ALGÈBRE GÉNÉRALE

1. Groupes

1.1. Groupes $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.1.1. **I**

Soit $(G,+)$ un groupe abélien fini, $P = \{x \in G \mid \omega(x) \text{ premier}\}$ où $\omega(x)$ désigne l'ordre de x. Si A est un sous-groupe propre de G (i.e. $A \neq \{0\}$, $A \neq G$), on dit que A est dense dans G si, pour tout sous-groupe propre H de G, $A \cap H \neq \{0\}$.
Montrer l'équivalence des trois propriétés :

(*i*) A est dense dans G.
(*ii*) $\forall x \in G \setminus \{0\}$, $\exists m \in \mathbb{N}^* \mid mx \in A$ et $mx \neq 0$.
(*iii*) $P \subset A$.

Trouver les sous-groupes denses de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.1.2. **I**

Soit p un nombre premier, on note $G_p = \{z \in \mathbb{C} \mid \exists k \in \mathbb{N},\ z^{p^k} = 1\}$.

(1) Montrer que G_p est un groupe multiplicatif.
(2) Montrer que les sous-groupes propres H de G_p sont cycliques et qu'aucun d'eux n'est maximal (i.e. si H est un sous-groupe propre de G_p alors il existe K sous-groupe propre de G_p tel que $H \subset K$ et $H \neq K$).
(3) Montrer que G_p n'est pas engendré par une famille finie.

1.2. Groupes.

Exercice 1.2.1. **D C**

Chercher tous les groupes de cardinal 6.

Exercice 1.2.2. **I**

Soit n un entier supérieur ou égal à 2. Un sous-groupe G de $\mathfrak{S}_n$ est dit régulier ssi $\operatorname{Card} G = n$ et l'application $\sigma \mapsto \sigma_i$ de G dans $[\![1,n]\!]$ est une surjection.
Montrer que toute permutation σ de G différente de la permutation identique est un dérangement (i.e. $\sigma_i \neq i$ pour tout i de $[\![1,n]\!]$).

Exercice 1.2.3. **D**

Soit G un groupe commutatif de cardinal 15.

(1) Montrer qu'il existe $a \in G$ d'ordre 3. Montrer qu'il existe un élément d'ordre 5.
(2) En déduire que G est cyclique.

Exercice 1.2.4. **D**
Soit p un nombre premier supérieur ou égal à 3 et G un groupe de cardinal $p+1$. On suppose trouvé un automorphisme α de G d'ordre p.

(1) Soit $x \in G$, on note $E_x = \{\alpha^n(x),\ n \in \mathbb{N}\}$. Montrer qu'il existe un élément x de G tel que $\operatorname{Card} E_x = p$ et que α induit un cycle sur E_x.
(2) En déduire que tout élément de G est de carré égal à e (où e est l'élément neutre de G) puis que G est abélien.

Exercice 1.2.5. **I**
Soit $(G,+)$ un groupe commutatif, x et y 2 éléments de G d'ordres respectifs p et q premiers entre eux.

(1) Montrer que le sous-groupe F de G engendré par $x+y$ contient x et y.
(2) Quel est le cardinal de F ?

---

2. Anneaux et corps

2.1. **Idéaux d'un anneau commutatif.**

Exercice 2.1.1. **F**
Soit A un anneau et $x \in A$, on suppose qu'il existe $p \in \mathbb{N}^*$ tel que $(1-x)^p = 0$.
Prouver que x est inversible. Montrer alors que $(1-x^{-1})^p = 0$.

Exercice 2.1.2. **I** Radical d'un idéal.
Soit A un anneau commutatif, $\mathcal{I}$ un idéal de A, on appelle radical de I (noté $\sqrt{\mathcal{I}}$) l'ensemble des éléments x de A tels qu'il existe $n \in \mathbb{N}$ vérifiant $x^n \in \mathcal{I}$.

(1) Montrer que $\sqrt{\mathcal{I}}$ est un idéal.
(2) Montrer que $\sqrt{\sqrt{\mathcal{I}}} = \sqrt{\mathcal{I}}$.
(3) Montrer aussi les relations

$$\sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}} = \sqrt{\mathcal{I} \cap \mathcal{J}},\ \sqrt{\mathcal{I}+\mathcal{J}} = \sqrt{\sqrt{\mathcal{I}} + \sqrt{\mathcal{J}}}.$$

Exercice 2.1.3. **F**
Soit $(A,+,.)$ un anneau commutatif, on suppose que tout idéal de A est principal (i.e. tout idéal de A est engendré par un élément).
Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante pour l'inclusion d'idéaux de A, montrer que (I_n) est stationnaire.

Exercice 2.1.4. **I**
Soit $A = \mathcal{F}(\mathbb{R},\mathbb{R})$, x_0 et x_1 2 réels distincts.

(1) Montrer que $I = \{f \in A \mid f(x_0) = 0\}$ est un idéal.
(2) Soit J un idéal de A tel que $I \subset J$ et $J \neq I$. Montrer que $J = A$.
(3) Que peut-t-on dire de $J = \{f \in A \mid f(x_0) = f(x_1) = 0\}$?

EXERCICE 2.1.5. **F**
Soit A l'ensemble des rationnels de dénominateur impair.

(1) Montrer que A est un anneau commutatif.
(2) Soit I un idéal de A.
   a) Montrer que si $\frac{m}{n} \in I$ avec m et n impairs alors $I = A$.
   b) On suppose que I ne contient aucun rationnel de la forme $\frac{m}{n}$ avec m et n impairs. Montrer qu'il existe $p \in \mathbb{N}^*$ tel que $I = 2^p A$.

2.2. Idéaux de $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$.

EXERCICE 2.2.1. **F**
Résolution de l'équation $x^2 + y^2 = z^2$ dans $\mathbb{Z}$ (équation diophantienne).

(1) Montrer que l'on peut se ramener au cas où $x \wedge y \wedge z = 1$. On suppose ceci réalisé par la suite.
(2) Montrer que x et y sont de parité différente.
(3) On suppose x pair et y impair. Montrer que
$$\exists (u, v) \in \mathbb{Z}^2 \mid u \wedge v = 1,\ y = u - v,\ z = u + v.$$
(4) Montrer que u et v sont les carrés de 2 entiers premiers entre eux.
Donner alors la forme de toutes les solutions de l'équation considérée.

EXERCICE 2.2.2. **I**
Démontrer que, pour tout n de $\mathbb{N}$:

(1) $4^{2^n} + 2^{2^n} + 1 \equiv 0 \mod 7$.
(2) $2^{2n} + 15n - 1 \equiv 0 \mod 9$.

EXERCICE 2.2.3. **I**
Montrer que, si 9 divise $a^3 + b^3 + c^3$ alors 3 divise a ou b ou c.

EXERCICE 2.2.4. **I**

(1) Soit a un entier impair premier avec 3 et 5. Prouver que
$$(a^2 - 1)(a^4 - 16)[a^2 - (2n + 1)^2]^2 \equiv 0 \mod (23040).$$
(2) Soit a un entier impair premier avec 5. Prouver que
$$(a^2 - 1)(a^4 - 16)(a^2 - 49) \equiv 0 \mod (23040).$$

EXERCICE 2.2.5. **I**
Soit p un nombre premier $p \geqslant 3$ et $k \in \mathbb{N}$.
Montrer que $(1 + p)^{p^k} \equiv 1 + p^{k+1} \mod (p^{k+2})$.

EXERCICE 2.2.6. **I**
Soit p un nombre premier et $q \geqslant p$ un entier.

(1) Montrer que tout diviseur premier de $\dfrac{(q!)^p - 1}{q! - 1}$ est congru à 1 modulo p.
(2) En déduire qu'il existe une infinité de nombre premiers congrus à 1 modulo p.

2.3. **Application à la cryptographie.**

EXERCICE 2.3.1. **F**
Si φ est l'indicatrice d'Euler, montrer que $\varphi(n) = \sum_{k=1}^{n-1} \left[\dfrac{1}{n \wedge k}\right]$ ($[x]$ est la partie entière de x).

EXERCICE 2.3.2. **I**
Montrer que dans toute progression arithmétique : $u_n = an + b$ où $a \wedge b = 1$, il existe une infinité d'éléments premiers avec tout nombre donné c, à toute famille finie $\{c_1, \ldots, c_p\}$.

EXERCICE 2.3.3. **I**
Soient m et n deux entiers naturels distincts, montrer que $F_m = 2^{2^m} + 1$ et $F_n = 2^{2^n} + 1$ sont premiers entre eux.
En déduire que l'ensemble des nombres premiers est infini.

EXERCICE 2.3.4. **I**
Soit φ l'application qui à un entier n de $\mathbb{N}$ écrit en base 10 associe la somme de ses chiffres.
Calculer $\varphi \circ \varphi \circ \varphi(4444^{4444})$.

EXERCICE 2.3.5. **I**
On a vu le petit théorème de Fermat : si p est un nombre premier alors pour tout entier k on a $k^p \equiv k[p]$ (cf. *question (iii) page 176*) et donc, si $k \not\equiv 0[p]$, en simplifiant par k (dans $\mathbb{Z}/p\mathbb{Z}$ qui est un corps), $k^{p-1} \equiv 1[p]$.
On s'intéresse a des réciproques à ce théorème qui seront alors des critères de primalité. Soit p un entier, $p \geqslant 3$, montrer que p est premier si

(1) Test de Lucas (1876)
   a) il existe $k \in \mathbb{N} \setminus \{0, 1\}$ tel que $\begin{cases} (i) & k^{p-1} \equiv 1[p] \\ (ii) & \forall m \in [1, p-2],\ k^m \not\equiv 1[p] \end{cases}$,
   b) si on remplace (ii) par $(ii)]$ $\forall m$ diviseur de $p-1$, $k^m \not\equiv 1[p]$.
(2) Test de Brillart-Selfridge (1967)
   pour tout facteur premier q de $p-1$, il existe k_q tq $\begin{cases} (i) & k^{p-1} \equiv 1[p] \\ (ii) & k^{(p-1)/q} \not\equiv 1[p] \end{cases}$.

EXERCICE 2.3.6. **F**
Résoudre les congruences $\begin{cases} x & \equiv 2 \mod (88) \\ x & \equiv 1 \mod (27) \end{cases}$, $\begin{cases} x & \equiv 3 \mod (4) \\ x & \equiv 4 \mod (5) \\ x & \equiv 1 \mod (3) \end{cases}$.

2.4. **Idéaux de $\mathbb{K}[X]$.**

EXERCICE 2.4.1. **I**
L'anneau $\mathbb{Z}[X]$ est-il principal (i.e. tout idéal de $\mathbb{Z}[X]$ est-il engendré par un seul élément ?)

---

1. INDICATIONS :

Indication 1.1.1 $(i) \Rightarrow (ii)$ prendre $H = (x)$, $(ii) \Rightarrow (iii)$ utiliser Bézout avec $\omega(x)$ premier et $mx \in A$, $m \geqslant 2$, $(iii) \Rightarrow (i)$ $h \in H \setminus \{0\}$, $\omega(h) = pq$ avec p premier montrer que $qh \in A$.
Décomposer n en produit de facteurs premiers : $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, montrer que $P = \{lq_i,\ i \in [1,k],\ l \leqslant p_i - 1\}$ où $q_i = \frac{n}{p_i}$ et en conclure que les sous-groupes denses de $\mathbb{Z}/n\mathbb{Z}$ sont ceux qui contiennent le groupe engendré par P.

Indication 1.1.2 Remarquer que $G_p = \bigcup_{k=0}^{+\infty} \mathbb{U}_{p^k}$.

(1) Vérification immédiate.
(2) Si $z_0 \in G_p \setminus H$ d'ordre p^{k_0} et $z \in G_p$ d'ordre p^k avec $k \geqslant k_0$, prouver par l'absurde que $z \notin H$, en déduire que l'ensemble des ordres des éléments de H est borné. Si k_1 est son plus grand élément, montrer que $H = \mathbb{U}_{p^{k_1}}$.
(3) Raisonner par l'absurde en prenant le maximum des ordres des générateurs.

Indication 1.2.1 En considérant les sous-groupes possibles d'un groupe de cardinal 6, montrer que si G est commutatif alors $G \simeq \mathbb{Z}/6\mathbb{Z}$, si G n'est pas commutatif, alors $G \simeq \mathcal{S}_3$.

Indication 1.2.2 Montrer que l'application $\sigma \mapsto \sigma_1$ de G dans $[\![1,n]\!]$ est bijective.

Indication 1.2.3

(1) Supposer que tous les éléments sont d'ordre 5 et munir G d'une structure d'espace vectoriel sur $\mathbb{Z}/5\mathbb{Z}$, raisonner de la même manière avec 3.
(2) Soit a d'ordre 3 et b d'ordre 5, montrer que ab est d'ordre 15.

Indication 1.2.4

(1) Montrer que E_x est soit un singleton, soit un ensemble de cardinal p et raisonner par l'absurde.
(2) Montrer que tous les éléments de G différents de e vérifient $\operatorname{Card} E_x = p$ puis qu'ils ont tous le même ordre ω, nécessairement premier, que $p + 1 = 1 + n(\omega - 1)$ et finalement $\omega = 2$. Pour la commutativité, remarquer que tout élément est égal à son propre inverse.

Indication 1.2.5

(1) Utiliser Bézout $up + vq = 1$ et chercher un entier k tel que $x = kz = kx + ky$.
(2) Prouver que $t \in F \Leftrightarrow \exists!(\alpha,\beta) \in [\![0,p-1]\!] \times [\![0,q-1]\!] \mid t = \alpha x + \beta y$.

Indication 2.1.1 Développer avec la formule du binôme, x est inversible d'inverse $\sum_{k=1}^{p} \binom{p}{k} (-1)^{k-1} x^{k-1}$. Utiliser ensuite le fait que $(1-x)^p = (-x)^p (1-x^{-1})^p = 0$.

Indication 2.1.2

(1) Calculer $(x+y)^{m+n}$ où m et n sont les entiers associés à x et y.
(2) $\sqrt{\mathcal{I}} \subset \sqrt{\sqrt{\mathcal{I}}}$ et $\sqrt{\sqrt{\mathcal{I}}} \subset \sqrt{\mathcal{I}}$ sont immédiats.
(3) $\sqrt{\mathcal{I} \cap \mathcal{J}} \subset \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$ immédiat, pour $\supset$, prendre x^{p+q} où $x^p \in \mathcal{I}$ et $x^q \in \mathcal{J}$.
Ensuite, la somme de deux idéaux est un idéal d'où $\sqrt{\mathcal{I} + \mathcal{J}} \subset \sqrt{\sqrt{\mathcal{I}} + \sqrt{\mathcal{J}}}$ et pour l'inclusion dans l'autre sens, on utilise le même argument qu'au (1).

Indication 2.1.3 Montrer que $I = \bigcup_{n \in \mathbb{N}} I_n$ est un idéal, $I = zA$ et conclure.

Indication 2.1.4

(1) I idéal : immédiat.
(2) Il existe $f_0 \in J \setminus I$ donc $f_0(x_0) \neq 0$ et prendre $g = f_0^2 + 1_{x_0}^2 \in J$.
(3) Montrer que si K est un idéal tel que $J \subset K \subset I$ alors $K = J$ ou $K = I$.

Indication 2.1.5

(1) On vérifie que A est un sous-anneau de $\mathbb{Q}$.
(2) a) Immédiat.
b) Tous les éléments de I s'écrivent sous la forme $2^q\frac{m}{n}$ et prendre p le plus petit des entiers q.

Indication 2.2.1

(1) Diviser par le P.G.C.D. de (x, y, z).
(2) Raisonner dans $\mathbb{Z}/4\mathbb{Z}$.
(3) Poser $u = \frac{y+z}{2}$, $v = \frac{z-y}{2}$ et montrer que, si $d = u \wedge v$, alors $d|x$.
(4) Poser $x = 2x'$, $x'^2 = uv$ et utiliser la décomposition de x' en produit de facteurs premiers. Toutes les solutions recherchées s'écrivent $y = a^2 - b^2,\ z = a^2 + b^2,\ x = 2ab$.

Indication 2.2.2

(1) Par récurrence, écrire $4^{2(n+1)} \equiv 2^{2^n} \mod 7$, $2^{2^{n+1}} = 4^{2^n}$.
(2) $2^{2(n+1)} + 15(n+1) - 1 = 4(2^{2n} + 15n - 1) - 45n + 18 \equiv 0 \mod 9$.

Indication 2.2.3 Diviser a, b et c par 3 avec le plus petit reste $r \in \{-1, 0, 1\}$.

Indication 2.2.4

(1) $p = (a^2-1)(a^4-16)[a^2-(2n+1)^2]^2$ est divisible par 23040 ssi il est divisible séparément par 2^9, 3^2 et 5.
(2) Prouver que $p \equiv 0 \mod 2^9$: écrire $a = 2q + 1$ car a est impair et $a^2 - (2n + 1)^2 \equiv 0 \mod 2^3$.

Indication 2.2.5 Procéder par récurrence sur k en utilisant le fait que $p|\binom{p}{q}$ pour $1 \leqslant q \leqslant p-1$.

Indication 2.2.6

(1) Se placer dans $\mathbb{Z}/p\mathbb{Z}$ et montrer que tout diviseur premier de $\frac{(q!)^p-1}{q!-1}$ est congru à 1 modulo p.
(2) Prendre $K_1 = \frac{(p!)^p-1}{p!-1}$ et r_1 diviseur premier de K_1, $K_2 = \frac{(r_1)^p-1}{r_1!-1}$, $r_2 > r_1$ diviseur premier de K_2...

Indication 2.3.1 La somme considérée correspond au nombre d'entiers k de l'intervalle $[1, n-1]$ premiers avec n.

Indication 2.3.2 Décomposer $c = c_1c_2$ tel que c_2 ne contienne que des facteurs premiers de b, c_1 étant premier avec b, puis $x = x_1c_1$, x_1 ne contenant aucun facteur premier de b. Montrer alors que $ax + b = ax_1c_1 + b$ est premier avec $c = c_1c_2$.

Indication 2.3.3 Si $m = n + p$ alors $F_m = \left(2^{2^n}\right)^{2^p} + 1 = (F_n - 1)^{2^p} + 1$ et $F_m \equiv 2 \mod F_n$. Poser ensuite p_n le plus petit nombre premier divisant $2^{2^n} + 1$.

Indication 2.3.4 Montrer que $4444^{4444} \leqslant 10^{16211}$ puis que $\varphi(4444^{4444}) \leqslant 150000$ et enfin que $\varphi\circ\varphi(4444^{4444}) \leqslant 37$. Conclure en remarquant que le nombre trouvé doit être congru à 7 modulo 9.

Indication 2.3.5

(1) a) Se placer dans $\mathbb{Z}/p\mathbb{Z}$ et montrer que $H = \{k \in \mathbb{Z} \mid \dot{k}^m = 1\}$ est un sous-groupe $\mathbb{Z}$, $H = a\mathbb{Z}$ et $a = p - 1$. En déduire que $\mathbb{Z}/p\mathbb{Z}$ est un corps.
b) Montrer là aussi que $a = p - 1$.
(2) Il suffit de prouver (par l'absurde) que $\varphi(p) = p - 1$: supposer qu'il existe q premier et $r \geqslant 1$ tels que $q^r|p - 1$ et q^r ne divise pas $\varphi(p)$. Soit k le nombre dépendant de q et ω l'ordre de k dans le groupe des inversibles de $\mathbb{Z}/p\mathbb{Z}$, montrer que $\omega|p - 1$ puis $p - 1|\omega$.

Indication 2.3.6 Premières congruences : l'ensemble des solutions s'écrit $S = -350 + 27\times88\mathbb{Z}$. Deuxièmes congruences : on trouve $x \equiv 10 \mod (60)$.

Indication 2.4.1 Prendre $\mathcal{I}$ l'idéal engendré par $1 + X^2$ et $2X$ et montrer que $\mathcal{I}$ n'est pas principal.

1. Solutions

Solution 1.1.1

$(i) \Rightarrow (ii)$ Soit $H = (x)$ alors $A \cap H \neq \{0\}$ ce qui signifie qu'il existe $m \neq 0$ tel que $mx \in A$.
$(ii) \Rightarrow (iii)$ Si $\omega(x)$ est premier et si $mx \in A$, $m \geqslant 2$ alors $m \wedge \omega(x) = 1$ (car $m \notin \omega(x)\mathbb{Z}$) donc, par Bézout, $u\omega(x) + vm = 1$ i.e. $vmx = x$ et donc $x \in A$.
$(iii) \Rightarrow (i)$ Soit $h \in H \setminus \{0\}$, si $\omega(h) = pq$ avec p premier alors $\omega(qh) = p \Rightarrow qh \in A$.

On décompose n en produit de facteurs premiers : $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.
Si on pose $q_i = \dfrac{n}{p_i}$ alors $P = \{lq_i,\ i \in [1,k],\ l \leqslant p_i - 1\}$.
En effet si on note $Q = \{lq_i,\ i \in [1,k],\ l \leqslant p_i - 1\}$ alors on a évidemment $Q \subset P$ (l'ordre de l'élément lq_i est p_i qui est premier).
Soit $x \in P$ alors il existe un nombre premier p tel que $px = 0$ soit, en passant aux éléments de $\mathbb{Z}$, $px = kn$ avec $k \leqslant p - 1$ et $x \leqslant n - 1$. p est un diviseur premier de n (p ne peut pas diviser k car cela signifierait que x est un multiple de n ce qui est écarté) donc il est égal à un p_i.
Les sous-groupes denses de $\mathbb{Z}/n\mathbb{Z}$ sont ceux qui contiennent le groupe engendré par P. Il contiennent donc les sommes $\sum_{i=1}^{k} k_i q_i$ (qui forment un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, sous-groupe engendré par les q_i).

Solution 1.1.2 On remarque que $G_p = \bigcup_{k=0}^{+\infty} \mathbb{U}_{p^k}$.

(1) On a donc $z \in G_p \Leftrightarrow z = \exp\left(2i\pi \dfrac{h}{p^k}\right)$.
- $1 \in G_p$,
- si z et z' sont dans G_p alors, si $z^{p^k} = 1$ et $z^{p^{k'}} = 1$, on a $(zz')^{p^{k+k'}} = 1$ donc $zz' \in G_p$.
- On a aussi $z^{-1} \in G_p$

donc G_p est un sous-groupe de $\mathbb{U}$.

(2) Soit $z_0 \in G_p \setminus H$ d'ordre p^{k_0} (z_0 est donc racine de l'équation $X^{p^{k_0}} = 1$) et $z \in G_p$ d'ordre p^k avec $k \geqslant k_0$. On va prouver par l'absurde que $z \notin H$.
Si $z \in H$ alors $z' = z^{p^{k-k_0}}$ est d'ordre p^{k_0}. Comme (z'), groupe engendré par z', est de cardinal p^{k_0} et que l'équation $X^{p^{k_0}} = 1$ a exactement p^{k_0} solutions alors $z_0 \in (z')$ ce qui est impossible.
Les éléments d'ordre $\geqslant p^{k_0}$ n'appartiennent donc pas à H donc l'ensemble des ordres des éléments de H est borné. Soit k_1 son plus grand élément. Si $z \in H$ est d'ordre k_1 alors $(z) = \mathbb{U}_{p^{k_1}}$ (par le même raisonnement que ci-dessus). On a alors $\mathbb{U}_{p^{k_1}} \subset H$ et si $z' \in H$ alors l'ordre de z' est inférieur à p^{k_1} donc $z'^{p^{k_1}} = 1$ donc $H \subset \mathbb{U}_{p^{k_1}}$.
Conclusion : tout sous-groupe propre de G_p est de la forme $H = \mathbb{U}_{p^{k_1}}$ ensemble des racines p^{k_1}-ième de l'unité qui est un groupe cyclique.
Aucun de ces sous-groupes n'est maximal car ils sont tous emboîtés.

(3) G_p n'est pas engendré par une famille finie. En effet si $G = \mathrm{gr}\,(z_1, \dots, z_n)$ alors en prenant pour p^k le maximum des ordres des z_i, G ne contiendrait pas les éléments d'ordre $\geqslant p^{k+1}$.

Solution 1.2.1 Soit G un groupe de cardinal 6, si G est commutatif alors il est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ (lui même isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$). Utiliser pour cela le même genre d'argument que pour l'exercice 1.2.3.

Si G n'est pas commutatif, alors il est isomorphe à $\mathcal{S}_3$. Il suffit pour cela de considérer les sous-groupes de ces différents groupes.

Solution 1.2.2 Soit $i \in [\![1, n]\!]$ alors, comme G est régulier et que G et $[\![1, n]\!]$ sont de même cardinal l'application $\sigma \mapsto \sigma_i$ de G dans $[\![1, n]\!]$ est bijective. Il existe donc un seul élément σ de G tel que $\sigma_i = i$, c'est l'identité.
Conclusion : tout élément différent de l'identité est un dérangement.

Solution 1.2.3

(1) Supposons que tous les éléments soient d'ordre 5, G peut alors être muni d'une structure d'espace vectoriel sur $\mathbb{Z}/5\mathbb{Z}$ ($\bar{a}.x = ax$ pour a représentant de $\bar{a}$ dans $\mathbb{Z}/5\mathbb{Z}$). Comme G est fini, G est de dimension finie sur $\mathbb{Z}/5\mathbb{Z}$ et donc, il existe $p \in \mathbb{N}$ tel que $G \simeq (\mathbb{Z}/5\mathbb{Z})^p$. $\operatorname{Card} G = 5^p$ ce qui est impossible.
Conclusion, tous les éléments ne sont pas d'ordre 5.
On raisonne de la même manière avec 3.
Il existe donc un élément a d'ordre 3 et un élément b d'ordre 5.

(2) ab est alors un élément d'ordre 15. Le sous-groupe engendré par ab est de même cardinal que G, il est donc égal à G donc G est cyclique, engendré par ab.

Solution 1.2.4

(1) Si $x \in G$, l'ensemble des n de $\mathbb{Z}$ tels que $\alpha^n(x) = x$ est un sous-groupe de $\mathbb{Z}$ qui contient $p\mathbb{Z}$ puisque α est d'ordre p. Vu que p est un nombre premier ce sous-groupe est soit $p\mathbb{Z}$, soit $\mathbb{Z}$. E_x est donc soit un singleton, soit un ensemble de cardinal p. Si tous les E_x étaient réduits à un singleton, α serait l'identité de G et ne serait pas d'ordre p. Il existe donc un élément x de G tel que E_x possède p éléments : $\{x, \alpha(x), \ldots, \alpha^{p-1}(x)\}$ et aucun de ces éléments n'est égal à e.

(2) Soit $y \in G \setminus \{e\}$, alors il existe $i \in [0, p-1]$ tel que $y = \alpha^i(x)$ car $\operatorname{Card} G = p+1$. E_y ne peut être réduit à un seul élément, donc tous les éléments de G différents de e vérifient $\operatorname{Card} E_x = p$ i.e. il existe $j \in [0, p-1]$ tel que $y = \alpha^j(x)$.
On en déduit que les éléments de $G \setminus \{e\}$ ont tous le même ordre ω.
ω est nécessairement premier car si $\omega = ab$ alors x^a est d'ordre b i.e. $b = 1$ ou $b = \omega$.
On pourra alors trouver des éléments $x_1, \ldots, x_n$ tels que les ensembles $\{x_j^i, i \in [1, \omega-1]\}$ soient disjoints. Donc $p + 1 = 1 + n(\omega - 1)$ i.e. $\omega - 1$ est impair donc ω est un nombre premier pair. On a alors $\omega = 2$.
Enfin, tout élément étant égal à son propre inverse, on aura $xy = x^{-1}y^{-1} = (yx)^{-1} = yx$ c.q.f.d.
Remarque : on peut aussi raisonner par l'absurde. Si $y^{-1} \neq y$ pour tout $y \in E_{x_0}$ alors, comme E_{x_0} contient aussi les inverses, on regroupe ses éléments 2 par 2 donc $\operatorname{Card} E_{x_0} = p$ serait pair ce qui est impossible donc il existe $y \in E_{x_0}$ tel que $y^2 = e$ et $\forall x \in E_{x_0}$, $x = \alpha^q(y)$ donc $x^2 = e$.

Solution 1.2.5

(1) Soit $z = x + y$. Comme p et q sont premiers entre eux alors il existe u et v tels que $up + vq = 1$. On cherche ensuite un entier k tel que $x = kz = kx + ky$ et pour cela il suffit d'avoir $ky = 0$ et $kx = x$. $k = vq = 1 - up$ convient. $x \in F$ et par symétrie, $y \in F$.

(2) On va prouver que $t \in F \Leftrightarrow t = \alpha x + \beta y$ avec $0 \leqslant \alpha \leqslant p-1$ et $0 \leqslant \beta \leqslant q-1$.
$\Rightarrow$ Si $t \in F$ alors $t = lz = lx + ly = \alpha x + \beta y$ en prenant pour α et β les restes respectifs de la division de l par p et par q.
$\Leftarrow$ Si $t = \alpha x + \beta y$, comme $x \in F$ et $y \in F$ on a $t \in F$.
Pour terminer, montrons que cette écriture est unique : si $t = \alpha x + \beta y = \alpha' x + \beta' y$ alors $(\alpha - \alpha')x = (\beta' - \beta)y = a$. a est un élément dont l'ordre divise p et q donc l'ordre de a vaut 1 soit $a = 0$.

Solution 2.1.1 On développe avec la formule du binôme, on trouve alors

$$1 - x\left(\sum_{k=1}^{p} \binom{p}{k} (-1)^{k-1} x^{k-1}\right)$$

ce qui prouve bien que x est inversible d'inverse $\sum_{k=1}^{p} \binom{p}{k}(-1)^{k-1}x^{k-1}$.
On utilise ensuite le fait que $(1-x)^p = (-x)^p(1-x^{-1})^p = 0$ d'où le résultat.

Solution 2.1.2

(1) On montre facilement que si $x \in \sqrt{\mathcal{I}}$ alors $ax \in \sqrt{\mathcal{I}}$ pour tout a de A. Soit $(x, y) \in \sqrt{\mathcal{I}}^2$, n et m les entiers associés alors

$$(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k} = \sum_{k=0}^{n} \underbrace{\binom{n+m}{k} x^k y^{n-k} y^m}_{\in \mathcal{I}} + \sum_{h=1}^{m} \underbrace{\binom{n+m}{n+h} x^n x^h y^{m-h}}_{\in \mathcal{I}}$$

appartient bien à $\mathcal{I}$.

(2) D'une manière générale, on a $\mathcal{I} \subset \sqrt{\mathcal{I}}$ donc $\sqrt{\mathcal{I}} \subset \sqrt{\sqrt{\mathcal{I}}}$.
Montrons l'inclusion dans l'autre sens :
Si $x \in \sqrt{\sqrt{\mathcal{I}}}$ alors il existe n tel que $x^n \in \sqrt{\mathcal{I}}$ puis il existe m tel que $(x^n)^m \in \mathcal{I}$ donc $x^{nm} \in \mathcal{I}$ i.e. $x \in \sqrt{\mathcal{I}}$.
Conclusion : on a bien $\sqrt{\sqrt{\mathcal{I}}} = \sqrt{\mathcal{I}}$.

(3) Si $x \in \sqrt{\mathcal{I} \cap \mathcal{J}}$ alors $\exists p \in \mathbb{N}$ tel que $x^p \in \mathcal{I} \cap \mathcal{J}$ donc $x \in \sqrt{\mathcal{I}}$ et $x \in \sqrt{\mathcal{J}}$ et en conclusion $x \in \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$.
Si $x \in \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$ alors $\exists (p, q) \in \mathbb{N}^2$ tel que $x^p \in \mathcal{I}$ et $x^q \in \mathcal{J}$ donc $x^{p+q} \in \mathcal{I} \cap \mathcal{J}$ et $x \in \sqrt{\mathcal{I} \cap \mathcal{J}}$.
Conclusion : on a bien $\sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}} = \sqrt{\mathcal{I} \cap \mathcal{J}}$.
Ensuite, on remarque que la somme de deux idéaux est bien un idéal. On aura donc

$$\sqrt{\mathcal{I} + \mathcal{J}} \subset \sqrt{\sqrt{\mathcal{I}} + \sqrt{\mathcal{J}}}$$

Il reste là encore à prouver l'inclusion dans l'autre sens.
Soit $x \in \sqrt{\sqrt{\mathcal{I}} + \sqrt{\mathcal{J}}}$ alors il existe n, $y \in \sqrt{\mathcal{I}}$ et $z \in \sqrt{\mathcal{J}}$ tels que $x^n = y + z$ puis, il existe p et q tels que $y^p \in \mathcal{I}$ et $z^q \in \mathcal{J}$. Par le même argument qu'au (1), on en déduit que $x^{n(p+q)} = (y+z)^{p+q} \in \mathcal{I} + \mathcal{J}$. Ce qui prouve l'inclusion dans l'autre sens.

Solution 2.1.3 Soit $I = \bigcup_{n \in \mathbb{N}} I_n$, I est un idéal :
$I \neq \emptyset$, si x et y sont dans I alors $x \in I_{n_1}$ et $y \in I_{n_2}$, on prend $n = \max(n_1, n_2)$ d'où x et y sont dans I_n, il en est de même de $x - y$. On a facilement $ax \in I$ pour $a \in A$ et $x \in I$.

Soit $I = zA$ alors $\exists n \in \mathbb{N}$, $z \in I_n$. On a donc $I \subset I_n$ et par construction $I_n \subset I$ donc $I = I_n$, la suite est bien stationnaire.

Solution 2.1.4

(1) I idéal : immédiat.

(2) Comme $J \neq I$ alors il existe $f_0 \in J \setminus I$ donc $f_0(x_0) \neq 0$. Soit 1_{x_0} la fonction constante égale à 1 sauf en x_0 où elle s'annule. Soit $g = f_0^2 + 1_{x_0}^2 \in J$, g ne s'annule pas sur $\mathbb{R}$. Toute fonction f de A peut s'écrire $f = \dfrac{f}{g} g$ donc $f \in J$.
Conclusion : $J = A$.

(3) On a bien sûr $J \subset I$. Montrons que si K est un idéal tel que $J \subset K \subset I$ alors $K = J$ ou $K = I$.
Si $K \neq J$ alors il existe $f_1 \in K \setminus J$ donc $f_1(x_1) \neq 0$. On définit $1_{x_0,x_1}$ comme étant la fonction constante égale à 1 sauf en x_0 et x_1 où elle s'annule. $g = f_1^2 + 1_{x_0,x_1}^2 \in K$. Toute fonction f de I peut s'écrire $f = \frac{f}{g} g$ sauf en x_0 où elle s'annule. On a ainsi $K = I$.

Solution 2.1.5

(1) On vérifie que A est un sous-anneau de $\mathbb{Q}$.

(2) a) $\dfrac{n}{m} \in A$ vu que m est impair donc $\dfrac{n}{m}\dfrac{m}{n} = 1 \in I$ par conséquent $I = A$.

b) Tous les éléments de I s'écrivent sous la forme $2^q \dfrac{m}{n}$ avec $q \geqslant 1$ et m, n entiers impairs. Soit p le plus petit des entiers q alors il existe un élément de I qui s'écrit $2^p \dfrac{m}{n}$. Comme au a) on a $2^p = 2^p \dfrac{m}{n}\dfrac{n}{m} \in I$ donc $2^p A \subset I$. L'autre inclusion étant évidente, on peut conclure.

Solution 2.2.1

(1) Il suffit de diviser par le P.G.C.D. de (x, y, z).

(2) On raisonne dans $\mathbb{Z}/4\mathbb{Z}$.
- Si x et y sont pairs alors $z^2 \equiv 0 \mod 4$ et z pair est impossible (on a supposé que x, y, z étaient premiers dans leur ensemble).
- Si x et y sont impairs alors $x^2 \equiv 1 \mod 4$ et $y^2 \equiv 1 \mod 4$ donc $z^2 \equiv 2 \mod 4$ ce qui est impossible (les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont 1 et 0).

Conclusion : x et y sont de parité différente.

(3) Posons $u = \dfrac{y+z}{2}$, $v = \dfrac{z-y}{2}$ alors u et v sont des entiers qui vérifient $y = u - v$, $z = u + v$. Soit $d = u \wedge v$, comme $x^2 = 4uv$ alors $d|x$ et comme (x, y, z) sont premiers entre eux alors $d = 1$ i.e. $u \wedge v = 1$.

(4) Si $x = 2x'$ alors $x'^2 = uv$. Si $x' = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ alors $p_1^{2\alpha_1} \dots p_k^{2\alpha_k} = uv$ et si $p_1|u$ alors, comme $u \wedge v = 1$, $p_1^{2\alpha_1}|u$, il existe donc (I, J) un partage de $[1, k]$ tel que $u = \displaystyle\prod_{i\in I} p_i^{2\alpha_i}$ et $v = \displaystyle\prod_{i\in J} p_i^{2\alpha_i}$ i.e. u et v sont les carrés d'entiers premiers entre eux.

Toutes les solutions recherchées s'écriront donc sous la forme

$$y = a^2 - b^2,\ z = a^2 + b^2,\ x = 2ab.$$

Solution 2.2.2

(1) Par récurrence, si $n = 0$, $n = 1$ c'est acquis. Si $4^{2n} + 2^{2^n} + 1 \equiv 0 \mod 7$ alors, comme $16 \equiv 2 \mod 7$, on écrit

$$4^{2(n+1)} = 4^{2.2^n} = (16)^{2^n} \equiv 2^{2^n} \mod 7 \quad \text{et} \quad 2^{2^{n+1}} = 4^{2^n}$$

d'où $4^{2(n+1)} + 2^{2^{n+1}} \equiv 2^{2^n} + 4^{2^n} \equiv 0 \mod 7$ c.q.f.d.

(2) On procède là aussi par récurrence. C'est vrai pour $n = 0$, $n = 1$. Si $2^{2n} + 15n - 1 \equiv 0 \mod 9$ alors

$$2^{2(n+1)} + 15(n+1) - 1 = 4(2^{2n} + 15n - 1) - 45n + 18 \equiv 0 \mod 9.$$

Solution 2.2.3 On divise a, b et c par 3 avec le plus petit reste $r \in \{-1, 0, 1\}$. On a $a^3 \equiv r_a^3 \equiv r_a \mod 9$ donc $a + b + c \equiv r_a + r_b + r_c \mod 9$. Or $r_a + r_b + r_c \in [-3, 3]$ donc $r_a + r_b + r_c = 0$ ce qui n'est possible que si l'un des entiers r_a, r_b, r_c vaut 0 c.q.f.d.

Solution 2.2.4

(1) On remarque que $23040 = 2^9 \times 3^2 \times 5$, alors $p = (a^2 - 1)(a^4 - 16)[a^2 - (2n+1)^2]^2$ est divisible par 23040 ssi il est divisible séparément par 2^9, 3^2 et 5.

Comme a est premier avec 5, on sait que $a^4 \equiv 1 \mod 5$ et donc 5 divise $a^4 - 16$.

Comme a est premier avec 3 alors $a \equiv \pm x \mod 9$ où $x \in \{1, 2, 4\}$, donc $a^2 \equiv y \mod 9$ où $y \in \{1, 4, 7\}$. Si $y \in \{1, 4\}$ alors $(a^2 - 1)(a^4 - 16) = (a^2 - 1)(a^2 - 4)(a^2 + 4) \equiv 0 \mod 9$, de même si $a^2 \equiv 7 \mod 9$.

(2) Il reste à prouver que $p \equiv 0 \mod 2^9$: on peut écrire $a = 2q + 1$ car a est impair donc $a^2 - 1 = 4q(q+1) \equiv 0 \mod 2^3$, de même $a^2 - (2n+1)^2 \equiv 0 \mod 2^3$ c.q.f.d.

Solution 2.2.5 On procède par récurrence sur k et on utilise le fait que $p \mid \binom{p}{q}$ pour $1 \leqslant q \leqslant p-1$.

$k = 1$: $(1+p)^p = 1 + p \times p + \binom{p}{2} p^2 + \cdots + \binom{p}{q} p^q + \cdots + p^p$. Tous les termes de cette somme sont divisibles par p^3 sauf les 2 premiers, on obtient bien le résultat.
On suppose alors la propriété vraie à l'ordre k.

$$\begin{aligned}(1+p)^{p^{k+1}} &= \left((1+p)^{p^k}\right)^p = \left(1 + p^{k+1} + \alpha p^{k+2}\right)^p \\ &= \left(1 + p^{k+1}\right)^p + p\left(1 + p^{k+1}\right)\alpha p^{k+2} + \cdots + \binom{p}{q}\left(1 + p^{k+1}\right)^q \left(\alpha p^{k+2}\right)^{p-q} \\ &= 1 + p^{k+2} + \beta p^{k+3}\end{aligned}$$

en développant le produit $\left(1 + p^{k+1}\right)^p$ et en remarquant que les autres termes sont tous divisibles par p^{k+3}.

Solution 2.2.6

(1) Dans $\mathbb{Z}/p\mathbb{Z}$, $(q)! = 0$ et donc

$$K = \frac{(q!)^p - 1}{q! - 1} = (q!)^{p-1} + \cdots + 1 = 1$$

Si r est un diviseur premier de K alors, dans $\mathbb{Z}/p\mathbb{Z}$ on a $r|1$ soit $r = 1$ et donc r est congru à 1 modulo p.

(2) Soit $K_1 = \dfrac{(p!)^p - 1}{p! - 1}$ alors il existe r_1 nombre premier congru à 1 modulo p. Soit $K_2 = \dfrac{(r_1)^p - 1}{r_1! - 1}$, K_2 n'est pas divisible par aucun nombre $\leqslant r_1$ donc il existe $r_2 > r_1$ nombre premier congru à 1 modulo p.
On peut ainsi construire par récurrence une suite strictement croissante de nombres premiers r_k tous congrus à 1 modulo p donc il existe une infinité de tels nombres.

Solution 2.3.1 Évident, $\left[\dfrac{1}{n \wedge k}\right] = 0$ ssi n et k ne sont pas premiers entre eux, la somme considérée correspond donc au nombre d'entiers k de l'intervalle $[1, n-1]$ premiers avec n.

Solution 2.3.2 On décompose $c = c_1 c_2$ tel que c_2 ne contienne que des facteurs premiers de b, c_1 étant premier avec b. On prend ensuite $x = x_1 c_1$, x_1 ne contenant aucun facteur premier de b. Comme l'ensemble des nombres premiers est infini, il existe une infinité de tels x.
On a alors $ax + b = ax_1c_1 + b$ qui est premier avec $c = c_1c_2$. En effet, si $ax + b$ et c ont un facteur premier commun $p > 1$, ce facteur figure dans c_1 ou c_2 (il divise $c = c_1c_2$).

- Si p divise c_1, il est premier avec b, il divise aussi $ax = ax_1c_1$. Il serait donc premier avec $ax + b$ alors qu'il le divise : contradiction.
- Si p divise c_2, il divise b, il divise alors $ax_1c_1 = ax + b - b$ or il ne figure dans aucun des facteurs de a, x_1 ou c_1. Là encore, on a une contradiction.

Dans cette même suite, on pourra encore trouver une infinité de nombre premiers à chacun des nombres d'un ensemble fini de nombres donnés, il suffit de les prendre premiers à leur P.P.C.M.

Solution 2.3.3 Supposons $m > n$, avec $m = n + p$ on a $F_m = \left(2^{2^n}\right)^{2^p} + 1 = (F_n - 1)^{2^p} + 1$ et donc $F_m \equiv 2 \mod F_n$. On peut donc écrire $F_m = 2 + uF_n$ i.e. le P.G.C.D. de F_m et F_n divise 2 et comme F_m et F_n sont impairs, ce ne peut être que 1.
Soit, pour tout n entier, p_n le plus petit nombre premier divisant $2^{2^n}+1$, vu le résultat précédent, l'application $n \in \mathbb{N} \mapsto p_n \in \mathcal{P}$ est injective ($\mathcal{P}$ désignant l'ensemble des nombres premiers).
Conclusion : l'ensemble des nombres premiers est infini car il contient un ensemble équipotent à $\mathbb{N}$.
Remarque : on aura reconnu les nombres de Fermat...

Solution 2.3.4 On sait que $\varphi(n) \equiv n \mod 9$ par conséquent $\varphi(4444) \equiv 7 \mod 9$. On a donc $4444^{4444} \equiv 7^{4444} \mod 9$. Puis, comme $7^3 \equiv 1 \mod 9$ et que $4444 \equiv 1 \mod 3$ on en déduit dans un premier temps que $4444^{4444} \equiv 7 \mod 9$.
Ensuite $4444^{4444} = 10^{4444 \ln 4444 / \ln 10} \leqslant 10^{16211}$ on en déduit que $\varphi(4444^{4444}) \leqslant 16211 \times 9 \leqslant 150000$ et donc $\varphi \circ \varphi(4444^{4444}) \leqslant 1 + 4 \times 9 = 37$.
Comme le nombre trouvé doit être congru à 7 modulo 9 et que $\varphi \circ \varphi \circ \varphi(4444^{4444}) \leqslant 2 + 9 = 11$ on en déduit que $\varphi \circ \varphi \circ \varphi(4444^{4444}) = 7$.

Solution 2.3.5

(1) a) Si on se place dans $\mathbb{Z}/p\mathbb{Z}$ alors l'ensemble des entiers m tels que $\dot{k}^m = 1$ est un sous-groupe H de $\mathbb{Z}$ ($\dot{k}$ désigne la classe d'équivalence de k dans $\mathbb{Z}/p\mathbb{Z}$). En effet on utilise la *proposition 1.1.4 page 172* en prenant comme groupe l'ensemble des éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$. Or on sait que tout sous-groupe de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ (cf. *proposition 1.1.1 page 171*) et $p - 1$ est un élément de ce groupe donc

$a|p-1$. Ensuite aucun élément de $\mathbb{N}^*$ inférieur à $p-1$ n'appartient à ce groupe donc $a = p-1$.
$\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ est un groupe multiplicatif et $\mathbb{Z}/p\mathbb{Z}$ est un corps ce qui entraîne que p est premier (cf. *théorème 1.7 page 176*).

b) On reprend la démonstration précédente. L'hypothèse que l'on a signifie que tout diviseur strict de $p-1$ n'appartient pas à H donc $a = p-1$. On conclut alors comme dans le premier cas.

(2) Il suffit de prouver que $\varphi(p) = p-1$ et, comme $\varphi(p) \leqslant p-1$, que $p-1|\varphi(p)$. On va raisonner par l'absurde.

On suppose qu'il existe q premier et $r \geqslant 1$ tels que $q^r|p-1$ et q^r ne divise pas $\varphi(p)$. Soit k le nombre dépendant de q et ω l'ordre de k dans le groupe des inversibles de $\mathbb{Z}/p\mathbb{Z}$ (i.e. $\omega = \text{Card}\{k^s[p],\ k \geqslant 1\}$. ω divise $p-1$ (théorème de Lagrange) et ω ne divise pas $\dfrac{p-1}{q}$ donc q^r divise ω. En effet on a $r\omega = p-1 = q^r s$, si $q|r$ alors $\omega|\frac{p-1}{q}$ ce qui est écarté par hypothèse donc $q \wedge r = 1$ et $q^r|\omega$.
Comme $k^{\varphi(p)} \equiv 1[p]$ et que ω divise $\varphi(p)$ alors q^r divise $\varphi(p)$ ce qui mène à une contradiction.

Conclusion : si on écrit $p-1 = \displaystyle\prod_{i=1}^{k} q_i^{r_i}$ alors $q_i^{r_i}|\omega$ donc $p-1|\omega$ soit $p-1 = \omega$.

Remarque : ce test peut servir à voir quels sont les nombres de Fermat qui sont premiers en effet si $F_n = 2^{2^n}+1$ alors le seul nombre premier qui divise $F_n - 1$ est 2.

Solution 2.3.6 Premières congruences : par l'algorithme d'Euclide on obtient $4\times88 - 13\times27 = 1$ d'où une solution particulière $x = -350$. L'ensemble des solutions s'écrit donc $S = -350 + 27\times88\mathbb{Z}$.
Deuxièmes congruences : $x = -1$ vérifie les deux premières congruences, on cherche alors à résoudre $\begin{cases} x \equiv -1 \mod (20) \\ x \equiv 1 \mod (3) \end{cases}$ qui donne $x \equiv 10 \mod (60)$.

Solution 2.4.1 Soit $\mathcal{I}$ l'idéal engendré par $1+X^2$ et $2X$. On a $\mathcal{I} = \{(1+X^2)P + 2XQ,\ (P,Q) \in \mathbb{Z}[X]\}$. Or $2 = 2(1+X^2) - X(2X)$ donc $\mathcal{I}$ contient tous les multiples de 2. Or $1+X^2$ n'est pas multiple de 2 donc, si $\mathcal{I}$ est principal, il doit être engendré par un diviseur de 2 i.e. par 1.
Conclusion partielle : si $\mathcal{I}$ est principal alors $\mathcal{I} = \mathbb{Z}[X]$, en particulier, on a l'existence de P et Q dans $\mathbb{Z}[X]$ tels que

$$(1+X^2)P(X) + 2XQ(X) = 1$$

ce qui, en substituant 1 à X, donne $2P(1) + 2Q(1) = 1$ ce qui est impossible dans $\mathbb{Z}$.
Conclusion : $\mathbb{Z}[X]$ n'est pas principal.
Remarque : on peut aussi prendre $I = X\mathbb{Z}[X] + 2\mathbb{Z}[X] = X\mathbb{Z}[X] + 2\mathbb{Z}$.
