Université Pierre & Marie Curie — Master de mathématiques 1
Année 2012-2013 — Module MM020

# Théorie des Nombres - TD2
# Corps finis

**Exercice 1 :** Montrer les isomorphismes suivants et exhiber un générateur du groupe des éléments inversibles :

a) $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2+X+1)$.

b) $\mathbb{F}_8 \cong \mathbb{F}_2[X]/(X^3+X+1)$.

c) $\mathbb{F}_{16} \cong \mathbb{F}_2[X]/(X^4+X+1)$.

d) $\mathbb{F}_{16} \cong \mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y)$.

*Solution de l'exercice* 1. Puisque pour tout $n \geq 1$, le corps $\mathbb{F}_2$ admet une unique extension de degré $n$ à l'intérieur d'une clôture algébrique $\overline{\mathbb{F}_2}$ fixée, il suffit de vérifier pour les trois premiers isomorphismes que les polynômes en question sont irréductibles sur $\mathbb{F}_2$.

a) Il est clair que le polynôme $X^2+X+1$ n'a pas de racine dans $\mathbb{F}_2$, donc il est irréductible sur $\mathbb{F}_2$. Alors $\mathbb{F}_2[X]/(X^2+X+1)$ est une extension de degré 2 de $\mathbb{F}_2$, donc il est isomorphe à $\mathbb{F}_4$. En outre, $\mathbb{F}_4^*$ est cyclique d'ordre 3, donc tout élément de $\mathbb{F}_4$ distinct de 0 et 1 engendre $\mathbb{F}_4^*$. Par conséquent, la classe de $X$ (ou celle de $X+1$) engendre le groupe des inversibles de $\mathbb{F}_2[X]/(X^2+X+1)$.

b) Le polynôme $X^3+X+1$ n'a pas de racine dans $\mathbb{F}_2$, il est donc irréductible sur $\mathbb{F}_2$. D'où l'isomorphisme recherché. Or $\mathbb{F}_8^* \cong \mathbb{Z}/7\mathbb{Z}$, donc tout élément de $\mathbb{F}_8$ distinct de 0 et 1 engendre $\mathbb{F}_8^*$. Par exemple, la classe de $X$ engendre le groupe des inversibles de $\mathbb{F}_2[X]/(X^3+X+1)$.

c) On voit que $X^4+X+1$ n'a pas de racine dans $\mathbb{F}_2$. Montrons qu'il ne peut se décomposer en produit de deux polynômes irréductibles de degré 2 sur $\mathbb{F}_2$. Or on sait que le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$ est $X^2+X+1$, et il est clair que son carré n'est pas $X^4+X+1$. On peut aussi montrer que $X^4+X+1$ est irréductible en montrant qu'il n'a pas de racine dans $\mathbb{F}_4$. Cela assure que $\mathbb{F}_{16} \cong \mathbb{F}_2[X]/(X^4+X+1)$. Or le groupe $\mathbb{F}_{16}^*$ est isomorphe à $\mathbb{Z}/15\mathbb{Z}$. Donc les générateurs de $\mathbb{F}_{16}^*$ sont les éléments de ce groupes qui sont distincts de 1 et d'ordre ni 3, ni 5. Considérons la classe de $X$ (notée abusivement $X$) dans $\mathbb{F}_2[X]/(X^4+X+1)$. On dispose de la base $(1, X, X^2, X^3)$ de $\mathbb{F}_2[X]/(X^4+X+1)$ sur $k$, et il est donc clair que $X^3-1$ et $X^5-1 = X^2+X+1$ ne sont pas nuls dans le quotient. Par conséquent, $X$ n'est pas d'ordre 3, ni d'ordre 5, il est donc d'ordre 15. C'est donc un générateur du groupe des inversibles.

d) On dispose d'un isomorphisme naturel :

$$\mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y) \cong \big(\mathbb{F}_2[Y]/(Y^2+Y+1)\big)[X]/(X^2+X+Y).$$

Par la première question, on a un isomorphisme $\mathbb{F}_2[Y]/(Y^2+Y+1) \cong \mathbb{F}_4$, par conséquent, il suffit de montrer que pour $y \in \mathbb{F}_4$, $y \neq 0, 1$, le polynôme $X^2+X+y \in \mathbb{F}_4[X]$ est irréductible, i.e. que ce polynôme n'a pas de racine dans $\mathbb{F}_4$. Ceci est clair (tester 0, 1, $y$ et $y^2$), donc $\mathbb{F}_{16} \cong \mathbb{F}_4[X]/(X^2+X+y) \cong \mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+X+Y)$. On dispose alors de la base (sur $\mathbb{F}_2$) $(1, X, Y, XY)$, et on vérifie qu'un générateur de $\mathbb{F}_{16}^*$ est alors donné par la classe de $X$ (la classe de $Y$ en revanche est d'ordre 3).

**Exercice 2 :** Montrer que dans un corps fini, tout élément est somme de deux carrés.

*Solution de l'exercice* 2. Soit $\mathbb{F}_q$ le corps fini en question (où $q = p^r$). On considère le morphisme de groupes multiplicatifs $\varphi : \mathbb{F}_q^* \to \mathbb{F}_q^*$ défini par $\varphi(x) := x^2$. Alors par définition $\mathrm{Im}(\varphi)$ est l'ensemble des

carrés dans $\mathbb{F}_q^*$. Notons que $\mathrm{Ker}(\varphi)$ est réduit à $\pm 1$. Par conséquent, le cardinal de $\mathrm{Ker}(\varphi)$ vaut 2 si $p \neq 2$, il vaut 1 si $p = 2$. En particulier, si $p = 2$, $\varphi$ est injectif, donc surjectif, donc tout élément e $\mathbb{F}_q$ est un carré, donc en particulier tout élément est somme de deux carrés.
On suppose maintenant $p$ impair. On sait que

$$\#\mathbb{F}_q^* = \#\mathrm{Ker}(\varphi)\#\mathrm{Im}(\varphi)\,,$$

et $\#\mathbb{F}_q^* = q - 1$. Par conséquent, on en déduit que

$$\#\mathrm{Im}(\varphi) = \frac{q-1}{2}\,.$$

Soit alors $a \in \mathbb{F}_q$. Considérons l'ensemble $C := \mathrm{Im}(\varphi) \cup \{0\}$ des carrés dans $\mathbb{F}_q$. On a montré que $\#C = \frac{q+1}{2}$. Or l'ensemble $C_a := \{a - x^2 : x \in \mathbb{F}_q\}$ est en bijection avec $C$, donc il est aussi de cardinal $\frac{q+1}{2}$. Donc

$$\#C + \#C_a = \frac{q+1}{2} + \frac{q+1}{2} = q + 1 > q = \#\mathbb{F}_q\,,$$

par conséquent les ensembles $C$ et $C_a$ ne peuvent pas être disjoints, i.e. $C \cap C_a \neq \emptyset$. Prenons alors $c \in C \cap C_a$. Par définition, il existe $x, y \in \mathbb{F}_q$ tels que $c = x^2$ et $c = a - y^2$. Finalement, on a bien $a = x^2 + y^2$, ce qui conclut.

**Exercice 3 :**

a) Soit $q = p^r$, $p$ un nombre premier impair. Montrer que $x \in \mathbb{F}_q^*$ est un carré si et seulement si $x^{\frac{q-1}{2}} = 1$.

b) En étudiant les diviseurs de $(n!)^2 + 1$, montrer qu'il existe une infinité de nombres premiers de la forme $4k + 1$ ($k \in \mathbb{N}$).

*Solution de l'exercice* 3.

a) On suppose d'abord que $x$ est un carré, i.e. il existe $y \in \mathbb{F}_q^*$ tel que $x = y^2$. Alors $x^{\frac{q-1}{2}} = y^{q-1} = 1$ (puisque $\mathbb{F}_q^*$ est d'ordre $q - 1$).

Considérons l'ensemble $R$ des racines du polynôme $P(X) = X^{\frac{q-1}{2}} - 1$. Il contient, par la remarque précédente, tous les carrés de $\mathbb{F}_q^*$. Or on a vu (exercice 2) que $\mathbb{F}_q^*$ contenait $\frac{q-1}{2}$ carrés. Par conséquent, puisque $P(X)$ est de degré $\frac{q-1}{2}$, $R$ coïncide avec l'ensemble des carrés dans $\mathbb{F}_q^*$, ce qui conclut.

b) Soit $n \in \mathbb{N}$ et $p$ un diviseur premier de $(n!)^2 + 1$. Alors $p > n$ (sinon $p$ diviserait $n!$, donc $p$ diviserait 1, ce qui n'est pas). Vérifions que $p$ est congru à 1 modulo 4 : puisque $p$ divise $(n!)^2 + 1$, on a $(n!)^2 = -1$ dans $\mathbb{F}_p$. En particulier, $-1$ est un carré dans $\mathbb{F}_p$. Par la question précédente, cela assure que $(-1)^{\frac{p-1}{2}} = 1$, donc $\frac{p-1}{2}$ est pair, donc $p$ est congru à 1 modulo 4.

En prenant des entiers $n$ tendant vers l'infini, on obtient ainsi une infinité de nombres premiers $p$ congrus à 1 modulo 4.

**Exercice 4 :** Soit $p$ un nombre premier impair. Montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1$ [8].
[Indication : on pourra considérer $\zeta$ une racine primitive 8-ième de l'unité dans $\overline{\mathbb{F}_p}$ et étudier $\zeta + \zeta^{-1}$.]

*Solution de l'exercice* 4. On calcule que $(\zeta + \zeta^{-1})^2 = 2$. Donc 2 est un carré modulo $p$ si et seulement si $\zeta + \zeta^{-1} \in \mathbb{F}_p$, si et seulement si $(\zeta + \zeta^{-1})^p = \zeta + \zeta^{-1}$ si et seulement si $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$. Or $\zeta^5 = -\zeta$ et $\zeta^3 = -\zeta^{-1}$, donc il est clair que la condition $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ équivaut à la condition $p \equiv \pm 1$ [8].

**Exercice 5 :**

a) Soit $k$ un corps, $a \in k$, $p$ un nombre premier. Montrer que $X^p - a$ est irréductible dans $k[X]$ si et seulement si il n'admet pas de racine dans $k$.

[Indication : si $X^p - a$ est réductible, on pourra écrire une décomposition de ce polynôme dans $k[X]$, puis utiliser la décomposition de $X^p - a$ en facteurs de degré 1 sur $\overline{k}$, pour en déduire que $a$ est une puissance $p$-ième dans $k$.]

b) Soient $p, l$ deux nombres premiers tels que $l$ divise $p-1$. Soit $n \in \mathbb{Z}$ tel que la classe de $n$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que le polynome $X^l + pX^k - n$ est irréductible dans $\mathbb{Z}[X]$, pour tout $1 \leq k < l$.

*Solution de l'exercice* 5.

a) Il est clair que si $X^p - a$ a une racine dans $k$, alors ce polynôme est réductible. Supposons maintenant que le polynôme $X^p - a$ soit réductible. Alors il existe $P, Q \in k[X]$ de degrés respectifs $d$ et $p - d$, avec $1 \leq d < p$. On note $b$ le coefficient constant de $P$.

Sur $\overline{k}$, le polynôme $X^p - a$ se décompose sous la forme $X^p - a = \prod_{i=0}^{p-1}(X - \zeta^i \alpha)$, où $\zeta \in \overline{k}$ est une racine primitive $p$-ième de l'unité, et $\alpha^p = a$, $\alpha \in \overline{k}$ (si $k$ est de caractéristique $p$, alors $\zeta = 1$). Or $P$ divise $X^p - a$, donc $P$ se décompose sous la forme $P(X) = \prod_{i \in I}(X - \zeta^i \alpha)$, où $I$ est une partie non vide (et non pleine) de $\{0, \dots, p-1\}$. En particulier, on a $b = \zeta^r \alpha^d$, pour un certain entier $r$. Donc on a $b^p = \alpha^{pd} = a^d$. Or $d$ et $p$ sont premiers entre eux (car $p$ est premier et $1 \leq d < p$, donc il existe $u, v \in \mathbb{Z}$ tels que $ud + vp = 1$. Alors $(a^d)^u = (b^p)^u$, donc $a = (a^v b^u)^p$, donc $a$ est une puissance $p$-ième dans $k$, donc $X^p - a$ admet une racine dans $k$ (en l'occurrence, cette racine est $a^v b^u$).

b) On considère la réduction modulo $p$ du polynôme $P$ considéré : on a $\overline{P} = X^l - n \in \mathbb{F}_p[X]$. Alors pour appliquer la question a) à $k = \mathbb{F}_p$, au nombre premier $l$ et à $a = n$, il suffit de montrer que $n$ n'est pas une puissance $l$-ième dans $\mathbb{F}_p$. Si c'était le cas, alors il existerait $b \in \mathbb{F}_p$ tel que $b^l = n$. Alors $n$ serait d'ordre divisant $\frac{p-1}{l}$ dans $\mathbb{F}_p^*$, ce qui contredirait le fait que $n$ engendre $\mathbb{F}_p^*$. Donc la question a) assure que $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$. Donc $P(X) = X^l + pX^k - n$ est irréductible dans $\mathbb{Z}[X]$.

**Exercice 6 :**

a) Si $p$ et $l$ sont des nombres premiers, montrer qu'il existe un morphisme de corps $\mathbb{F}_{p^n} \to \mathbb{F}_{l^m}$ si et seulement si $p = l$ et $n$ divise $m$.

b) Ce morphisme de corps est-il unique ?

c) Fixons, pour tout $n, m$ tels que $n$ divise $m$, un morphisme $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, de façon compatible. Montrer que $\overline{\mathbb{F}_p} := \bigcup_{n \geq 1} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de $\mathbb{F}_p$.

*Solution de l'exercice* 6.

a) On remarque d'abord que pour toute extension de corps $L/K$, la caractéristique de $L$ est égale à celle de $K$. Donc la condition $p = l$ est clairement nécessaire.

Supposons que l'on a une inclusion de corps $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$. Alors $\mathbb{F}_{p^n}^*$ est un sous-groupe d'ordre $p^n - 1$ dans le groupe $\mathbb{F}_{p^m}^*$ d'ordre $p^m - 1$. On en déduit que $p^n - 1$ divise $p^m - 1$. On effectue alors la division euclidienne de $m$ par $n$ : $m = nq + r$ avec $0 \leq r < n$. Alors $p^m - 1 = p^r((p^n)^q - 1) + (p^r - 1)$, et $p^n - 1$ divise $(p^n)^q - 1$. Donc $p^r - 1$ est le reste de la division euclidienne de $p^m - 1$ par $p^n - 1$. Il est alors clair que $p^n - 1$ divise $p^m - 1$ si et seulement si $r = 0$ si et seulement si $n$ divise $m$.

On peut également montrer que $n$ divise $m$ en disant que $\mathbb{F}_{p^m}$ est un $\mathbb{F}_{p^n}$-espace vectoriel de dimension finie (disons $d$), il est donc isomorphe (comme espace vectoriel) à $(\mathbb{F}_{p^n})^d$, donc en calculant les cardinaux, on a $p^m = (p^n)^d$, donc $m = n.d$, donc $n$ divise $m$.

Réciproquement, si $n$ divise $m$, alors on $\mathbb{F}_{p^n}$ s'identifie à l'ensemble des $x \in \mathbb{F}_{p^m}$ tels que $x^{p^n} = x$, puisque $p^n - 1$ divise $p^m - 1$.

b) Ce morphisme n'est pas unique en général, on peut toujours le composer avec un automorphisme non trivial du corps $\mathbb{F}_{p^n}$ (le Frobenius $x \mapsto x^p$ par exemple, si $n > 1$).

c) Tout d'abord, on remarque que les corps $\mathbb{F}_{p^{n!}}$ forment une famille croissante de corps puisque $n!$ divise $(n+1)!$. L'ensemble $\overline{\mathbb{F}_p}$ est une réunion croissante de corps, donc on vérifie facilement que c'est lui-même de façon naturelle un corps (étant donnés $x, y \in \overline{\mathbb{F}_p}$, il existe un $n \in \mathbb{N}$ tel que $x, y \in \mathbb{F}_{p^{n!}}$, et donc la somme et le produit $x+y$, $xy$ sont bien définis dans $\mathbb{F}_{p^{n!}}$, donc dans $\overline{\mathbb{F}_p}$ puisque les images de $x+y$ et $xy$ dans $\overline{\mathbb{F}_p}$ ne dépendent pas de l'entier $n$ choisi). Par construction, on dispose d'un morphisme de corps $\mathbb{F}_p \subset \overline{\mathbb{F}_p}$. En outre, $\overline{\mathbb{F}_p}$ est une réunion d'extensions finies (donc algébriques) de $\mathbb{F}_p$, donc l'extension $\overline{\mathbb{F}_p}/\mathbb{F}_p$ est algébrique. Par conséquent, il reste donc à montrer que le corps $\overline{\mathbb{F}_p}$ est algébriquement clos. Soit $P \in \overline{\mathbb{F}_p}[X]$ un polynôme non constant. Par construction de $\overline{\mathbb{F}_p}$ et puisque $P$ n'a qu'un nombre fini de coefficients, il existe $n \in \mathbb{N}$ tel que $P \in \mathbb{F}_{p^{n!}}[X]$. En prenant par exemple un corps de décomposition de $P$, il existe $d \in \mathbb{N}$ tel que $P$ ait une racine dans une $\mathbb{F}_{p^{n!d}}$. Or le corps $\mathbb{F}_{p^{n!d}}$ est contenu dans $\mathbb{F}_{p^{N!}}$ pour $N$ assez grand (par exemple $N = nd$), donc $P$ a une racine dans $\mathbb{F}_{p^{N!}}$, donc dans $\overline{\mathbb{F}_p}$. Cela conclut la preuve.

**Exercice 7 :** Soit $p$ un nombre premier. Montrer que le groupe $\mathbb{F}_{p^n}^*$ s'identifie à un sous-groupe du groupe $\mathbf{GL}_n(\mathbb{F}_p)$.

*Solution de l'exercice* 7. On voit $\mathbb{F}_{p^n}$ comme un $\mathbb{F}_p$-espace vectoriel de dimension $n$. On dispose d'une action par multiplication de $\mathbb{F}_{p^n}^*$ sur $\mathbb{F}_{p^n}$, qui induit un morphisme de groupes évident $\mathbb{F}_{p^n}^* \to \mathbf{GL}(\mathbb{F}_{p^n})$. Ce morphisme est clairement injectif. Enfin, si on fixe une base de $\mathbb{F}_{p^n}$ sur $\mathbb{F}_p$ (comme espace vectoriel), on peut identifier les groupes $\mathbf{GL}(\mathbb{F}_{p^n})$ et $\mathbf{GL}_n(\mathbb{F}_p)$

**Exercice 8 :**

a) Donner la liste de tous les polynômes irréductibles de degré $\leq 5$ sur $\mathbb{F}_2$.

b) Donner la liste de tous les polynômes irréductibles unitaires de degré $\leq 3$ sur $\mathbb{F}_3$.

c) Donner le nombre et la liste de tous les polynômes irréductibles unitaires de degré $\leq 2$ sur $\mathbb{F}_4$.

*Solution de l'exercice* 8.

a) Il est facile d'énumérer tous les polynômes de degré $\leq 5$ sur $\mathbb{F}_2$. Ensuite on teste si chacun de ces polynômes est irréductible ou non. On obtient la liste suivante de polynômes irréductibles : $X$, $X+1$, $X^2+X+1$, $X^3+X+1$, $X^3+X^2+1$, $X^4+X+1$, $X^4+X^3+1$, $X^4+X^3+X^2+X+1$, $X^5+X^2+1$, $X^5+X^3+1$, $X^5+X^3+X^2+X+1$, $X^5+X^4+X^2+X+1$, $X^5+X^4+X^3+X+1$, $X^5+X^4+X^3+X^2+1$.

b) On note $\mathbb{F}_3 = \{0, 1, 2\}$. On énumère tous les polynômes unitaires non constants de degré 2 et 3 à coefficients dans $\mathbb{F}_3$, et on ne conserve que ceux qui n'ont pas de racine dans $\mathbb{F}_3$. On obtient la liste suivante :
$X$, $X+1$, $X+2$, $X^2+1$, $X^2+X+2$, $X^2+2X+2$, $X^3+2X+1$, $X^3+2X+2$, $X^3+X^2+2$, $X^3+X^2+X+2$, $X^3+X^2+2X+1$, $X^3+2X^2+1$, $X^3+2X^2+X+1$, $X^3+2X^2+2X+2$.

c) On dispose de deux méthodes : la première, analogue à la précédente, consiste à énumérer tous les polynômes unitaires de degré 2 sur $\mathbb{F}_4$ (il y en a seize), puis de tester si chacun de ces polynômes a ou non une racine dans $\mathbb{F}_4$ (il y a quatre éléments dans $\mathbb{F}_4$ à tester).

Un autre méthode plus "élaborée" est la suivante : un polynôme irréductible de degré 4 sur $\mathbb{F}_2$ a une racine dans $\mathbb{F}_{16}$. Donc il se décompose en produit de deux polynômes irréductibles dans $\mathbb{F}_4$ (car $\mathbb{F}_{16}$ est une extension de degré 2 de $\mathbb{F}_4$). Réciproquement, étant donné un polynôme irréductible de degré 2 sur $\mathbb{F}_4$, le produit avec son conjugué (par l'unique $\mathbb{F}_2$-automorphisme non trivial de $\mathbb{F}_4$ : cet automorphisme est l'élévation au carré, i.e. le Frobenius de $\mathbb{F}_2$) est un polynôme de $\mathbb{F}_2[X]$ (les coefficients sont invariants par le groupe de Galois) irréductible de degré 4. Par conséquent, il y a deux fois plus de polynômes irréductibles unitaires de degré 2 dans $\mathbb{F}_4$ que de polynômes irréductibles de degré 4 dans $\mathbb{F}_2$, et ils sont obtenus en factorisant dans $\mathbb{F}_4[X]$ les polynômes de degré 4 obtenus à la question précédente. Par conséquent, il y a exactement

6 polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_4$. Notons $j$ un élément de $\mathbb{F}_4 \setminus \mathbb{F}_2$, alors $\mathbb{F}_4 = \{0, 1, j, j^2\}$.
Les polynômes unitaires irréductibles de degré 1 sont $X$, $X+1$, $X+j$ et $X+j^2$. Ceux de degré 2 sont obtenus en décomposant les polynômes irréductibles de degré 4 sur $\mathbb{F}_2$ :

$$X + X + 1 = (X^2 + X + j)(X^2 + X + j^2)\,,$$

$$X^4 + X^3 + 1 = (X^2 + jX + j)(X^2 + j^2X + j^2)\,,$$

$$X^4 + X^3 + X^2 + X + 1 = (X^2 + jX + 1)(X^2 + j^2X + 1)\,.$$

**Exercice 9 :** Montrer (sans utiliser les résultats généraux sur les polynômes cyclotomiques) que le polynôme $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$, et qu'il est réductible dans $\mathbb{F}_p[X]$ pour tout nombre premier $p$.

*Solution de l'exercice* 9. Pour montrer l'irréductibilité sur $\mathbb{Q}$, il suffit de montrer l'irréductibilité sur $\mathbb{Z}$. Or il est clair que le polynôme $X^4+1$ n'a pas de racines dans $\mathbb{Z}$. Par conséquent, s'il est réductible, sa décomposition dans $\mathbb{Z}[X]$ s'écrit :

$$X^4 + 1 = (X^2 + aX + b)(X^2 + cX + d)\,,$$

avec $a, b, c, d \in \mathbb{Z}$. On voit facilement que ceci est impossible, donc $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$. Dans $\mathbb{F}_2[X]$, on a $X^4 + 1 = (X + 1)^4$, donc le polynôme est réductible modulo 2. Soit $p$ un nombre premier impair. On remarque que trouver une racine de $X^4 + 1$ revient à trouver une racine primitive 8-ième de l'unité. Or on voit que l'entier $p^2 - 1 = (p - 1)(p + 1)$ est divisible par 8, ce qui signifie que $\mathbb{F}_{p^2}$ contient toutes les racines 8-ièmes de l'unité. Soit alors $\zeta \in \mathbb{F}_{p^2}$ une racine primitive 8-ième de l'unité. Alors $t := \zeta^4 \in \mathbb{F}_p$ vérifie $t^2 = 1$ et $t \neq 1$, donc $t = -1$, donc $\zeta$ est racine de $X^4 + 1$. Par conséquent, le polynôme $X^4 + 1 \in \mathbb{F}_p[X]$ admet une racine dans l'extension quadratique $\mathbb{F}_{p^2}/\mathbb{F}_p$, donc il n'est pas irréductible dans $F_p[X]$.

**Exercice 10 :** Soit $n \geq 2$ un entier.

a) Soit $p$ un nombre premier. Montrer que $p \equiv 1\ [n]$ si et seulement si $\mathbb{F}_p$ contient une racine primitive $n$-ième de l'unité.
b) Soit $k \in \mathbb{N}$, et $p$ un diviseur premier de $\phi_n(k!)$. Montrer que $p > k$ et soit $p$ divise $n$, soit $p \equiv 1\ [n]$.
c) Montrer qu'il existe une infinité de nombres premiers $p \equiv 1\ [n]$.

*Solution de l'exercice* 10.

a) Le groupe $\mathbb{F}_p^*$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$ (c'est un groupe cyclique d'ordre $p - 1$). Alors $\mathbb{F}_p$ contient une racine primitive $n$-ième de l'unité si et seulement si de groupe admet un élément d'ordre $n$ si et seulement si $n$ divise $p - 1$ si et seulement si $p \equiv 1\ [n]$.
b) Si on écrit $\phi_n(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$, avec $a_i \in \mathbb{Z}$, alors $a_0 = \phi(0) = \pm 1$, et $\phi_n(k!) = k!^d + a_{d-1}k!^{d-1} + \cdots + a_0$. Or si $p \leq k$, alors $p$ divise $k!$, donc $p$ divise $\phi_n(k!) - a_0$, donc $p$ divise $a_0 = \pm 1$, ce qui est contradictoire. Donc $p > k$. Supposons que $p$ ne divise pas $n$. Alors modulo $p$, on a $\phi_n(k!) \equiv 0\ [p]$, donc la classe de $k!$ est une racine primitive $n$-ième de l'unité dans $\mathbb{F}_p$. Donc la question a) assure que $p \equiv 1\ [n]$.
c) Si $p_1, \ldots, p_r$ sont des nombres premiers distincts congrus à 1 modulo $n$, on pose $k := \max(p_i, n)$. Alors $\phi_n(k!)$ admet un facteur premier $p$. Par la question b), on a $p > n$ et $p > p_i$ pour tout $i$, et $p \equiv 1\ [n]$. Cette construction assure qu'il existe une infinité de nombres premiers $p \equiv 1\ [n]$.

**Exercice 11 :** Soit $\mathrm{Irr}(n, q)$ l'ensemble des polynômes irréductibles unitaires de degré $n$ sur $\mathbb{F}_q$ et $I(n, q)$ le cardinal de cet ensemble.

a) Montrer que si $d$ divise $n$, alors pour tout $P \in \mathrm{Irr}(d,q)$, $P$ divise $X^{q^n} - X$.

b) Montrer que si $P \in \mathrm{Irr}(d,q)$ divise $X^{q^n} - X$, alors d divise n.

c) En déduire la formule

$$\sum_{d|n} dI(d,q) = q^n \,.$$

d) On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ par $\mu(n) = (-1)^r$ si $n$ est le produit de $r$ nombres premiers distincts, et par $\mu(n) = 0$ si $n$ admet un facteur carré. Montrer que si $f, g : \mathbb{N}^* \to \mathbb{C}$ sont deux fonctions, on a $f(n) = \sum_{d|n} g(d)$ pour tout $n$ si et seulement si $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$ pour tout $n$.

e) En déduire la formule

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \,.$$

f) Montrer que pour tout $n \geq 1$, $I(n,q) \geq 1$.

g) Montrer le “théorème des nombres premiers pour les polynômes” :

$$I(n,q) = \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right)$$

quand $n$ tend vers $+\infty$.

[remarque : si on pose $x = q^n$, cette formule devient $I(x,q) = \frac{x}{\log_q(x)} + O\left(\frac{\sqrt{x}}{\log_q(x)}\right)$, qui est l'exacte analogue de la forme précise (conjecturée !) du classique théorème des nombres premiers.]

*Solution de l'exercice* 11.

a) On suppose que $d$ divise $n$. Soit $P \in \mathbb{F}_q[X]$ irréductible de degré $d$. Alors $\mathbb{F}_{q^d}$ est un corps de rupture de $\mathbb{F}_q$. Or $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$ puisque $d$ divise $n$, donc les racines de $P$ sont annulées par $X^{q^n} - X$. Donc $P$ divise $X^{q^n} - X$.

b) Soit $P \in \mathrm{Irr}(d,q)$ divisant $X^{q^n} - X$. Le corps $\mathbb{F}_{q^n}$ est un corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}_q$, donc il contient les racines de $P$, donc il contient un corps de décomposition de $P$. Or un corps de décomposition de $P$ est de degré $d$ sur $\mathbb{F}_q$, et $\mathbb{F}_{q^n}$ est de degré $n$ sur $\mathbb{F}_q$, donc $d$ divise $n$.

c) Les deux questions précédentes assurent que l'on a légalité suivante dans $\mathbb{F}_q[X]$ :

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathrm{Irr}(d,q)} P(X) \,.$$

En prenant les degrés des deux côtés, on obtient l'égalité souhaitée :

$$q^n = \sum_{d|n} dI(d,q) \,.$$

d) On montre d'abord la formule suivante :

$$\sum_{d|n} \mu(d) = 0 \text{ si } n \geq 2 \;,\; \sum_{d|n} \mu(d) = 1 \text{ si } n = 1 \,.$$

La seconde formule est évidente. Pour la première, on décompose $n$ en facteurs premiers distincts $n = p_1^{r_1} \dots p_s^{r_s}$, avec $r_i \geq 1$. Alors on a

$$\sum_{d|n} \mu(d) = \sum_{(t_1,\dots,t_s) \in \{0,1\}^s} \mu(p_1^{t_1} \dots p_s^{t_s}) = \sum_{(t_1,\dots,t_s) \in \{0,1\}^s} (-1)^{\sum_{i=1}^s t_i} = \sum_{k=0}^{d} \binom{s}{k} (-1)^k = (1-1)^s = 0 \,.$$

Montrons alors le résultat demandé : supposons que $f(n) = \sum_{d|n} g(d)$. Alors on a

$$\sum_{d|n} \mu(\frac{n}{d}) f(d) = \sum_{d|n} \mu(\frac{n}{d}) \sum_{d'|d} g(d') = \sum_{d'|n} g(d') \sum_{d'|d|n} \mu(\frac{n}{d}) .$$

Or on a

$$\sum_{d'|d|n} \mu(\frac{n}{d}) = \sum_{k|\frac{n}{d'}} \mu(k) = 0$$

sauf si $d' = n$ auquel cas la somme vaut 1. Donc on en déduit que

$$\sum_{d|n} \mu(\frac{n}{d}) f(d) = g(n) .$$

Réciproquement, supposons que $\sum_{d|n} \mu(\frac{n}{d}) f(d) = g(n)$. Alors on a

$$\sum_{d|n} g(d) = \sum_{d|n} \sum_{d'|d} \mu(\frac{d}{d'}) f(d') = \sum_{d'|n} f(d') \sum_{d'|d|n} \mu(\frac{d}{d'}) = \sum_{d'|n} f(d') \sum_{k|\frac{n}{d'}} \mu(k) = f(n)$$

en utilisant à nouveau que $\sum_{k|\frac{n}{d'}} \mu(k) \neq 0$ si et seulement si $d' = n$.

e) On applique la question précédente à la relation $q^n = \sum_{d|n} dI(d,q)$. On obtient alors immédiatement

$$nI(n,q) = \sum_{d|n} \mu(\frac{n}{d}) q^d ,$$

d'où la formule souhaitée.

f) On déduit de la question précédente une formule de la forme

$$nI(n,q) = q^n + \sum_{d|n, d<n} \mu(\frac{n}{d}) q^d .$$

Or pour tout $d|n$, $|\mu(\frac{n}{d})| \leq 1$, donc il est clair que $\left| \sum_{d|n,d<n} \mu(\frac{n}{d}) q^d \right| \leq q^{\frac{n}{2}+1}$, donc $nI(n,q) \neq 0$, donc $I(n,q) \neq 0$, donc $I(n,q) \geq 1$.

g) On reprend la formule de la question précédente :

$$nI(n,q) = q^n + \sum_{d|n, d<n} \mu(\frac{n}{d}) q^d .$$

On en déduit que

$$|nI(n,q) - q^n| \leq q^{\frac{n}{2}} + \sum_{d \leq \frac{n}{3}} q^d \leq 2q^{\frac{n}{2}} .$$

Par conséquent, après division par $n$, on obtient

$$\left| I(n,q) - \frac{q^n}{n} \right| \leq \frac{2q^{\frac{n}{2}}}{n} ,$$

d'où la conclusion.

**Exercice 12 :** Soient $p, l$ deux nombres premiers impairs, tels que $l \equiv 2$ [3] et la classe de $p$ modulo $l$ engendre $(\mathbb{Z}/l\mathbb{Z})^*$.
Montrer que $X^{l+1} - X + p$ est irréductible dans $\mathbb{Z}[X]$.
[Indication : on pourra considérer les réductions de ce polynôme modulo 2 et $p$.]

*Solution de l'exercice* 12. Modulo $p$, ce polynôme s'écrit $X^{l+1} - X = X(X^l - 1) = X(X-1)\phi_l(X)$ dans $\mathbb{F}_p[X]$. Or la classe de $p$ engendre $(\mathbb{Z}/l\mathbb{Z})^*$, donc le polynôme $\phi_l$ est irréductible dans $\mathbb{F}_p[X]$. Supposons que le polynôme initial n'est pas irréductible dans $\mathbb{Z}$. Alors il admet un facteur de degré $\leq 2$. Or modulo 2, ce polynôme s'écrit $X^{l+1} + X + 1$. Il est clair qu'il n'a pas de racine dans $\mathbb{F}_2$, donc il admet un facteur irréductible de degré 2. Donc il est divisible par $X^2 + X + 1$ (qui est l'unique polynôme irréductible de degré 2 sur $\mathbb{F}_2$). Or pour tout $n \geq 5$, on a $X^n + X + 1 = (X^2 + X + 1)(X^{n-2} - X^{n-3}) + X^{n-3} + X + 1$. Donc on a $\text{pgcd}(X^n + X + 1, X^2 + X + 1) = \text{pgcd}(X^{n-3} + X + 1, X^2 + X + 1)$. Une récurrence simple assure alors que $\text{pgcd}(X^{l+1} + X + 1, X^2 + X + 1) = \text{pgcd}(X^3 + X + 1, X^2 + X + 1)$ (car $l + 1$ est divisble par 3, par hypothèse). Mais il est clair que $X^2 + X + 1$ ne divise pas $X^3 + X + 1$ (ce dernier n'a pas de racine dans $\mathbb{F}_2$), donc ceci contredit le fait que $X^2 + X + 1$ divise $X^{l+1} + X + 1$. Donc finalement le polynôme initial est irréductible dans $\mathbb{Z}[X]$.

**Exercice 13 :** Soit $\mathbb{F}$ un corps fini de cardinal $q = p^r$. Pour tout $Q \in \mathbb{F}[X_1, \dots, X_n]$, on pose $S(Q) := \sum_{x \in \mathbb{F}^n} Q(x) \in \mathbb{F}$.

a) Pour $a_1, \dots, a_n \in \mathbb{N}$, calculer $S(X_1^{a_1} \dots X_n^{a_n})$.

b) Soient $P_1, \dots, P_r$ des polynômes de $\mathbb{F}[X_1, \dots, X_n]$, de degrés $d_1, \dots, d_r$. On note $Z := \{x \in \mathbb{F}^n : P_1(x) = \dots = P_r(x) = 0\}$.
Si $P(x) := \prod_{i=1}^r (1 - P_i(x)^{q-1})$, exprimer $S(P)$ en fonction du cardinal $\#Z$ de $Z$.

c) En déduire que si $d_1 + \dots + d_r < n$, alors $\#Z$ est multiple de $p$ (théorème de Chevalley-Warning).

d) En déduire que si les $P_i$ sont des polynômes homogènes non constants (ou au moins si les $P_i$ sont sans terme constant) et si $d_1 + \dots + d_r < n$, alors le système $P_1(x) = \dots = P_r(x) = 0$ a une solution non nulle dans $\mathbb{F}^n$.
On dit que le corps $\mathbb{F}$ est un corps $C_1$.

e) Montrer l'application suivante (théorème de Erdös-Ginzburg-Ziv) : pour tout $n \geq 1$, pour tout $a_1, \dots, a_{2n-1} \in \mathbb{Z}$, il existe un sous-ensemble $I \subset \{1, \dots, 2n-1\}$ de cardinal exactement $n$ tel que $\sum_{i \in I} a_i \equiv 0 \ [n]$.

*Solution de l'exercice* 13.

a) On remarque d'abord que si l'un des $a_i$ est nul, on a $S(X_1^{a_1} \dots X_n^{a_n}) = 0 \in \mathbb{F}$, puisque $\sum_{x \in \mathbb{F}} 1 = q.1 = 0$. On suppose désormais qu'aucun des $a_i$ n'est nul. On a alors

$$S(X_1^{a_1} \dots X_n^{a_n}) = \sum_{x \in \mathbb{F}^n} x_1^{a_1} \dots x_n^{a_n} = \prod_{i=1}^n \left( \sum_{x \in \mathbb{F}} x^{a_i} \right).$$

On sait que le groupe $\mathbb{F}^*$ est cyclique d'ordre $N = q - 1$. Notons $\zeta \in \mathbb{F}^*$ un générateur Pour chaque $i$, on a

$$\sum_{x \in \mathbb{F}} x^{a_i} = \sum_{x \in \mathbb{F}^*} x^{a_i} = \sum_{k=0}^{N-1} \zeta^{a_i k}.$$

Alors deux cas se présentent : soit $\zeta^{a_i} = 1$, i.e. $q - 1$ divise $a_i$, et alors $\sum_{k=0}^{N-1} \zeta^{a_i k} = N = q - 1 = -1 \in \mathbb{F}$. Soit $\zeta^{a_i} = 1$, i.e. $q - 1$ ne divise pas $a_i$, et alors $\sum_{k=0}^{N-1} \zeta^{a_i k} = \frac{\zeta^{N a_i} - 1}{\zeta^{a_i} - 1} = 0$.
Finalement, on conclut que

$$S(X_1^{a_1} \dots X_n^{a_n}) = (-1)^n \text{ si } q - 1 \text{ divise tous les } a_i,$$

et

$$S(X_1^{a_1} \dots X_n^{a_n}) = 0 \text{ sinon}.$$

b) On remarque d'abord que pour tout $1 \leq i \leq r$ et pour tout $x \in \mathbb{F}^n$, on a $1 - P_i(x)^{q-1} = 1$ si $P_i(x) = 0$ et $1 - P_i(x)^{q-1} = 0$ sinon. Par conséquent, on a :

$$S(P) = \sum_{x \in \mathbb{F}^n} \prod_{i=1}^r (1 - P_i(x)^{q-1}) = \sum_{x \in Z} 1 = \#Z.1 \in \mathbb{F}.$$

c) On suppose $d_1 + \cdots + d_r < n$. Le degré de $P$ est égal à

$$\deg(P) = (d_1 + \cdots + d_r)(q-1) < n(q-1)\,.$$

Par conséquent, si on développe le polynôme $P$, tout monôme $X_1^{a_1} \dots X_n^{a_n}$ apparaissant dans ce développement a un degré $0 \leq a_1 + \cdots + a_n < n(q-1)$, donc soit il existe $1 \leq j \leq n$ tel que $a_j = 0$, soit il existe un indice $1 \leq i \leq n$ tel que $a_i$ ne soit pas multiple de $q-1$. Par conséquent, tout monôme $X_1^{a_1} \dots X_n^{a_n}$ apparaissant dans $P$ vérifie $S(X_1^{a_1} \dots X_n^{a_n}) = 0$ (voir la première question). Donc on en déduit que $S(P) = 0 \in \mathbb{F}$. Or par la question b), on sait que $\#Z.1 = S(P) \in \mathbb{F}$, donc on en déduit que $\#Z.1$ est nul dans $\mathbb{F}$, donc $\#Z$ est divisible par $p$.

d) Sous ces hypothèses, l'élément $(0, \dots, 0) \in \mathbb{F}^n$ est solution du système, donc $Z \neq \emptyset$, donc par la question d), l'ensemble $Z$ est de cardinal au moins $p$, donc il contient un élément distinct de la solution nulle.

e) Pour montrer l'application, on se ramène au cas où $n$ est premier par récurrence. En effet, écrivons $n = m.k$, avec $m, k \geq 2$ et supposons le résultat connu pour $m$ et $k$. Une récurrence simple à partir du résultat pour $k$ assure qu'il existe des sous-ensembles $I_1, \dots, I_{2m-1}$ de $\{1, \dots, (2m)k-1\}$ deux-à-deux disjoints, tels que pour tout $1 \leq j \leq 2m-1$, $\sum_{i \in I_j} a_i \equiv 0\ [k]$. Posons alors pour tout $j$, $b_j := \sum_{i \in I_j} a_j$ et $c_j := \frac{b_j}{k}$. On dispose alors de $2m-1$ entiers $(c_j)$, donc le résultat pour $m$ assure qu'il existe un sous-ensemble $J \subset \{1, \dots, 2m-1\}$ de cardinal $m$ tel que $\sum_{j \in J} c_j \equiv 0\ [m]$. Cette dernière égalité se réécrit, en posant $I := \bigcup_{j \in J} I_j$,

$$\sum_{i \in I} a_i \equiv \sum_{j \in J} \sum_{i \in I_j} a_i \equiv \sum_{j \in J} k c_j \equiv 0\ [n]$$

ce qui permet de montrer le résultat pour l'entier $n$ puisque $\#I = n$.

Il reste donc à montrer le cas où $n = p$ est premier : pour cela, on considère les deux polynômes $P_1(X_1, \dots, X_{2p-1}) := \sum_{i=1}^{2p-1} a_i X_i^{p-1}$ et $P_2(X_1, \dots, X_{2p-1}) := \sum_{i=1}^{2p-1} X_i^{p-1}$. Puisque $\deg(P_1) + \deg(P_2) = 2p-2 < 2p-1$, la question d) assure qu'il existe $x = (x_1, \dots, x_{2p-1}) \in \mathbb{F}_p^{2p-1}$, $x \neq 0$, tel que $P_1(x) = P_2(x) = 0$. Or pour tout $y \in \mathbb{F}_p$, $y^{p-1} = 1$ si $y \neq 0$ et $0^{p-1} = 0$, donc les égalités $P_1(x) = P_2(x) = 0$ se réécrivent dans $\mathbb{F}_p$ de la façon suivante $\sum_{i \in I} a_i = 0$ et $\sum_{i \in I} 1 = 0$, où $I := \{1 \leq i \leq 2p-1 : x_i \neq 0\}$. Autrement dit, on trouve $\#I \equiv 0\ [p]$ et $\sum_{i \in I} a_i \equiv 0\ [p]$, donc $\#I = p$ et $\sum_{i \in I} a_i \equiv 0\ [p]$, ce qui conclut la preuve.

**Exercice 14 :** On appelle "algèbre à division" (ou "corps gauche") tout anneau non nul $A$ (pas forcément commutatif) dans lequel tout élément non nul est inversible.
Dans tout l'exercice, on fixe une algèbre à division finie $A$. On souhaite montrer que $A$ est commutatif, c'est-à-dire que $A$ est un corps (théorème de Wedderburn).

a) Montrer que le centre $Z$ de $A$ est un corps fini de cardinal $q$, et que $A$ est un $Z$-espace vectoriel de dimension $n$.

b) Supposons $n > 1$, i.e. $A$ non commutative. Écrire l'équation aux classes pour l'action de $A^*$ sur lui-même par conjugaison. En déduire que $q^n - 1 = q - 1 + \sum \frac{q^n-1}{q^d-1}$, la somme portant sur un certain nombre de diviseurs stricts de $n$.

c) En déduire que $\phi_n(q)$ divise $q-1$, où $\phi_n$ est le $n$-ième polynôme cyclotomique.

d) En déduire une contradiction.

e) Conclure.

*Solution de l'exercice* 14.

a) Il est clair que $Z \subset A$ est un sous-anneau commutatif (il est stable par somme, par produit, il contient 0 et 1). Montrons que c'est un corps : pour cela, il suffit de montrer que $Z$ est stable par inverse. Soit $z \in Z \setminus \{0\}$. Alors par hypothèse, $z$ admet un inverse $z^{-1} \in A$. Alors pour tout

$a \in A$, on a $za = az$ puisque $z$ est central. En multipliant à gauche et à droite par $z^{-1}$, on en déduit que $az^{-1} = z^{-1}a$, donc $z^{-1} \in Z$. Donc $Z$ est un corps fini, et on note $q = p^r$ son cardinal. Montrons que $A$ est naturellement un $Z$-espace vectoriel. La multiplication extérieure $Z \times A \to A$ est définie par la multiplication dans $A$. On vérifie alors facilement que cette action de $Z$ sur $A$ munit le groupe abélien $A$ d'une structure de $Z$-espace vectoriel. Enfin, $A$ est de dimension finie sur $Z$ puisque $A$ est fini. On note $n$ sa dimension.

b) Le groupe $A^*$ agit sur lui-même par conjugaison : un élément $a \in A^*$ agit sur un élément $x \in A^*$ par la formule $a.x := axa^{-1}$. On vérifie que cela définit bien une action du groupe $A^*$ sur $A^*$. On note $\{x_1, \dots, x_r\}$ un ensemble de représentants des orbites pour cette action.
Alors l'équation aux classes s'écrit :

$$\#A^* = \sum_{i=1}^{r} \frac{\#A^*}{\#\mathrm{Stab}(x_i)}$$

où $\mathrm{Stab}(x_i)$ désigne le sous-groupe de $A^*$ formé des $a \in A^*$ tels que $a.x_i = x_i$.
Or pour tout $i$, $\mathrm{Stab}(x_i) = A^*$ si et seulement si $x_i \in Z \setminus \{0\}$. Par conséquent, l'équation précédente se réécrit ainsi :

$$\#A^* = \#(Z \setminus \{0\}) + \sum_{i : x_i \notin Z} \frac{\#A^*}{\#\mathrm{Stab}(x_i)} .$$

Soit alors $x_i \notin Z$. Calculons $\#\mathrm{Stab}(x_i)$. On sait que $\mathrm{Stab}(x_i)$ est un sous-groupe de $A^*$, donc son cardinal divise $q^n - 1$, et on vérifie que $\mathrm{Stab}(x_i) \cup \{0\}$ est un sous $Z$-espace vectoriel de $A$ : c'est exactement l'ensemble des $a \in A$ tels que $ax_i = x_i a$. Donc il existe un entier $1 \leq d < n$ tel que $\#\mathrm{Stab}(x_i) = q^d - 1$. Enfin, puisque $q^d - 1 | q^n - 1$, on sait que $d$ doit diviser $n$. Finalement, on obtient que

$$q^n - 1 = q - 1 + \sum_{d} \frac{q^n - 1}{q^d - 1}$$

où chaque $d$ apparaissant dans la somme est un diviseur strict de $n$ (a priori, un même diviseur $d$ peut apparaître plusieurs fois).

c) On sait que $\phi_n(X)$ divise $X^n - 1$ dans $\mathbb{Z}[X]$. Si $d < n$ divise $n$, en utilisant les formules $X^n - 1 = \prod_{k|n} \phi_k(X)$ et $X^d - 1 = \prod_{m|d} \phi_m(X)$, on en déduit que $\frac{X^n-1}{X^d-1} = \prod_{k|n, k \nmid d} \phi_k(X)$ dans $\mathbb{Z}[X]$, donc en particulier $\phi_n(X) | \frac{X^n-1}{X^d-1}$. En évaluant en $X = q$, on trouve que $\phi_n(q) | \frac{q^n-1}{q^d-1}$, et la question précédente assure alors que $\phi_n(q) | q - 1$.

d) On a $\phi_n(q) = \prod_{\zeta} (q - \zeta)$, où $\zeta$ décrit les racines primitives $n$-ièmes de l'unité. Or pour toute racine de l'unité $\zeta$ différente de 1, on a clairement $|q - \zeta| > |q - 1|$ (faire un dessin !). En particulier, on a $|\phi_n(q)| > |q - 1|$, ce qui contredit la question précédente.

e) La contradiction ainsi obtenue assure que l'hypothèse de la question b) (à savoir $n > 1$) n'est pas vérifiée. Par conséquent, $n = 1$, donc $A = Z$, donc $A$ est commutative.

**Exercice 15 :** L'objectif de cet exercice est de montrer une partie du résultat suivant.
Soit $(P_i)_{i \in I}$ une famille de polynôme de $\mathbb{Z}[X_1, \dots, X_n]$. Alors les assertions suivantes sont équivalentes :
– les polynômes $(P_i)_{i \in I}$ ont un zéro commun dans $\mathbb{C}^n$.
– il existe un ensemble infini de nombres premiers $p$ tels que les $(P_i)_{i \in I}$ aient un zéro commun dans $\mathbb{F}_p^n$.
– pour tout nombre premier $p$ assez grand, il existe un corps de caractéristique $p$ où les $(P_i)_{i \in I}$ ont un zéro commun.
On va montrer que la deuxième assertion implique la première, et que la troisième implique également la première.
Pour ce faire, on répondra aux questions suivantes :

a) (Nullstellensatz faible) : soient $(Q_j)_{j\in J}$ des polynômes dans $\mathbb{C}[X_1,\dots,X_n]$, sans zéro commun dans $\mathbb{C}^n$.

   i) Montrer que, pour tout $(a_1,\dots,a_n)\in\mathbb{C}^n$, l'idéal $(X_1-a_1,\dots,X_n-a_n)\subset\mathbb{C}[X_1,\dots,X_n]$ est maximal.
   [Indication : on pourra comparer cet idéal avec le noyau du morphisme $\mathbb{C}[X_1,\dots,X_n]\to\mathbb{C}$ défini par $P\mapsto P(a_1,\dots,a_n)$]

   ii) Soit $\mathfrak{m}\subset\mathbb{C}[X_1,\dots,X_n]$ un idéal maximal. Définissons pour $1\le i\le n$, $\phi_i:\mathbb{C}[X_i]\to\mathbb{C}[X_1,\dots,X_n]/\mathfrak{m}=:K$. Montrer que $K=\mathbb{C}$, puis que $\mathrm{Ker}(\phi_i)$ est un idéal premier non nul, donc maximal. En déduire qu'il existe $(a_1,\dots,a_n)\in\mathbb{C}^n$ tels que $\mathfrak{m}=(X_1-a_1,\dots,X_n-a_n)$.

   iii) En déduire que l'idéal engendré par les $(Q_j)_{j\in J}$ est $\mathbb{C}[X_1,\dots,X_n]$ tout entier.

b) Soit $K/k$ une extension de corps. Soient $(a_{i,j})_{0\le i\le n,1\le j\le n}$ des éléments de $k$. Supposons qu'il existe $(x_1,\dots,x_n)\in K^n$ tels que $\sum_{i=1}^n a_{i,j}x_i=a_{0,j}$ pour tout $1\le j\le n$.
   Montrer qu'il existe $(y_1,\dots,y_n)\in k^n$ tels que $\sum_{i=1}^n a_{i,j}y_i=a_{0,j}$ pour tout $1\le j\le n$.

c) Soient $(P_i)_{i\in I}$ une famille de polynôme de $\mathbb{Z}[X_1,\dots,X_n]$ sans zéro commun dans $\mathbb{C}^n$. En utilisant le Nullstellensatz, montrer qu'il existe un ensemble fini $E$ de nombres premiers tel que pour tout $p\notin E$, pour tout corps $F$ de caractéristique $p$, les $(P_i)_{i\in I}$ n'aient pas de zéro commun dans $F$.

d) En déduire la réponse à la question initiale.

*Solution de l'exercice* 15.

a) i) Considérons le morphisme indiqué $\phi:\mathbb{C}[X_1,\dots,X_n]\to\mathbb{C}$ défini par $\phi(P):=P(a_1,\dots,a_n)$. Alors il est clair que $\phi$ est surjectif. Notons $\mathfrak{m}$ son noyau, qui est donc un idéal maximal. Par définition de $\phi$, on a $(X_1-a_1,\dots,X_n-a_n)\subset\mathfrak{m}$. Soit $P\in\mathbb{C}[X_1,\dots,X_n]$. Une récurrence simple sur $n$ assure que le polynôme $P$ s'écrit dans $\mathbb{C}[X_1,\dots,X_n]$

$$P(X_1,\dots,X_n)=(X_1-a_1).P_1(X_1,\dots,X_n)+(X_2-a_2)P_2(X_2,\dots,X_n)+\dots,+(X_n-a_n)P_n(X_n)+\alpha$$

avec $\alpha\in\mathbb{C}$. Supposons que $P\in\mathfrak{m}$. En évaluant cette égalité en $(a_1,\dots,a_n)$, on obtient $\alpha=0$, donc $P\in(X_1-a_1,\dots,X_n-a_n)$. Donc finalement $(X_1-a_1,\dots,X_n-a_n)=\mathfrak{m}$ est un idéal maximal.

ii) Le morphisme composé $\mathbb{C}\to\mathbb{C}[X_1,\dots,X_n]\xrightarrow{\phi}K$ est clairement un morphisme de corps, donc on a une inclusion naturelle $\mathbb{C}\subset K$. Si l'extension $K/\mathbb{C}$ n'était pas algébrique, alors $K$ serait un $\mathbb{C}$-espace vectoriel de dimension infinie non dénombrable. Or $\mathbb{C}[X_1,\dots,X_n]$ est clairement engendré sur $\mathbb{C}$ par un nombre dénombrable de générateurs, donc $K/\mathbb{C}$ est de dimension dénombrable. Donc $K/\mathbb{C}$ est algébrique, or $\mathbb{C}$ est algébriquement clos, donc $K=\mathbb{C}$.
Supposons $\phi_i$ injectif. Alors $\mathbb{C}$ contient $\mathbb{C}(X_i)$, mais ceci est impossible pour des raisons de dimension. Donc $\mathrm{Ker}(\phi_i)\ne 0$. Le morphisme $\phi_i$ n'est pas le morphisme nul puisque $\phi_i(1)\ne 0$ ($1\notin\mathfrak{m}$). Donc on en déduit que $\mathrm{Ker}(\phi_i)$ est un idéal propre de $\mathbb{C}[X_i]$. C'est clairement un idéal premier, donc maximal, de $\mathbb{C}[X_i]$. Par conséquent, $\mathrm{Ker}(\phi_i)$ est l'idéal engendré par un polynôme irréductible unitaire $Q(X_i)\in\mathbb{C}[X_i]$. Un tel $Q$ est nécessairement de la forme $Q(X_i)=X_i-a_i$, pour un $a_i\in\mathbb{C}$. Donc finalement $\mathrm{Ker}(\phi_i)=(X_i-a_i)$, donc $(X_i-a_i)\mathbb{C}[X_1,\dots,X_n]\subset\mathfrak{m}$. Ceci étant vrai pour tout $i$, on en déduit que $(X_1-a_1,\dots,X_n-a_n)\subset\mathfrak{m}$.
Alors la question a) i) assure que $\mathfrak{m}=(X_1-a_1,\dots,X_n-a_n)$.

iii) On raisonne par l'absurde : on suppose que l'idéal $I$ engendré par les $(Q_j)_{j\in J}$ n'est pas $\mathbb{C}[X_1,\dots,X_n]$ tout entier. Alors il existe un idéal maximal $\mathfrak{m}$ de cet anneau contenant $I$. Par la question a) ii) assure qu'il existe $(a_1,\dots,a_n)\in\mathbb{C}^n$ tels que $\mathfrak{m}=(X_1-a_1,\dots,X_n-a_n)$. Alors $I\subset(X_1-a_1,\dots,X_n-a_n)$, donc pour chaque $j\in J$, il existe des polynômes $P_{1,j},\dots,P_{n,j}\in\mathbb{C}[X_1,\dots,X_n]$ tels que $Q_j=(X_1-a_1)P_{1,j}+\dots+(X_n-a_n)P_{n,j}$. En particulier, $Q_j(a_1,\dots,a_n)=0$ pour tout $j\in J$. Donc les polynômes $(Q_j)_{j\in J}$ ont un zéro commun dans $\mathbb{C}^n$, ce qui contredit l'hypothèse. Par conséquent, l'idéal engendré par les $(Q_j)_{j\in J}$ est l'anneau $\mathbb{C}[X_1,\dots,X_n]$ tout entier.

b) On voit l'équation de l'énoncé comme un système linéaire de la forme $AX = B$, où $A$ est une matrice carrée de taille $n$ à coefficients dans $k$, et $B \in k^n$. Alors on sait que si cette équation a des solutions dans une extension, alors elle a des solutions dans $k$ (en utilisant par exemple les formules de Cramer qui expriment les solutions en fonction des coefficients de $A$ et de $B$).

c) Par la question a) iii), on sait que l'idéal engendré par les $(P_i)_{i\in I}$ est $\mathbb{C}[X_1, \dots, X_n]$. Par conséquent, cet idéal contient le polynôme constant égal à 1. Donc il existe un sous-ensemble fini $J \subset I$ et des polynômes $(Q_j)_{j\in J}$ tels que $\sum_{j\in J} Q_j P_j = 1$. On voit cette relation comme un système d'équations linéaires en les coefficients des polynômes $Q_j$. Puisque ce système linéaire a une solution en nombres complexes (en l'occurence les coefficients des polynômes $Q_j$), la question b) assure qu'il admet une solution rationnelle. Par conséquent, on peut supposer que les polynômes $Q_j$ ont leurs coefficients dans $\mathbb{Q}$.

Si on note $N \in \mathbb{N}^*$ le PPCM des dénominateurs des coefficients des $Q_j$, en définissant $R_j := NQ_j \in \mathbb{Z}[X_1, \dots, X_n]$, on a la relation suivante dans $\mathbb{Z}[X_1, \dots, X_n]$ :

$$\sum_{j\in J} R_j P_j = N\,.$$

On définit alors $E$ comme l'ensemble des diviseurs premiers de $N$. Alors $E$ est un ensemble fini de nombres premiers. Soit $p$ un nombre premier et $F$ un corps de caractéristique $p$. Si les polynômes $(P_i)_{i\in I}$ ont un zéro commun $(a_1, \dots, a_n) \in F^n$, alors on a $N = 0$ dans $F$, donc $p$ divise $N$, donc $p \in E$. Par conséquent, on a bien montré que pour tout $p \notin E$, pour tout corps $F$ de caractéristique $p$, les polynômes $(P_i)_{i\in I}$ n'ont pas de zéro commun dans $F^n$.

d) C'est une conséquence directe de la question précédente.