[3]{18}, \sqrt[3]{12}, \sqrt[3]{36}.$$

Il est de plus sans torsion. C'est donc un groupe abélien libre de type fini. Comme A est un sous-groupe de B, il est aussi abélien libre de type fini. De plus, il est engendré par les puissances de a. On en déduit qu'il existe N tel que A est engendré par $1, a, ..., a^N$ en tant que groupe abélien. Par conséquent, il existe $a_0, ..., a_N \in \mathbb{Z}$ tels que $a^{N+1} = a_N a^N + a_{N-1} a^{N-1} + ... + a_0$. Le nombre a est donc bien un entier algébrique.

Remarque : Le polynôme caractéristique de multiplication par a sur B est, d'après le théorème de Cayley-Hamilton, un polynôme annulateur de a.

3. Généraliser le raisonnement précédent pour montrer que l'ensemble des éléments de $\mathbb{C}$ qui sont des entiers algébriques est un anneau.

Indications : Soient a et b deux entiers algébriques. On considère $A = \mathbb{Z}[a+b]$, $A' = \mathbb{Z}[ab]$ et $B = \mathbb{Z}[a, b]$. Comme a et b sont des entiers algébriques, B est de type fini en tant que groupe abélien. On déduit comme alors comme à la question 2. que A et A' sont des groupes abéliens libres de type fini, puis que $a+b$ et ab sont des entiers algébriques.

Remarque : Le polynôme caractéristique de multiplication par $a+b$ (resp. ab) sur B est, d'après le théorème de Cayley-Hamilton, un polynôme annulateur de $a+b$ (resp. ab).

Exercice 5 : Anneau des entiers algébriques, le retour

1. Soient P et Q deux polynômes à coefficients dans $\mathbb{Q}$ de degrés respectifs d et e. On considère l'application $\mathbb{Q}$-linéaire :

$$f : \mathbb{Q}[X]_{<e} \times \mathbb{Q}[X]_{<d} \mapsto \mathbb{Q}[X]_{<d+e}, (U, V) \mapsto PU + QV,$$

On appelle résultant de P et Q le déterminant de f (dans les bases $((1,0), (X,0), ..., (X^{e-1}, 0), (0,1), (0,X), ..., (0, X^{d-1}))$ de $\mathbb{Q}[X]_{<e} \times \mathbb{Q}[X]_{<d}$ et $(1, X, ..., X^{d+e-1})$ de $\mathbb{Q}[X]_{<d+e}$). On le note $\mathrm{Res}(P, Q)$. Montrer que $\mathrm{Res}(P, Q)$ est non nul si, et seulement si, P et Q n'ont pas de racines communes dans $\mathbb{C}$. Remarquer que le résultat subsiste si l'on remplace $\mathbb{Q}$ par un autre corps contenu dans $\mathbb{C}$.

Indications : Le rationnel $\mathrm{Res}(P,Q)$ est nul si, et seulement f est un isomorphisme. Cela équivaut à l'injectivité de f.
Si P et Q sont premiers entre eux et $(U,V) \in \mathrm{Ker}(f)$, alors $PU = -QV$, donc P divise V et Q divise U. Comme $\deg U < \deg Q$ et $\deg V < \deg P$, on déduit que $U = V = 0$, et que f est injectif.
Réciproquement, si P et Q ne sont pas premiers entre eux, alors $\left(\frac{Q}{P\wedge Q}, -\frac{P}{P\wedge Q}\right) \in \mathrm{Ker}(f)$ et f n'est pas injectif.
Donc $\mathrm{Res}(P,Q)$ est non nul si, et seulement si, P et Q sont premiers entre eux.
Or le pdcg de deux polynômes est invariant par extension de corps (d'après l'algorithme d'Euclide). Donc P et Q sont premiers entre eux dans $\mathbb{Q}[X]$ si, et seulement si, ils le sont dans $\mathbb{C}[X]$. Cela équivaut à ce que P et Q n'aient pas de racines communes dans $\mathbb{C}$.

Remarque : Avec le même raisonnement, on voit que le résultat subsiste si $\mathbb{Q}$ est remplacé par un autre corps contenu dans $\mathbb{C}$.

2. En déduire que l'ensemble des entiers algébriques est un anneau.

Indications : Soient a et b deux entiers algébriques. Soient P et Q des polynômes annulateurs respectifs unitaires à coefficients dans $\mathbb{Z}$. Soit e le degré de Q. Considérons :

$$g : \mathbb{Q} \to \mathbb{Q}, z \mapsto \mathrm{Res}(P(X), Q(z-X)),$$
$$h : \mathbb{Q}\setminus\{0\} \to \mathbb{Q}, z \mapsto \mathrm{Res}(P(X), z^e Q(X/z)).$$

Ces fonctions coïncident avec des polynômes unitaires G et H de $\mathbb{Z}[Z]$. Comme P, $Q(a+b-X)$ et $(ab)^e Q(X/(ab))$ ont tous a pour racine, d'après la remarque à la fin de la question 1., $G(a+b) = H(ab) = 0$. Donc $a+b$ et ab sont des entiers algébriques.

3. Exhiber un polynôme annulateur unitaire à coefficients dans $\mathbb{Z}$ de l'entier algébrique $\sqrt[3]{2} + \sqrt[3]{3}$.

Indications : Il suffit de prendre la fonction polynômiale :

$$g : \mathbb{Q} \to \mathbb{Q}, z \mapsto \mathrm{Res}(X^3 - 2, (z-X)^3 - 3).$$

Elle coïncide avec le polynôme :

$$G(Z) = \begin{vmatrix} -2 & 0 & 0 & Z^3-3 & 0 & 0 \\ 0 & -2 & 0 & -3Z^2 & Z^3-3 & 0 \\ 0 & 0 & -2 & 3Z & -3Z^2 & Z^3-3 \\ 1 & 0 & 0 & -1 & 3Z & -3Z^2 \\ 0 & 1 & 0 & 0 & -1 & 3Z \\ 0 & 0 & 1 & 0 & 0 & -1 \end{vmatrix}.$$

C'est un polynôme de degré 27.

Exercice 6 : Un entier algébrique

Montrer que $a = \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}$ est un entier algébrique. On pourra étudier le morphisme de groupes :

$$\phi : \mathbb{Z}[\sqrt[3]{10}] \to \mathbb{Z}[\sqrt[3]{10}], x \mapsto ax.$$

Indications : Le groupe abélien $\mathbb{Z}[\sqrt[3]{10}]$ est engendré par la famille $(1, \sqrt[3]{10}, \sqrt[3]{100})$. Montrons que c'est une famille libre.
Soient $s, t, u \in \mathbb{Z}$ tels que $s + t\sqrt[3]{10} + u\sqrt[3]{100} = 0$. Alors :

$$s + t\sqrt[3]{10} + u\sqrt[3]{100} = 0$$
$$s\sqrt[3]{10} + t\sqrt[3]{100} + 10u = 0$$
$$s\sqrt[3]{100} + 10t + 10\sqrt[3]{10}u = 0.$$

La matrice de ce système est une matrice de Vandermonde inversible, et donc $s = t = u = 0$. On en déduit que $(1, \sqrt[3]{10}, \sqrt[3]{100})$ est une base du groupe abélien libre $\mathbb{Z}[\sqrt[3]{10}]$.
D'après le théorème de Cayley-Hamilton, le polynôme caractéristique de ϕ est un polynôme annulateur de a. Dans la base $(1, \sqrt[3]{10}, \sqrt[3]{100})$, la matrice de ϕ est :

$$\begin{pmatrix} \frac{1}{3} & \frac{10}{3} & \frac{10}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{10}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}.$$

Le polynôme caractéristique est $P = X^3 - X^2 - 3X - 3$. Donc a est un entier algébrique, annulé par P.

Exercice 8 : L'anneau $\mathbb{Z}[\sqrt{5}]$

Soit $A = \mathbb{Z}[\sqrt{5}]$.

1. (a) Montrer que A possède une infinité d'éléments inversibles.

Indications : Soit $N : A \to \mathbb{Z}, a + b\sqrt{5} \mapsto a^2 - 5b^2$. On vérifie que $N(xy) = N(x)N(y)$ pour tous $x, y \in A$.

Soit $u \in A^\times$. Il existe $v \in A$ tel que $uv = 1$. Donc $N(u)N(v) = 1$. Donc $N(u) \in \{\pm 1\}$.
Réciproquement, si $u \in A$ est tel que $N(u) \in \{\pm 1\}$, alors, en écrivant $u = a + b\sqrt{5}$, on a $u(a - b\sqrt{5}) = N(u) = \pm 1$ et donc $u \in A^\times$.
On en déduit que les inversibles de A sont les éléments u de A tels que $N(u) = \pm 1$.

Remarquons maintenant que $N(9+4\sqrt{5}) = 1$. On en déduit que, pour tout $n \in \mathbb{Z}$, on a $(9+4\sqrt{5})^n \in A^\times$. Cela montre que $A^\times$ est infini (il contient en fait une copie de $\mathbb{Z}$).

(b) Montrer que 2, $3 + \sqrt{5}$ et $3 - \sqrt{5}$ sont irréductibles dans A.

Indications : Le nombre 2 n'est pas inversible car $N(2) \neq 1$. Soient $x, y \in A$ tels que $xy = 2$. Alors $N(x)N(y) = 4$. Comme il n'existe pas d'entiers a, b tels que $a^2 - 5b^2 = 2$ (regarder modulo 5), on obtient que $N(x) = 1$ ou $N(y) = 1$. Donc x est inversible ou y est inversible. On en déduit que 2 est irréductible.
On procède de manière tout à fait analogue pour $3 + \sqrt{5}$ et $3 - \sqrt{5}$.

(c) Montrer qu'il n'y a pas d'unicité de la décomposition de 4 en facteurs irréductibles dans A.

Indications : Il suffit de vérifier que $2 \times 2 = (3+\sqrt{5})(3-\sqrt{5})$ et que 2 ne divise pas $3+\sqrt{5}$ dans A.

2. (a) Justifier que tous les éléments de A sont des entiers algébriques.

Indications : Soit $x = a + b\sqrt{5} \in A$, avec $a, b \in \mathbb{Z}$. Alors $(x-a)^2 = 5b^2$. Donc x est un entier algébrique.

Considérons $K = \mathbb{Q}[\sqrt{5}]$ le corps des fractions de A.

(b) Exhiber un entier algébrique dans $K \setminus A$.

Indications : Considérons $x = \frac{1+\sqrt{5}}{2} \in K \setminus A$. Alors $x^2 = x + 1$, donc x est un entier algébrique.

Soit $x = a + b\sqrt{5} \in K$ avec $a, b \in \mathbb{Q}$. Supposons que x est un entier algébrique.

(c) Montrer que $2a \in \mathbb{Z}$ et que $a^2 - 5b^2 \in \mathbb{Z}$.

Indications : Soit $\phi : K \to K, a+b\sqrt{5} \mapsto a-b\sqrt{5}$. On vérifie immédiatement que ϕ est un morphisme d'anneaux. Donc $\phi(x)$ est un entier algébrique. Cela montre que $x + \phi(x) = 2a$ et $x\phi(x) = a^2 - 5b^2$ sont dans $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$.

(d) Montrer que $x \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Indications : Soit $k \in \mathbb{Z}$ tel que $2a = k$. On a $\frac{k^2}{4} - 5b^2 \in \mathbb{Z}$. Donc $b^2 \in \frac{1}{20}\mathbb{Z}$. Donc il existe $l \in \mathbb{Z}$ tel que $2b = l$. Par conséquent, $k^2 - 5l^2 \in 4\mathbb{Z}$, et k et l ont même parité. Cela montre que $x \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

L'anneau A n'est pas intégralement clos, mais il est contenu dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ qui est intégralement clos.

(e) Vérifier que 2 et $3+\sqrt{5}$ sont associés dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. De même, vérifier que 2 et $3-\sqrt{5}$ sont associés dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

Indications : On a $\frac{3+\sqrt{5}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ et $\frac{2}{3+\sqrt{5}} = \frac{3-\sqrt{5}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Donc 2 et $3+\sqrt{5}$ sont associés dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Il en est de même pour 2 et $3-\sqrt{5}$.

On peut montrer que l'anneau $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ est principal (donc factoriel).

Exercice 9 : Une équation diophantienne

Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $y^2 = x^3 + 16$.

Indications : On écrit $(y+4)(y-4) = x^3$. Soit $d = (y+4) \wedge (y-4)$. Alors d divise 8.

Supposons que $d = 1$. Alors $y+4$ et $y-4$ sont des cubes parfaits. Donc $y+4 = 0$ et $y-4 = -8$, ou $y+4 = 8$ et $y-4 = 0$. Cela contredit que $d = 1$.

Donc $d \neq 1$. Alors 2 divise y. Donc 2 divise x. Donc 4 divise y. Donc 4 divise x. Donc, en écrivant $x = 4t$ et $y = 4u$, on obtient :

$$(u+1)(u-1) = 4t^3.$$

On en déduit que u est impair et que $t^3 = \frac{u+1}{2}\frac{u-1}{2}$. Comme $\frac{u+1}{2}$ et $\frac{u-1}{2}$ sont premiers entre eux, ce sont des cubes parfaits. Ce sont de plus des entiers consécutifs. Donc $\frac{u+1}{2} = 0$ et $\frac{u-1}{2} = -1$, ou $\frac{u+1}{2} = 1$ et $\frac{u-1}{2} = 0$. Donc $(x, y) \in \{(0, 4), (0, -4)\}$.

Exercice 11 : Finitude et intégrité

Soit k un corps. Soit A une k-algèbre de dimension finie intègre. Montrer que A est un corps. En déduire qu'un anneau fini intègre est un corps.

Indications : Soit $a \in A \setminus \{0\}$. Soit $\phi : A \to A, x \mapsto ax$. C'est une application k-linéaire. Comme A est intègre, ϕ est injective. C'est donc un isomorphisme, et $a \in A^\times$. Par conséquent, A est un corps.
Soit B un anneau fini intègre non nul. Soit $I = \{n \in \mathbb{Z} | n \times 1_B = 0\}$. C'est un idéal de $\mathbb{Z}$, différent de 0 car B est fini. Soit $p \in \mathbb{N}$ tel que $I = (p)$. Comme B est intègre, p est premier. On vérifie alors que B est naturellement une $\mathbb{Z}/p\mathbb{Z}$-algèbre intègre de dimension finie. Donc B est un corps.

Exercice 12 : Produits d'anneaux

Soient A un anneau.

1. Supposons que A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Montrer que A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_i e_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$.

   Indications : Il suffit de choisir $e_i = (\delta_{ij})_{1 \leq j \leq n} \in A_1 \times .... \times A_n$. Ici δ_{ij} désigne le symbole de Kronecker.

2. Réciproquement, montrer que si A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_i e_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$, alors A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Décrire alors les idéaux de A.

Indications : Considérons :

$$\phi : A \to Ae_1 \times .... \times Ae_n, x \mapsto (xe_1, ..., xe_n).$$

On vérifie que chaque Ae_i est un anneau et que ϕ est un morphisme d'anneaux. De plus,

$$\psi : Ae_1 \times .... \times Ae_n \to A, (x_1, ..., x_n) \mapsto x_1 + ... + x_n$$

est l'inverse de ϕ. Donc ϕ est un isomorphisme.

Soit I un idéal de A. Notons $\phi_i : A \to Ae_i, x \mapsto xe_i$ et $I_i = \phi(I)$. Chaque I_i est un idéal de Ae_i et $I_1 \times ... \times I_n \subseteq \phi(I)$. De plus, si $x \in I$, alors $xe_i \in I_i$ pour chaque i, et donc $\phi(x) \in I_1 \times ... \times I_n$. On en déduit que $p(I) = I_1 \times ... \times I_n$. Donc les idéaux de A sont les produits d'idéaux des Ae_i.

3. Soit $m > 0$ un entier. Quel est le plus grand entier n tel qu'il existe des anneaux non nuls A_1, ..., A_n vérifiant $\mathbb{Z}/m\mathbb{Z} = A_1 \times ... \times A_n$?

Indications : On cherche le plus grand entier n tel qu'il existe des idempotents non nuls $e_1, ..., e_n$ vérifiant $e_i e_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$.
Écrivons $m = p_1^{\alpha_1} ... p_r^{\alpha_r}$ (décomposition en produit de facteurs premiers de m). Le lemme chinois donne un isomorphisme :

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

Donc $n \geq r$. De plus, les idempotents de $\mathbb{Z}/p_i^{\alpha_i}$ sont 0 et 1. Donc les idempotents de $\prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ sont les $(x_1, ..., x_r)$ avec $x_i \in \{0, 1\}$. On en déduit que $n \leq r$. Finalement n est le nombre de facteurs premiers distincts de m.

Exercice 13 : Anneau de polynômes

Soit A un anneau.

1. Supposons A intègre.

(a) Montrer que $A[X]$ est intègre.

Indications : Soient P et Q dans $A[X]$ non nuls de degrés respectifs d et e. Soient a et b les coefficients dominants respectifs. Alors le coefficient de X^{d+e} dans PQ est ab. Comme A est intègre, $ab \neq 0$. Donc $PQ \neq 0$ et $A[X]$ est intègre.

(b) Quels sont les éléments inversibles de $A[X]$?

Indications : Soit $P \in A[X]^\times$. Il existe $Q \in A[X]$ tel que $PQ = 1$. En procédant comme dans 1.(a), on remarque alors que P et Q sont de degré 0. Donc $P \in A^\times$. Réciproquement, on a bien $A^\times \subseteq A[X]^\times$. Donc $A^\times = A[X]^\times$.

2. On ne suppose plus A intègre.

(a) Quel est le nilradical de $A[X]$?

Indications : Montrons par récurrence sur le degré que tous les coefficients d'un polynôme nilpotent sont nilpotents.
Il est clair que les coefficients d'un polynôme nilpotent constant sont nilpotents. Supposons maintenant la propriété prouvée pour les polynômes de degré d. Soit $P \in A[X]$ nilpotent de degré $d+1$. Soit $N \in \mathbb{N}$ tel que $P^N = 0$ et écrivons $P = a_{d+1}X^{d+1} + ... + a_0$. Alors $a_{d+1}^N = 0$. Donc $P - a_dX^d$ est nilpotent de degré d. Par hypothèse de récurrence, $a_0, ..., a_d$ sont nilpotents. Donc tous les coefficients de P sont nilpotents.
Réciproquement, un polynôme dont les coefficients sont nilpotents est nilpotent.

(b) Quels sont éléments inversibles de $A[X]$?

Indications : Montrons par récurrence sur d que si un polynôme $P = a_dX^d + ... + a_0$ de degré au plus d est inversible, alors $a_d, ..., a_1$ sont nilpotents et a_0 est inversible.
Pour $d = 0$, le résultat est évident.
Supposons le résultat prouvé pour un certain entier $d-1$. Soit $P \in A[X]$ inversible de dégré d. Soit Q son inverse. Écrivons $P = a_dX^d + ... + a_0$ et $Q = b_eX^e + ...b_0$. Comme $a_0b_0 = 1$, il est clair que a_0 et b_0 sont inversibles. Par une récurrence simple on montre que, pour chaque $r \geq 0$, on a $a_d^{r+1}b_{e-r} = 0$. En particulier, $a_d^{e+1}b_0 = 0$. Comme b_0 est inversible, a_d est nilpotent (plus précisément $a_d^{e+1} = 0$). Du coup, $P - a_dX^d$ est inversible : son inverse est :

$$P^{-1} \cdot \sum_{k=0}^{e} (a_dX^dP^{-1})^k.$$

Par hypothèse de récurrence, on obtient que $a_{d-1}, ..., a_1$ sont nilpotents et a_0 est inversible, ce qui achève la preuve.

Réciproquement, si $a_d, ..., a_1$ sont nilpotents et a_0 est inversible, alors $P = a_dX^d + ... + a_0$ est inversible puisque son inverse est :

$$a_0^{-1} \cdot \sum_{k=0}^{\infty} (-1)^k (a_dX^d + ... + a_1X)^k.$$

(c) À quelle condition sur A peut-on écrire $A[X] = B_1 \times B_2$ pour certains anneaux non nuls B_1 et B_2 ?

Indications : Si A possède un idempotent différent de 0 ou 1, alors $A[X]$ aussi et donc on peut écrire $A[X] = B_1 \times B_2$ pour certains anneaux non nuls B_1 et B_2.

Supposons que A ne possède pas d'idempotents autres que 0 ou 1. Soit $P \in A[X]$ un idempotent. Écrivons $P = a_dX^d + ... + a_0$. Alors a_0 est un idempotent : $a_0 = 0$ ou $a_0 = 1$. Dans les deux cas, on montre aisément par récurrence que $a_i = 0$ pour chaque $i > 0$. Donc $P = 0$ ou $P = 1$, et on ne peut pas écrire $A[X] = B_1 \times B_2$ pour certains anneaux non nuls B_1 et B_2.

Nous avons donc montré que $A[X] = B_1 \times B_2$ pour certains anneaux non nuls B_1 et B_2 si, et seulement si, $A = C_1 \times C_2$ pour certains anneaux non nuls C_1 et C_2.

Exercice 14 : Opérations sur les idéaux de $\mathbb{Z}$

Soient $a, b \in \mathbb{Z}$. Donner des générateurs de $(a)+(b)$, de $(a)(b)$ et de $(a)\cap(b)$.

Indications : On a : $(a)+(b)=(a\wedge b)$, de $(a)(b)=(ab)$ et de $(a)\cap(b)=(a\vee b)$.

Exercice 15 : Radical d'un idéal

Soient A un anneau et I un idéal de A. On appelle radical de I l'ensemble $\sqrt{I}=\{a\in A|\exists n\in\mathbb{N}^*, a^n\in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal.

2. Reconnaître $\sqrt{A}$ et $\sqrt{(0)}$.

3. Soit J un idéal de A. Déterminer si les assertions suivantes sont vraies ou fausses. Corriger celles qui sont fausses.

(a) $\sqrt{\sqrt{I}}=\sqrt{I}$.

(b) $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$.

(c) $\sqrt{IJ}=\sqrt{I}\cdot\sqrt{J}$.

(d) $\sqrt{I+J}=\sqrt{I}+\sqrt{J}$.

4. Montrer que $\sqrt{I}$ est l'intersection des idéaux premiers contenant I. On pourra utiliser le lemme de Zorn.

5. Prenons $A=\mathbb{Z}$ et $I=N\mathbb{Z}$. Calculer $\sqrt{I}$.