Xavier GOURDON

LES **CONCOURS**
DES PLUS **GRANDES ÉCOLES**

MP*

ALGÈBRE
PROBABILITÉS

Pour les **étoilés**

ellipses

CHAPITRE 1

Arithmétique, Groupes et Anneaux

1. Arithmétique sur les entiers

Soient a, b deux entiers.
— On note $a \mid b$ si a divise b, et $a \nmid b$ si a ne divise pas b.
— Si $n \in \mathbb{N}^*$ divise $a-b$, on dit que a est *congru* à b *modulo* n, on note $a \equiv b \pmod{n}$. La congruence est stable par somme et par produit.

1.1. pgcd, ppcm

Pgcd. Le pgcd de $a, b \in \mathbb{Z}^*$ est l'unique entier $d \in \mathbb{N}^*$ tel que $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$. On le note $\operatorname{pgcd}(a,b)$ ou encore $a \wedge b$. C'est aussi le plus grand diviseur commun à a et à b, et on a la propriété :

$$(d \mid a \text{ et } d \mid b) \quad \Longleftrightarrow \quad d \mid \operatorname{pgcd}(a,b).$$

On dit que a et b sont premiers entre eux si $\operatorname{pgcd}(a,b) = 1$.

Une conséquence de la définition du pgcd donnée plus haut est la suivante :

> Théorème de Bézout. $a, b \in \mathbb{N}^*$ sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au+bv = 1$.

On peut choisir u, v de sorte que $au - bv = 1$ avec $0 \leq u < b$ et $0 \leq v < a$ et u, v se calculent avec l'*algorithme d'Euclide* (voir [Algèbre §1.1.3 Ex.2]).

On déduit le résultat suivant, utilisé dans presque tout exercice d'arithmétique :

> Théorème de Gauss. Si $a, b, c \in \mathbb{N}^*$ et si $a \mid bc$ avec $\operatorname{pgcd}(a,b) = 1$, alors $a \mid c$.

Ppcm. Le ppcm de $a, b \in \mathbb{Z}^*$ est l'unique entier $m \in \mathbb{N}^*$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. On le note $\operatorname{ppcm}(a,b)$ ou encore $a \vee b$. C'est aussi le plus petit multiple commun à a et à b, et on a la propriété :

$$(a \mid m \text{ et } b \mid m) \quad \Longleftrightarrow \quad \operatorname{ppcm}(a,b) \mid m.$$

On a la propriété

$$\operatorname{pgcd}(a,b) \cdot \operatorname{ppcm}(a,b) = |ab|.$$

1.2. Nombres premiers, factorisation

Un entier $p \in \mathbb{N}^*$ est dit premier si $p \geq 2$ et si ses seuls diviseurs sont 1 et p. Le *théorème fondamental de l'arithmétique* affirme que tout entier

$n \geq 2$ s'écrit de manière unique à l'ordre près sous la forme $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (appelée la *décomposition de n en facteurs premiers*) où les p_i sont des nombres premiers distincts et les $\alpha_i \in \mathbb{N}^*$.

– L'entier α_i s'appelle la *valuation* p_i-adique de n, notée $v_{p_i}(n)$. La classique *formule de Legendre*, permet de calculer $v_p(m!)$ (voir l'exercice 3 page 7).

– Si $p \nmid a$ alors a et p sont premiers entre eux.

– Si p premiers divise $a_1 \cdots a_n$, il existe i tel que $p \mid a_i$.

– Il existe une infinité de nombres premiers. On trouve de nombreuses démonstrations de ce résultat (la preuve d'origine d'Euclide fait l'objet de [Algèbre §1.2 Prop.8]), une belle preuve fait l'objet de l'exercice 8 page 24 (dans lequel on prouve aussi que $\sum_{p \text{ premier}} 1/p$ diverge).

– Si p est un nombre premier et $1 \leq k \leq p-1$, alors p divise $\binom{p}{k}$.

Théorème de Fermat, théorème de Wilson. Les deux résultats qui suivent se prouvent naturellement en travaillant dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$

> Théorème de Fermat. Si p est un nombre premier et $a \in \mathbb{Z}$ premier avec p, alors $a^{p-1} \equiv 1 \pmod{p}$. Si $a \in \mathbb{Z}$ on a $a^p \equiv a \pmod{p}$.
>
> Théorème de Wilson. Un entier $p \geq 2$ est un nombre premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.

1.3. Exercices de consolidation

Exercice 1. Soit $n \in \mathbb{N}^*$. Déterminer le pgcd des entiers

$$\binom{2n}{1}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1}$$

Solution. Notons d le pgcd recherché. L'entier d divise la somme

$$\sum_{k=0}^{n-1} \binom{2n}{2k+1} = \frac{\displaystyle\sum_{j=0}^{2n} \binom{2n}{j} - \sum_{j=0}^{2n} (-1)^j \binom{2n}{j}}{2} = \frac{(1+1)^{2n} - (1-1)^{2n}}{2} = 2^{2n-1}$$

donc il existe $\ell \in \mathbb{N}$ tel que $d = 2^\ell$. Par ailleurs d divise chaque terme de la liste, en particulier $d \mid \binom{2n}{1} = 2n$, donc $\ell \leq 1 + v_2(n)$ où $v_2(n)$ est la *valuation dyadique* de n, définie comme l'exposant de la plus grande puissance de 2 qui divise n.

Considérons maintenant l'identité binomiale, valable pour $0 \leq k < n$

$$(2k+1)\binom{2n}{2k+1} = 2n\binom{2n-1}{2k}.$$

Le terme de droite divise $2n$ donc $2^{1+v_2(n)}$ divise $(2k+1)\binom{2n}{2k+1}$, donc divise $\binom{2n}{2k+1}$ car $2^{1+v_2(n)}$ est premier avec $2k+1$. On en déduit que le pgcd recherché est $d = 2^{1+v_2(n)}$.

EXERCICE 2. Soient $a, b \in \mathbb{N}^*$ premiers entre eux. On note

$$A = \{a + nb, n \in \mathbb{N}\}.$$

a) Montrer qu'il existe une infinité d'entiers de A qui ont les mêmes facteurs premiers.
b) Montrer qu'il existe une infinité d'entiers de A premiers entre eux deux à deux.

Solution. **a)** On cherche une suite de la forme rq^m qui prend ses valeurs dans A. Ce sera le cas si $q \equiv 1 \pmod b$ et $r \equiv a \pmod b$. Il suffit de choisir $r = a$ et $q = b + 1$. On a $q > 1$ donc les entiers aq^m pour $m \in \mathbb{N}^*$ sont distincts et forment une famille infinie, ils vérifient tous $aq^m \in A$ et ils répondent à la question car leurs facteurs premiers sont ceux de a et de q.

b) Nous construisons une suite qui ressemble à celle de la preuve d'Euclide de l'infinité des nombres premiers. Soit $(n_k)_{k\in\mathbb{N}}$ la suite à valeurs dans A définie par

$$n_0 = a + b, \qquad \forall k \in \mathbb{N}^*, \quad n_k = a + b\, n_0 n_1 \cdots n_{k-1}.$$

Montrons par récurrence sur $k \in \mathbb{N}$ que $\operatorname{pgcd}(n_k, a) = 1$. C'est vrai pour $k = 0$ car $\operatorname{pgcd}(n_0, a) = \operatorname{pgcd}(n_0 - a, a) = \operatorname{pgcd}(b, a) = 1$. Supposons cette propriété vérifiée jusqu'à $k-1$ et montrons-la pour k. Si p premier divise n_k et a, alors p divise $n_k - a = bn_0 \cdots n_{k-1}$. Comme $p \nmid b$ (car $p \mid a$ et $\operatorname{pgcd}(a, b) = 1$), le théorème de Gauss assure l'existence de $j < k$ tel que $p \mid n_j$. Donc $p \mid a$ et $p \mid n_j$, ce qui est impossible car l'hypothèse de récurrence au rang j fournit $\operatorname{pgcd}(n_j, a) = 1$. On a donc bien $\operatorname{pgcd}(n_k, a) = 1$ pour tout $k \in \mathbb{N}$.

Montrons maintenant que si $j, k \in \mathbb{N}$ avec $j < k$, alors $\operatorname{pgcd}(n_k, n_j) = 1$. Si d divise n_k et n_j, alors d divise $n_k - b\prod_{0\le i<k} n_i = a$. Donc d divise n_k et a, ce qui entraîne $d = 1$ car $\operatorname{pgcd}(n_k, a) = 1$. Les entiers n_k pour $k \in \mathbb{N}$ sont des éléments de A, ils sont bien distincts car (n_k) est strictement croissante, et ils sont premiers entre eux deux à deux, ce qui répond à la question.

EXERCICE 3. Montrer que pour tout $n \in \mathbb{N}^*$, les nombres rationnels

$$\textbf{a)} \quad A_n = \frac{(2n)!}{(n+1)!n!} \qquad \text{et} \qquad \textbf{b)} \quad B_n = \frac{(6n)!n!}{(3n)!((2n)!)^2}$$

sont entiers.

Solution. **a)** C'est classique, A_n est le *nombre de Catalan* d'indice n (voir page 296, ou [Algèbre §6.1.4 Ex.10]). Pour montrer que A_n est entier on peut l'exprimer en fonction des coefficients binomiaux, sous la forme

$$A_n = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \frac{n}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}.$$

On peut aussi utiliser des arguments similaires à ceux de la question suivante.

b) Ici on ne peut pas se ramener à des coefficients binomiaux. Notons $N_n = (6n)!n!$ et $D_n = (3n)!((2n)!)^2$, il s'agit de montrer que D_n divise N_n. Pour tout nombre premier p et tout $m \in \mathbb{N}^*$, on note $v_p(m)$ la *valuation p-adique* de m, définie par l'exposant α le plus élevé tel que $p^\alpha \mid m$. On va montrer que pour tout p premier, $v_p(D_n) \leq v_p(N_n)$, ce qui prouvera le résultat.

Soit p un nombre premier et $m \in \mathbb{N}^*$. Montrons la *formule de Legendre*

$$v_p(m!) = \sum_{\substack{\alpha \geq 1 \\ p^\alpha \leq m}} \left\lfloor \frac{m}{p^\alpha} \right\rfloor \qquad (*)$$

où $\lfloor x \rfloor$ désigne le plus grand entier $\leq x$. Si $q \in \mathbb{N}^*$, les entiers de $\{1, 2, \ldots, m\}$ divisibles par q sont $q, 2q, \ldots, \lfloor m/q \rfloor q$, donc au nombre de $\lfloor m/q \rfloor$. Les entiers k de $\{1, 2, \ldots, m\}$ qui vérifient $v_p(k) = \alpha$, sont ceux divisibles par p^α mais pas par $p^{\alpha+1}$, donc au nombre de $\lfloor m/p^\alpha \rfloor - \lfloor m/p^{\alpha+1} \rfloor$. On en déduit

$$v_p(m!) = \sum_{\substack{\alpha \geq 1 \\ p^\alpha \leq m}} \alpha \left(\left\lfloor \frac{m}{p^\alpha} \right\rfloor - \left\lfloor \frac{m}{p^{\alpha+1}} \right\rfloor \right) = \sum_{\substack{\alpha \geq 1 \\ p^\alpha \leq m}} \alpha \left\lfloor \frac{m}{p^\alpha} \right\rfloor - \sum_{\substack{\alpha \geq 2 \\ p^\alpha \leq m}} (\alpha - 1) \left\lfloor \frac{m}{p^\alpha} \right\rfloor$$

d'où découle la formule de Legendre $(*)$.

En appliquant maintenant (*) on obtient

$$v_p(N_n) = v_p((6n)!) + v_p(n!) = \sum_{\substack{\alpha \geq 1 \\ p^\alpha \leq 6n}} \left(\left\lfloor \frac{6n}{p^\alpha} \right\rfloor + \left\lfloor \frac{n}{p^\alpha} \right\rfloor \right)$$

$$v_p(D_n) = v_p((3n)!) + 2v_p((2n)!) = \sum_{\substack{\alpha \geq 1 \\ p^\alpha \leq 6n}} \left(\left\lfloor \frac{3n}{p^\alpha} \right\rfloor + 2 \left\lfloor \frac{2n}{p^\alpha} \right\rfloor \right),$$

donc

$$v_p(N_n) - v_p(D_n) = \sum_{\substack{\alpha \geq 1 \\ p^\alpha \leq 6n}} f\left(\frac{n}{p^\alpha} \right), \qquad f(x) = \lfloor 6x \rfloor + \lfloor x \rfloor - \lfloor 3x \rfloor - 2\lfloor 2x \rfloor.$$

Pour montrer que $v_p(D_n) \leq v_p(N_n)$ il suffit de montrer que $f(n/p^\alpha) \geq 0$. Montrons que f est positive sur $\mathbb{R}$. On remarque déjà que f est 1-périodique, donc il suffit de vérifier $f(x) \geq 0$ sur $[0, 1[$. Par ailleurs f est constante sur chaque intervalle de la forme $[k/6, (k+1)/6[$ avec $k \in \mathbb{N}$, donc il suffit de montrer que $f(k/n) \geq 0$ pour $0 \leq k \leq 5$ et $k \in \mathbb{N}$. Ceci est bien vérifié car

$$f(0) = 0, \quad f(1/6) = 1, \quad f(2/6) = 1, \quad f(3/6) = 0, \quad f(4/6) = 0, \quad f(5/6) = 1,$$

ce qui prouve que $v_p(D_n) \leq v_p(N_n)$. Ceci étant vrai pour tout nombre premier p, on en déduit que D_n divise N_n, donc que B_n est entier.

2. Groupes

2.1. Définitions

Un ensemble G muni d'une loi de composition (souvent notée multiplicativement) associative est appelé *groupe* s'il a un élément neutre e, et si tout élément $x \in G$ admet un inverse, noté x^{-1}.

— Un groupe est dit *abélien* s'il est commutatif. Dans ce cas on utilise parfois la notation additive.

— Soit $H \subset G$ non vide. Alors

$$H \text{ est un sous-groupe de } G \iff \forall (x,y) \in H^2,\ xy^{-1} \in H.$$

— Le *centre* d'un groupe G est un sous-groupe de G, défini par

$$\mathcal{Z}(G) = \{x \in G \mid \forall y \in G, xy = yx\}.$$

Il est abélien, et c'est un sous-groupe distingué de G (voir plus bas).

— Si $A \subset G$ et $A \neq \varnothing$, le *sous-groupe engendré par* A, noté $\langle A \rangle$, est l'intersection des sous-groupes de G contenant A. On a

$$\langle A \rangle = \{a_1^{\varepsilon_1} \cdots a_p^{\varepsilon_p} \mid p \in \mathbb{N}^*, a_i \in A, \varepsilon_i \in \{-1, 1\}\}.$$

2.2. Groupes finis

Soit G un groupe fini. Son cardinal $|G|$ est appelé *ordre* de G. Le résultat suivant est fréquemment utilisé sur les groupes finis :

> Théorème de Lagrange. Soit H un sous-groupe d'un groupe fini G. Alors l'ordre de H divise celui de G.

La preuve doit être maîtrisée. On définit la relation d'équivalence sur G : $x \mathcal{R} y \iff x^{-1}y \in H$. La classe de $x \in G$ est $\overline{x} = \{y \in G, x^{-1}y \in H\} = xH$, et est appelée *classe à gauche* suivant H (on peut de même définir les *classes à droite*). Pour tout $x \in G$, on a $|xH| = |H|$. Le nombre de classes est noté $[G : H]$ et appelé *indice de H dans G*. Les classes formant une partition de G, on en déduit $|G| = [G : H]|H|$, d'où le résultat.

Ordre d'un élément. L'ordre de $x \in G$ est le plus petit entier $m \in \mathbb{N}^*$ tel que $x^m = e$. Le sous-groupe $\langle x \rangle = \{x^n, n \in \mathbb{N}\}$ engendré par x est d'ordre m, donc m divise $|G|$. On a $\langle x^s \rangle = \langle x \rangle$ si et seulement si $\operatorname{pgcd}(m, s) = 1$. S'il existe $x \in G$ pour lequel $G = \langle x \rangle$ on dit que G est *cyclique*

Exposant d'un groupe fini. Le plus petit entier $r \in \mathbb{N}^*$ tel que $x^r = e$ pour tout $x \in G$, s'appelle *l'exposant* de G. L'ordre de tout élément divise r. Si G est abélien, il existe un élément de G d'ordre r (voir [Algèbre §1.2.5 Ex.10]). Ce résultat entraîne que si p est un nombre premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique : en effet, son exposant r vérifie $x^r = \overline{1}$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$, et comme $X^r - \overline{1}$ a au plus r racines dans $\mathbb{Z}/p\mathbb{Z}[X]$ (car $\mathbb{Z}/p\mathbb{Z}$ est un corps), on a $p - 1 \leq r$, donc forcément $r = p - 1$. On conclut

car $(\mathbb{Z}/p\mathbb{Z})^*$ étant abélien, il existe $y \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $r = p-1$, donc $(\mathbb{Z}/p\mathbb{Z})^* = \langle y \rangle$.

2.3. Sous-groupes distingués

Un sous-groupe H de G est dit *distingué* dans G si pour tout $x \in G$, $xH = Hx$. Dans ce cas, les classes $\overline{x}$ de la relation d'équivalence $x\mathcal{R}y \iff x^{-1}y \in H$, vérifient la propriété que $\overline{xy}$ ne dépend pas des représentants x, y des classes. Muni de la loi $\overline{x} \cdot \overline{y} = \overline{xy}$, l'ensemble quotient $G/\mathcal{R}$ a une structure de groupe, appelé *groupe quotient* et noté G/H. Si G est fini on a $|G| = |G/H| \cdot |H|$.

- Si G est abélien, tous les sous-groupes de G sont distingués dans G.
- Les sous-groupes distingués permettent de montrer des propriétés des groupes finis, en procédant par récurrence via le groupe quotient.
- Un sous-groupe est distingué si et seulement si, pour tout $(g, h) \in G \times H$, $ghg^{-1} \in H$ (ghg^{-1} s'appelle le *conjugué* de h par g).

2.4. Morphismes de groupe

Soient G et G' deux groupes, d'éléments neutres e et e'. Un morphisme de groupes est une application $\varphi : G \to G'$ vérifiant $\varphi(xy) = \varphi(x)\varphi(y)$ pour tout $x, y \in G$. Il en découle $\varphi(e) = e'$ et $\varphi(x^{-1}) = \varphi(x)^{-1}$.

– Le *noyau* de φ est $\operatorname{Ker}\varphi = \varphi^{-1}(\{e'\})$. C'est un sous-groupe de G. Le morphisme φ est injectif si et seulement si $\operatorname{Ker}\varphi = \{e\}$.

– Si φ est bijectif on dit que c'est un *isomorphisme* de groupe.

– Si H' est un sous-groupe distingué dans G', $\varphi^{-1}(H')$ est un sous-groupe distingué dans G.

– En particulier $\operatorname{Ker}\varphi$ est distingué dans G. Le groupe quotient $G/\operatorname{Ker}\varphi$ est isomorphe à $\varphi(G)$. En particulier si G est fini, alors $|G|/|\operatorname{Ker}\varphi| = |\varphi(G)|$.

2.5. Groupe symétrique

Le groupe des permutations de $\{1, \ldots, n\}$, muni de la loi de composition, est appelé *groupe symétrique d'indice* n et noté $\mathcal{S}_n$. On a $|\mathcal{S}_n| = n!$.

– Les *transpositions* sont les permutations qui permutent deux éléments i et j, notées $(i\ j)$. Les transpositions engendrent le groupe symétrique.

– L'*orbite* de $a \in \{1, \ldots, n\}$ suivant $\sigma \in \mathcal{S}_n$ est $\mathcal{O}_\sigma(a) = \{\sigma^k(a), k \in \mathbb{Z}\}$. Si σ n'a qu'une seule orbite $\mathcal{O}_\sigma(a)$ non réduite à un élément, on dit que σ est un *cycle*. Le *support* de σ est $\mathcal{O}_\sigma(a)$, sa *longueur* est $\ell = |\mathcal{O}_\sigma(a)|$. On a aussi $\ell = \min\{k \in \mathbb{N}^*, \sigma^k(a) = a\}$, ordre de σ (en tant qu'élément de $\mathcal{S}_n$), et $\sigma = (a\ \sigma(a)\ \ldots\ \sigma^{\ell-1}(a))$.

– Les transpositions sont des cycles de longueur 2.

– De manière générale, le *support* de $\sigma \in \mathcal{S}_n$ est $\mathrm{Supp}(\sigma) = \{x \mid \sigma(x) \neq x\}$. Deux permutations à supports disjoints commutent.

– Toute permutation est le produit de cycles à supports disjoints.

– La signature d'une permutation σ, notée $\varepsilon(\sigma)$, est un morphisme de groupe de $\mathcal{S}_n$ dans $\{-1, 1\}$. Une transposition τ vérifie $\varepsilon(\tau) = -1$, un cycle γ de longueur ℓ vérifie $\varepsilon(\gamma) = (-1)^{\ell-1}$.

Groupe alterné. L'ensemble des permutations σ vérifiant $\varepsilon(\sigma) = 1$ est un sous-groupe de $\mathcal{S}_n$ noté $\mathcal{A}_n$ et appelé *groupe alterné* d'indice n. On a $|\mathcal{A}_n| = n!/2$. Comme $\mathcal{A}_n = \mathrm{Ker}\,\varepsilon$, c'est un sous-groupe distingué dans $\mathcal{S}_n$. Tout $\sigma \in \mathcal{A}_n$ est le produit d'un nombre pair de transpositions.

– Le groupe $\mathcal{A}_n$ est engendré par les cycles de longueur 3 (faire un parallèle avec la propriété que $\mathcal{S}_n$ est engendré par les cycles de longueur 2). Ce résultat classique permet de montrer des propriétés sur $\mathcal{A}_n$ en se limitant aux cycles de longueur 3. Une preuve fait l'objet de [Algèbre §1.2.5 Ex.7]) que nous reprenons ici ; il suffit de montrer que le produit de deux transpositions est un produit de cycles de longueur 3. C'est vrai car si i, j, k, ℓ sont distincts deux à deux, alors $(i\ j)(k\ \ell) = (i\ j\ k)(j\ k\ \ell)$, si i, j, k sont distincts deux à deux alors $(i\ j)(i\ k) = (i\ k\ j)$ et si $i \neq j$, $(i\ j)(j\ i) = \mathrm{Id}$.

2.6. Exercices de consolidation

Exercice 1. Soit G un groupe fini, A et B deux parties de G telles que $|A| + |B| > |G|$. Montrer que $AB = G$, où $AB = \{ab \mid (a, b) \in A \times B\}$.

Solution. Soit $g \in G$. On veut montrer qu'il existe $(a, b) \in A \times B$ tel que $g = ab$. On considère l'ensemble $gB^{-1} = \{gb^{-1}, b \in B\}$. L'application $B \to gB^{-1} \quad b \mapsto gb^{-1}$ étant bijective, on a $|gB^{-1}| = |B|$. Donc $|gB^{-1}| + |A| > |G|$, donc $(gB^{-1}) \cap A \neq \varnothing$. Soit $a \in (gB^{-1}) \cap A$. On a $a \in A$ et il existe $b \in B$ tel que $a = gb^{-1}$, donc $g = ab$.

Exercice 2. Soit G un ensemble fini non vide, muni d'une loi de composition interne associative, notée multiplicativement. Montrer que G admet un élément idempotent (*i.e.* $\exists x \in G,\ x^2 = x$).

Solution. Fixons $a \in G$. Comme G est fini, les éléments a^n pour $n \in \mathbb{N}$ ne sont pas tous distincts. Donc il existe $m, n \in \mathbb{N}$ avec $m < n$, tels que $a^n = a^m$. Notons $p = n - m \in \mathbb{N}^*$. Partant de l'égalité $a^{m+p} = a^m$, une récurrence immédiate fournit $a^{m+kp} = a^m$ pour tout $k \in \mathbb{N}$. On en déduit, pour tout $\ell \geq m$ et tout $k \in \mathbb{N}$, que $a^{\ell+kp} = a^{\ell-m}a^{m+kp} = a^{\ell-m}a^m = a^\ell$. Cherchons k et ℓ tels que $\ell + kp = 2\ell$, ce qui entrainera que $x = a^\ell$ est idempotent. On choisit $k \in \mathbb{N}^*$ tel que $kp \geq m$ puis $\ell = kp$. Avec ces choix, on voit que $x = a^\ell = a^{\ell+kp} = a^{2\ell}$ est idempotent.

Remarque. *Muni de sa loi, on dit que G est un* magma associatif. *Un groupe est un magma associatif, son élément neutre est idempotent. Un magma associatif n'a pas forcément d'élément neutre, comme par exemple* $(\mathbb{N}^*, +)$, $(n\mathbb{Z}, \times)$ *et* $(2\mathbb{Z}/2^n\mathbb{Z}, \times)$

EXERCICE 3. Soit $n \geq 2$ un entier, et $\sigma \in \mathcal{S}_n$ un cycle de longueur $m \geq 2$. Soit $r \in \mathbb{N}^*$. Montrer que σ^r est un cycle si et seulement si m est premier avec r.

Solution. Par définition d'un cycle de longueur m, il existe $a \in \{1, \dots, n\}$ tel que l'orbite $\mathcal{O}_\sigma(a) = \{\sigma^k(a), k \in \mathbb{Z}\}$ soit le support de σ (*i.e* $\sigma(x) = x$ si $x \notin \mathcal{O}_\sigma(a)$), et tel que $m = \min\{k \in \mathbb{N}^*, \sigma^k(a) = a\}$. On a $|\mathcal{O}_\sigma(a)| = m$ et $\mathcal{O}_\sigma(a) = \{a, \sigma(a), \dots, \sigma^{m-1}(a)\}$. Par commodité, notons $a_k = \sigma^k(a)$.

La solution de l'exercice repose sur le résultat suivant :

> LEMME. Soit $r \in \mathbb{N}^*$. On note $\delta = \text{pgcd}\,(r, m)$ et $m_1 = m/\delta$. Alors σ^r a δ orbites non réduites à un élément, qui sont les $\Gamma_p = \{a_p, a_{p+\delta}, \dots, a_{p+(m_1-1)\delta}\}$ pour $0 \leq p < \delta$.

Prouvons le lemme. Notons $r_1 = r/\delta$. Les Γ_p (pour $0 \leq p < \delta$) sont bien des orbites de σ^r. En effet, soit $p \in \mathbb{N}$, $0 \leq p < \delta$ et $k \in \mathbb{N}$. Soit $r_1 k = m_1 q + s$ la division euclidienne de $r_1 k$ par m_1, avec $0 \leq s < m_1$. On a

$$(\sigma^r)^k(a_p) = \sigma^{\delta r_1 k}(a_p) = \sigma^{\delta m_1 q + \delta s}(a_p) = \sigma^{mq+\delta s}(a_p) = \sigma^{\delta s}(a_p) = a_{p+s\delta} \in \Gamma_p,$$

donc $\mathcal{O}_{\sigma^r}(a_p) \subset \Gamma_p$. Réciproquement soit $x = a_{p+s\delta} \in \Gamma_p$. On a $\text{pgcd}\,(r, m) = \delta$ donc il existe $u, v \in \mathbb{Z}$ vérifiant $ur + vm = \delta$ de sorte que $r(us) + (vs)m = s\delta$ et

$$x = \sigma^{s\delta}(a_p) = \sigma^{r(us)+m(vs)}(a_p) = \sigma^{r(us)}(a_p) = (\sigma^r)^{us}(a_p) \in \mathcal{O}_{\sigma^r}(a_p),$$

donc $\Gamma_p \subset \mathcal{O}_{\sigma^r}(a_p)$.

Les $(\Gamma_p)_{0 \leq p < \delta}$ sont bien distincts deux à deux, car si $0 \leq p < \delta$ on a $a_p \in \Gamma_p$ et $a_p \notin \Gamma_k$ pour $k \neq p$, donc il y a bien δ orbites distinctes.

Montrons maintenant que ce sont les seules orbites non réduites à un élément. Soit $x \in \{1, \dots, n\}$. Si $x \notin \mathcal{O}_\sigma(a)$, alors $\sigma(x) = x$ donc $\sigma^r(x) = x$, donc $\mathcal{O}_{\sigma^r}(x) = \{x\}$. Sinon $x \in \mathcal{O}_\sigma(a)$. Soit $k \in \mathbb{N}$, $0 \leq k < m$, tel que $x = \sigma^k(a)$. Soit $k = \delta q + p$ la division euclidienne de k par δ, avec $0 \leq p < \delta$. On a $x = \sigma^k(a) = a_{p+q\delta} \in \Gamma_p$, donc il n'y a pas d'autres orbites de σ^r non réduites à un élément.

Concluons : le lemme assure que σ^r a une seule orbite non réduite à un élément, si et seulement si $\delta = \text{pgcd}\,(m, r) = 1$. Un cycle étant une permutation qui n'a qu'une seule orbite non réduite à un élément, on en déduit le résultat.

EXERCICE 4 (GROUPE DÉRIVÉ). Soit G un groupe. Si $x, y \in G$ le *commutateur de x et y* est $[x, y] = xyx^{-1}y^{-1}$. On appelle *groupe dérivé* de G et on note $D(G)$ le sous-groupe de G engendré par les commutateurs de G.
a) Montrer que $D(G)$ est un sous-groupe distingué de G et que $G/D(G)$

est abélien.
b) Soit H un sous-groupe de G tel que $D(G) \subset H$. Montrer que H est distingué et G/H abélien.
c) Soit H un sous-groupe distingué de G tel que G/H est abélien. Montrer que $D(G) \subset H$.
d) Quel est le groupe dérivé du groupe symétrique $\mathcal{S}_n$ (pour $n \geq 3$) ?

Solution. **a)** Notons $C = \{[x, y] \mid x, y \in G\}$. Soit $c \in C$, et $x, y \in G$ tels que $c = [x, y]$. Pour tout $g \in G$, on a

$$gcg^{-1} = gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}\, gyg^{-1}\, gx^{-1}g^{-1}\, gy^{-1}g^{-1} = [gxg^{-1}, gyg^{-1}],$$

donc $gcg^{-1} \in C$. Pour tout $x, y \in G$, on a $[x, y]^{-1} = (xyx^{-1}y^{-1})^{-1} = yxy^{-1}x^{-1} = [y, x]$, donc C est stable par l'inverse.

Considérons maintenant $a \in D(G) = \langle C \rangle$. Comme C est stable par l'inverse, on peut écrire $a = c_1 \cdots c_p$ avec $p \in \mathbb{N}^*$ et $c_1, \ldots, c_p \in C$. Pour tout $g \in G$, on a $gag^{-1} = gc_1g^{-1}\, gc_2g^{-1} \cdots gc_pg^{-1} = b_1 \cdots b_p$ avec pour tout i, $b_i = gc_ig^{-1} \in C$. Donc $b_1 \cdots b_p \in \langle C \rangle$ donc $gag^{-1} \in \langle C \rangle = D(G)$.

Enfin, $G/D(G)$ est bien abélien car pour tout $x, y \in G$ on a

$$\begin{aligned}\overline{x} \cdot \overline{y} = \overline{xy} = (xy)D(G) = (yx)(x^{-1}y^{-1}xy)D(G) \\ = (yx)[x^{-1}, y^{-1}]D(G) = (yx)D(G) = \overline{y} \cdot \overline{x}.\end{aligned}$$

b) Soit $h \in H$ et $x \in G$. On a $ghg^{-1} = (ghg^{-1}h^{-1})h = [g, h]\, h \in H$, car $[g, h] \in D(G) \subset H$ et H est stable par produit Donc H est bien distingué dans G. Si $x, y \in H$, la même formule que plus haut donne (ici les classes sont dans G/H)

$$\overline{xy} = (xy)H = yx[x^{-1}, y^{-1}]H = yxH = \overline{yx},$$

donc G/H est bien abélien.

c) Dans le groupe quotient G/H, pour tout $x, y \in G$, la commutativité de H entraîne $\overline{[x, y]} = \overline{x}\,\overline{y}\,\overline{x}^{-1}\,\overline{y}^{-1} = \overline{e}$ où e désigne l'élément neutre de G. Donc $[x, y] \in H$, donc H contient tous les commutateurs, donc $D(G) \subset H$.

d) Soit $\gamma = [\gamma_1, \gamma_2]$ un commutateur de $\gamma_1, \gamma_2 \in \mathcal{S}_n$. La signature de γ est

$$\varepsilon(\gamma) = \varepsilon(\gamma_1\gamma_2\gamma_1^{-1}\gamma_2^{-1}) = \varepsilon(\gamma_1)\varepsilon(\gamma_2)\varepsilon(\gamma_1)^{-1}\varepsilon(\gamma_2)^{-1} = 1$$

donc $D(\mathcal{S}_n) \subset \mathcal{A}_n$. Réciproquement montrons $\mathcal{A}_n \subset \mathcal{D}(\mathcal{S}_n)$. Compte tenu du fait que $\mathcal{A}_n$ est engendré par les cycles de longueur 3 (c'est classique, voir la partie sur les groupes alternés, page 11), il suffit de montrer que tout cycle de longueur 3 est dans $D(\mathcal{S}_n)$. C'est bien le cas car si $i, j, k \in \{1, \ldots, n\}$ sont distincts, alors

$$(i\ j\ k) = (i\ k\ j)^2 = ((i\ j)(i\ k))^2 = (i\ j)(i\ k)(i\ j)(i\ k) = (i\ j)(i\ k)(i\ j)^{-1}(i\ k)^{-1},$$

donc $(i\ j\ k)$ est un commutateur, donc dans $D(\mathcal{S}_n)$.

3. Anneaux

3.1. Définitions

Un anneau est un ensemble A muni de deux lois de composition internes notées "+" et "$\cdot$", telles que $(A,+)$ est un groupe abélien (son élément neutre est souvent noté "0") et la loi "$\cdot$" associative et distributive par rapport à "+". Si la loi "$\cdot$" admet un élément neutre, on dit que A est *unitaire*, son élément neutre est souvent noté "1" ou "e".

L'anneau A est dit commutatif s'il l'est pour la loi "$\cdot$". Les anneaux souvent rencontrés sont $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathcal{M}_n(\mathbb{K})$ ou $\mathbb{K}[X]$.

— L'anneau A est dit *intègre* si $A \neq \{0\}$, s'il est commutatif, et si $ab = 0$ implique $a = 0$ ou $b = 0$.

— Un élément $a \in A$ est dit *nilpotent* s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$. Le plus petit entier n vérifiant $a^n = 0$ s'appelle *l'ordre de nilpotence* de a. Un anneau intègre n'a pas d'élément nilpotents non nuls.

— On dit que $a \in A$ est *inversible* s'il existe $b \in A$ tel que $ab = ba = 1$. Si tout $a \in A$ non nul est inversible, on dit que A est un *corps*.

— Si A est commutatif, et $a, b \in A$ nilpotents, alors ab et $a + b$ sont nilpotents. En effet si $a^p = 0$ et $b^q = 0$, A étant commutatif on a $(ab)^r = a^r b^r$ avec $r = \min\{p, q\}$, et

$$(a+b)^{p+q-1} = \sum_{k=0}^{p+q-1} \binom{p+q-1}{k} a^k b^{p+q-1-k} = 0$$

car si $k \geq p$, $a^k = 0$ et si $k < p$, $p+q-1-k \geq q$ donc $b^{p+q-1-k} = 0$.

— Si A est commutatif, $a \in A$ inversible et $n \in A$ nilpotent, alors $a + n$ est inversible. En effet, soit $p \in \mathbb{N}^*$ tel que $n^p = 0$. Notons $c = -a^{-1}n$. On a

$$(1-c)\sum_{k=0}^{p-1} c^k = \sum_{k=0}^{p-1} c^k - \sum_{k=0}^{p-1} c^{k+1} = 1 - c^p = 1,$$

(dans le cas $A \in \mathcal{M}_n(\mathbb{K})$, on retrouve la formule de l'inverse de $I_n - N$ avec N nilpotent, voir [Algèbre §3.6 Pb 3]) donc $1 - c$ est inversible, donc $a + n = a(1 - c)$ est inversible (d'inverse $a^{-1}(1 - c)^{-1}$).

3.2. Idéal, anneau quotient

Ideal. On dit que $I \subset A$ est un *idéal* de l'anneau A si

$$(I,+) \text{ est un sous-groupe de } (A,+) \quad \text{et} \quad \forall (x,a) \in I \times A, xa \in I \text{ et } ax \in I.$$

Un idéal I d'un anneau commutatif A est dit *principal* s'il existe $x \in A$ tel que $I = xA$, et on note $I = (x)$. Si A est commutatif, unitaire et intègre, il est dit *principal* si tous ses idéaux sont principaux. Les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ sont principaux.

Anneau quotient. Lorsque I est un idéal de A, les classes de la relation d'équivalence $x\mathcal{R}y \iff x-y \in I$ définissent l'*anneau quotient* A/I, muni des lois "+" et "$\cdot$" sur les classes $\overline{x}$ de $A/\mathcal{R}$ par $\overline{x}+\overline{y}=\overline{x+y}$ et $\overline{x}\cdot\overline{y}=\overline{xy}$ (le fait que I soit un idéal assure que ces opérations sont bien définies — le résultat ne dépend pas des représentants x et y choisis).

Les anneaux quotients classiques sont $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{K}[X]/(P)$. Si n est premier, $\mathbb{Z}/n\mathbb{Z}$ est un corps, si P est irréductible, $\mathbb{K}[X]/(P)$ est un corps.

Théorème des restes chinois. Partant d'une factorisation de n, le théorème qui suit fournit une structure importante pour $\mathbb{Z}/n\mathbb{Z}$:

> Théorème des restes chinois. Supposons $n = n_1 \cdots n_r$ où les n_i sont premiers entre eux deux à deux. Pour tout $k \in \mathbb{Z}$, notons $c_i(k)$ sa classe dans $\mathbb{Z}/n_i\mathbb{Z}$. L'application
>
> $$\psi : \ \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \quad \overline{k} \mapsto (c_1(k), \ldots, c_r(k))$$
>
> est un isomorphisme d'anneaux.

Ainsi, pour tout $k_1, \ldots, k_r \in \mathbb{Z}$ il existe $k \in \mathbb{Z}$ (unique modulo n), tel que

$$\forall i \in \{1, \ldots, r\} \qquad k \equiv k_i \pmod{n_i}. \tag{$*$}$$

On peut déterminer k explicitement comme suit. On pose pour tout i, $m_i = \prod_{j \neq i} n_j$. L'entier m_i est premier avec n_i donc il existe $u_i \in \mathbb{Z}$ tel que $u_i m_i \equiv 1 \pmod{n_i}$. Alors $k = \sum_{i=1}^{r} u_i m_i k_i$ est solution de $(*)$.

3.3. Groupe des inversibles

L'ensemble des inversibles d'un anneau unitaire A , pour la loi "$\cdot$", est un groupe appelé *groupe des inversibles* de A, souvent noté A^* (ou $U(A)$).

Groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^*$**.** Soit $n \in \mathbb{N}^*$, $n \geq 2$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers.

– Si $k \in \mathbb{Z}$, $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\operatorname{pgcd}(k, n) = 1$.

– D'après le théorème des restes chinois, $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*$ si et seulement si pour tout i, sa classe $c_i(k)$ est inversible dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. On en déduit que le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donné par l'*indicateur d'Euler*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

L'indicateur d'Euler vérifie $\sum_{d|n} \varphi(d) = n$.

L'ordre du groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^*$ est $\varphi(n)$. On en déduit le résultat suivant, qui généralise le théorème de Fermat

> Théorème d'Euler. Pour tout $x \in \mathbb{Z}$ premier avec n, on a $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Il est classique que si p est premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique (voir une preuve page 9 dans la partie sur l'ordre des élements d'un groupe, ou voir [Algèbre §1.6 Pb.7]). Une condition nécessaire et suffisante sur n pour que $(\mathbb{Z}/n\mathbb{Z})^*$ soit cyclique fait l'objet de l'exercice 14 page 32.

Carrés dans $\mathbb{Z}/p\mathbb{Z}$**.** Soit $p > 2$ un nombre premier, et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. L'étude de $(\mathbb{F}_p^*)^2 = \{x^2, x \in \mathbb{F}_p^*\}$ est classique. Les résultats ci-dessous font l'objet de l'exercice 1 page 16, et des questions 1/a), 1/b) du problème 1 page 41.

— L'ensemble $(\mathbb{F}_p^*)^2$ a $(p-1)/2$ éléments

— Un élément $x \in \mathbb{F}_p^*$ est un carré si et seulement si $x^{(p-1)/2} = \overline{1}$.

— Le *symbole de Legendre*, défini par

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } \dot{a} \neq \dot{0} \text{ et } \dot{a} \in (\mathbb{F}_p^*)^2, \\ -1 & \text{si } \dot{a} \neq \dot{0} \text{ et } \dot{a} \notin (\mathbb{F}_p^*)^2, \\ 0 & \text{si } \dot{a} = \dot{0} \end{cases}$$

vérifie les propriétés suivantes :

$$\forall a \in \mathbb{Z}, p \nmid a, \quad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \qquad (\textit{critère d'Euler})$$

$$\forall a, b \in \mathbb{Z}, \qquad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

— Citons un célèbre résultat appelé *loi de réciprocité quadratique* (voir [Algèbre §1.5 Sujet d'étude 2]), qui affirme que si $p, q > 2$ sont deux nombres premiers distincts, alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

3.4. Exercices de consolidation

Exercice 1. Soient $p > 2$ un nombre premier et $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$. Montrer que pour tout $c \in \mathbb{Z}/p\mathbb{Z}$, il existe $x, y \in \mathbb{Z}/p\mathbb{Z}$ tels que $c = ax^2 + by^2$.

Solution. Notons $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Le résultat suivant est classique :

Lemme. L'ensemble $(\mathbb{F}_p^*)^2 = \{x^2, x \in \mathbb{F}_p^*\}$ a $(p-1)/2$ éléments.

Nous proposons deux preuves de ce lemme.

Méthode 1. L'application $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^* \quad x \mapsto x^2$ est un morphisme de groupe, donc $\operatorname{Im}\varphi = (\mathbb{F}_p^*)^2$ est isomorphe à $\mathbb{F}_p^*/\operatorname{Ker}\varphi$. Or

$$x \in \operatorname{Ker}\varphi \iff x^2 = \overline{1} \iff (x-\overline{1})(x+\overline{1}) = \overline{0} \iff x \in \{-\overline{1}, \overline{1}\}$$

Donc $\operatorname{Ker}\varphi = \{-\overline{1}, \overline{1}\}$ donc $|(\mathbb{F}_p^*)^2| = |\mathbb{F}_p^*|/|\operatorname{Ker}\varphi| = (p-1)/2$.

Méthode 2 Notons $q = (p-1)/2$. On a

$$\mathbb{F}_p^* = \{-\overline{q}, \dots, -\overline{2}, -\overline{1}, \overline{1}, \overline{2}, \dots, \overline{q}\} \quad \text{donc} \quad (\mathbb{F}_p^*)^2 = \{\overline{1}^2, \overline{2}^2, \dots, \overline{q}^2\}$$

car $(-\overline{k})^2 = \overline{k}^2$. Lorsque $1 \leq k < \ell \leq q$ on a $\overline{\ell}^2 - \overline{k}^2 = (\overline{\ell-k})(\overline{\ell+k}) \neq \overline{0}$ car $1 \leq \ell - k \leq q$ et $2 \leq k + \ell \leq 2q = p-1$, donc $\overline{\ell}^2 \neq \overline{k}^2$, on en déduit que $(\mathbb{F}_p^*)^2 = \{\overline{1}^2, \overline{2}^2, \dots, \overline{q}^2\}$ est de cardinal $q = (p-1)/2$.

Fixons maintenant $a, b \in \mathbb{F}_p^*$ et $c \in \mathbb{F}_p$. En comptant $\overline{0}^2$, le lemme entraîne que $(\mathbb{F}_p)^2 = \{x^2, x \in \mathbb{F}_p\}$ est de cardinal $(p+1)/2$. Les applications $f : \ w \mapsto c - aw$ et $g : \ w \mapsto bw$ sont injectives sur $\mathbb{F}_p$ donc les ensembles

$$A = \{c - ax^2, x \in \mathbb{F}_p\} = f((\mathbb{F}_p)^2) \qquad \text{et} \qquad B = \{by^2, y \in \mathbb{F}_p\} = g((\mathbb{F}_p)^2)$$

sont de cardinal $|(\mathbb{F}_p)^2| = (p+1)/2$. Donc

$$|A \cap B| = |A| + |B| - |A \cup B| \geq |A| + |B| - p \geq 2(p+1)/2 - p = 1,$$

donc $A \cap B \neq \varnothing$. Choisissons $z \in A \cap B$. On a $z \in A$ donc il existe $x \in \mathbb{F}_p$ tel que $z = c - ax^2$, et $z \in B$ donc il existe $y \in \mathbb{F}_p$ tel que $z = by^2$. On en déduit $c - ax^2 = by^2$, ou encore $c = ax^2 + by^2$.

Exercice 2. Soit p un nombre premier et $r \geq 2$ un entier. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $(\mathbb{F}_p^*)^r = \{x^r, x \in \mathbb{F}_p^*\}$. Montrer que $(\mathbb{F}_p^*)^r$ est un sous-groupe de $\mathbb{F}_p^*$ vérifiant $|(\mathbb{F}_p^*)^r| = (p-1)/\delta$ où $\delta = \operatorname{pgcd}(p-1, r)$, et montrer que

$$(\mathbb{F}_p^*)^r = \left\{x \in \mathbb{F}_p^*, \ x^{(p-1)/\delta} - 1 = 0\right\}.$$

(on pourra utiliser la propriété de cyclicité de $\mathbb{F}_p^*$, voir la partie sur le groupe des inversibles page 16).

Solution. Cet exercice généralise le cas classique des carrés de $\mathbb{F}_p^*$ (voir page 16). L'application $\varphi : \ \mathbb{F}_p^* \to \mathbb{F}_p^* \ x \mapsto x^r$ est un morphisme de groupe, donc $(\mathbb{F}_p^*)^r = \operatorname{Im}(\varphi)$ est un sous-groupe de $\mathbb{F}_p^*$ et $|(\mathbb{F}_p^*)^r| = |\mathbb{F}_p^*|/|\operatorname{Ker}\varphi|$. On a $\operatorname{Ker}\varphi = \Pi_r$ où pour tout $n \in \mathbb{N}^*$, $\Pi_n = \{x \in \mathbb{F}_p^*, x^n = 1\}$ désigne l'ensemble des racines n-ièmes de l'unité de $\mathbb{F}_p^*$.

Montrons $\Pi_r = \Pi_\delta$. Soit $x \in \Pi_\delta$. On a $\delta \mid r$ donc $x^r = (x^\delta)^{r/\delta} = 1$, donc $x \in \Pi_r$. Réciproquement soit $x \in \Pi_r$ et d son ordre. On a $d \mid r$, et d divise aussi $|\mathbb{F}_p^*| = p-1$ donc d divise δ, donc $x^\delta = (x^d)^{\delta/d} = 1$ et $x \in \Pi_\delta$.

Montrons $|\Pi_\delta| = \delta$. Le groupe $\mathbb{F}_p^*$ est cyclique, donc il existe $y \in \mathbb{F}_p^*$ tel que $\mathbb{F}_p^* = \langle y \rangle$. Soit $n \in \mathbb{N}^*$ tel que $\delta n = p-1$. Les δ éléments y^{kn} pour $0 \leq k < \delta$ sont distincts (car y engendre $\mathbb{F}_p^*$ de cardinal $p-1$), et vérifient tous $(y^{kn})^\delta = y^{k(p-1)} = (y^{p-1})^k = 1$ d'après le théorème de Lagrange. Donc $|\Pi_\delta| \geq \delta$. Par ailleurs, les $(y^{kn})_{0 \leq k < \delta}$ forment un ensemble de δ racines du polynôme $X^\delta - 1$, qui a au plus δ racines dans le corps $\mathbb{F}_p$, donc $X^\delta - 1$ a δ racines dans $\mathbb{F}_p$. On en déduit $|\Pi_\delta| = \delta$, donc

$$|(\mathbb{F}_p^*)^r| = \frac{|\mathbb{F}_p^*|}{|\operatorname{Ker}\varphi|} = \frac{|\mathbb{F}_p^*|}{|\Pi_\delta|} = \frac{p-1}{\delta}.$$

Il reste à montrer que $(\mathbb{F}_p^*)^r = \Pi_{(p-1)/\delta}$. Soit $m \in \mathbb{N}^*$ tel que $r = \delta m$. On a $(\mathbb{F}_p^*)^r \subset \Pi_{(p-1)/\delta}$ car si $y = x^r \in (\mathbb{F}_p^*)^r$, alors $y^{(p-1)/\delta} = x^{r(p-1)/\delta} = x^{m(p-1)} = (x^{p-1})^m = 1$. Or $\Pi_{(p-1)/\delta}$ a au plus $(p-1)/\delta$ éléments car le polynôme $X^{(p-1)/\delta} - 1$ a au plus $(p-1)/\delta$ racines dans le corps $\mathbb{F}_p$. Comme $|(\mathbb{F}_p^*)^r| = (p-1)/\delta$, on en déduit $(\mathbb{F}_p^*)^r = \Pi_{(p-1)/\delta}$.

Remarque. *Notons* $\mathbb{F}_p^r = (\mathbb{F}_p^*)^r \cup \{0\}$*, de cardinal* $(p-1)/\delta + 1$*. En appliquant* $\delta - 1$ *fois le théorème de Cauchy-Davenport (voir l'exercice 16 page 35), à* $\delta\,\mathbb{F}_p^r = \mathbb{F}_p^r + \cdots + \mathbb{F}_p^r$ *(*δ *fois), on en déduit que* $|\delta\,\mathbb{F}_p^r| \geq 1 + \delta(|\mathbb{F}_p^r| - 1) = p$*, donc* $\delta\,\mathbb{F}_p^r = \mathbb{F}_p$ *ce qui entraîne que tout élément de* $\mathbb{F}_p$ *est la somme de* δ *puissances* r*-ièmes de* $\mathbb{F}_p$ *(résultat obtenu par Cauchy en 1813).*

4. Exercices

Exercice 1. Soit G un groupe.
a) S'il n'existe qu'un nombre fini de sous-groupes de G, montrer que G est fini.
b) S'il n'existe qu'un nombre dénombrable de sous-groupes de G, G est il dénombrable ?

Solution. **a)** Pour tout $x \in G$, on note $\langle x \rangle$ le sous-groupe de G engendré par x. Soit $x \in G$. Pour tout $k \in \mathbb{N}^*$, $\langle x^k \rangle$ est un sous-groupe de G. Comme il n'y en a qu'un nombre fini, il existe $k, \ell \in \mathbb{N}^*$ tels que $0 < k < \ell$ et $\langle x^k \rangle = \langle x^\ell \rangle$. On a alors $x^k \in \langle x^\ell \rangle$ dont il existe $q \in \mathbb{Z}$ tel que $x^k = x^{q\ell}$ donc $x^m = e$ (où e est l'élément neutre de G) avec $m = q\ell - k$, et comme $0 < k < \ell$ on a $m \neq 0$, donc x est d'ordre fini. Donc $\langle x \rangle$ est fini.

Or $(\langle x \rangle)_{x \in G}$ est une famille de sous-groupes de G, il n'y en a qu'un nombre fini, donc il existe $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in G$ tels que $\cup_{x \in G} \langle x \rangle = \cup_{k=1}^n \langle x_k \rangle$. Donc $G = \cup_{k=1}^n \langle x_k \rangle$. Comme chaque $\langle x_k \rangle$ est fini, on en déduit que G est fini.

b) On raisonne de la même manière. Comme $(\langle x \rangle)_{x \in G}$ est une famille de sous-groupes de G, il n'y en a qu'un nombre au plus dénombrable qui sont distincts, donc il existe I au plus dénombrable et un ensemble $\{x_i, i \in I\} \subset G$ tel que $G = \cup_{x \in G} \langle x \rangle = \cup_{i \in I} \langle x_i \rangle$. Donc G, réunion au plus dénombrable d'ensembles au plus dénombrables, est au plus dénombrable (notons que pour tout $x \in G$, $\langle x \rangle = \{x^k, k \in \mathbb{Z}\}$ est au plus dénombrable). Comme G n'est pas fini (il existe un nombre dénombrable de sous-groupes de G), on en déduit que G est dénombrable.

Exercice 2. Soit $\sigma : \mathbb{N} \to \mathbb{N}$ une bijection.

1/ On note $A = \{n \in \mathbb{N} \mid \sigma(n) \geq n\}$ et $B = \{n \in \mathbb{N} \mid \sigma(n) < n\}$.
a) Peut-on avoir A infini et B fini ?
b) Peut-on avoir A et B infinis ?
c) Peut-on avoir A fini et B infini ?

2/ On note $C = \{n \in \mathbb{N} \mid \sigma(n) > n\}$ et $D = \{n \in \mathbb{N} \mid \sigma(n) \leq n\}$.
Répondre aux mêmes questions en remplaçant A par C et B par D.

Solution. **1/ a)** Oui, par exemple si $\sigma(n) = n$ sur $\mathbb{N}$, on a $A = \mathbb{N}$ et $B = \varnothing$.

b) Oui, par exemple si $\sigma(2n) = 2n+1$ et $\sigma(2n+1) = 2n$ pour tout $n \in \mathbb{N}$, on a $A = 2\mathbb{N}$ et $B = 1 + 2\mathbb{N}$.

c) Nous allons prouver que c'est impossible. Supposons B infini et A fini. Notons N le plus grand élément de A. Alors pour tout $n > N$, on a $\sigma(n) < n$. Notons $M = 1 + \max\{\sigma(0), \dots, \sigma(N)\}$. Soit $n \leq M$. Si $n \leq N$, alors $\sigma(n) \in \{\sigma(0), \dots, \sigma(N)\}$ donc $\sigma(n) < M$. Sinon $n > N$ donc $\sigma(n) < n \leq M$. On a donc $\sigma(\{0, \dots, M\}) \subset \{0, \dots, M-1\}$ ce qui est impossible car σ est injective.

2/ Nous proposons deux méthodes :

– *Méthode 1.* On se ramène au problème précédent en notant $\pi = \sigma^{-1}$, qui est également une bijection de $\mathbb{N}$ dans $\mathbb{N}$. Soit $n \in \mathbb{N}$ et $m = \sigma(n)$. On a

$$(\sigma(n) > n \iff m > \pi(m)) \qquad \text{et} \qquad (\sigma(n) \leq n \iff m \leq \pi(m)).$$

On en déduit que les ensembles

$$C' = \{m \in \mathbb{N} \mid m > \pi(m)\} \qquad \text{et} \qquad D' = \{m \in \mathbb{N} \mid m \leq \pi(m)\}$$

vérifient $C' = \sigma(C)$ et $D' = \sigma(D)$. Donc C et C' ont même cardinal (éventuellement infini), ainsi que D et D'. On est donc dans le cas 1/ où la bijection σ est remplacée par π, où A est remplacé par D' et B par C'. On en déduit que :

- D'après 1/c), on ne peut pas avoir C' infini et D' fini. Donc on ne peut pas avoir C infini et D fini.
- D'après 1/b), on peut avoir C' et D' infinis, de même pour C et D.
- D'après 1/a), on peut avoir C' fini et D' infini. Donc on peut avoir C fini et D infini.

– *Méthode 2.* On peut aussi procéder directement.
a) On ne peut pas avoir C infini et D fini. En effet, supposons D fini et notons $N = \max D$. Pour tout $n \geq N+1$ on a $n \in C$ donc $\sigma(n) > n \geq N+1$, donc $\sigma(n) \geq N+2$. Donc si $n \leq N+1$, on a $\sigma^{-1}(n) \leq N$ (si $m = \sigma^{-1}(n) \geq N+1$ alors $\sigma(m) \geq N+2$, impossible car $\sigma(m) = n \leq N+1$). On en déduit que $\sigma^{-1}(\{0, 1, \dots, N+1\}) \subset \{0, 1, \dots, N\}$ ce qui est impossible car σ^{-1} est injective.
b) Le même cas particulier 1/b) montre que l'on peut avoir C et D infini.
c) On peut avoir C fini et D infini, par exemple si $\sigma = \mathrm{Id}_{\mathbb{N}}$, on a $C = \varnothing$ et $D = \mathbb{N}$.

EXERCICE 3. Soit $n \geq 2$. Quel est le nombre minimal m de transpositions nécessaires pour engendrer le groupe symétrique $\mathcal{S}_n$?

Solution. On va montrer que le nombre minimal recherché est $m = n-1$.

Il existe bien un ensemble de $n-1$ transpositions de $\mathcal{S}_n$ qui engendre $\mathcal{S}_n$. C'est le cas de $\Gamma = \{(1\ i) \mid 2 \leq i \leq n\}$; pour tout $i, j \in \{1, \dots, n\}$, $i \neq j$, la transposition $(i\ j) = (1\ i)(1\ j)(1\ i)$ est bien générée par des éléments de Γ. Or toute permutation de $\mathcal{S}_n$ est un produit de transpositions, donc Γ génère bien $\mathcal{S}_n$. (d'autres choix sont possibles, par exemple $\Gamma = \{(i\ i+1), 1 \leq i \leq n-1\}$ génère $\mathcal{S}_n$ comme démontré dans [Algèbre §1.2.5 Ex.6]). Donc $m \leq n-1$.

Montrons maintenant $m \geq n-1$. Soit $\Gamma \subset \mathcal{S}_n$ un ensemble de m transpositions qui engendre $\mathcal{S}_n$. Il sera commode d'utiliser les définitions suivantes :

— Le *support* d'une transposition $(i\ j)$ est la partie $\{i, j\}$ de $\{1, \ldots, n\}$.

— On dit que $\sigma \in \mathcal{S}_n$ *laisse stable* une partie A de $\{1, \ldots, n\}$ si $\sigma(A) \subset A$.

Montrons par récurrence sur k $(1 \leq k \leq n-1)$ l'existence de k transpositions distinctes $\tau_1, \ldots, \tau_k \in \Gamma$ et d'une partie $A_k \subset \{1, \ldots, n\}$ de $k+1$ éléments, tels que les supports des τ_i (pour $1 \leq i \leq k$) sont dans A_k.

Le résultat est trivial pour $k = 1$ (choisir $\tau_1 \in \Gamma$ et A_1 le support de τ_1).

Supposons le résultat vrai pour $k < n-1$ et montrons le pour $k+1$. On a $k+1 < n$ donc $B_k = \{1, \ldots, n\} \setminus A_k$ est non vide. Il existe une transposition τ_{k+1} dans $\Gamma \setminus \{\tau_1, \ldots, \tau_k\}$ dont le support intersecte A_k et B_k. En effet, sinon toutes les transpositions de Γ ont un support dans A_k ou dans B_k, donc les transpositions de Γ laissent stables A_k et B_k, donc tout produit de transpositions de Γ laisse stable A_k et B_k, donc Γ ne peut pas engendrer $\mathcal{S}_n$ (toute transposition qui échange un élément de A_k et un élément de B_k ne laisse stable ni A_k ni B_k). Le support de τ_{k+1} a donc la forme $\{i_k, j_k\}$ avec $i_k \in A_k$ et $j_k \in B_k$. En notant $A_{k+1} = A_k \cup \{j_k\}$, $\tau_1, \ldots, \tau_{k+1}$ sont des transpositions distinctes de Γ, dont le support est dans A_{k+1} de cardinal $k+2$. Le résultat est ainsi prouvé au rang $k+1$.

Le cas particulier $k = n-1$ montre que $m \geq n-1$.

EXERCICE 4 (SIMPLICITÉ DE $\mathcal{A}_n$). Soit $n \geq 5$ un entier. **1/a)** Montrer que le groupe alterné $\mathcal{A}_n$ est engendré par les cycles de longueur 3.
b) Montrer que deux cycles $c_1, c_2 \in \mathcal{A}_n$ de longueur 3 sont conjugués dans $\mathcal{A}_n$ (*i.e.* $\exists \sigma \in \mathcal{A}_n$, $c_2 = \sigma c_1 \sigma^{-1}$).

2/ Soit $H \neq \{\mathrm{Id}\}$ un sous-groupe distingué de $\mathcal{A}_n$. On veut montrer que $H = \mathcal{A}_n$ (on dit alors que $\mathcal{A}_n$ est *simple*).
a) Si H contient un cycle de longueur 3, montrer que $H = \mathcal{A}_n$.
b) Soit $\sigma \in H \setminus \{\mathrm{Id}\}$ et $i \in \{1, \ldots, n\}$ tel que $i \neq \sigma(i)$. Montrer qu'il existe un cycle de longueur 3 de la forme $c = (i, k, \sigma(i))$ qui ne commute pas avec σ, et que $\sigma' = \sigma c \sigma^{-1} c^{-1} \in H$. Décomposer σ' en cycles de supports disjoints (après avoir étudié son support) pour en déduire $H = \mathcal{A}_n$.

Solution. **1/a)** C'est classique, voir la section 2.5 page 10

b) Soient $c_1 = (i_1\ i_2\ i_3)$ et $c_2 = (j_1\ j_2\ j_3)$ deux cycles de longueur 3. Il existe une permutation $\sigma \in \mathcal{S}_n$ telle que $\sigma(i_k) = j_k$ pour $k = 1, 2, 3$, on en déduit $c_2 = \sigma c_1 \sigma^{-1}$. Si $\sigma \in \mathcal{A}_n$ c'est terminé. Sinon, l'hypothèse $n \geq 5$ assure l'existence de $k, \ell \in \{1, \ldots, n\}$ tel que $\{k, \ell\} \cap \{j_1, j_2, j_3\} = \varnothing$. Les cycles c_2 et $\tau = (k, \ell)$ ont leurs supports disjoints donc ils commutent. Ceci entraîne

$$c_2 = \tau c_2 \tau^{-1} = \tau(\sigma c_1 \sigma^{-1})\tau^{-1} = \sigma' c_1 {\sigma'}^{-1}. \quad \text{où} \quad \sigma' = \tau\sigma$$

Or $\sigma' \in \mathcal{A}_n$ car $\varepsilon(\sigma') = \varepsilon(\sigma)\varepsilon(\tau) = 1$, donc c_1 et c_2 sont conjugués dans $\mathcal{A}_n$.

2/a) Si H contient un cycle c de longueur 3, alors comme H est distingué dans $\mathcal{A}_n$ il contient tous les conjugués de c dans $\mathcal{A}_n$, donc tous les cycles de longueur 3 d'après la question 1/b), donc $H = \mathcal{A}_n$ d'après 1/a).

b) Si $c = (i, k, \sigma(i))$ avec $k \notin \{i, \sigma(i)\}$ on a $\sigma c \sigma^{-1} = (\sigma(i), \sigma(k), \sigma^2(i))$. Comme c est aussi égal à $(\sigma(i), i, k)$ on sera assuré que $c \neq \sigma c \sigma^{-1}$ si $k \neq \sigma^{-1}(i)$. On choisit donc k dans $\{1, \dots, n\} \setminus \{i, \sigma(i), \sigma^{-1}(i)\}$ (c'est possible car $n \geq 5$), de sorte que $c = (i, k, \sigma(i))$ ne commute pas avec σ.

Notons $\sigma' = \sigma c \sigma^{-1} c^{-1}$. Vu que $c \in \mathcal{A}_n$, que $\sigma^{-1} \in H$ et que H est distingué dans $\mathcal{A}_n$, on a $c\sigma^{-1}c^{-1} \in H$. Donc $\sigma' = \sigma(c\sigma^{-1}c^{-1})$, produit de deux éléments de H, est dans H. Par ailleurs on a

$$\sigma' = (\sigma c \sigma^{-1})c^{-1} = (\sigma(i), \sigma(k), \sigma^2(i))(\sigma(i), k, i),$$

donc le support de σ' (rappelons que c'est l'ensemble des points non fixes de σ') est dans $\{\sigma(i), \sigma(k), \sigma^2(i), k, i\}$, de cardinal ≤ 5. Ainsi dans l'écriture de σ' comme le produit de cycles à supports disjoints, il y a au plus deux cycles. Comme σ ne commute pas avec c, on a $\sigma' \neq \{\mathrm{Id}\}$. Or $\sigma' \in \mathcal{A}_n$, de signature 1, ne peut ni être un cycle de longueur 4, ni le produit d'un cycle de longueur 2 et d'un autre de longueur 3 Il ne reste donc que trois cas :

- σ' est un cycle de longueur 3. Alors d'après 2/a), on a $H = \mathcal{A}_n$.
- σ' est un cycle de longueur 5. On écrit $\sigma' = (i_1\ i_2\ i_3\ i_4\ i_5)$ et on pose $\gamma = (i_1\ i_2\ i_3)$. On a alors

$$\sigma'' = \gamma^{-1}\sigma'\gamma\sigma'^{-1} = (i_3\ i_2\ i_1)\sigma'(i_1\ i_2\ i_3)\sigma'^{-1} = (i_3\ i_2\ i_1)(i_2\ i_3\ i_4) = (i_1\ i_3\ i_4).$$

  Or $\sigma'' = (\gamma^{-1}\sigma'\gamma)\sigma'^{-1}$, produit de deux éléments de H, est dans H. Donc H contient un cycle de longueur 3 donc $H = \mathcal{A}_n$.
- $\sigma' = (i_1\ i_2)(i_3\ i_4)$ où i_1, i_2, i_3, i_4 sont distincts deux à deux. Comme $n \geq 5$, il existe $i_5 \in \{1, \dots, n\} \setminus \{i_1, i_2, i_3, i_4\}$. Soit $\gamma = (i_3\ i_4\ i_5)$. On a

$$\sigma'' = \gamma^{-1}\sigma'\gamma\sigma'^{-1} = (i_5\ i_4\ i_3)\sigma'(i_3\ i_4\ i_5)\sigma'^{-1} = (i_3\ i_4\ i_5).$$

  Comme précédemment, on voit que $\sigma'' = (\gamma^{-1}\sigma'\gamma)\sigma'^{-1}$ est dans H. Donc H contient un cycle de longueur 3 donc $H = \mathcal{A}_n$.

Exercice 5 (Sous-groupes distingués de $\mathcal{S}_n$). Soit $n \geq 5$ un entier.
1/ Soit H un sous-groupe distingué de $\mathcal{S}_n$.
a) Montrer que $H \cap \mathcal{A}_n = \mathcal{A}_n$ ou $H \cap \mathcal{A}_n = \{\mathrm{Id}\}$ (on pourra utiliser le résultat de l'exercice précédent).
b) Montrer que H est égal à $\mathcal{S}_n$, $\mathcal{A}_n$ ou $\{\mathrm{Id}\}$.

2/ Soit H un sous-groupe de $\mathcal{S}_n$ dont l'indice $[\mathcal{S}_n : H] = |\mathcal{S}_n|/|H|$ vérifie $[\mathcal{S}_n : H] \leq n - 1$.
a) On note $E = \mathcal{S}_n/\mathcal{R}$ l'ensemble des classes à gauche pour la relation d'équivalence $x\mathcal{R}y \iff xH = yH$, et $\mathcal{S}(E)$ le groupe des permutations de E. Pour tout $\sigma \in \mathcal{S}_n$, on note $p_\sigma : E \to E \quad \gamma H \mapsto (\sigma\gamma)H$.

Montrer que $\psi : \mathcal{S}_n \to \mathcal{S}(E) \quad \sigma \mapsto p_\sigma$, est un morphisme de groupe.
b) En déduire que $H = \mathcal{S}_n$ ou $H = \mathcal{A}_n$.

Solution. **1/a)** Le sous groupe $H' = H \cap \mathcal{A}_n$ est distingué dans $\mathcal{A}_n$, car $\mathcal{A}_n$ étant distingué dans $\mathcal{S}_n$ on peut écrire

$$\forall \sigma \in \mathcal{S}_n, \qquad \sigma H' = \sigma(H \cap \mathcal{A}_n) = \sigma H \cap \sigma \mathcal{A}_n = H\sigma \cap \mathcal{A}_n \sigma = H'\sigma.$$

Ceci est vrai en particulier si $\sigma \in \mathcal{A}_n$, donc H' est distingué dans $\mathcal{A}_n$. L'exercice précédent assure donc que $H' = \{\mathrm{Id}\}$ ou $H' = \mathcal{A}_n$.

b) Si $H \cap \mathcal{A}_n = \mathcal{A}_n$, alors $\mathcal{A}_n \subset H$, donc $[\mathcal{S}_n : H] = |\mathcal{S}_n|/|H| \leq |\mathcal{S}_n|/|\mathcal{A}_n| = 2$. Or $[\mathcal{S}_n : H]$ est un entier, on en déduit $|\mathcal{S}_n|/|H| \in \{1, 2\}$, donc $|H| = |\mathcal{S}_n|$ ou $|H| = |\mathcal{S}_n|/2$. Si $|H| = |\mathcal{S}_n|$ alors $H = \mathcal{S}_n$, sinon $|H| = |\mathcal{S}_n|/2 = |\mathcal{A}_n|$ et comme $\mathcal{A}_n \subset H$ on en déduit $H = \mathcal{A}_n$.

Supposons maintenant $H \cap \mathcal{A}_n = \{\mathrm{Id}\}$. Supposons $H \neq \{\mathrm{Id}\}$. Soit $\sigma \in H$, $\sigma \neq \mathrm{Id}$. On va montrer $H = \{\mathrm{Id}, \sigma\}$. Soit $\gamma \in H$, $\gamma \neq \mathrm{Id}$. Comme $H \cap \mathcal{A}_n = \{\mathrm{Id}\}$, on a $\sigma, \gamma \notin \mathcal{A}_n$. Donc les signatures de σ et γ vérifient $\varepsilon(\sigma) = \varepsilon(\gamma) = -1$. Donc $\varepsilon(\sigma\gamma) = 1$, donc $\sigma\gamma \in \mathcal{A}_n$. Comme H est un sous-groupe, on a aussi $\sigma\gamma \in H$, donc $\sigma\gamma \in H \cap \mathcal{A}_n = \{\mathrm{Id}\}$, donc $\sigma\gamma = \mathrm{Id}$. On en déduit $\gamma = \sigma^{-1}$. En particulier $\sigma = \sigma^{-1}$ donc $\sigma^2 = \mathrm{Id}$. Donc tout élément de $H \smallsetminus \{\mathrm{Id}\}$ est égal à σ, donc $H = \{\mathrm{Id}, \sigma\}$.

Le groupe H est distingué dans $\mathcal{S}_n$, donc pour tout $\gamma \in \mathcal{S}_n$ on a $\gamma H = H\gamma$ et comme $H = \{\mathrm{Id}, \sigma\}$ ceci entraîne $\gamma\sigma = \sigma\gamma$ pour tout $\gamma \in \mathcal{S}_n$. Il est classique que le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{Id}\}$, donc $\sigma = \mathrm{Id}$. Redémontrons ce résultat. La permutation σ commute avec toutes les transpositions $(i\ j)$ de $\mathcal{S}_n$, ce qui fournit $(i, j) = \sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$ pour tout $i, j \in \{1, \ldots, n\}$ distincts. Or $\sigma \neq \mathrm{Id}$, donc il existe $i \in \{1, \ldots, n\}$ tel que $\sigma(i) \neq i$. On a $n \geq 5$, donc il existe $j \in \{1, \ldots, n\}$, $j \notin \{i, \sigma(i)\}$, et on a donc $(i\ j) = (\sigma(i)\ \sigma(j))$. Vu que $i \neq \sigma(i)$, ceci n'est possible que si $i = \sigma(j)$ et $j = \sigma(i)$, ce qui est absurde. Donc $\sigma = \mathrm{Id}$, ce qui est absurde. Ainsi, si $H \cap \mathcal{A}_n = \{\mathrm{Id}\}$ on a forcément $H = \{\mathrm{Id}\}$.

2/a) Les applications p_σ sont bien définies car si $\gamma H = \gamma' H$, on a $\sigma\gamma H = \sigma\gamma' H$ (car $\gamma' = \gamma h$ avec $h \in H$ donc $\sigma\gamma' H = \sigma\gamma(hH) = \sigma\gamma H$). Par ailleurs p_σ est bijective, donc on a bien $p_\sigma \in \mathcal{S}(E)$. Il est immédiat que $p_{\sigma\sigma'} = p_\sigma p'_\sigma$, donc ψ est un morphisme de groupe.

b) Comme $|\mathcal{S}(E)| = r!$ avec $r = |\mathcal{S}_n|/|H| \leq n - 1$, on a $|\mathcal{S}_n| > |\mathcal{S}(E)|$ donc ψ n'est pas injective. Donc son noyau vérifie $|\operatorname{Ker}\psi| > 1$. Comme $\operatorname{Ker}\psi$ est le noyau d'un morphisme de groupe, c'est un sous-groupe distingué de $\mathcal{S}_n$, et comme $|\operatorname{Ker}\psi| > 1$, d'après 1/b) on a $\operatorname{Ker}\psi = \mathcal{A}_n$ ou $\operatorname{Ker}\psi = \mathcal{S}_n$. Par ailleurs, si $\sigma \in \operatorname{Ker}\psi$ on a $p_\sigma = \mathrm{Id}_{\mathcal{S}(E)}$, donc $\gamma H = \sigma\gamma H$ pour tout $\gamma \in \mathcal{S}_n$, en particulier $H = \sigma H$ donc $\sigma \in H$. Donc $\operatorname{Ker}\psi \subset H$, donc $\mathcal{A}_n \subset H$. On conclut comme plus haut : on en déduit $[\mathcal{S}_n : H] = |\mathcal{S}_n|/|H| \leq |\mathcal{S}_n|/|\mathcal{A}_n| = 2$. Or $[\mathcal{S}_n : H]$ est un entier, donc $|\mathcal{S}_n|/|H| \in \{1, 2\}$, donc $|H| = |\mathcal{S}_n|$ ou $|H| = |\mathcal{S}_n|/2$. Si $|H| = |\mathcal{S}_n|$ alors $H = \mathcal{S}_n$, sinon $|H| = |\mathcal{S}_n|/2 = |\mathcal{A}_n|$ et comme $\mathcal{A}_n \subset H$ on en déduit $H = \mathcal{A}_n$.

Remarque. *Le résultat 2/b) généralise celui de [Algèbre §1.2.5 Ex.8] où on supposait que n est un nombre premier ≥ 5.*

EXERCICE 6. Soit G un groupe fini et A une partie non vide de G. On note $AA^{-1} = \{xy^{-1} \mid (x,y) \in A^2\}$ et $A^{-1}A = \{x^{-1}y \mid (x,y) \in A^2\}$. On suppose que $|AA^{-1}| < 3|A|/2$.
a) Montrer que $H = A^{-1}A$ est un sous-groupe de G.
b) Montrer que $|A^{-1}A| < 2|A|$.
c) Montrer que AA^{-1} est un sous-groupe de G.

Solution. **a)** Notons $n = \lfloor 1 + |A|/2 \rfloor$ le plus petit entier $> |A|/2$. Tout repose sur le lemme suivant :

> LEMME. Soit $a \in A^{-1}A$. Il existe n éléments distincts $y_1, \dots, y_n$ de A et n éléments distincts $z_1, \dots, z_n$ de A tels que $a = y_k^{-1} z_k$ pour tout k.

Prouvons le lemme. Soit $a = \alpha^{-1}\beta \in A^{-1}A$ où $\alpha, \beta \in A$. Les ensembles αA^{-1} et βA^{-1} sont de cardinal $|A|$ (par injectivité des applications $x \mapsto \alpha x^{-1}$ et $x \mapsto \beta x^{-1}$ sur A), donc

$$|(\alpha A^{-1}) \cap (\beta A^{-1})| = 2|A| - |(\alpha A^{-1}) \cup (\beta A^{-1})| \geq 2|A| - |AA^{-1}| > |A|/2.$$

On a $|(\alpha A^{-1}) \cap (\beta A^{-1})| \geq n$ donc il existe n éléments distincts $x_1, \dots, x_n \in (\alpha A^{-1}) \cap (\beta A^{-1})$. Pour tout k, il existe $y_k, z_k \in A$ tels que $x_k = \alpha y_k^{-1} = \beta z_k^{-1}$, donc $a = \alpha^{-1}\beta = y_k^{-1} z_k$ pour tout k. Les x_k étant distincts deux à deux, les y_k (resp. z_k) sont distincts deux à deux, ce qui prouve le lemme.

Prouvons maintenant le résultat demandé. Soient $a, a' \in A^{-1}A$. D'après le lemme, on peut écrire $a = y_k^{-1} z_k$ et $a' = {y'_k}^{-1} z'_k$ avec les y_k, z_k, y'_k, z'_k dans A et où $Z = \{z_1, \dots, z_n\}$ et $Z' = \{z'_1, \dots, z'_n\}$ vérifient $|Z| = |Z'| = n$. On a $|Z \cap Z'| = |Z| + |Z'| - |Z \cup Z'| \geq 2n - |A| > 0$, donc il existe i, j tels que $z_i = z'_j$. On en déduit $aa'^{-1} = y_i^{-1} z_i {z'_j}^{-1} y'_j = y_i^{-1} y'_j \in A^{-1}A$. Comme $A^{-1}A$ est non vide, on en déduit que $A^{-1}A$ est bien un sous-groupe de G.

b) D'après le lemme, l'application $\varphi : A \times A \to H \quad (a,b) \mapsto a^{-1}b$ est telle que $|\varphi^{-1}(\{h\})| \geq n$ pour tout $h \in H$. Or $\cup_{h \in H} \varphi^{-1}(\{h\})$ forme une partition de $A \times A$, on en déduit $|A \times A| \geq n|H|$, donc $|H| \leq |A|^2/n < 2|A|$.

c) Soient $\alpha = ab^{-1}$ et $\beta = cd^{-1}$ deux éléments de AA^{-1} avec $a, b, c, d \in A$. Montrons que $\alpha\beta^{-1} \in AA^{-1}$. Pour cela il faut montrer qu'il existe $x, y \in A$ tels que $ab^{-1}dc^{-1} = xy^{-1}$. Ceci équivaut à l'existence de $x, y \in A$ tels que $b^{-1}dc^{-1}y = a^{-1}x$. Par injectivité de $y \mapsto b^{-1}dc^{-1}y$ et $x \mapsto a^{-1}x$, les ensembles $B = \{b^{-1}dc^{-1}y, y \in A\}$ et $C = \{a^{-1}x, x \in A\}$ vérifient $|B| = |C| = |A|$. Or $B \subset H$ (car H est un sous-groupe de G d'après a)) et $C \subset H$ donc

$$|B \cap C| = |B| + |C| - |B \cup C| \geq |B| + |C| - |H| = 2|A| - |H|$$

donc $|B \cap C| > 0$ d'après la question précédente. On en déduit l'existence de $z \in B \cap C$. En écrivant $z = b^{-1}dc^{-1}y$ et $z = a^{-1}x$ avec $x, y \in A$ on en déduit $b^{-1}dc^{-1}y = a^{-1}x$ d'où le résultat demandé.

EXERCICE 7 (THÉORÈME DE LUCAS). Soient $n, k \in \mathbb{N}$, et p un nombre premier. On écrit le développement de n et k en base p, sous la forme

$$n = \sum_{j=0}^{r} n_j p^j \quad (0 \leq n_j < p) \quad \text{et} \quad k = \sum_{j=0}^{r} k_j p^j \quad (0 \leq k_j < p).$$

Montrer que $\binom{n}{k} \equiv \prod_{j=0}^{r} \binom{n_j}{k_j} \pmod{p}$.

Solution. La clé de la solution est la formule polynomiale

$$(1+X)^p \equiv 1 + X^p \pmod{p}$$

conséquence du fait que p divise $\binom{p}{k}$ lorsque $0 < k < p$. Une récurrence immédiate sur j fournit ensuite

$$\forall j \in \mathbb{N}, \qquad (1+X)^{p^j} \equiv 1 + X^{p^j} \pmod{p}.$$

On en déduit

$$\sum_{k=0}^{n} \binom{n}{k} X^k = (1+X)^n = \prod_{j=0}^{r} \left((1+X)^{p^j}\right)^{n_j} \equiv \prod_{j=0}^{r} \left(1 + X^{p^j}\right)^{n_j} \pmod{p}.$$

Or $\left(1 + X^{p^j}\right)^{n_j} = \sum_{k_j=0}^{p-1} \binom{n_j}{k_j} X^{k_j p^j}$ (car $\binom{n_j}{k_j} = 0$ si $k_j > n_j$), donc

$$\begin{aligned} \sum_{k=0}^{n} \binom{n}{k} X^k &\equiv \prod_{j=0}^{r} \left(\sum_{k_j=0}^{p-1} \binom{n_j}{k_j} X^{k_j p^j} \right) \\ &\equiv \sum_{\substack{0 \leq k_0 < p \\ \cdots \\ 0 \leq k_r < p}} \left(\prod_{j=0}^{r} \binom{n_j}{k_j} \right) X^{k_0 + k_1 p + \cdots + k_r p^r} \pmod{p}. \end{aligned}$$

On en déduit le résultat en faisant l'égalité des coefficients de X^k dans les premiers et derniers termes de ces égalités modulo p.

Remarque. *Une autre preuve consiste à montrer* $\binom{n}{k} \equiv \binom{\lfloor n/p \rfloor}{\lfloor k/p \rfloor} \binom{n \mod p}{k \mod p} \pmod{p}$, *puis à procéder par récurrence sur* r.

EXERCICE 8 (INFINITÉ DE L'ENSEMBLE DES NOMBRES PREMIERS, PAR ERDÖS). Cet exercice propose une jolie preuve, attribuée à Paul Erdös (mathématicien particulièrement prolixe du XX$^{\text{e}}$ siècle), de l'infinité de l'ensemble des nombres premiers, et de la divergence de $\sum_{p \text{ premier}} 1/p$.

a) Montrer que tout entier $n \in \mathbb{N}^*$ s'écrit $n = a_n b_n^2$ où $a_n, b_n \in \mathbb{N}^*$ avec a_n sans facteur carré. En supposant qu'il n'y ait qu'un nombre fini de

nombres premiers, étudier les valeurs possibles de a_n puis de $n = a_n b_n^2$ pour les entiers $n \leq N$, et en déduire une contradiction si N est grand.

b) On veut montrer que la série $\sum_{i=1}^{+\infty} 1/p_i$ diverge, où p_i désigne le i-ème nombre premier. On raisonne par l'absurde en supposant que $\sum 1/p_i$ converge. Soit k tel que $\sum_{i \geq k+1} 1/p_i < 1/2$. Majorer pour tout N, le nombre N_0 d'entiers $\leq N$ dont les facteurs premiers sont tous dans $\{p_1, \ldots, p_k\}$ et le nombre N_1 d'entiers $\leq N$ ayant au moins un facteur premier dans $\{p_i, i > k\}$, et en déduire une contradiction.

Solution. **a)** Soit $n = \prod_{i=1}^r p_i^{\alpha_i}$ la factorisation de n en produit de facteurs premiers distincts $p_1, \ldots, p_r$. On écrit $\alpha_i = 2\beta_i + \varepsilon_i$ où $\varepsilon_i \in \{0, 1\}$ et $\beta_i \in \mathbb{N}$. En notant $a_n = \prod_{i=1}^r p_i^{\varepsilon_i}$ et $b_n = \prod_{i=1}^r p_i^{\beta_i}$, on a bien $n = a_n b_n^2$ où a_n est sans facteur carré.

Supposons qu'il n'y ait qu'un nombre fini k de nombres premiers $p_1, p_2, \ldots, p_k$. Soit $N \in \mathbb{N}^*$. Tout entier $n \leq N$ s'écrit sous la forme $n = a_n b_n^2$ où a_n est sans facteur carré. La factorisation de a_n en produit de facteurs premiers est de la forme $a_n = \prod_{i=1}^k p_i^{\varepsilon_i}$ où $\varepsilon_i \in \{0, 1\}$ pour tout i, donc ne peut prendre que 2^k valeurs différentes. Par ailleurs, $b_n^2 \leq N$ donc $b_n \leq \sqrt{N}$. On en déduit qu'il n'y a au plus $2^k\sqrt{N}$ valeurs possibles d'entiers $n \leq N$, ce qui implique $N \leq 2^k\sqrt{N}$ donc $\sqrt{N} \leq 2^k$. Ceci est absurde dès qu'on choisit $N > 2^{2k}$.

b) En procédant comme dans a), on obtient $N_0 \leq 2^k\sqrt{N}$. Pour tout $i > k$, les entiers $\leq N$ qui ont p_i comme facteur sont $p_i, 2p_i, \ldots, \lfloor N/p_i \rfloor p_i$ donc il y en a $\lfloor N/p_i \rfloor \leq N/p_i$. On a donc moins de $\sum_{i>k} N/p_i < N/2$ entiers $\leq N$ ayant au moins un facteur premier dans $\{p_i, i > k\}$. On en déduit $N = N_0 + N_1 \leq 2^k\sqrt{N} + N/2$ donc $N/2 \leq 2^k\sqrt{N}$ donc $\sqrt{N} \leq 2^{k+1}$, ce qui est absurde dès que l'on choisit $N > 2^{2(k+1)}$.

Remarque. *La question a) entraîne que le k-ième nombre premier p_k est inférieur à $1+2^{2(k-1)}$, ce qui est très sous-optimal (le théorème des nombres premiers entraîne $p_k \sim k \ln k$) mais bien meilleur que la borne obtenue par la méthode d'Euclide qui fournit $p_k \leq 2^{2^{k-1}}$.*

– La preuve b) de la divergence de $\sum 1/p_i$ est d'une simplicité remarquable. La preuve historique de la divergence de cette série est due à Euler et est présentée dans [Analyse §4.6 Pb.22 d)].

Exercice 9. Soit $n > 2$ un entier impair. On note r le *radical de n*, défini par le produit des nombres premiers distincts qui divisent n (*i.e* si $n = \prod_i p_i^{\alpha_i}$ avec les p_i premiers distincts, $r = \prod_i p_i$). Soient $x, y \in \mathbb{Z}$ tels que $r \mid x^n + y^n$. Montrer que $nr \mid x^n + y^n$.

Solution. On commence par le cas où $n = p$ est un nombre premier. Si $p \mid x^p + y^p$, le théorème de Fermat entraîne $x \equiv x^p \pmod p$ et $y \equiv y^p \pmod p$, donc $x + y \equiv$

$x^p + y^p \pmod p$ est divisible par p. En posant $s = x + y$, comme p est impair on a

$$x^p + y^p = x^p + (s-x)^p = \sum_{k=0}^{p-1} \binom{p}{k} s^{p-k} x^k = s \cdot z, \qquad z = \sum_{k=0}^{p-1} \binom{p}{k} s^{p-k-1} x^k.$$

Chaque terme de la somme qui définit z est divisible par p (car $p \mid s = x + y$ et $p \mid \binom{p}{k}$ pour $1 \leq k < p$), donc $p \mid z$. Ainsi $p \mid s$ et $p \mid z$ donc $rp = p^2 \mid sz = x^p + y^p$.

Traitons le cas où $n = p^\alpha$ (avec $\alpha \in \mathbb{N}^*$) est la puissance d'un nombre premier p. On procède par récurrence sur α. Le cas $\alpha = 1$ a été traité plus haut. Supposons le résultat vrai pour α et montrons le pour $\alpha + 1$. Le résultat précédent appliqué à $X = x^{p^\alpha}$ et $Y = y^{p^\alpha}$, montre que $X^p + Y^p = S \cdot Z$ où $S = X + Y$ et $Z \in \mathbb{Z}$ est divisible par p. D'après l'hypothèse de récurrence $S = x^{p^\alpha} + y^{p^\alpha}$ est divisible par $p^{\alpha+1}$. On en déduit que $x^{p^{\alpha+1}} + y^{p^{\alpha+1}} = S \cdot Z$ est divisible par $p^{\alpha+2} = rn$.

Dans le cas général, soit la décomposition en facteurs premiers $n = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$. Il s'agit de montrer que $rn = p_1^{\alpha_1+1} \cdots p_\ell^{\alpha_\ell+1}$ divise $x^n + y^n$. Il suffit de montrer que $p_k^{\alpha_k+1}$ divise $x^n + y^n$ pour tout k. Pour cela on écrit

$$x^n + y^n = X^{p^{\alpha_k}} + Y^{p^{\alpha_k}}, \qquad X = x^m,\ Y = y^m, \quad m = n/p^{\alpha_k} = \prod_{i \neq k} p_i^{\alpha_i}$$

et comme $r = p_1 \cdots p_\ell$ divise $x^n + y^n$, on a $p_k \mid X^{p^{\alpha_k}} + Y^{p^{\alpha_k}}$, donc comme prouvé plus haut $p_k^{\alpha_k+1} \mid X^{p^{\alpha_k}} + Y^{p^{\alpha_k}} = x^n + y^n$.

Remarque. *Si $p \mid x^n + y^n$, la solution s'étend facilement pour montrer $v_p(x^n+y^n) = v_p(x+y)+v_p(n)$, , où $v_p(m) = \max\{\alpha, p^\alpha \mid m\}$ (lemme LTE, ou lemme de Manea).*

EXERCICE 10. **a)** Soit $n \geq 2$ un entier. Montrer que $H_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k} \notin \mathbb{N}$

b) Soient $m, n \in \mathbb{N}$ avec $2 \leq m \leq n$. Montrer que $H_{m,n} = \displaystyle\sum_{k=m}^{n} \frac{1}{k} \notin \mathbb{N}$.

c) Soient $m, n \in \mathbb{N}$ avec $1 \leq m \leq n$. Montrer que $I_{m,n} = \displaystyle\sum_{k=m}^{n} \frac{1}{2k+1} \notin \mathbb{N}$.

Solution. **a)** C'est classique et pas si simple à résoudre. On choisit la puissance de 2 vérifiant $2^r \leq n < 2^{r+1}$, avec $r \in \mathbb{N}^*$. On note π_n le produit des nombres impairs $\leq n$ et on écrit

$$2^{r-1}\pi_n H_n = A + B \quad \text{où} \quad A = \sum_{\substack{1 \leq k \leq n \\ k \neq 2^r}} \frac{2^{r-1}\pi_n}{k}, \quad B = \frac{2^{r-1}\pi_n}{2^r} = \frac{\pi_n}{2}.$$

Les termes de la somme de A sont entiers, car si $1 \leq k \leq n$ et $k \neq 2^r$, on peut écrire $k = 2^s \ell$ avec $0 \leq s \leq r-1$ et $\ell \leq n$ impair, donc $(\pi_n 2^{r-1})/k = (\pi_n/\ell)2^{r-1-s}$ est un entier (ℓ est un des termes du produit π_n), donc A est entier. Or π_n étant impair, $B = \pi_n/2$ n'est pas entier, donc $2^{r-1}\pi_n H_n$ n'est pas entier, donc $H_n \notin \mathbb{N}$.

b) On reprend les arguments précédents, en considérant la plus grande valuation dyadique r des entiers de $\{m,\dots,n\}$, où la valuation dyadique de $k\in\mathbb{N}^*$ est définie par $v_2(k)=\max\{\alpha\in\mathbb{N}, 2^\alpha \mid k\}$. Il n'y a qu'un seul entier de $\{m,\dots,n\}$ de valuation dyadique r. En effet, si $m\le k<\ell\le n$ et $v_2(k)=v_2(\ell)=r$, on peut écrire $k=2^r a$ et $\ell=2^r b$, où a et b sont impairs, avec $a<b$. Soit $c=a+1$. L'entier c est pair et vérifie $a<c<b$, donc $j=2^r c$ vérifie $m\le k<j<\ell\le n$ et $v_2(j)=r+v_2(c)>r$ (car c est pair), ce qui est absurde par construction de r.

Notons ℓ l'unique entier de $\{m,\dots,n\}$ tel que $v_2(\ell)=r$ et a impair tel que $\ell=2^r a$. Comme plus haut, π_n désigne le produit des nombres impairs $\le n$. On a

$$2^{r-1}\pi_n H_{m,n}=A+B \quad\text{où}\quad A=\sum_{\substack{1\le k\le n\\ k\ne\ell}}\frac{2^{r-1}\pi_n}{k},\quad B=\frac{2^{r-1}\pi_n}{\ell}=\frac{a\pi_n}{2}.$$

Vu que $v_2(k)\le r-1$ pour $1\le k\le n$ et $k\ne\ell$, A est entier. Or B n'est pas entier car $a\pi_n$ est impair, on en déduit que $2^{r-1}\pi_n H_{m,n}$ n'est pas entier.

c) Tentons de généraliser l'approche précédente avec approche triadique. Pour cela, il faut qu'il n'y ait qu'un seul entier de $\Gamma=\{2m+1,2m+3,\dots,2n+1\}$ dont la valuation triadique est maximale, ce qui n'est pas vrai tout le temps. On s'y ramène, en traitant plusieurs cas. Si $n=m$, alors $I_{m,n}=1/(2m+1)\notin\mathbb{N}$. Si $n\le 3m$ et $m<n$, alors

$$0<I_{m,n}<\frac{n-m+1}{2m+1}\le\frac{2m+1}{2m+1}=1\quad\text{donc}\quad I_{m,n}\notin\mathbb{N}.$$

Sinon $n>3m$, donc $2n+1\ge 3(2m+1)$, donc dans Γ il y a une puissance de 3. En effet, l'entier $r=\max\{\alpha\in\mathbb{N}, 3^\alpha\le 2n+1\}$ vérifie $(2n+1)/3<3^r\le 2n+1$ donc $\ell=3^r$ est un entier impair vérifiant $2m+1\le\ell\le 2n+1$ donc $\ell\in\Gamma$. Par ailleurs, ℓ est le seul entier de Γ divisible par 3^r (s'il existe un autre entier $\ell'=3^r q\in\Gamma$ alors $q\ge 3$ car ℓ' est impair, donc $3^{r+1}\in\Gamma$ ce qui contredit la définition de r). Ainsi, en notant π_n le produit des entiers $\le n$ non divisibles par 3, le nombre $A=3^{r-1}\pi_n(I_{m,n}-1/\ell)$ est un entier. Donc $3^{r-1}\pi_n I_{m,n}=A+\pi_n/3$, somme d'un entier et d'un rationnel non entier, n'est pas entier, donc $I_{m,n}$ n'est pas entier.

Remarque. *Ces résultats ont été généralisés par Paul Erdös qui a montré en 1932 que si a et $b\ge 2$ sont premiers entre eux, alors $\sum_{k=m}^{n}\frac{1}{a+kb}$ n'est pas entier.*

Exercice 11 (Théorème de Wolstenholme). Soit $p\ge 5$ un nombre premier. On souhaite montrer le *théorème de Wolstenholme* qui affirme

$$\text{si}\quad H_{p-1}=1+\frac{1}{2}+\cdots+\frac{1}{p-1}=\frac{a}{b},\quad \text{avec } a,b\in\mathbb{N}^*,\quad \text{alors } p^2\mid a. \quad (*)$$

1/ (Première méthode). **a)** Pour tout $n\in\mathbb{Z}$, on note $\overline{n}$ sa classe dans $\mathbb{Z}/p\mathbb{Z}$. Pour tout $k\in\{1,2,\dots,p-1\}$, montrer

$$\overline{\pi_k}=(\overline{k})^{-2},\quad\text{où}\quad \pi_k=\frac{(p-1)!}{k(p-k)}.$$

b) En déduire $(*)$.

2/ (Deuxième méthode). Soit $F = (X-1)(X-2)\cdots(X-p+1) \in \mathbb{Z}[X]$, qu'on écrit sous la forme $F = X^{p-1} - a_1X^{p-2} + \cdots - a_{p-2}X + a_{p-1}$.
a) Montrer que le polynôme $-a_1X^{p-2} + \cdots - a_{p-2}X$ est nul modulo p.
b) En déduire $(*)$.

Solution. **1/a)** L'entier $\pi_k = (p-1)!/(k(p-k))$ vérifie $k(p-k)\pi_k \equiv (p-1)! \pmod p$. Le théorème de Wilson affirme que $(p-1)! \equiv -1 \pmod p$, on en déduit

$$k(p-k)\pi_k \equiv -1 \pmod p \quad \text{donc} \quad -k^2\pi_k \equiv -1 \pmod p,$$

d'où le résultat.

b) On commence par regrouper les termes de H_{p-1} deux à deux,

$$H_{p-1} = \sum_{k=1}^{(p-1)/2} \left(\frac{1}{k} + \frac{1}{p-k}\right) = \sum_{k=1}^{(p-1)/2} \frac{p}{k(p-k)}.$$

ce qui entraîne

$$H_{p-1} = p\frac{A}{(p-1)!}, \quad \text{où} \quad A = \sum_{k=1}^{(p-1)/2} \frac{(p-1)!}{k(p-k)} = \sum_{k=1}^{(p-1)/2} \pi_k. \qquad (**)$$

D'après a), on peut écrire dans $\mathbb{Z}/p\mathbb{Z}$

$$\overline{A} = \sum_{k=1}^{(p-1)/2} (\overline{k})^{-2} \quad \text{donc} \quad 2\overline{A} = \sum_{k=1}^{(p-1)/2} (\overline{k})^{-2} + \sum_{k=1}^{(p-1)/2} (-\overline{k})^{-2}.$$

Le dernier terme est la somme des $(\overline{k})^{-2}$ pour $k = -(p-1)/2, \ldots, -1, 1, \ldots, (p-1)/2$, c'est-à-dire la somme des carrés des inverses des $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. L'application $x \mapsto 1/x$ étant bijective sur $(\mathbb{Z}/p\mathbb{Z})^*$, l'ensemble des inverses de $(\mathbb{Z}/p\mathbb{Z})^*$ est l'ensemble des éléments de $(\mathbb{Z}/p\mathbb{Z})^*$, on en déduit

$$2\overline{A} = \sum_{k=1}^{p-1} (\overline{k})^2 \quad \text{donc} \quad 2A \equiv \frac{(p-1)p(2p-1)}{6} \pmod p$$

(on a utilisé l'identité $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$). L'entier $q = \frac{1}{6}(p-1)p(2p-1)$ vérifie $p \mid 6q$ et comme $p \geq 5$ est premier, $p \mid q$. Donc $p \mid 2A$, donc $p \mid A$. Donc si $H_{p-1} = a/b$, l'égalité $a/b = pA/(p-1)!$ obtenue dans $(**)$ entraîne $a(p-1)! = pAb$ donc p^2 divise $a(p-1)!$ et comme $p^2 \wedge (p-1)! = 1$, on a bien $p^2 \mid a$.

2/a) Pour tout $x \in \{1, 2, \ldots, p-1\}$ on a

$$0 = F(x) = x^{p-1} - a_1x^{p-2} + \cdots + a_{p-3}x^2 - a_{p-2}x + a_{p-1}. \qquad (***)$$

Par ailleurs $a_{p-1} = F(0) = (-1)^{p-1}(p-1)! = (p-1)!$ et le théorème de Wilson fournit $a_{p-1} \equiv -1 \pmod p$. Lorsque $x \in \{1, \ldots, p-1\}$ le petit théorème de Fermat fournit $x^{p-1} \equiv 1 \pmod p$, donc $x^{p-1} + a_{p-1} \equiv 0 \pmod p$. Avec $(***)$ on en déduit

$$\forall x \in \{1, \ldots, p-1\}, \quad G(x) \equiv 0 \pmod p, \quad \text{où} \quad G = -a_1X^{p-2} + \cdots - a_{p-2}X.$$

Ainsi le polynôme $\overline{G} = -\overline{a}_1X^{p-2} + \cdots - \overline{a}_{p-2}X \in (\mathbb{Z}/p\mathbb{Z})[X]$ s'annule au moins $p-1$ fois sur $\mathbb{Z}/p\mathbb{Z}$, et comme $\deg \overline{G} \leq p-2$, on en déduit $\overline{G} = 0$.

b) On écrit

$$(p-1)! = F(p) = p^{p-1} - a_1 p^{p-2} + \cdots + a_{p-3}p^2 - a_{p-2}p + a_{p-1}.$$

On a vu plus haut que $a_{p-1} = (p-1)!$, donc ceci entraîne

$$a_{p-2} = p^{p-2} - a_1 p^{p-3} p + \cdots - p^2 a_{p-4} + p a_{p-3}.$$

D'après la question précédente on a $p \mid a_{p-3}$, on en déduit $p^2 \mid a_{p-2}$. Pour conclure, il suffit de remarquer que les relations coefficients-racines fournissent

$$a_{p-2} = \sum_{k=1}^{p-1} \prod_{\substack{1 \le j < p \\ j \ne k}} j = \sum_{k=1}^{p-1} \frac{(p-1)!}{k} = (p-1)! H_{p-1},$$

et on conclut de manière similaire à 1/b).

EXERCICE 12. Soit $n \ge 2$ un entier et $k \in \mathbb{Z}$. On note $N(n,k) = \sum_{i=1}^{n} k^{i \wedge n}$. Montrer que $N(n,k) \equiv 0 \pmod{n}$.

Solution. On regroupe d'abord les indices i qui ont même pgcd avec n, en écrivant

$$N(n,k) = \sum_{d \mid n} \sum_{\substack{1 \le i \le n \\ i \wedge n = d}} k^d = \sum_{d \mid n} k^d \sum_{\substack{1 \le i \le n \\ i \wedge n = d}} 1.$$

Soit $d \in \mathbb{N}^*$, $d \mid n$. On a $i \wedge n = d$ si et seulement si $d \mid i$ et $(i/d) \wedge (n/d) = 1$. Ainsi le nombre d'indices $i \in \{1, \ldots, n\}$ tel que $i \wedge n = d$ est égal au nombre d'indices $j = i/d$ dans $\{1, \ldots, n/d\}$ tel que $j \wedge (n/d) = 1$, donc égal à $\varphi(n/d)$ (où φ désigne l'indicateur d'Euler) ce qui donne

$$N(n,k) = \sum_{d \mid n} \varphi(n/d)\, k^d. \qquad (*)$$

Montrons $N(n,k) \equiv 0 \pmod{n}$. On traite plusieurs cas en fonction de n.

– ***Cas 1 :*** $n = p$ est un nombre premier. Alors le théorème de Fermat entraîne

$$N(p,k) = \varphi(p)\, k + \varphi(1)\, k^p = (p-1)k + k^p \equiv (p-1)k + k \equiv pk \equiv 0 \pmod{p}.$$

– ***Cas 2 :*** $n = p^2$ où p est un nombre premier. D'après $(*)$ on a

$$N(p^2,k) = \varphi(p^2)\, k + \varphi(p)\, k^p + \varphi(1)\, k^{p^2} = p(p-1)k + (p-1)k^p + k^{p^2}.$$

Comme $k^p \equiv k \pmod{p}$, il existe $m \in \mathbb{Z}$ tel que $k^p = k + pm$, donc

$$k^{p^2} = (k+pm)^p = k^p + \sum_{j=1}^{p-1} \binom{p}{j} p^j m^j k^{p-j} + p^p m^p \equiv k^p \pmod{p^2} \qquad (**)$$

car si $1 \le j \le p-1$, $p \mid \binom{p}{j}$ donc $p^2 \mid \binom{p}{j} p^j m^j k^{p-j}$. Par ailleurs $k^p \equiv k \pmod{p}$, donc $(p-1)k^p \equiv pk^p - k^p \equiv pk - k^p \pmod{p^2}$. Avec $(**)$ on en déduit

$$N(p^2,k) \equiv p(p-1)k + (pk - k^p) + k^p \equiv p(p-1)k + pk \equiv p^2 k \equiv 0 \pmod{p^2}.$$

– ***Cas 3 :*** $n = p^\alpha$ avec $\alpha \geq 2$. D'après $(*)$ on a

$$N(p^\alpha, k) = \sum_{\beta=0}^{\alpha} \varphi(p^{\alpha-\beta}) k^{p^\beta} = \sum_{\beta=0}^{\alpha-1} (p-1) p^{\alpha-\beta-1} k^{p^\beta} + k^{p^\alpha}. \qquad (***)$$

Généralisons le résultat $(**)$, en montrant

$$\forall \beta \in \mathbb{N}^*, \qquad k^{p^\beta} \equiv k^{p^{\beta-1}} \pmod{p^\beta}. \qquad (****)$$

On procède par récurrence. On l'a déjà montré pour $\beta = 1$ et $\beta = 2$. Supposons $(****)$ vrai pour β, de sorte qu'il existe $m \in \mathbb{Z}$ tel que $k^{p^\beta} = k^{p^{\beta-1}} + p^\beta m$. On a

$$k^{p^{\beta+1}} = \left(k^{p^\beta}\right)^p = \left(k^{p^{\beta-1}} + p^\beta m\right)^p = k^{p^\beta} + \sum_{j=1}^{p-1} \binom{p}{j} p^{j\beta} m^j k^{(p-j)p^{\beta-1}} + p^{p\beta} m^p.$$

Lorsque $1 \leq j \leq p-1$, on a $p \mid \binom{p}{j}$ donc $p^{\beta+1}$ divise chaque terme de la somme plus haut. On a également $p^{\beta+1} \mid p^{p\beta} m^p$, on en déduit $k^{p^{\beta+1}} \equiv k^{p^\beta} \pmod{p^{\beta+1}}$.

La congruence $(****)$ entraîne, lorsque $1 \leq \beta \leq \alpha - 1$,

$$(p-1)p^{\alpha-\beta-1}k^{p^\beta} = p^{\alpha-\beta}k^{p^\beta} - p^{\alpha-\beta-1}k^{p^\beta} \equiv p^{\alpha-\beta}k^{p^{\beta-1}} - p^{\alpha-\beta-1}k^{p^\beta} \pmod{p^\alpha}.$$

En reportant dans $(***)$, et compte tenu de $(****)$ appliqué à $\beta = \alpha$, on en déduit

$$\begin{aligned} N(p^\alpha, k) &\equiv (p-1)p^{\alpha-1}k + \sum_{\beta=1}^{\alpha-1} (p^{\alpha-\beta}k^{p^{\beta-1}} - p^{\alpha-\beta-1}k^{p^\beta}) + k^{p^{\alpha-1}} \pmod{p^\alpha} \\ &\equiv (p-1)p^{\alpha-1}k + (p^{\alpha-1}k - p^0 k^{p^{\alpha-1}}) + k^{p^{\alpha-1}} \equiv p^\alpha k \equiv 0 \pmod{p^\alpha} \end{aligned}$$

– ***Cas 4 :*** Traitons maintenant le cas général. Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers. Montrons $N(n,k) \equiv 0 \pmod{p_j^{\alpha_j}}$ pour tout j, ce qui entraînera $N(n,k) \equiv 0 \pmod{n}$. Fixons $j \in \{1, \ldots, r\}$. Pour alléger les notations on note $p = p_j$ et $\alpha = \alpha_j$. L'entier $m = n/p^\alpha$ est premier avec p. Les diviseurs d de n s'écrivent de manière unique sous la forme $d = cp^\beta$ avec $c \mid m$ et $0 \leq \beta \leq \alpha$, de sorte que l'égalité $(*)$ s'écrit

$$N(n,k) = \sum_{c \mid m} \sum_{\beta=0}^{\alpha} \varphi\left(\frac{m}{c} p^{\alpha-\beta}\right) k^{cp^\beta} = \sum_{c \mid m} \varphi\left(\frac{m}{c}\right) \sum_{\beta=0}^{\alpha} \varphi(p^{\alpha-\beta})(k^c)^{p^\beta},$$

où on a utilisé la propriété $\varphi(ab) = \varphi(a)\varphi(b)$ si $a \wedge b = 1$. Compte tenu de l'expression de $N(p^\alpha, k^c)$ fournie par $(*)$, cette dernière expression s'écrit aussi

$$N(n,k) = \sum_{c \mid m} \varphi\left(\frac{m}{c}\right) N(p^\alpha, k^c).$$

Le cas 3, où k est remplacé par k^c, donne $N(p^\alpha, k^c) \equiv 0 \pmod{p^\alpha}$, on en déduit $N(n,k) \equiv 0 \pmod{p^\alpha}$. Ainsi, $p_j^{\alpha_j} \mid N(n,k)$, et ceci pour tout j, donc $n \mid N(n,k)$.

Remarque. *On peut montrer que l'entier $N(n,k)/n$ est le nombre de colliers non-équivalents à n perles et k couleurs (deux colliers sont équivalents si l'un s'obtient de l'autre par rotation ou par permutation des couleurs). La preuve est difficile.*

EXERCICE 13. Soit $n \geq 2$ un entier et $r \in \mathbb{N}$. Quel est le nombre d'inversibles dans $\mathbb{Z}/n\mathbb{Z}[X]$ de degré $\leq m$?

Solution. Notons $A = \mathbb{Z}/n\mathbb{Z}$. L'anneau $A[X]$ est unitaire, d'unité $\overline{1}$. Soit

$$P = a_0 + a_1X + \cdots + a_rX^r \in A[X], \quad \text{inversible dans } A[X].$$

Il existe $Q = b_0 + b_1X + \cdots + b_sX^s \in A[X]$ tel que $PQ = \overline{1}$.

Le coefficient constant de PQ est égal à $\overline{1}$, ce qui s'écrit $a_0b_0 = \overline{1}$, donc a_0 est inversible dans A.

Montrons maintenant que si $r > 0$, le coefficient a_r est nilpotent. Comme $PQ = \overline{1}$, le coefficient de degré $r + s - k$ de PQ est nul pour $0 \leq k \leq s$, ce qui s'écrit

$$\forall k \in \{0, 1, \ldots, s\}, \qquad a_rb_{s-k} + a_{r-1}b_{s-k+1} + \cdots + a_{r-k}b_s = 0. \tag{$*$}$$

(où par commodité, on a posé $a_i = 0$ pour $i < 0$).

— Si $k = 0$, $(*)$ s'écrit $a_rb_s = 0$.

— Si $s \geq 1$ et $k = 1$ $(*)$ s'écrit $a_rb_{s-1} + a_{r-1}b_s = 0$, en multipliant par a_r, on obtient $a_r^2b_{s-1} + a_{r-1}a_rb_s = 0$ donc $a_r^2b_{s-1} = 0$.

Montrons ainsi par récurrence sur $j \in \mathbb{N}^*$ que

$$\forall j \in \mathbb{N}, j \leq s, \qquad a_r^{j+1}b_{s-j} = 0. \tag{$**$}$$

On a vu que $(**)$ est vraie pour $j = 0$. Supposons $(**)$ vraie pour $j \leq k - 1$ avec $k \leq s$ et montrons le pour $j = k$. En multipliant l'égalité $(*)$ par a_r^k, on obtient

$$a_r^{k+1}b_{s-k} + a_{r-1}a_r^kb_{s-k+1} + \cdots + a_{r-k}a_r^kb_s = 0. \tag{$***$}$$

L'hypothèse de récurrence assure $a_r^kb_{s-j} = a_r^{k-j-1}(a_r^{j+1}b_{s-j}) = 0$ pour $0 \leq j \leq k - 1$, donc $(***)$ entraîne $a_r^{k+1}b_{s-k} = 0$, donc $(**)$ est vraie au rang $j = k$. En particulier $(**)$ est vraie pour $k = s$, ce qui fournit $a_r^{s+1}b_0 = 0$, et comme b_0 est inversible (on a vu plus haut que $a_0b_0 = \overline{1}$), on a $a_r^{s+1} = 0$. Donc a_r est nilpotent.

Rappelons que dans un anneau commutatif, la somme d'un inversible et d'un nilpotent est inversible (voir la partie sur les définition des anneaux, page 14). En appliquant cette propriété à l'anneau $A[X]$ à P inversible et $-a_rX^r$ nilpotent, on en déduit que $P - a_rX^r = \sum_{i=0}^{r-1} a_iX^i$ est inversible. Comme plus haut, on en déduit que si $r - 1 > 0$ le coefficient a_{r-1} est nilpotent. De proche en proche, on voit ainsi que tous les coefficients a_i pour $1 \leq i \leq r$ sont nilpotents.

Réciproquement, soit $P = \sum_{i=0}^{r} a_iX^i$ un polynôme tel que a_0 est inversible et a_i nilpotent pour $i > 0$. Une récurrence sur $k \in \mathbb{N}$ montre que $P_k = \sum_{i=0}^{k} a_iX^i$ est inversible. En effet, $P_0 = a_0$ est inversible, et si P_{k-1} est inversible, $P_k = P_{k-1} + a_kX^k$, somme d'un inversible et d'un nilpotent, est inversible. En particulier $P = P_r$ est inversible.

Pour répondre à la question de l'exercice, il faut maintenant compter les inversibles et les nilpotents de $A = \mathbb{Z}/n\mathbb{Z}$. Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ la décomposition de n en facteurs premiers. Le nombre d'inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est donné par l'indicateur d'Euler $\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1)$. Par ailleurs, si $\overline{x}$ est nilpotent dans $\mathbb{Z}/n\mathbb{Z}$ il existe $r > 0$ tel que $\overline{x}^r = \overline{0}$, ce qui s'écrit $n \mid x^r$, donc $p_i \mid x$ pour tout i, donc $p_1 \cdots p_k$ divise x. Réciproquement si $p_1 \cdots p_k \mid x$, alors $(p_1 \cdots p_k)^r \mid x^r$, où $r = \max \alpha_i$, donc $n \mid x^r$ et $\overline{x}$ est bien nilpotent dans $\mathbb{Z}/n\mathbb{Z}$. Les nilpotents de $\mathbb{Z}/n\mathbb{Z}$

sont donc les éléments $\overline{x}$ avec $0 \leq x < n$ et x divisible par $p_1 \cdots p_k$, au nombre de $n/(p_1 \cdots p_k)$. On en déduit que le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}[X]$ dont le degré est $\leq m$ est $\varphi(n) \left(\dfrac{n}{p_1 \cdots p_k}\right)^m = (p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1})^{m+1}(p_1 - 1) \cdots (p_k - 1)$.

Exercice 14 (Conditions de cyclicité de $(\mathbb{Z}/n\mathbb{Z})^*$). Pour tout entier $n \geq 2$, on note $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.
1/ Soit $p > 2$ un nombre premier. **a)** Montrer que

$$\forall k \in \mathbb{N}, \qquad (1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}. \qquad (*)$$

b) Montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique pour tout $\alpha \in \mathbb{N}^*$ (on pourra utiliser la propriété de cyclicité de $(\mathbb{Z}/p\mathbb{Z})^*$, voir page 9 dans la partie sur l'ordre des élements d'un groupe).

2/a) Montrer que $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ est cyclique si et seulement si $\alpha \leq 2$.
b) Montrer

$$\forall k \in \mathbb{N}, \qquad 5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}.$$

c) Si $x \in (\mathbb{Z}/2^\alpha\mathbb{Z})^*$ montrer qu'il existe $(\varepsilon, k) \in \{-1, 1\} \times \mathbb{N}$ tel que $x = \varepsilon\overline{5}^k$.

3/ Déterminer les valeurs de n pour lesquelles $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique.

Solution. **1/a)** On procède par récurrence sur $k \in \mathbb{N}$. Pour $k = 0$ c'est trivial. Supposons le résultat vrai pour $k \in \mathbb{N}$, de sorte qu'il existe $m \in \mathbb{Z}$ tel que $(1+p)^{p^k} = 1 + p^{k+1} + p^{k+2}m = 1 + p^{k+1}q$ avec $q = 1 + mp$, et montrons le pour $k+1$. La formule du binôme fournit

$$(1+p)^{p^{k+1}} = (1 + p^{k+1}q)^p = 1 + p \cdot p^{k+1}q + \sum_{j=2}^{p} \binom{p}{j} (p^{k+1}q)^j.$$

Lorsque $2 \leq j \leq p-1$, p divise $\binom{p}{j}$ donc $\binom{p}{j}(p^{k+1}q)^j$ est divisible par $p \cdot p^{2k+2}$ donc par p^{k+3}. Lorsque $j = p$, $\binom{p}{j}(p^{k+1}q)^j = (p^{k+1}q)^p$ est divisible par p^{pk+p} donc par p^{k+3}. On en déduit le résultat au rang $k+1$ car

$$(1+p)^{p^{k+1}} \equiv 1 + p \cdot p^{k+1}q \equiv 1 + p^{k+2} + p^{k+3}m \equiv 1 + p^{k+2} \pmod{p^{k+3}}.$$

b) Soit $a \in \mathbb{Z}$ tel que $\dot{a}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$, soit s l'ordre de $\overline{a}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. On a $a^s \equiv 1 \pmod{p^\alpha}$ donc $a^s \equiv 1 \pmod{p}$, et comme $\dot{a}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$ on en déduit que $(p-1)$ divise s. Ainsi l'ordre de $x = \overline{a}^{s/(p-1)}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est $p-1$.

La congruence $(*)$ appliquée avec $k = \alpha - 1$ puis avec $k = \alpha - 2$ entraîne

$$(1+p)^{p^{\alpha-1}} \equiv 1 + p^\alpha \pmod{p^{\alpha+1}} \quad \text{donc} \quad (1+p)^{p^{\alpha-1}} \equiv 1 \pmod{p^\alpha},$$
$$(1+p)^{p^{\alpha-2}} \equiv 1 + p^{\alpha-1} \pmod{p^\alpha} \quad \text{donc} \quad (1+p)^{p^{\alpha-2}} \not\equiv 1 \pmod{p^\alpha}.$$

La première ligne entraîne que l'ordre de $\overline{1+p}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ divise $p^{\alpha-1}$, donc est de la forme p^β avec $\beta \leq \alpha-1$. La deuxième ligne fournit $\beta > \alpha-2$. On en déduit $\beta = \alpha-1$, donc $y = \overline{1+p}$ est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

En résumé, on a montré qu'il existe $x, y \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ avec x d'ordre $p-1$ et y d'ordre $p^{\alpha-1}$. On va montrer que l'ordre r de $z = xy$ est le ppcm des ordres de x et de y, ce qui est classique dans un groupe abélien. L'égalité $z^r = \overline{1}$ entraîne $x^r = \overline{1}/y^r$ donc $\overline{1} = (x^{(p-1)})^r = x^{r(p-1)} = \overline{1}/y^{r(p-1)}$ donc $y^{r(p-1)} = \overline{1}$, donc $p^{\alpha-1}$ divise $r(p-1)$ donc divise r car $p^{\alpha-1} \wedge (p-1) = 1$. De même, $x^{rp^{\alpha-1}} = \overline{1}/y^{rp^{\alpha-1}} = \overline{1}$, donc $p-1$ divise $rp^{\alpha-1}$ donc divise r puisque $(p-1) \wedge p^{\alpha-1} = 1$. Ainsi, r est divisible par $p^{\alpha-1}$ et $p-1$, et comme $p^{\alpha-1} \wedge (p-1) = 1$, $p^{\alpha-1}(p-1)$ divise r. Or le cardinal de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$, on en déduit que $r = p^{\alpha-1}(p-1)$. Donc $\langle z \rangle = (\mathbb{Z}/p^\alpha\mathbb{Z})^*$, *i.e.* $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique.

2/a) Les groupes des inversibles $(\mathbb{Z}/2\mathbb{Z})^* = \{\overline{1}\}$ et $(\mathbb{Z}/4\mathbb{Z})^* = \{\overline{1}, \overline{-1}\}$ sont cycliques. Dans $(\mathbb{Z}/8\mathbb{Z})^*$ on a $\overline{3}^2 = \overline{1}$, $\overline{5}^2 = \overline{1}$ et $\overline{7}^2 = \overline{1}$, donc les 4 éléments de $(\mathbb{Z}/8\mathbb{Z})^*$ sont d'ordre 1 ou 2. Ainsi $(\mathbb{Z}/8\mathbb{Z})^*$ n'est pas cyclique.

Si $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ n'est pas cyclique. En effet, raisonnons par l'absurde et supposons $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ cyclique, engendré par $\overline{x}$ avec $x \in \mathbb{Z}$. Soit $\dot{y} \in (\mathbb{Z}/8\mathbb{Z})^*$ avec $y \in \mathbb{Z}$. Il existe $m \in \mathbb{N}^*$ tel que $\overline{x}^m = \overline{y}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$, on en déduit $x^m \equiv y \pmod 8$. Ainsi, tout élément de $(\mathbb{Z}/8\mathbb{Z})^*$ s'écrit sous la forme $\dot{x}^m$, donc $(\mathbb{Z}/8\mathbb{Z})^*$ est cyclique, ce qui est absurde. On en déduit que $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$ n'est pas cyclique.

b) On procède par récurrence sur $k \in \mathbb{N}$. Pour $k = 0$ c'est évident. Supposons le résultat vrai pour k, de sorte qu'il existe $m \in \mathbb{Z}$ tel que $(1+4)^{2^k} = 1 + 2^{k+2} + 2^{k+3}m = 1 + 2^{k+2}q$ avec $q = 1 + 2m$. Le résultat est vrai pour $k+1$ car

$$5^{2^{k+1}} = (1 + 2^{k+2}q)^2 = 1 + 2^{k+3}(1+2m) + 2^{2k+4}q^2 \equiv 1 + 2^{k+3} \pmod{2^{k+4}}.$$

c) Si $\alpha \in \{1, 2\}$ c'est immédiat. Supposons $\alpha \geq 3$. La congruence précédente appliquée avec $k = \alpha - 3$ puis avec $k = \alpha - 2$ entraine

$$5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \not\equiv 1 \pmod{2^\alpha} \qquad \text{et} \qquad 5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}. \qquad (**)$$

Donc $\overline{5}$ est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$. Ainsi $\Gamma_+ = \{\overline{5}^k, \mid 0 \leq k < 2^{\alpha-2}\}$ et $\Gamma_- = \{-\overline{5}^k, \mid 0 \leq k < 2^{\alpha-2}\}$ sont de cardinal $2^{\alpha-2}$. Par ailleurs Γ_+ et Γ_- sont disjoints, car si $\overline{5}^k = -\overline{5}^\ell$ avec $0 \leq k, \ell < 2^{\alpha-2}$ alors $\overline{5}^{k-\ell} = -\overline{1}$. On a $\overline{5}^{2(k-\ell)} = \overline{1}$ donc $2^{\alpha-2}$ (ordre de $\overline{5}$) divise $2(k-\ell)$, donc $2^{\alpha-3}$ divise $k-\ell$. Par ailleurs, $0 \leq k, \ell < 2^{\alpha-2}$ donc $-2^{\alpha-2} < k - \ell < 2^{\alpha-2}$, donc $k - \ell = \varepsilon 2^{\alpha-3}$ avec $\varepsilon \in \{-1, 0, 1\}$. Or $\overline{5}^{k-\ell} = -\overline{1}$ donc $\varepsilon \neq 0$. Si $\varepsilon = 1$ on a $\overline{5}^{2^{\alpha-3}} = -\overline{1}$, ce qui est incompatible avec la première égalité de $(**)$. Le cas $\varepsilon = -1$ entraîne la même contradiction. Ainsi, les deux ensembles Γ_+ et Γ_- sont bien disjoints. Or $|\Gamma_-| = |\Gamma_+| = |(\mathbb{Z}/2^\alpha\mathbb{Z})^*|/2$, donc $\Gamma_+ \cup \Gamma_-$ forme une partition de $(\mathbb{Z}/2^\alpha\mathbb{Z})^*$, ce qui entraîne le résultat demandé.

3/ Montrons que $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique si et seulement si $n \in \{2, 4\}$, $n = p^\alpha$ ou $p = 2p^\alpha$ avec $p > 2$ premier et $\alpha \in \mathbb{N}^*$.

Condition nécessaire. Supposons $(\mathbb{Z}/n\mathbb{Z})^*$ cyclique et considérons la décomposition de n en produits de facteurs premiers : $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Si $k = 1$, d'après 2/a)

on ne peut pas avoir $p_1 = 2$ et $\alpha_1 \geq 3$, donc $n \in \{2, 4\}$ ou $n = p_1^{\alpha_1}$ avec $p_1 > 2$ premier et $\alpha_1 > 0$.

Supposons maintenant $k \geq 2$. On s'appuie sur le lemme suivant :

> LEMME. Si $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique et si $n = qr$ où $q > 1$ et $r > 1$ sont premiers entre eux, alors $q = 2$ ou $r = 2$.

Prouvons le lemme. Le théorème des restes chinois assure que $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ sont isomorphes en tant qu'anneau, ce qui induit un isomorphisme de groupe entre $(\mathbb{Z}/n\mathbb{Z})^*$ et $(\mathbb{Z}/q\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^*$, donc ce dernier est cyclique, *i.e.* il existe $(x, y) \in (\mathbb{Z}/q\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^*$ d'ordre $\varphi(n)$ (où φ désigne l'indicateur d'Euler). En notant $m = \operatorname{ppcm}(\varphi(q), \varphi(r))$ on a $(x^m, y^m) = (\dot{1}, \tilde{1})$, donc $\varphi(n) \mid m$. Si $q > 2$ et $r > 2$ alors $\varphi(q)$ et $\varphi(r)$ sont pairs (si q a un facteur premier $p > 2$, $p-1$ divise $\varphi(q)$ donc $\varphi(q)$ est pair, sinon $q = 2^\beta$ avec $\beta \geq 2$ donc $\varphi(q) = 2^{\beta-1}$ est pair ; de même $\varphi(r)$ est pair), donc $\operatorname{pgcd}(\varphi(p), \varphi(q)) \geq 2$ donc $m = \varphi(q)\varphi(r)/\operatorname{pgcd}(\varphi(q), \varphi(r)) \leq \varphi(q)\varphi(r)/2 = \varphi(n)/2$ ce qui est absurde car $\varphi(n) \mid m$. Donc $q = 2$ ou $r = 2$.

Le lemme entraîne que n est de la forme $n = 2p^\alpha$ avec $p > 2$ premier et $\alpha \in \mathbb{N}^*$.

Condition suffisante. Si $n \in \{2, 4\}$ ou $n = p^\alpha$ avec $p > 2$ premier et $\alpha \in \mathbb{N}^*$, on a déjà vu que $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique. Si $n = 2p^\alpha$ avec $p > 2$ premier et $\alpha \in \mathbb{N}^*$, l'isomorphisme $(\mathbb{Z}/n\mathbb{Z})^* \sim (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ entraîne l'existence de $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ générant $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$. Alors $(\dot{1}, x) \in (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ génère $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^\alpha\mathbb{Z})^*$, donc ce dernier est cyclique, tout comme $(\mathbb{Z}/n\mathbb{Z})^*$ qui lui est isomorphe.

EXERCICE 15 (THÉORÈME DE MIDY). Soient $a, p \in \mathbb{N}$ tels que $0 < a < p$ et $\operatorname{pgcd}(p, 10) = 1$. On considère le développement décimal de a/p

$$\frac{a}{p} = 0, a_1 a_2 a_3 \cdots = \sum_{n=1}^{+\infty} \frac{a_n}{10^n} \qquad \text{où} \qquad \forall n \in \mathbb{N}^*,\ a_n \in \{0, 1, \ldots, 9\}.$$

1/ Montrer qu'il existe $\ell \in \mathbb{N}^*$ tel que $a_{n+\ell} = a_n$ pour tout $n \in \mathbb{N}^*$, et caractériser la plus petite valeur de $\ell \in \mathbb{N}^*$ vérifiant cette propriété (appelée *période* du développement décimal de a/p).

2/a) (Théorème de Midy). Si $p \notin \{2, 5\}$ est un nombre premier et si ℓ est pair, montrer que $a_n + a_{n+k} = 9$ pour tout $n \in \mathbb{N}^*$, où $k = \ell/2$.
b) Montrer que ce résultat n'est pas vrai dans le cas général (où p n'est pas supposé premier). Réciproquement, si $a_n + a_{n+k} = 9$ pour tout $n \in \mathbb{N}^*$, l'entier p est il nécessairement premier ?

Solution. **1/** C'est classique. Si le développement décimal de a/p est périodique de période ℓ, notons A l'entier dont la représentation décimale est $A = (a_1 \ldots a_\ell)_{10}$. Alors $a/p = \sum_{n=1}^{+\infty} A/10^{n\ell} = A/(10^\ell - 1)$, ou encore $a(10^\ell - 1) = pA$, ce qui entraîne $10^\ell \equiv 1 \pmod{p}$, donc la période ℓ est un multiple de l'ordre r de 10 dans $(\mathbb{Z}/p\mathbb{Z})^*$.

Réciproquement, soit $\ell = r$ l'ordre de 10 dans $(\mathbb{Z}/p\mathbb{Z})^*$. Alors $A = a(10^\ell - 1)/p$ est un entier, et $a/p = A/(10^\ell - 1)$. On a $0 < A < 10^\ell$, donc sa représentation décimale s'écrit $A = (a_1 \dots a_\ell)_{10}$ avec les $a_k \in \{0, \dots, 9\}$, et $a/p = \sum_{n=1}^{+\infty} A/10^{n\ell} = 0, \overline{a_1 \dots a_\ell}$ a un développement décimal ℓ-périodique. Ainsi, $\ell = r$ est une période, et on a vu plus haut que forcément $r \mid \ell$ donc $\ell = r$ est bien la période recherchée.

2/a) On a vu plus haut que $10^\ell \equiv 1 \pmod p$, donc $(10^k)^2 \equiv 1 \pmod p$. Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc $10^k \equiv 1 \pmod p$ ou $10^k \equiv -1 \pmod p$. Or la période $\ell = 2k$ du développement décimal de a/p est le plus petit entier r tel que $10^r \equiv 1 \pmod p$, donc $10^k \not\equiv 1 \pmod p$. On en déduit $10^k \equiv -1 \pmod p$.

Notons $y = 0, a_{k+1}a_{k+2}\dots$. On a $10^k a/p = N + y$, où $N = (a_1 \dots a_k)_{10}$, donc $(10^k + 1)a/p = N + y + a/p$. Or $(10^k + 1)a/p$ est entier car $10^k \equiv -1 \pmod p$, donc $y + a/p$ est entier. Ce dernier est égal à 1 car $0 < y < 1$ et $0 < a/p < 1$, donc $0 < y + a/p < 2$ et 1 est le seul entier vérifiant ces inégalités. Donc

$$y = 1 - a/p = \sum_{n=1}^{+\infty} \frac{9}{10^n} - \sum_{n=1}^{+\infty} \frac{a_n}{10^n} = \sum_{n=1}^{+\infty} \frac{9 - a_n}{10^n},$$

et par unicité du développement décimal (lorsque la suite des décimales n'est pas ultimement égale à 9), on en déduit $a_{k+n} = 9 - a_n$ pour tout $n \in \mathbb{N}^*$.

b) Le résultat n'est pas vrai dans le cas général (par exemple il n'est pas vérifié si $p = 21$, pour lequel $1/p = 0, \overline{047619}$), mais reste vrai en supposant uniquement $10^k \equiv -1 \pmod p$ (c'est la seule propriété, conséquence de la primalité de p, utilisée pour montrer le résultat dans la question précédente). Par exemple pour n'importe quel diviseur p de $10^3 + 1 = 7 \times 11 \times 13$, on a $10^3 \equiv -1 \pmod p$. Avec le choix $p = 7 \times 11 = 77$ on a $1/77 = 0, \overline{012987}$ qui vérifie bien la propriété souhaitée, alors que $p = 77$ n'est pas premier.

Remarque. *Cette propriété reste vraie en remplaçant* 10 *par n'importe quelle base* B *(et* 9 *par* $B - 1$*).*

– Ce résultat fut prouvé par le mathématicien français Etienne Midy en 1836. Une formulation équivalente est $(a_1 \dots a_k)_{10} + (a_{k+1} \dots a_{2k})_{10} = 10^k - 1$*. Ce résultat s'étend comme suit : on peut montrer que si la période* ℓ *de* a/p *vérifie* $\ell = hk$ *avec* $h, k \in \mathbb{N}^*$*, alors* $\sum_{j=0}^{h-1} (a_{jk+1} \dots a_{jk+k})_{10}$ *est un multiple de* $10^k - 1$*.*

Exercice 16 (Théorème de Cauchy-Davenport). Si A, B sont deux parties d'un groupe abélien $(G, +)$, on note $A + B = \{a + b \mid a \in A, b \in B\}$.

1/ (Cas réel.) Si A et B sont deux parties finies non vides de $\mathbb{R}$, montrer que $|A+B| \geq |A|+|B|-1$ (où $|X|$ désigne le cardinal de X), et caractériser le cas d'égalité.

2/ (Cas de $\mathbb{Z}/p\mathbb{Z}$). Soient p un nombre premier et A et B deux sous-ensembles non vides de $\mathbb{Z}/p\mathbb{Z}$.
a) Si $|A| < p$ et $|B| > 1$, montrer que $|A + B| > |A|$.

b) (Théorème de Cauchy-Davenport). Démontrer l'inégalité

$$|A+B| \geq \min\{|A|+|B|-1, p\}. \qquad (*)$$

Solution. **1/** Notons $p = |A|$ et $q = |B|$, puis $a_1 < \ldots < a_p$ les éléments de A, $b_1 < \ldots < b_q$ ceux de B. Alors

$$a_1+b_1 < a_2+b_1 < \ldots < a_p+b_1 < a_p+b_2 < \ldots < a_p+b_q, \qquad (**)$$

ces nombres réels forment ainsi $p+(q-1) = |A|+|B|-1$ éléments distincts de $A+B$, d'où l'inégalité.

Supposons l'égalité $|A+B| = |A|+|B|-1$ vérifiée. Les $p+q-1$ éléments de $A+B$ sont alors exactement ceux de $(**)$. Soit $i \in \{1, \ldots, p-1\}$. Les éléments

$$a_1+b_1 < \ldots < a_i+b_1 < a_i+b_2 < \ldots < a_i+b_q < a_{i+1}+b_q < \ldots < a_p+b_q \quad (***)$$

forment un ensemble de $p+q-1$ éléments de $A+B$, qui sont donc égaux à ceux de $(**)$. En particulier, l'élément $a_{i+1}+b_1$ qui suit a_i+b_1 dans $(**)$, est égal à a_i+b_2 qui suit a_i+b_1 dans $(***)$, donc $a_{i+1}-a_i = b_2-b_1$. En notant $r = b_2-b_1$, on a donc $a_i = a_1+(i-1)r$ pour $1 \leq i \leq p$. Les rôles de A et B sont symétriques car $A+B = B+A$, donc on a également $b_{i+1}-b_i = a_2-a_1$ pour $1 \leq i \leq q-1$, et comme $a_2-a_1 = r$, on a $b_i = b_1+(i-1)r$ pour $1 \leq i \leq q$. Réciproquement, s'il existe $r \in \mathbb{R}^*$ tel que $a_i = a_1+(i-1)r$ et $b_i = b_1+(i-1)r$, alors $A+B = \{a_1+b_1+kr, 0 \leq k \leq p+q-2\}$ a $p+q-1$ éléments. Ainsi, $|A+B| = |A|+|B|-1$ si et seulement A et B sont les termes de deux suites arithmétiques de même raison.

2/a) Raisonnons par l'absurde et supposons $|A+B| = |A|$. Choisissons $b_0 \in B$ et notons $C = B-b_0 = \{b-b_0 \mid b \in B\}$. On a $A+B = (A+C)+b_0$ donc $|A+B| = |A+C|$. Comme $0 \in C$, on a $A \subset A+C$, et vu que $|A| = |A+B| = |A+C|$ on a $A = A+C$. Comme $|C| = |B| > 1$, il existe $c \in C$, $c \neq 0$. L'égalité $A = A+C$ entraîne $a+c \in A$ dès que $a \in A$. Une récurrence immédiate fournit $a+kc \in A$ pour tout $k \in \mathbb{N}$. Or $c \neq 0$ est inversible dans le corps $\mathbb{Z}/p\mathbb{Z}$, donc l'application $\varphi : \mathbb{N} \to \mathbb{Z}/p\mathbb{Z}$ $k \mapsto a+kc$ est surjective. Donc $\mathbb{Z}/p\mathbb{Z} = \varphi(\mathbb{N}) \subset A$, ce qui est contraire aux hypothèses puisque $|A| < p$.

b) On prouve le résultat par récurrence sur $|B|$. Si $|B| = 1$, c'est évident car $|A+B| = |A|$.

Supposons le résultat vrai pour $|B| \leq n-1$ avec $n \geq 2$ et montrons le pour $|B| = n$. Si $|A| \geq p$ c'est terminé. Sinon, d'après la question précédente, on a $|A+B| > |A|$ donc il existe $a_0 \in A$ tel que $a_0+B \not\subset A$. Alors $B \not\subset C = A-a_0$. On a $A+B = (C+B)-c_0$ donc $|A+B| = |C+B|$. Notons

$$A_1 = C \cup B, \ B_1 = B \cap C, \text{ de sorte que } |A_1|+|B_1| = |B|+|C| = |B|+|A|.$$

On a

$$A_1+B_1 = (C+B_1) \cup (B+B_1) \subset (C+B) \cup (B+C) = B+C.$$

On peut appliquer l'hypothèse de récurrence à (A_1, B_1) car $|B_1| < |B|$, qui fournit

$$|A+B| = |C+B| \geq |A_1+B_1| \geq \min\{|A_1|+|B_1|-1, p\} = \min\{|A|+|B|-1, p\}.$$

Remarque. - *Le résultat* $(*)$ *a été prouvé par Cauchy en 1813 (qu'il utilisa pour donner une nouvelle preuve d'un résultat de Lagrange de 1770 associé au célèbre théorème des quatre carrés — tout entier naturel est somme de quatre carrés, voir [Algèbre §1.5 Sujet d'étude 3]), puis redécouvert par Davenport en 1935.*

– *Dans* $\mathbb{Z}/p\mathbb{Z}$*, si* $|A|, |B| \geq 2$ *et* $|A+B| \leq p-2$*, l'égalité dans* $(*)$ *se produit (comme dans le cas réel) si et seulement si* A *et* B *sont les termes de deux suites arithmétiques de même raison (théorème de Vosper).*

– *Une preuve intéressante et surprenante du résultat* $(*)$ *via une approche polynomiale fait l'objet de la question 3/ de l'exercice 24 page 100.*

Exercice 17 (Nombre de caractères d'un groupe fini). Soit G un groupe fini de cardinal $n \in \mathbb{N}^*$ dont l'élément neutre est noté e. On note $\widehat{G}$ le groupe des morphismes de $(G, \cdot)$ vers $(\mathbb{C}^*, \cdot)$ et E le $\mathbb{C}$-e.v des fonctions de G vers $\mathbb{C}$. Les éléments de $\widehat{G}$ sont appelés *caractères* de G, et $\widehat{G}$ le *dual* de G.

1/a) Quelle est la dimension de E ?
b) Montrer le *Lemme de Dedekind* : toute famille finie d'éléments distincts de $\widehat{G}$ est libre dans E. En déduire $|\widehat{G}| \leq n$.

2/ On suppose G abélien.
a) Pour tout $(a, f) \in G \times E$, on note $f_a : \ E \to \mathbb{C}\ x \mapsto f(ax)$. On note $T_a \in \mathcal{L}(E)$ l'endomorphisme de E défini sur E par $T_a(f) = f_a$. Montrer qu'il existe une base de E diagonalisant tous les $(T_a)_{a\in G}$.
b) Montrer que $|\widehat{G}| = |G|$.

3/ Montrer que le résultat 2/b) est faux si G n'est pas supposé abélien.

Solution. **1/a)** Notons $\delta_a \in E$ la fonction définie par $\delta_a(x) = 1$ si $x = a$, $\delta_a(x) = 0$ si $x \neq a$. La famille $(\delta_a)_{a\in G}$ est libre car si $\sum_{a\in G} \lambda_a \delta_a = 0$, pour tout $x \in G$ on a $0 = \sum_{a\in G} \lambda_a \delta_a(x) = \lambda_x$. C'est aussi une famille génératrice car pour tout $f \in E$, on a $f = \sum_{a\in G} f(a)\delta_a$. Donc E est un $\mathbb{C}$-e.v de dimension $|G| = n$.

b) Notons que si $\chi \in \widehat{G}$, alors $\chi(e) = 1$ car $\chi(e) = \chi(e^2) = (\chi(e))^2$ et $\chi(e) \neq 0$.

Prouvons maintenant le lemme de Dedekind. Montrons par récurrence sur $m \in \mathbb{N}^*$ qu'une famille $(\chi_k)_{1\leq k\leq m}$ de m éléments distincts de $\widehat{G}$ est libre. Pour $m = 1$, c'est immédiat, car si $\chi_1 \in \widehat{G}$ et $\lambda_1\chi_1 = 0$ alors $\lambda_1\chi_1(e) = 0 = \lambda_1$. Supposons maintenant le résultat vrai pour $m-1 \in \mathbb{N}^*$ et montrons le pour m. Supposons $\sum_{k=1}^m \lambda_k\chi_k = 0$ où $(\chi_k)_{1\leq k\leq m}$ est une famille de m éléments distincts de $\widehat{G}$ et $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$. On écrit, pour tout $a, b \in G$

$$\sum_{k=1}^{m} \lambda_k\chi_k(ab) - \left(\sum_{k=1}^{m} \lambda_k\chi_k(a)\right)\chi_m(b) = 0 = \sum_{k=1}^{m-1} \lambda_k\chi_k(a)\left(\chi_k(b) - \chi_m(b)\right). \quad (*)$$

Soit $\ell \in \{1, \dots, m-1\}$. Comme $\chi_\ell \neq \chi_m$, il existe $b \in G$ tel que $\chi_\ell(b) \neq \chi_m(b)$ et l'égalité $(*)$ entraîne

$$\forall a \in G, \qquad \sum_{k=1}^{m-1} \mu_k \chi_k(a) = 0 \quad \text{où} \quad \mu_k = \lambda_k(\chi_k(b) - \chi_m(b)),$$

donc $\sum_{k=1}^{m-1} \mu_k \chi_k = 0$. D'après l'hypothèse de récurrence ceci entraîne $\mu_k = 0$ pour $1 \leq k \leq m-1$, en particulier $\mu_\ell = \lambda_\ell(\chi_\ell(b) - \chi_m(b)) = 0$, et comme $\chi_\ell(b) \neq \chi_m(b)$ on en déduit $\lambda_\ell = 0$. Ceci est vrai pour tout ℓ, donc les $(\lambda_\ell)_{1 \leq \ell \leq m-1}$ sont tous nuls. On en déduit que $\sum_{k=1}^{m} \lambda_k \chi_k = \lambda_m \chi_m = 0$, donc $\lambda_m = 0$, et le lemme de Dedekind est démontré.

Si $\widehat{G}$ a au moins $n+1$ éléments, on peut appliquer le lemme à $n+1$ éléments de $\widehat{G}$, ce qui est absurde car toute famille libre dans un e.v de dimension n n'a pas plus de n éléments. Donc $|\widehat{G}| \leq n$.

2/a) Les $(T_a)_{a \in G}$ commutent deux à deux. En effet si $a, b \in G$ alors

$$\forall f \in E, \forall x \in G, \quad T_a \circ T_b(f)(x) = T_a(f_b)(x) = f_b(ax) = f(b(ax)) = f_{ba}(x)$$

donc $T_a \circ T_b(f) = f_{ba}$. De même $T_b \circ T_a(f) = f_{ab}$. Or G est abélien donc $ba = ab$, on en déduit $T_a \circ T_b(f) = T_b \circ T_a(f)$, donc T_a et T_b commutent.

Soit $a \in G$. L'égalité $T_a \circ T_b(f) = f_{ba}$ entraîne $(T_a)^k(f) = f_{a^k}$ pour tout $k \in \mathbb{N}$ et tout $f \in E$. Vu que G est fini d'ordre n, on a $a^n = e$ donc $(T_a)^n = \mathrm{Id}_E$. Ainsi, pour tout $a \in G$ l'endomorphisme T_a est annulé par le polynôme $X^n - 1$ qui n'a que des racines simples dans $\mathbb{C}$, donc T_a est diagonalisable. De plus les $(T_a)_{a \in G}$ commutent deux à deux, il est classique que ceci entraîne qu'ils sont diagonalisables dans une base commune de vecteurs propres de E (voir la partie 1.3 page 167).

b) La question précédente assure l'existence d'une base $\mathcal{B}$ de E qui diagonalise tous les $(T_a)_{a \in G}$. Fixons $f \in \mathcal{B}$. Pour tout $a \in G$, il existe $\lambda_a \in \mathbb{C}$ tel que $T_a(f) = \lambda_a f$, de sorte que $f(ax) = \lambda_a f(x)$ pour tout $x \in G$, donc $f(a) = \lambda_a f(e)$. Comme f est non nulle (c'est un vecteur d'une base), il existe $a \in G$ tel que $f(a) \neq 0$ donc $f(a) = \lambda_a f(e) \neq 0$, donc $f(e) \neq 0$. Ainsi le vecteur $\tilde{f} = f/f(e)$ vérifie $\tilde{f}(e) = 1$, $\lambda_a = \tilde{f}(a)$, et $T_a(\tilde{f}) = \lambda_a \tilde{f}$. Donc pour tout $x \in G$, $\tilde{f}(ax) = \lambda_a \tilde{f}(x) = \tilde{f}(a)\tilde{f}(x)$. Ceci est vrai pour tout $a \in G$, et comme $\tilde{f}(e) = 1$, on en déduit que $\tilde{f} \in \widehat{G}$.

La famille $(\tilde{f})_{f \in \mathcal{B}}$ est une base de E (car les $\tilde{f}$ et f sont colinéaires et $\tilde{f} \neq 0$), et vu que $\dim E = n$, l'ensemble $\{\tilde{f}, f \in \mathcal{B}\}$ a n éléments. Comme $\tilde{f} \in \widehat{G}$ pour $f \in \mathcal{B}$, on en déduit $|\widehat{G}| \geq n$. Avec 1/b) on en déduit $|\widehat{G}| = n = |G|$.

3/ Le résultat 2/b) est faux si G n'est pas supposé abélien. Par exemple si $G = \mathcal{S}_n$ est le groupe symétrique d'indice n, et $n \geq 3$, montrons $\widehat{G} = \{\chi_0, \varepsilon\}$ où $\chi_0 = 1_G$ et ε est la signature des permutations de $\mathcal{S}_n$, ce qui entrainera $|\widehat{G}| = 2 < |G| = n!$.

Soit $\chi \in \widehat{\mathcal{S}_n}$. Considérons la transposition $\tau = (1\ 2)$. Pour tout $\sigma \in \mathcal{S}_n$, on a

$$\chi(\sigma\tau\sigma^{-1}) = \chi(\sigma)\chi(\tau)\chi(\sigma^{-1}) = \chi(\sigma)\chi(\sigma^{-1})\chi(\tau) = \chi(\mathrm{Id})\chi(\tau) = \chi(\tau).$$

Or $\sigma\tau\sigma^{-1}$ est la transposition $\tau_{\sigma(1),\sigma(2)} = (\sigma(1)\ \sigma(2))$, donc $\chi(\tau_{\sigma(1),\sigma(2)}) = \chi(\tau)$. Pour tout $i, j \in \{1, \dots, n\}$ avec $i \neq j$, il existe une permutation σ telle que $\sigma(1) = i$ et $\sigma(2) = j$, on en déduit $\chi(\tau_{i,j}) = s$ où $s = \chi(\tau)$. Comme $s^2 = \chi(\tau^2) = \chi(\mathrm{Id}) = 1$, on a $s \in \{-1, 1\}$. Considérons maintenant $\sigma \in \mathcal{S}_n$. On peut écrire σ comme un produit de transpositions $\sigma = \prod_{i=1}^{m} \tau_i$, on en déduit $\chi(\sigma) = \prod_{i=1}^{m} \chi(\tau_i) = s^m$ avec

$s \in \{-1, 1\}$. Donc $\chi = \chi_0$ ou $\chi = \varepsilon$. Réciproquement, il est clair que χ_0 et ε sont bien deux morphismes distincts de $\mathcal{S}_n$ dans $\mathbb{C}^*$.

Remarque. *L'exercice suivant propose une méthode constructive permettant de montrer $|\widehat{G}| = |G|$ lorsque G est un groupe abélien fini.*

Exercice 18 (Caractères d'un groupe abélien fini). Soit G un groupe abélien fini dont l'élément neutre est noté e. On appelle *caractère* tout morphisme de groupe $\chi : G \to \mathbb{C}^*$. Le caractère χ_0 défini par $\chi_0(g) = 1$ pour tout $g \in G$ est appelé *caractère trivial* de G.

a) Montrer qu'un caractère χ de G est à valeurs dans $\mathbb{U} = \{z \in \mathbb{C},\ |z| = 1\}$.
b) On note $\widehat{G}$ l'ensemble des caractères de G, muni du produit $\chi_1\chi_2$ défini par $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$ sur G. Montrer que $\widehat{G}$ est un groupe abélien. On l'appelle *dual* de G.
c) Soit H un sous-groupe de G tel que G/H est cyclique. Montrer que chaque caractère de H est la restriction de $|G|/|H|$ caractères de G.
d) Montrer que le résultat précédent reste vrai sans supposer G/H cyclique.
e) Montrer $|\widehat{G}| = |G|$.
f) Montrer (en notant $\overline{\chi(h)}$ le conjugué de $\chi(h)$)

$$\forall \chi \in \widehat{G} \qquad \sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{si } \chi = \chi_0, \\ 0 & \text{sinon.} \end{cases}$$

$$\forall a \in G, \forall g \in G, \qquad \sum_{\chi \in \widehat{G}} \overline{\chi(a)}\chi(g) = \begin{cases} |G| & \text{si } g = a, \\ 0 & \text{sinon.} \end{cases}$$

Solution. **a)** Soit χ est un caractère de G. On a $\chi(e) = \chi(e^2) = \chi(e)^2$ et comme $\chi(e) \neq 0$ on en déduit $\chi(e) = 1$. Soit $g \in G$. Posons $n = |G|$. On a $g^n = e$ donc $\chi(g)^n = \chi(g^n) = \chi(e) = 1$, donc $\chi(g) \in \mathbb{U}$.

b) La caractère trivial χ_0 est un élément neutre pour $\widehat{G}$. Il s'agit de montrer que tout élément de $\widehat{G}$ admet un inverse. Si $\chi \in \widehat{G}$, on définit le caractère χ' sur G par $\chi'(g) = 1/\chi(g)$. On vérifie facilement qu'il s'agit d'un caractère, et ce dernier vérifie $\chi'\chi = \chi\chi' = \chi_0$. Enfin, il est immédiat que $\widehat{G}$ est abélien.

c) Notons $m = |G/H|$ et aH un générateur de G/H avec $a \in G$. On a $a^m \in H$, et tout élément de G s'écrit de manière unique sous la forme $g = a^k h$ avec $0 \leq k < m$ et $h \in H$.

Soit $\chi \in \widehat{H}$. Si $\psi \in \widehat{G}$ vérifie $\psi_{|H} = \chi$ alors $\psi(a)^m = \psi(a^m) = \chi(a^m)$, donc $\omega = \psi(a)$ est une racine m-ième de $\zeta = \chi(a^m)$. Un choix de ω tel que $\omega^m = \zeta$ étant fait, le caractère ψ est déterminé sur G car $\psi(a^k h) = \psi(a)^k\psi(h) = \omega^k\chi(h)$ pour $0 \leq k < m$ et $h \in H$. Ainsi défini, ψ est bien un caractère. En effet, considérons

$g_1 = a^{k_1}h_1$ et $g_2 = a^{k_2}h_2$ avec $0 \leq k_1, k_2 < m$ et $h_1, h_2 \in H$. On a

$$\psi(g_1)\psi(g_2) = \psi(a^{k_1}h_1)\psi(a^{k_2}h_2) = \omega^{k_1+k_2}\chi(h_1)\chi(h_2).$$

Soit $\varepsilon \in \{0,1\}$ défini par $\varepsilon = 0$ si $k_1 + k_2 < m$, $\varepsilon = 1$ si $k_1 + k_2 \geq m$, de sorte que l'on a toujours $0 \leq k_1 + k_2 - \varepsilon m < m$. On a

$$\begin{aligned}\psi(g_1g_2) &= \psi(a^{k_1+k_2}h_1h_2) = \psi(a^{k_1+k_2-\varepsilon m}a^{\varepsilon m}h_1h_2) = \omega^{k_1+k_2-\varepsilon m}\chi(a^{\varepsilon m}h_1h_2)\\ &= \omega^{k_1+k_2-\varepsilon m}\chi(a)^{\varepsilon m}\chi(h_1)\chi(h_2) = \omega^{k_1+k_2}\chi(h_1)\chi(h_2) = \psi(g_1)\psi(g_2).\end{aligned}$$

Ainsi ψ est bien un caractère de G. Sa restriction à H est égale à χ. Il y a autant de caractères ψ possibles ayant cette propriété que de valeurs possibles de $\omega = \psi(a)$, donc m valeurs possibles car ω est une racine m-ième de $\zeta = \chi(a^m)$.

d) On fait une récurrence sur $[G : H] = |G|/|H|$. Si $[G : H] = 1$ on a $H = G$ et il n'y a rien à montrer. Supposons maintenant le résultat vrai pour tout sous-groupe H_1 de G tel que $[G : H_1] < [G : H]$ et montrons le pour H. On a $H \neq G$ donc il existe $a \in G$, $a \notin H$. Soit $H_1 = \langle a\rangle H$, sous-groupe de G constitué des éléments de la forme $a^k h$ avec $k \in \mathbb{Z}$ et $h \in H$. Le groupe H_1/H est cyclique (il est engendré par aH), donc d'après la question précédente, tout caractère χ de H est la restriction de $[H_1 : H]$ caractères de H_1. Or $|H_1| > |H|$, donc d'après l'hypothèse de récurrence, tout caractère de H_1 est la restriction de $[G : H_1]$ caractères de G. On en déduit que tout caractère de H est la restriction de $[H_1 : H][G : H_1] = [G : H]$ caractères de G, ce qui prouve le résultat.

e) Le résultat précédent appliqué dans le cas $H = \{e\}$ (pour lequel $\widehat{H} = \{\chi_0\}$ donc $|\widehat{H}| = 1$) entraîne que le caractère $\chi_0 \in \widehat{H}$ est la restriction de $[G : H] = |G|$ caractères de G, donc $|\widehat{G}| \geq |G|$. Or la restriction à $\{e\}$ de tout caractère de G est égale à χ_0, donc il n'y a pas d'autre caractère de G, donc $|\widehat{G}| = |G|$.

f) Commençons par la première identité. Si $\chi = \chi_0$ c'est évident. Sinon $\chi \neq \chi_0$ donc il existe $a \in G$ tel que $\chi(a) \neq 1$. Or $g \mapsto ag$ est une permutation de G, donc

$$\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(ag) = \sum_{g\in G}\chi(a)\chi(g) = \chi(a)\sum_{g\in G}\chi(g),$$

on en déduit $\sum_{g\in G}\chi(g) = 0$.

Démontrons maintenant la deuxième identité. On commence par le cas $a = e$, pour lequel $\chi(e) = 1$ pour tout $\chi \in \widehat{G}$. Si $g = e$, l'identité est immédiate. Sinon on considère le caractère χ_g de $\langle g\rangle$ défini par $\chi_g(g^k) = \omega^k$ où $\omega = e^{2i\pi/m}$ avec $m = |\langle g\rangle|$. La question précédente assure l'existence de $\psi \in \widehat{G}$ dont la restriction à $\langle g\rangle$ est égale à χ_g, et on a $\psi(g) = \omega \neq 1$. Comme $\chi \mapsto \psi \cdot \chi$ est une permutation de $\widehat{G}$ on a

$$\sum_{\chi\in\widehat{G}}\chi(g) = \sum_{\chi\in\widehat{G}}(\psi\chi)(g) = \psi(g)\sum_{\chi\in\widehat{G}}\chi(g)$$

donc $\sum_{\chi\in\widehat{G}}\chi(g) = 0$. Dans le cas général, on remarque que $\overline{\chi(a)} = \chi(a^{-1})$ donc si $a = g$ c'est immédiat, sinon $a^{-1}g \neq e$ donc

$$\sum_{\chi\in\widehat{G}}\overline{\chi(a)}\chi(g) = \sum_{\chi\in\widehat{G}}\chi(a^{-1})\chi(g) = \sum_{\chi\in\widehat{G}}\chi(a^{-1}g) = 0.$$

5. Problèmes

Problème 1 (Sommes de Gauss). Soit $p > 2$ un nombre premier.
1/ On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $(\mathbb{F}_p^*)^2 = \{x^2 \mid x \in \mathbb{F}_p^*\}$. Pour tout $a \in \mathbb{Z}$ on note $\dot{a}$ sa classe dans $\mathbb{F}_p$. On considère le *symbole de Legendre*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } \dot{a} \neq \dot{0} \text{ et } \dot{a} \in (\mathbb{F}_p^*)^2, \\ -1 & \text{si } \dot{a} \neq \dot{0} \text{ et } \dot{a} \notin (\mathbb{F}_p^*)^2, \\ 0 & \text{si } \dot{a} = \dot{0}. \end{cases}$$

a) Montrer le *critère d'Euler* :

$$\forall a \in \mathbb{Z}, p \nmid a, \qquad \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

b) Montrer : $\forall a, b \in \mathbb{Z}, \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

2/ On considère la *somme de Gauss* définie par

$$G = \sum_{n=0}^{p-1} \omega^{n^2} \quad \text{où} \quad \omega = e^{2i\pi/p}.$$

a) Montrer $G = \displaystyle\sum_{a=0}^{p-1} \left(\frac{a}{p}\right)\omega^a$.

b) Si $c \in \mathbb{Z}$, $p \nmid c$, on note $G_c = \displaystyle\sum_{a=0}^{p-1} \left(\frac{a}{p}\right)\omega^{ca}$. Montrer $G_c = \left(\frac{c}{p}\right)G$.

c) Montrer que si $c \in \mathbb{Z}$ et $p \nmid c$, on a $G_c = \displaystyle\sum_{n=0}^{p-1} \omega^{cn^2}$.

d) Montrer que $G\overline{G} = p$ (on remarquera que $\sum_{n=0}^{p-1} \omega^{n^2} = \sum_{n=0}^{p-1} \omega^{(n+m)^2}$).
e) En déduire que $G^2 = p$ si $p \equiv 1 \pmod 4$, $G^2 = -p$ si $p \equiv 3 \pmod 4$.

Solution. **1/a)** C'est classique. On sait déjà que $|(\mathbb{F}_p^*)^2| = (p-1)/2$ (voir la solution de l'exercice 1 page 16). Lorsque $a \in (\mathbb{F}_p^*)^2$ on écrit $a = b^2$ avec $b \in \mathbb{F}_p^*$, donc $a^{(p-1)/2} = b^{p-1} = \dot{1}$. Or le polynôme $X^{(p-1)/2} - \dot{1}$ a au plus $(p-1)/2$ racines, qui sont donc exactement les éléments de $(\mathbb{F}_p^*)^2$. On en déduit que si $a \notin (\mathbb{F}_p^*)^2$ et $a \neq \dot{0}$, alors $x = a^{(p-1)/2} \neq \dot{1}$. Comme $x^2 = a^{p-1} = \dot{1}$, on a forcément $x = -\dot{1}$, *i.e.* $a^{(p-1)/2} = -\dot{1}$. Dans tous les cas, si $p \nmid a$ on a montré $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p$.

b) Si $p \mid a$ ou $p \mid b$ c'est évident car le terme de gauche et le terme de droite sont nuls. Si $p \nmid a$ et $p \nmid b$, le critère d'Euler donne

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

et comme $p > 2$ et que les termes impliqués valent ± 1, ils sont égaux.