TD1-3 : Corrigés d'exercices traités pendant les séances

Diego Izquierdo

Remarque : Certaines questions ne sont pas détaillées... Si vous avez des problèmes avec certains exercices, il ne faut pas hésiter à venir me voir !

1 TD1

Exercice 1 (à préparer) : Groupe des unités de $\mathbb{Z}/n\mathbb{Z}$
Dans cet exercice, nous voulons étudier la structure du groupe des unités d'un groupe cyclique. On rappelle que tout sous-groupe fini du groupe des unités d'un corps est cyclique. Cela entraîne en particulier que $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ pour tout nombre premier p.

1. Rappeler quel est l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$.

> **Indications :** Si $n = p_1^{\alpha_1}...p_r^{\alpha_r}$ est la décomposition en produit de facteurs premiers de n, l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$ est $\phi(n) = n\prod_{k=1}^{r}\left(1-\frac{1}{p_k}\right)$.

2. Soient p un nombre premier impair et $m > 1$ un entier.

(a) Montrer que $(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \mod p^m$, puis que $1+p$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

> **Indications :** On procède par récurrence sur m. Pour $m = 2$, la propriété est évidente. Supposons que $(1+p)^{p^{m-2}} \equiv 1+p^{m-1} \mod p^m$ pour un certain $m > 1$. Soit k un entier tel que $(1+p)^{p^{m-2}} = 1+p^{m-1}+kp^m$. En développant, on vérifie alors que : $(1+p)^{p^{m-1}} = (1+p^{m-1}+kp^m)^p \equiv 1+p^m \mod p^{m+1}$, ce qui achève la récurrence.

(b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/p^{m-1}\mathbb{Z}$.

> **Indications :** Le noyau de la projection est d'ordre $\frac{|(\mathbb{Z}/p^m\mathbb{Z})^\times|}{|(\mathbb{Z}/p\mathbb{Z})^\times|} = p^{m-1}$. De plus, il contient $1+p$ et $1+p$ est d'ordre p^{m-1} d'après (a). Donc le noyau de la projection naturelle $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre p^{m-1}.

(c) Montrer qu'il existe $x_0 \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ d'ordre $p-1$.

> **Indications :** Soient $y_1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ un élément d'ordre $p-1$ et x_1 un relèvement de y_1 dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Soit r l'ordre de x_1. Comme y_1 est d'ordre $p-1$, on a $p-1|r$. Posons $x_0 = x_1^{\frac{r}{p-1}}$. On voit immédiatement que l'ordre de x_0 est $p-1$.

(d) Montrer que $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \to (\mathbb{Z}/p^m\mathbb{Z})^\times, (a,b) \mapsto x_0^a(1+p)^b$ est un isomorphisme. En déduire que $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z}$.

Indications : On vérifie immédiatement que $f : \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \to (\mathbb{Z}/p^m\mathbb{Z})^\times, (a,b) \mapsto x_0^a(1+p)^b$ est un morphisme de groupes. Étant donné que $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$ et $(\mathbb{Z}/p^m\mathbb{Z})^\times$ ont même ordre, il suffit de montrer que f est injectif.
Soit $(a,b) \in \mathrm{Ker}(f)$. On remarque alors que $x_0^a = (1+p)^{-b}$ est dans le noyau de la projection $\pi : (\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ et donc que $\pi(x_0)^a = 1$. Or, d'après la question précédente, $\pi(x_0)$ est d'ordre $p-1$. Donc $a = 0$, et $(1+p)^b = 1$. Comme $1+p$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$, cela montre que $b = 0$, et donc que f est injectif.

3. Soit $m > 2$ un entier.

(a) Montrer que $5^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m$, puis que 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$.

Indications : Analogue à la question 2.(a).

(b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/2^m\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2^{m-2}\mathbb{Z}$.

Indications : Analogue à la question 2.(b).

(c) En s'inspirant de la question 2.(d), montrer que $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Indications : L'isomorphisme est donné par $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z} \to (\mathbb{Z}/2^m\mathbb{Z})^\times, (a,b) \mapsto (-1)^a 5^b$. La preuve est analogue à la question 2.(d).

4. Quelle est la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$? Quand ce groupe est-il cyclique ?

Indications : Écrivons n comme produit de facteurs premiers $n = p_1^{\alpha_1}...p_r^{\alpha_r}$ et considérons le morphisme induit par les projections $g : (\mathbb{Z}/n\mathbb{Z})^\times \to \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$. C'est un morphisme injectif d'après le lemme chinois. De plus, les groupes $(\mathbb{Z}/n\mathbb{Z})^\times$ et $\prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ ont même ordre. Donc g est un isomorphisme. Par conséquent, si n n'est pas multiple de 4 :

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^r (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times \cong \prod_{i=1}^r \left(\mathbb{Z}/(p_i-1)\mathbb{Z} \times \mathbb{Z}/p_i^{\alpha_i-1}\mathbb{Z}\right),$$

et si n est multiple de 4, en supposant par exemple que $p_1 = 2$:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha_1-2}\mathbb{Z} \times \prod_{i=2}^r \left(\mathbb{Z}/(p_i-1)\mathbb{Z} \times \mathbb{Z}/p_i^{\alpha_i-1}\mathbb{Z}\right).$$

Lorsque n est impair :
- si $r > 1$, alors $(\mathbb{Z}/n\mathbb{Z})^\times$ contient $(\mathbb{Z}/2\mathbb{Z})^2$, et donc $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.
- si $r = 1$, alors $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/(p_1-1)p_i^{\alpha_1-1}\mathbb{Z}$ est cyclique.

Lorsque n est pair :
- si $r > 2$ ou si n est multiple de 4 et $r = 2$ ou encore si n est multiple de 8, alors $(\mathbb{Z}/n\mathbb{Z})^\times$ contient $(\mathbb{Z}/2\mathbb{Z})^2$, et donc $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.
- si n n'est pas multiple de 4 et $r = 2$, alors $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/(p_2-1)p_2^{\alpha_2-1}\mathbb{Z}$ est cyclique.
- le groupe $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ est cyclique.

On en déduit que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si, $n = 1$, $n = 2$, $n = 4$, n est de la forme p^α avec p premier impair ou n est de la forme $2p^\alpha$ avec p premier impair.

5. *Exemples :* Donner un générateur du groupe $(\mathbb{Z}/162\mathbb{Z})^\times$. Donner un élément d'ordre maximal dans $(\mathbb{Z}/2592\mathbb{Z})^\times$.

Indications : Cherchons d'abord un générateur de $(\mathbb{Z}/81\mathbb{Z})^\times \cong \mathbb{Z}/54\mathbb{Z}$. D'après 2.(a), 4 est d'ordre 27 dans $(\mathbb{Z}/81\mathbb{Z})^\times$. Par conséquent, 2 est d'ordre 54 dans $(\mathbb{Z}/81\mathbb{Z})^\times$: c'est un générateur de ce groupe. On en déduit que 83 est un générateur de $(\mathbb{Z}/162\mathbb{Z})^\times$.
On a $(\mathbb{Z}/2592\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$. On remarque que $(0,1,2) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}$ est un élément d'ordre maximal. Il correspond à l'élément $x \in (\mathbb{Z}/2592\mathbb{Z})^\times$ tel que $x \equiv 5 \mod 32$ et $x \equiv 4 \mod 81$. On calcule alors $x = 1381 \in (\mathbb{Z}/2592\mathbb{Z})^\times$.

Exercice 2 : Dual d'un groupe abélien fini

Soit A un groupe abélien fini. On appelle dual de A l'ensemble $\hat{A}$ constitué des caractères de A (c'est-à-dire des morphismes de groupes $A \to \mathbb{C}^\times$). On peut munir $\hat{A}$ d'une loi de groupe abélien définie par $(\chi\chi')(a) = \chi(a)\chi'(a)$.

1. Montrer que le dual de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Indications : Considérons le morphisme de groupes $ev : \widehat{\mathbb{Z}/n\mathbb{Z}} \to \mathbb{C}^\times, \chi \mapsto \chi(1)$. On vérifie immédiatement que ev est injectif, et que son image est le groupe des racines n-ièmes de l'unité dans $\mathbb{C}^\times$. On en déduit que $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

2. Soit B un groupe abélien fini. Montrer que $\widehat{A \times B} \cong \hat{A} \times \hat{B}$.

> **Indications :** Considérons les morphismes de groupes $f : \widehat{A \times B} \to \hat{A} \times \hat{B}, \chi \mapsto (a \mapsto \chi(a,0), b \mapsto \chi(0,b))$ et $g : \hat{A} \times \hat{B} \to \hat{A}, (\chi_A, \chi_B) \mapsto ((a,b) \mapsto \chi_A(a)\chi_B(b))$. On vérifie immédiatement f et g sont inverses l'un de l'autre.

3. Soit $f : A \to B$ un morphisme de groupes abéliens finis. Montrer que $\hat{f} : \hat{B} \to \hat{A}, \chi \mapsto \chi \circ f$ est un morphisme de groupes.

> **Indications :** Vérification immédiate.

4. Soit $f : A \to B$ un morphisme de groupes.

(a) Montrer que, si f est surjectif, alors $\hat{f}$ est injectif.

> **Indications :** Soit $\chi \in \mathrm{Ker}(\hat{f})$. Alors, pour tout $a \in \hat{A}$, on a $\chi(f(a)) = 1$. Comme f est surjectif, on déduit que $\chi = 1$, et donc $\hat{f}$ est injectif.

(b) Supposons f injectif. Soient $b_1, ..., b_r$ des éléments de B tels que, pour chaque $s \in \{1, ..., r\}$, on a $b_s \notin \langle A, b_1, b_2, ..., b_{s-1}\rangle$ et $B = \langle A, b_1, b_2, ..., b_r\rangle$. Montrer que, pour chaque $s \in \{1, ..., r+1\}$, tout caractère de $\langle A, b_1, b_2, ..., b_{s-1}\rangle$ peut s'étendre en un caractère de $\langle A, b_1, b_2, ..., b_s\rangle$. En déduire que $\hat{f}$ est surjectif.

> **Indications :** On peut supposer que $r = 1$. Soit $\chi \in \hat{A}$. On veut étendre χ à $B = \langle A, b_1\rangle$. Soient n l'ordre de la classe de b_1 dans B/A et $z \in \mathbb{C}^\times$ tel que $z^n = \chi(nb_1)$. Posons $\chi_B : B \to \mathbb{C}^\times, a + kb_1 \mapsto \chi(a)z^k$ pour $a \in A$ et $k \in \mathbb{Z}$. On vérifie immédiatement que χ_B est bien défini, que c'est un caractère de B et qu'il étend χ.

5. Soit e l'exposant du groupe A, c'est-à-dire le plus petit commun multiple des ordres des éléments de A. On rappelle qu'il existe un élément a de A d'ordre e.

(a) Montrer qu'il existe un caractère $\chi \in \hat{A}$ tel que $\chi(a)$ est d'ordre e.

> **Indications :** Soit $\chi_a \in \widehat{\langle a\rangle}$ tel que $\chi_a(a)$ est une racine primitive e-ième. D'après 4.(b), il existe $\chi \in \hat{A}$ tel que $\chi|_{\langle a\rangle} = \chi_a$. On voit alors immédiatement que $\chi(a)$ est d'ordre e.

(b) En déduire que $A = \langle a\rangle \times \mathrm{Ker}(\chi)$ puis que A est un produit de groupes cycliques.

> **Indications :** Soit $f : \langle a\rangle \times \mathrm{Ker}(\chi) \to A, (na, b) \mapsto na + b$.
> - Soient $n \in \{0, ..., e-1\}$ et $b \in \mathrm{Ker}(\chi)$ tels que $f(na, b) = 1$. Alors $na = -b \in \mathrm{Ker}(\chi)$. Donc, d'après (a), $n = 0$ et $b = 0$. On en déduit que f est injective.
> - Soit $c \in A$. Comme l'ordre de c divise e, $\chi(c)$ est une racine e-ième de l'unité. Par conséquent, il existe $n \in \{0, ..., e-1\}$ tel que $\chi(na) = \chi(c)$. On voit alors immédiatement que $c - na \in \mathrm{Ker}(\chi)$ et que $f(na, c - na) = c$. Donc f est surjective.
>
> Finalement, f est un isomorphisme. Pour montrer que A est un produit de groupes cycliques, il suffit alors de procéder par récurrence sur l'ordre de A.

6. À l'aide des questions précédentes, montrer les assertions suivantes :

(a) Le groupe A est isomorphe à son dual.

Indications : L'assertion est vraie lorsque A est cyclique d'après la question 1. Il suffit alors d'appliquer les questions 2 et 5.(b) pour déduire que l'assertion est vraie pour tout A.

(b) Le morphisme $A \to \hat{\hat{A}}, a \mapsto (\chi \mapsto \chi(a))$ est un isomorphisme.

Indications : D'après (a), $|A| = |\hat{\hat{A}}|$. Il suffit donc de montrer que $f : A \to \hat{\hat{A}}, a \mapsto (\chi \mapsto \chi(a))$ est injectif. Soit $a \in \mathrm{Ker}(f)$. Soit n l'ordre de a et considérons un caractère $\chi_a : \langle a \rangle \to \mathbb{C}^\times$ tel que $\chi_a(a)$ soit une racine primitive n-ième de l'unité. D'après 4.(b), il existe $\chi \in \hat{A}$ tel que $\chi|_{\langle a \rangle} = \chi_a$. Alors $\chi(a) = \chi_a(a)$ est une racine primitive n-ième. Mais $\chi(a) = 1$ puisque $a \in \mathrm{Ker}(f)$ Donc $n = 1$ et $a = 0$. On en déduit que f est injectif.

(c) Si B est un sous-groupe de A, alors le dual de A/B s'identifie au noyau de la surjection $\hat{A} \to \hat{B}$.

Indications : D'après la question 4.(a), on sait que le dual de A/B s'injecte dans $\hat{A}$. De plus, on vérifie immédiatement que la composée $\widehat{A/B} \to \hat{A} \to \hat{B}$ est nulle. Donc $\widehat{A/B}$ s'injecte dans le noyau de la surjection $\hat{A} \to \hat{B}$ (la surjectivité a été prouvée en 4.(b)). De plus, avec (a) :

$$|\widehat{A/B}| = |A/B| = |A|/|B| = |\hat{A}|/|\hat{B}| = |\mathrm{Ker}(\hat{A} \to \hat{B})|.$$

Cela prouve que $\widehat{A/B}$ s'identifie au noyau de la surjection $\hat{A} \to \hat{B}$.

(d) Si $0 \to B \to A \to C \to 0$ est une suite exacte de groupes abéliens finis, il en est de même de $0 \to \hat{C} \to \hat{A} \to \hat{B} \to 0$.

Indications : C'est une reformulation de (c).

(e) Tout sous-groupe de A est isomorphe à un quotient de A.

Indications : Si B est un sous-groupe de A, alors, d'après 4.(b), $\hat{B}$ est un quotient de $\hat{A}$, et d'après (a), on a $B \cong \hat{B}$.

Exercice 3 : Sous-groupes de D_8

On appelle D_8 le groupe des isométries du carré. Quels sont les sous-groupes de D_8 ? Lesquels sont distingués ?

Indications : Soit r la rotation d'angle $\pi/2$ et s la symétrie par rapport à l'une des diagonales du carré. Alors $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, et on a les relations $r^4 = 1$, $s^2 = 1$, $srs = r^{-1}$.

- Sous-groupes d'ordre 1 : $\{1\}$.
- Sous-groupes d'ordre 2 : $\{1, r^2\}$, $\{1, s\}$, $\{1, sr\}$, $\{1, sr^2\}$, $\{1, sr^3\}$.
- Sous-groupes d'ordre 4 : le seul sous-groupe cyclique d'ordre 4 de D_8 est $\{1, r, r^2, r^3\}$. Pour trouver les sous-groupes isomorphes à $(\mathbb{Z}/2\mathbb{Z})^2$, on remarque qu'ils sont tous des réunions de trois sous-groupes parmi $\{1, r^2\}$, $\{1, s\}$, $\{1, sr\}$, $\{1, sr^2\}$, $\{1, sr^3\}$. On vérifie alors aisément que ce sont les sous-groupes $\{1, r^2, s, sr^2\}$ et $\{1, r^2, sr, sr^3\}$.
- Sous-groupes d'ordre 8 : D_8.

Parmi ces sous-groupes, les sous-groupes distingués sont $\{1\}$, $\{1, r^2\}$, $\{1, r, r^2, r^3\}$, $\{1, r^2, s, sr^2\}$, $\{1, r^2, sr, sr^3\}$, D_8.

2 TD2

Exercice 1 (à préparer) : Idéaux principaux, idéaux de type fini

1. Soit k un corps. Rappeler pourquoi tout idéal de $k[X]$ est principal.

> **Indications :** Le stathme $k[X] \to \mathbb{N}, P \mapsto \deg P + 1$ montre que $k[X]$ est euclidien, donc principal.

2. Exhiber des idéaux non principaux dans $k[X,Y]$, $k[T^2,T^3]$ et $\mathbb{Z}[X]$.

> **Indications :** Dans $k[X,Y]$, l'idéal (X,Y) n'est pas principal. Dans $k[T^2,T^3]$, l'idéal (T^2,T^3) n'est pas principal. Dans $\mathbb{Z}[X]$, l'idéal $(2,X)$ n'est pas principal.

3. Montrer que $\mathbb{Z}[i\sqrt{5}]$ possède des idéaux non principaux.

> **Indications :** L'idéal $(2, 1+i\sqrt{5})$ n'est pas principal.

4. Soit k un corps. Montrer que la sous-k-algèbre de $k[X,Y]$ engendrée par les X^nY pour $n>0$ possède un idéal qui n'est pas de type fini.

> **Indications :** Soit A la sous-k-algèbre de $k[X,Y]$ engendrée par les X^nY pour $n>0$. On choisit $I = (XY, X^2Y, X^3Y, ...)$. Supposons que I soit de type fini. Alors il existe $N>0$ tel que $I = (XY, X^2Y, ..., X^NY)$, et on vérifie aisément que $X^{N+1}Y \notin I$: absurde! Donc I n'est pas de type fini.

Exercice 2 (à préparer) : Vrai ou faux ?

Soit A un anneau.

1. Pour tout couple d'idéaux (I,J) de A, on a $\sqrt{I+J} = \sqrt{I} + \sqrt{J}$.

> **Indications :** FAUX : En prenant $A = \mathbb{C}[X,Y]$, $I = (Y)$ et $J = (X^2+Y)$, on remarque que $\sqrt{I+J} = (X,Y) \neq (X^2,Y) = \sqrt{I} + \sqrt{J}$. En fait, si l'anneau A était principal, on aurait bien $\sqrt{I+J} = \sqrt{I} + \sqrt{J}$, mais en toute généralité, on a $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

2. Si a, b et u sont trois éléments A tels que $(a) = (b)$ et $a = bu$, alors $u \in A^\times$.

> **Indications :** FAUX : Il suffit de prendre $A = \mathbb{C} \times \mathbb{C}$ et $a = b = c = (1,0)$. L'assertion serait vraie si A était intègre.

3. Un sous-anneau d'un anneau euclidien est factoriel.

> **Indications :** FAUX : Soient $A = \mathbb{C}[T]$ et $B = \mathbb{C}[T^2,T^3]$. L'anneau A est euclidien, mais son sous-anneau B n'est pas factoriel puisque $(T^2)^3 = (T^3)^2$ et T^2 et T^3 sont irréductibles dans B.

4. L'anneau des nombres décimaux est euclidien.

Indications : VRAI : Notons $\mathbb{D}$ l'anneau des nombres décimaux. Soit $N : \mathbb{D} \to \mathbb{N}$ définie par :
- si $x \neq 0$, on écrit $x = p2^n5^m$ avec $p, n, m \in \mathbb{Z}$ tels que p n'est multiple ni de 2 ni de 5 et on pose $N(x) = |p|$;
- $N(0) = 0$.

Soient $x, y \in \mathbb{D}$, avec y non nul. Montrons qu'il existe $q, r \in \mathbb{D}$ tels que $x = dy+r$ et $N(r) < N(y)$. Si $x = 0$, il suffit de prendre $q = r = 0$. Supposons donc $x \neq 0$. On écrit alors $x = p2^n5^m$ et $y = q2^s5^t$ avec $p, q, n, s, m, t \in \mathbb{Z}$ tels que p et q ne sont multiples ni de 2 ni de 5. On écrit la division euclidienne (dans $\mathbb{Z}$) de p par q : on trouve ainsi $a, b \in \mathbb{Z}$ tels que $p = qa+b$ et $|b| < |q|$. On a alors $x = qa2^n5^m+b2^n5^m$. Comme 2 et 5 sont inversibles dans $\mathbb{D}$, on obtient une écriture $x = dy + r$ avec $r = b2^n5^m$. Cela achève la preuve puisque $N(r) = N(b) \leq |b| < |q| = N(y)$.

5. Les groupes $\mathbb{Q}^\times$ et $(\mathbb{Z}/3\mathbb{Z}(X))^\times$ sont isomorphes.

Indications : VRAI : Comme $\mathbb{Z}$ est un anneau factoriel (car principal) ayant un nombre infini dénombrable d'éléments irréductibles à unité près, on a $\mathbb{Q}^\times \cong \mathbb{Z}^\times \times \mathbb{Z}^{(\mathbb{N})} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^{(\mathbb{N})}$. De même, comme $\mathbb{Z}/3\mathbb{Z}[X]$ est un anneau factoriel (car principal) ayant un nombre infini dénombrable d'éléments irréductibles à unité près, on a $(\mathbb{Z}/3\mathbb{Z}(X))^\times \cong \mathbb{Z}/3\mathbb{Z}[X]^\times \times \mathbb{Z}^{(\mathbb{N})} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^{(\mathbb{N})}$.

Exercice 4 (à préparer) : Quotients d'anneaux

Soit k un corps.

1. Montrer que la k-algèbre $k[X, Y]/(X^2-Y^3)$ est isomorphe à $k[T^2, T^3]$.

Indications : L'isomorphisme est donné par $\varphi : k[X, Y]/(X^2 - Y^3) \to k[T^2, T^3], X \mapsto T^3, Y \mapsto T^2$.

2. Montrer que la k-algèbre $k[X, Y]/(X^2 - Y)$ est isomorphe à $k[T]$.

Indications : L'isomorphisme est donné par $\varphi : k[X, Y]/(X^2-Y) \to k[T], X \mapsto T, Y \mapsto T^2$.

3. Plus généralement, soient a et b deux entiers naturels non nuls. Réaliser l'anneau $k[T^a, T^b]$ comme quotient de $k[X, Y]$.

Indications : On écrit $a = da'$ et $b = db'$, avec $d = a \wedge b$. On a un isomorphisme $\varphi : k[X, Y]/(X^{a'} - Y^{b'}) \to k[T^a, T^b], X \mapsto T^b, Y \mapsto T^a$.

4. Montrer que la k-algèbre $k[X, Y]/(XY-1)$ n'est pas isomorphe à $k[T]$.

Indications : Soit $\varphi : k[X, Y]/(XY - 1) \to k[T]$ un morphisme de k-algèbres. Alors $\varphi(X)\varphi(Y) = 1$, donc $\varphi(X) \in k$ et $\varphi(Y) \in k$. On en déduit que φ n'est pas surjectif.

5. Réaliser les anneaux $\mathbb{Z}[i\sqrt{7}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ comme quotients de $\mathbb{Z}[X]$.

Indications : On a des isomorphismes $\psi : \mathbb{Z}[X]/(X^2 + 7) \to \mathbb{Z}[i\sqrt{7}], X \mapsto i\sqrt{7}$ et $\theta : \mathbb{Z}[X]/(X^2 - X - 1) \mapsto \mathbb{Z}[\frac{1+\sqrt{5}}{2}], X \mapsto \frac{1+\sqrt{5}}{2}$.

Exercice 5 (à préparer) : Idéaux dans un anneau principal

Soient A un anneau principal et $x \in A$ non nul. Montrer que les assertions suivantes sont équivalentes :

(i) l'élément x est irréductible ;
(ii) l'idéal (x) est premier, c'est-à-dire que $A/(x)$ est un anneau intègre ;
(iii) l'idéal (x) est maximal, c'est-à-dire que $A/(x)$ est un corps.

Indications : Il est évident que $(iii) \Rightarrow (ii) \Rightarrow (i)$. Supposons x irréductible. Soit $y \in A \setminus (x)$. Soit $z \in A$ tel que $(z) = (x, y)$. Comme $z|x$ dans l'anneau factoriel A et x est irréductible, z est soit une unité soit associé à x. Si z était associé à x, on en déduirait que x divise y : absurde ! Donc z est une unité et $(x, y) = A$. Il existe donc $u, v \in A$ tels que $xu + yv = 1$, et donc l'image de y dans $A/(x)$ admet un inverse (la classe de v). Cela prouve que (x) est maximal.

Exercice 6 : Idéaux d'un quotient

Soient A un anneau commutatif unitaire et I un idéal.

1. Montrer que les idéaux de A/I sont en bijection avec les idéaux de A contenant I.

Indications : Notons $p : A \to A/I$ la projection canonique. On définit les deux bijections réciproques de la manière suivante : à un idéal J de A contenant I on associe $p(J) = J/I$ et à un idéal J' de A/I on associe $p^{-1}(J')$.

2. Soit $J \supseteq I$ un idéal de A. Montrer que A/J est canoniquement isomorphe au quotient de A/I par J/I.

Indications : Immédiat avec la propriété universelle du quotient.

3. On dit que I est un idéal premier (resp. maximal) si A/I est intègre (resp. un corps). Montrer que les idéaux premiers (resp. maximaux) de A/I sont en bijection avec les idéaux premiers (resp. maximaux) de A contenant I.

Indications : Immédiat avec les deux questions précédentes.

4. Déterminer les idéaux des anneaux suivants :

$$\mathbb{R}[X]/(X^2+X+1), \mathbb{R}[X]/(X^3-6X^2+11X-6), \mathbb{R}[X]/(X^4-1), \mathbb{R}[X]/(X^5).$$

Lesquels sont premiers ? Et maximaux ?

Indications :
- Idéaux de $\mathbb{R}[X]/(X^2 + X + 1)$: (1) et (0). Premiers et maximaux : (0).
- Idéaux de $\mathbb{R}[X]/(X^3 - 6X^2 + 11X - 6)$: (1), $(X - 1)$, $(X - 2)$, $(X - 3)$, $((X-1)(X-2))$, $((X-2)(X-3))$, $((X-1)(X-3))$, (0). Premiers et maximaux : $(X - 1)$, $(X - 2)$, $(X - 3)$.
- Idéaux de $\mathbb{R}[X]/(X^4 - 1)$: (1), $(X + 1)$, $(X - 1)$, $(X^2 + 1)$, $((X + 1)(X - 1))$, $((X + 1)(X^2 + 1))$, $((X - 1)(X^2 + 1))$, (0). Premiers et maximaux : $(X + 1)$, $(X - 1)$, $(X^2 + 1)$.
- Idéaux de $\mathbb{R}[X]/(X^5)$: (1), (X), (X^2), (X^3), (X^4), (0). Premiers et maximaux : (X).

5. Combien l'anneau $\mathbb{R}[X]/(X^5(X^4-1))$ possède-t'il d'idéaux ? d'idéaux premiers ? d'idéaux maximaux ?

Indications : Il possède $6 \times 2 \times 2 \times 2 = 48$ idéaux. Parmi eux, il y en a 4 qui sont premiers. Ces derniers sont aussi maximaux.

Exercice 11 : Une équation diophantienne

1. Montrer que $\mathbb{Z}[\frac{1+i\sqrt{11}}{2}]$ est un anneau euclidien. Quelles sont ses unités ?

> **Indications :** Notons $A = \mathbb{Z}[\frac{1+i\sqrt{11}}{2}]$. On définit $N : \mathbb{Q}[\frac{1+i\sqrt{11}}{2}] \to \mathbb{N}, z \mapsto |z|^2$. On vérifie que $z \in A$ est une unité si, et seulement si, $N(z) = 1$. Donc $A^\times = \{-1, 1\}$.
> Soient maintenant $x, y \in A$ non nuls. On écrit $\frac{x}{y} = c_1 + c_2\frac{1+i\sqrt{11}}{2}$ avec $c_1, c_2 \in \mathbb{Q}$, et on note d_1 (resp. d_2) des entiers tels que $|d_1 - c_1| \leq 1/2$ et $|d_2 - c_2| \leq 1/2$. Plusieurs cas se présentent :
> - si $|d_1 - c_1 + \frac{d_2-c_2}{2}| \leq \frac{1}{2}$, alors on a $N(\frac{x}{y} - (d_1 + d_2\frac{1+i\sqrt{11}}{2})) < 1$;
> - si $\frac{1}{2} < d_1 - c_1 + \frac{d_2-c_2}{2} < \frac{3}{4}$, alors $N(\frac{x}{y} - (-1 + d_1 + d_2\frac{1+i\sqrt{11}}{2})) < 1$;
> - si $-\frac{3}{4} < d_1 - c_1 + \frac{d_2-c_2}{2} < -\frac{1}{2}$, alors $N(\frac{x}{y} - (1 + d_1 + d_2\frac{1+i\sqrt{11}}{2})) < 1$.
>
> Dans tous les cas, on trouve $q \in A$ tel que $N(\frac{x}{y} - q) < 1$. Par conséquent, en posant $r = x - qy$, on a $x = qy + r$ avec $N(r) = N(\frac{x}{y} - q)N(y) < N(y)$. Donc A est euclidien.

2. Trouver tous les couples $(x, y) \in \mathbb{Z}^2$ tels que $y^2 + 11 = x^3$.

> **Indications :** Dans A, on a $(y + i\sqrt{11})(y - i\sqrt{11}) = x^3$. Soit $d \in A$ divisant $y + i\sqrt{11}$ et $y - i\sqrt{11}$. Alors d divise $2i\sqrt{11}$ et $2y$. Comme $N(i\sqrt{11}) = 11$ est un nombre premier, $i\sqrt{11}$ est irréductible. Comme il n'existe pas d'élément $z \in A$ tel que $N(z) = 2$, 2 est irréductible. Donc d est associé à 1, 2, $i\sqrt{11}$ ou $2i\sqrt{11}$.
> Analysons les différents cas :
> - si d est associé à $i\sqrt{11}$ ou $2i\sqrt{11}$, alors $11|N(d)|y^2 + 11$. Donc $11|y$ et $11|x$. On en déduit que $y^2 + 11 \equiv 11 \mod 11^2$ et $x^3 \equiv 0 \mod 11^2$: absurde !
> - si d est associé à 2, alors $4 = N(2)|N(y+i\sqrt{11}) = y^2+11$. Donc y est impair et x est pair. On en déduit que $y^2 + 11 \equiv 4 \mod 8$ et $x^3 \equiv 0 \mod 8$: absurde !
>
> Par conséquent, $d \in A^\times$, et $y + i\sqrt{11}$ et $y - i\sqrt{11}$ sont premiers entre eux. Par factorialité de A, il existe donc $u \in A^\times$ et $z \in A$ tels que $y + i\sqrt{11} = uz^3$. En écrivant $z = a+b\frac{1+i\sqrt{11}}{2}$, on obtient $-2b^3+3a^2b+3ab^2 = \pm 2$. On vérifie alors que $(a, b) \in \{\pm(0, 1), \pm(-1, 1), \pm(1, 2), \pm(-3, 2)\}$. Donc les couples (x, y) solutions de l'équation sont $(3, \pm 4), (15, \pm 58)$.

3 TD3

Exercice 1 (à préparer) : Vrai ou faux ?

Soit A un anneau.

1. Si A est factoriel, alors tout idéal premier non nul est maximal.

> **Indications :** FAUX : Dans $\mathbb{C}[X, Y]$, l'idéal (X) est premier non maximal. L'assertion serait vraie si A était principal.

2. Le quotient d'un anneau factoriel par un idéal premier est factoriel.

> **Indications :** FAUX : L'anneau $\mathbb{C}[X, Y]/(X^2 - Y^3) \cong \mathbb{C}[T^2, T^3]$ n'est pas factoriel, mais est quotient de l'anneau factoriel $\mathbb{C}[X, Y]$.

3. Si A est un anneau factoriel et a et b sont des éléments non nuls de A, on a $(a, b) = (a \wedge b)$.

Indications : FAUX : Il suffit de prendre $A = \mathbb{C}[X,Y]$, $a = X$ et $b = Y$. L'assertient serait vraie si A était principal.

4. Si A est un anneau factoriel et a et b sont des éléments non nuls de A, on a $(a) \cap (b) = (a \vee b)$.

Indications : VRAI : L'inclusion $(a \vee b) \subseteq (a) \cap (b)$ est évidente. Soit maintenant $x \in (a) \cap (b)$. On écrit $a = up_1^{a_1}...p_r^{a_r}$, $b = vp_1^{b_1}...p_r^{b_r}$ et $x = wp_1^{c_1}...p_r^{c_r}$, avec $u, v, w \in A^\times$, $a_1, ..., a_r, b_1, ..., b_r, c_1, ..., c_r \in \mathbb{N}$ et $p_1, ..., p_r$ des éléments irréductibles de A qui sont deux à deux non associés. Comme a divise x, on a $a_i \leq c_i$ pour tout i. De même, $b_i \leq c_i$ pour tout i. Donc $\max\{a_i, b_i\} \leq c_i$ pour tout i, et $a \vee b = p_1^{\max\{a_1,b_1\}}...p_r^{\max\{a_r,b_r\}}$ divise x. On en déduit que $(a) \cap (b) = (a \vee b)$.

5. Dans $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$, l'idéal (3) n'est pas premier, mais il est contenu dans exactement deux idéaux premiers, qui sont maximaux.

Indications : VRAI : On calcule :

$$\mathbb{Z}[\frac{1+\sqrt{13}}{2}]/(3) \cong \mathbb{Z}/3\mathbb{Z}[X]/(X^2 - X) \cong (\mathbb{Z}/3\mathbb{Z})^2.$$

L'anneau $(\mathbb{Z}/3\mathbb{Z})^2$ possédant deux idéaux premiers qui sont en fait maximaux, l'assertion est vraie.

6. L'anneau $\mathbb{Z}[(X_n)_{n\in\mathbb{N}}]$ est factoriel.

Indications : VRAI : Notons $A = \mathbb{Z}[(X_n)_{n\in\mathbb{N}}]$. Nous allons d'abord déterminer les éléments irréductibles de A. Pour chaque entier naturel n, l'anneau $A_n = \mathbb{Z}[X_1, ..., X_n]$ est factoriel. Soient n un entier naturel et $P \in A_n$. Supposons que P est irréductible dans A. Soit $m \geq n$ et écrivons $P = QR$ avec $Q, R \in A_m$. On a alors $Q \in A^\times$ ou $R \in A^\times$. Or $A^\times = \{1, -1\}$. Donc $Q \in A_m^\times$ ou $R \in A_m^\times$ et P est irréductible dans A_m. Réciproquement, supposons que P est irréductible dans A_n. Écrivons $P = QR$ avec $Q, R \in A$. Soit $m \geq n$ tel que $Q, R \in A_m$. Comme P est irréductible dans A_n, il est aussi irréductible dans A_m. Donc $Q = \pm 1$ ou $R = \pm 1$. Cela prouve que P est irréductible dans A.
Soit maintenant $P \in A$ non nul. Soit $n \in \mathbb{N}$ tel que $P \in A_n$. Comme A_n est factoriel, on peut écrire $P = up_1...p_r$ avec $u \in A_n^\times$ et $p_1, ..., p_r$ irréductibles dans A_n. Mais alors u est une unité dans A et $p_1, ..., p_r$ sont irréductibles dans A. Supposons maintenant que l'on a $v \in A^\times$ et $q_1, ..., q_s \in A$ irréductibles tels que $P = vq_1...q_s$. Soit $m \geq n$ tel que $q_1, ..., q_s \in A_m$. D'après ce qui précède, $p_1, ..., p_r, q_1, ..., q_s$ sont irréductibles dans A_m. Comme $up_1...p_r = vq_1...q_s$ et A_m est factoriel, on a $r = s$ et il existe $u_1, ..., u_r \in A_m^\times = A^\times$ et $\sigma \in S_r$ tels que $p_i = u_i q_{\sigma(i)}$ pour tout i. On en déduit que A est factoriel.

7. Le polynôme $(X + Y)^{100} + 2(X + 5)^{98}Y + 57X^{87}Y^5 \in \mathbb{C}[X, Y]$ est irréductible.

Indications : VRAI : En voyant le polynôme dans $\mathbb{C}[Y][X]$, il est unitaire et Eisenstein pour l'idéal premier (Y) de $\mathbb{C}[Y]$, donc irréductible.

8. Il existe un morphisme d'anneaux injectif de $\mathbb{Z}[X]/(2X^2 + 3X + 2)$ dans $\mathbb{C}$.

Indications : VRAI : Soit $\phi : \mathbb{Z}[X] \to \mathbb{C}, P(X) \mapsto P(\frac{-3+i\sqrt{7}}{4})$. Soit K le noyau de ϕ. On vérifie immédiatement que K contient $(2X^2+3X+2)$. Réciproquement, soit $Q \in K$. On a alors $Q(\frac{-3+i\sqrt{7}}{4}) = 0$. En écrivant la division euclidienne de Q par $2X^2+3X+2$ dans $\mathbb{Q}[X]$, on vérifie immédiatement qu'il existe $R \in \mathbb{Q}[X]$ tel que $Q = (2X^2+3X+2)R$. On voit alors que $ct(Q) = ct(R)$, et donc $R \in \mathbb{Z}[X]$. Par conséquent, $K = (2X^2+3X+2)$.

Exercice 4 : Anneaux factoriels de dimension au plus 1

Soit A un anneau factoriel tel que tout idéal premier non nul est maximal.

1. Soient x, y des éléments non nuls de A, que l'on suppose premiers entre eux. Montrer qu'il existe $u, v \in A$ vérifiant $ux + vy = 1$.

Indications : Supposons dans un premier temps x irréductible. Comme A est factoriel, (x) est premier et il est donc maximal par hypothèse. Comme x et y sont premiers entre eux, y n'est pas un élément de (x) et on a alors par maximalité $xA + yA = A$.
Lorsque x n'est plus irréductible, écrivons $x = x_1 \cdots x_r$ avec les x_i irréductibles (à une unité de A près). Pour tout $1 \leq i \leq r$, x_i et y sont premiers entre eux. Prenons $u_i, v_i \in A$ vérifiant $x_i u_i + y v_i = 1$. Le produit de ces relations s'écrit

$$1 = \prod_{i=1}^{r}(x_i u_i + y v_i) = x\Big(\prod_{i=1}^{r} u_i\Big) + y\Sigma$$

où $\Sigma \in A$ correspond à tous les autres termes.

2. Soit I un idéal non nul de A. Montrer qu'il existe $d \in I$ non nul qui est un pgcd de tous les éléments de I.

Indications : Commençons par remarquer que, par (a), lorsque x et y sont des éléments non nuls de A, on peut trouver u et v tels que l'on ait $xu+yv = x \wedge y$. Soit $d \in I$ un élément minimal pour la relation de divisibilité. Alors, par la minimalité de d et la remarque précédente, on sait que l'on a $d \mid i$ pour tout $i \in I$. De ce fait, on a $I = (d)$ et d est le pgcd cherché.

3. Conclure que A est principal.

Indications : L'anneau A est intègre car factoriel. Le (b) dit alors qu'il est principal.

Exercice 5 : Produits d'idéaux premiers

Considérons les anneaux $A = \mathbb{Z}[i\sqrt{11}]$ et $B = \mathbb{Z}[i\sqrt{13}]$.

1. Montrer que A et B ne sont pas des anneaux factoriels.

Indications : Pour A, on a la relation $(1+i\sqrt{11})(1-i\sqrt{11}) = 2^2 \cdot 3$. On vérifie que 2 est irréductible dans A, mais 2 ne divise ni $1+i\sqrt{11}$ ni $1-i\sqrt{11}$. Donc A n'est pas factoriel. Pour B, on a la relation $(1+i\sqrt{13})(1-i\sqrt{13}) = 2 \cdot 7$. On vérifie que 2 est irréductible dans B, mais 2 ne divise ni $1+i\sqrt{13}$ ni $1-i\sqrt{13}$. Donc B n'est pas factoriel.

2. Faire la liste des idéaux premiers de A qui contiennent l'idéal (2). En déduire que l'idéal (2) ne s'écrit pas comme produit d'idéaux premiers

de A.

Indications : On calcule :

$$A/(2) \cong \mathbb{Z}/2\mathbb{Z}[X]/(X^2+11) \cong \mathbb{Z}/2\mathbb{Z}[X]/((X+1)^2).$$

Il existe donc un seul idéal premier de A contenant (2) : c'est l'image réciproque de $(X+1)\mathbb{Z}/2\mathbb{Z}[X]/((X+1)^2)$ dans A, autrement dit $\mathfrak{p} = (2, 1+i\sqrt{11})$. Si (2) était produit d'idéaux premiers de A, il serait bien sûr produit d'idéaux premiers le contenant, donc une puissance de $\mathfrak{p}$. Mais $\mathfrak{p}^2 = (4, 2(1+i\sqrt{11}), -10+2i\sqrt{11}) = (4, 2(1+i\sqrt{11})$ et donc $\mathfrak{p}^2 \subsetneq (2) \subsetneq \mathfrak{p}$.

3. À l'inverse, montrer que les idéaux (2), (3) et (7) s'écrivent bien comme des produit d'idéaux premiers de l'anneau B.

Indications : On calcule :

$$B/(2) \cong \mathbb{Z}/2\mathbb{Z}[X]/(X^2+13) \cong \mathbb{Z}/2\mathbb{Z}[X]/((X+1)^2);$$

$$B/(3) \cong \mathbb{Z}/3\mathbb{Z}[X]/(X^2+13) \cong \mathbb{Z}/3\mathbb{Z}[X]/(X^2+1);$$

$$B/(7) \cong \mathbb{Z}/7\mathbb{Z}[X]/(X^2+13) \cong \mathbb{Z}/7\mathbb{Z}[X]/((X+1)(X-1)) \cong (\mathbb{Z}/7\mathbb{Z})^2.$$

Les idéaux premiers contenant (2) sont donc : $(2, 1+i\sqrt{13})$; l'idéal (3) est maximal ; les idéaux premiers contenant (7) sont : $(7, 1+i\sqrt{13})$ et $(7, 1-i\sqrt{13})$. Or on voit que $(2, 1+i\sqrt{13})^2 = (4, 2(1+i\sqrt{13}), -12+2i\sqrt{11}) = (2)$ et $(7, 1+i\sqrt{13})(7, 1-i\sqrt{13}) = (49, 7(1+i\sqrt{13}), 7(1-i\sqrt{13}), 14) = (7)$.

Exercice 11 : Entiers p-adiques et équations

Soit p un nombre premier. On munit $\mathbb{Z}_p$ de la topologie induite par la topologie produit sur $\prod_n \mathbb{Z}/p^n\mathbb{Z}$.

1. Montrer que $\mathbb{Z}_p$ est compact.

Indications : On remarque que $\mathbb{Z}_p$ est un fermé de $\prod_n \mathbb{Z}/p^n\mathbb{Z}$ (muni de la topologie produit). Or ce produit est compact d'après le théorème de Tychonov. Donc $\mathbb{Z}_p$ est compact.

2. Soit $m > 0$. Soit $f \in \mathbb{Z}[X_1, ..., X_m]$. Montrer que l'équation $f(x_1, ..., x_m) = 0$ a des solutions dans $\mathbb{Z}_p$ si, et seulement si, elle a des solutions dans $\mathbb{Z}/p^r\mathbb{Z}$ pour tout r.

Indications : Il est évident que, si l'équation a des solutions dans $\mathbb{Z}_p$, alors elle a des solutions dans $\mathbb{Z}/p^r\mathbb{Z}$ pour tout r. Réciproquement, supposons que l'équation a des solutions dans $\mathbb{Z}/p^r\mathbb{Z}$ pour tout r. Pour chaque entier naturel r, soit E_r l'ensemble des éléments $x = (x_s)_{s\in\mathbb{N}}$ de $\mathbb{Z}_p$ tels que x_r est une solution de l'équation dans $\mathbb{Z}/p^r\mathbb{Z}$. On remarque que E_r est un fermé de $\mathbb{Z}_p$ et que, si $r' \geq r$, alors $E_{r'} \subseteq E_r$. Comme $\mathbb{Z}_p$ est compact, $\bigcap_r E_r \neq \emptyset$. Un élément de cette intersection est alors une solution de l'équation dans $\mathbb{Z}_p$.

Exercice 12 : Lemme de Hensel et applications

1. Soient A un anneau et I un idéal de A.

(i) Soit n entier naturel non nul. Soient $f \in A[X]$ et $x \in A$ tels que

$f(x) \equiv 0 \mod I^n$ et $f'(x) \in (A/I)^\times$. Montrer qu'il existe $y \in A$ tel que $y \equiv x \mod I^n$ et $f(y) \equiv 0 \mod I^{n+1}$. Montrer que si $z \in A$ est tel que $z \equiv x \mod I^n$ et $f(z) \equiv 0 \mod I^{n+1}$, alors $z \equiv y \mod I^{n+1}$.

Indications : On cherche y sous la forme $x + t$ avec $t \in I^n$. On calcule $f(y) = f(x+t) \equiv f(x)+tf'(x) \mod I^{n+1}$. On veut donc trouver $t \in I^n$ tel que $tf'(x) \equiv -f(x) \mod I^{n+1}$. Si $u \in A$ est tel que $uf'(x) \equiv 1 \mod I$, comme $t \in I^n$, on obtient $t \equiv -f(x)u \mod I^{n+1}$. Cela achève la preuve de l'unicité, et pour l'existence, il suffit de vérifier que $y = x - f(x)u$ convient. On a $f(x) \in I^n$, donc $f(y) \equiv f(x) - f'(x)uf(x) \equiv 0 \mod I^{n+1}$.

(ii) Soient $f \in A[X]$ et $x \in A$ tels que $f(x) \equiv 0 \mod I$ et $f'(x) \in (A/I)^\times$. Déduire de la question précédente qu'il existe un unique $y \in \varprojlim_n A/I^n$ tel que son image dans A/I coïncide avec celle de x et $f(y) = 0$.

Indications : En utilisant la question précédente, on construit pour chaque entier naturel non nul n un élément $x_n \in A/I^n$ de sorte que $x_1 = x$, $x_{n+1} \equiv x_n \mod I^n$ et $f(x_n) = 0$. L'élément $y = (x_n) \in \varprojlim_n A/I^n$ vérifie alors $f(y) = 0$ et $x_1 = x$. Quant à l'unicité, si $z = (z_n) \in \varprojlim_n A/I^n$ vérifie $z_1 = x$ et $f(z) = 0$, alors en utilisant la question précédente et par récurrence, on montre que $z_n = x_n$ pour tout n.

2. Est-ce que 14 possède une racine carrée dans $\mathbb{Z}_5$? Dans $\mathbb{Z}_7$? Dans $\mathbb{Z}_{11}$?

Indications : Soit $f = X^2 - 14 \in \mathbb{Z}[X]$. On remarque que $f(2) \equiv 0 \mod 5$ et $f'(2) \equiv 4 \mod 5$. On déduit alors du lemme de Hensel que 14 possède une racine carrée dans $\mathbb{Z}_5$. De même, $f(5) \equiv 0 \mod 11$ et $f'(5) \equiv 10 \mod 11$, donc 14 a une racine carrée dans $\mathbb{Z}_{11}$. Par contre, 14 ne possède pas de racine carrée dans $\mathbb{Z}_7$ puisqu'il n'en possède pas dans $\mathbb{Z}/7^2\mathbb{Z}$.

3. Soit p un nombre premier. En utilisant le lemme de Hensel, montrer que $\mathbb{Z}_p$ possède $p-1$ racines $p-1$-ièmes de l'unité.

Indications : L'anneau $\mathbb{Z}_p$ est intègre, donc $\mathbb{Z}_p$ a au plus $p-1$ racines $p-1$-ièmes de l'unité. Soit $f(X) = X^p - X$. Pour chaque $x \in \mathbb{Z}/p\mathbb{Z}$, on a $f(x) = 0$ et $f'(x) = 1$. Donc il existe $s(x) = (s(x)_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$ tel que $f(s(x)) = 0$ et $s(x)_1 = x$. On en déduit que $\mathbb{Z}_p$ possède $p-1$ racines $p-1$-ièmes de l'unité.

4. Montrer qu'il existe $f(T) \in \mathbb{Z}[[T]]$ tel que $f(T)^5 + f(T) + T = 0$. En écrivant $f(T) = \sum_{n\geq 0} a_n T^n$, calculer a_n pour $n \leq 6$.

Indications : Soit $g = X^5 + X + T \in \mathbb{Z}[T][X]$. On remarque que $g(0) \equiv 0 \mod T$ et $g'(0) \equiv 1 \mod T$. Il existe donc $f(T) = \sum_{n\geq 0} a_n T^n \in \mathbb{Z}[[T]]$ tel que $f(T)^5 + f(T) + T = 0$. En calculant, on obtient $f(T) = -T + T^5 \mod T^7$.