

1. Structure de groupe

1

Oral Mines Soit $(G, *)$ un groupe tel que pour tout $x \in G$, $x^2 = e$.

1. Montrer que $(G, *)$ est abélien.
2. Soient H un sous-groupe strict de $(G, *)$, $a \in G \setminus H$. Montrer que $H \cup aH$ est un sous-groupe de $(G, *)$.
3. Si G est fini, en créant par récurrence une suite de sous-groupe de G de cardinal une puissance de 2, montrer que le cardinal de G est une puissance de 2.
4. On veut retrouver le résultat précédent par une technique pour le moins inattendue. On admet que l'ensemble des entiers modulo 2 : $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$ forme un corps pour les lois d'addition et de multiplication modulo 2.
En interprétant G comme un $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel, montrer qu'il existe $n \in \mathbb{N}$ tel que $(G, *)$ est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$.
Retrouver en particulier le résultat de la question précédente.

Solution de 1 : Oral Mines

1. Tout $x \in G$ vérifie $x^{-1} = x$.
On a alors $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.
2. Tiens, une réunion de sous-groupe qui serait un sous-groupe ? Eh bien non. aH n'est pas un sous-groupe en général.
En utilisant $a^2 = e$, on obtient facilement que $H \cup aH$ est une partie non vide de G stable par la loi de groupe et par l'inversion.
3. Soit $G = \{e\}$ et c'est terminé.
Soit $G \neq \{e\}$ et $H_0 = \{e\}$ est un sous-groupe strict de cardinal 1. Par la question précédente, avec $a \in G \setminus \{e\}$, $H_1 = H_0 \cup a_0 H_0$, on obtient un sous-groupe de cardinal 2.
En itérant, on construit une suite de sous-groupes vérifiant $H_{n+1} = H_n \cup a_n H_n$, la réunion étant disjointe car $a_n \in G \setminus H_n$ et $|H_{n+1}| = 2|H_n| = 2^{n+1}$ (on voit facilement que $|H_n| = |a_n H_n|$ avec une bijection évidente). Comme G est fini, le procédé s'arrête, c'est-à-dire qu'il existe n tel que $G = H_n$ de cardinal 2^n .

Autre argument possible, directement : il existe alors des éléments $g_1, \dots, g_n$ de G tels que, en notant $\langle g_1, \dots, g_k \rangle$ le sous-groupe engendré par $\{g_1, \dots, g_k\}$ (i.e. le plus petit sous-groupe contenant $g_1, \dots, g_k$), on ait

$$\forall k \in \llbracket 2, m \rrbracket \quad g_k \notin \langle g_1, \dots, g_{k-1} \rangle$$

et $G = \langle g_1, \dots, g_m \rangle$ (sinon, on pourrait construire par récurrence une suite $(g_n)_{n \geq 1}$ d'éléments de G tels que

$$\forall k \geq 2 \quad g_k \notin \langle g_1, \dots, g_{k-1} \rangle$$

ce qui contredirait la finitude de G). On vérifie alors que

$$(h_1, \dots, h_n) \longrightarrow h_1 \cdots h_n$$

est un isomorphisme de $\langle g_1 \rangle \times \cdots \times \langle g_n \rangle$ sur $(G, *)$ où $\langle g \rangle = \{e, g\}$ est le sous-groupe engendré par g . Ou encore, tout élément de G s'écrit de manière unique sous la forme

$$g_1^{\epsilon_1} \cdots g_n^{\epsilon_n}$$

où les ϵ_k sont dans $\{0, 1\}$.

4. Le groupe $(G, *)$ est abélien.

Pour $\bar{0}, \bar{1} \in \mathbb{Z}/2\mathbb{Z}$ et $x \in G$, posons $\bar{0} \cdot x = e = x^0$ et $\bar{1} \cdot x = x = x^1$.

On vérifie que l'on définit alors un produit externe sur G munissant le groupe abélien $(G, *)$ d'une structure de $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel. En effet, pour $(x, y) \in G^2$ et $(\lambda, \mu) \in (\mathbb{Z}/2\mathbb{Z})^2$, on a

$$(\lambda + \mu) \cdot x = \lambda \cdot x * \mu \cdot x \quad \lambda \cdot (x + y) = \lambda \cdot x * \lambda \cdot y \quad \lambda \cdot (\mu \cdot x) = (\lambda \mu) \cdot x \quad \bar{1} \cdot x = x.$$

De plus, cet espace est de dimension finie car $|G|$ est fini (sinon, on pourrait construire une famille libre infinie), il est donc isomorphe à l'espace $((\mathbb{Z}/2\mathbb{Z})^n, +, \cdot)$ pour un certain $n \in \mathbb{N}^*$.

En particulier, le groupe $(G, *)$ est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$.

Dans la deuxième méthode de la question précédente, $(g_1, \dots, g_n)$ est une base du $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel G .

2 Oral Centrale Soit $(G, *)$ un groupe. On suppose que le cardinal de G s'écrit pq , avec q premier et $p < q$. Montrer que G contient au plus un sous-groupe de cardinal q .

Solution de 2 : Oral Centrale

Soit H un sous-groupe de cardinal q . Tout élément de H est d'ordre divisant q , donc d'ordre 1 ou q . Donc tout élément de H qui n'est pas d'ordre 1 (donc qui n'est pas l'élément neutre) est d'ordre q , donc engendre H . Supposons qu'il y ait deux sous-groupes H et H' d'ordre q , distincts. Alors $H \cap H' = \{e\}$ (car si $h \in H \cap H'$, si $h \neq e$, alors h engendre à la fois H et H' , qui sont alors égaux). Montrons que l'application

$$(h, h') \mapsto h * h'$$

est alors injective. En effet, si $h_1 * h'_1 = h_2 * h'_2$, on a $h_2^{-1} * h_1 = h'_2 * (h'_1)^{-1}$, cet élément de G étant à la fois dans H et H' est donc égal à e , d'où $h_1 = h_2$ et $h'_1 = h'_2$. Il y aurait donc au moins q^2 éléments dans G , ce qui est contraire à l'hypothèse.

- 3**
1. Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
 2. Déterminer tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}_+^*, \times)$.
 3. Déterminer tous les morphismes de groupes de $(\mathbb{U}_n, +)$ dans $(\mathbb{C}^*, \times)$.

Solution de 3 :

1. L'image d'un morphisme est un sous-groupe de $(\mathbb{Z}, +)$ donc de la forme $n\mathbb{Z}$. On a $x \in \mathbb{Q}$ tel que $f(x) = n$. Alors $\frac{n}{2} = f\left(\frac{x}{2}\right) \in n\mathbb{Z}$ donc $n = 0$.
Réciproquement, l'application nulle est bien un morphisme.
2. Si f est un tel morphisme et $r \in \mathbb{Q}^*$, pour tout $k \in \mathbb{N}^*$, $f(x) = f(x/k)^k \in \mathbb{Q}^*$. Alors toutes les valuations p -adiques de $f(x)$ (dans $\mathbb{Z}$) sont divisibles par tout $k \in \mathbb{N}^*$, donc sont toutes nulles.
 f est constamment égale à 1, ce qui donne bien un morphisme réciproquement.
3. Soit ϕ un tel morphisme. Si on connaît $\phi(\omega)$, où $\omega = e^{2i\pi/n}$, on connaît ϕ .
[Plus généralement, pour connaître un morphisme d'un groupe cyclique $(G, *)$ dans un groupe $(H, \cdot)$, il suffit de connaître l'image par ce morphisme d'un générateur de G . En effet, si g est un tel générateur, on a pour tout $n \in \mathbb{Z}$: $\phi(g^n) = (\phi(g))^n$, ce qui donne l'image par ϕ de tous les éléments de G .]
Soit $z_0 = \phi(\omega)$. On a, par propriété de morphisme,

$$z_0^n = \phi(\omega^n) = \phi(1) = 1$$

Donc $z_0^n = 1$. Et donc $z_0 \in \mathcal{U}_n$.

Réciproquement, soit z_0 un élément de $\mathbb{U}_n$. On montre que l'application

$$\phi_{z_0} : \begin{cases} \mathbb{U}_n & \longrightarrow \mathbb{C}^* \\ e^{2ik\pi/n} & \longmapsto z_0^k \end{cases}$$

est bien définie (il s'agit pour cela de montrer que, si $k \equiv \ell[n]$, $z_0^k = z_0^\ell$, ce qui se fait sans trop de mal). C'est assez clairement un morphisme. Les ϕ_{z_0} , $z_0 \in \mathbb{U}_n$ sont les morphismes cherchés.

4

Oral ENS Soit $(G, *)$ un groupe, $\text{Aut}(G)$ l'ensemble de ses automorphismes.

1. Montrer que $(\text{Aut}(G), \circ)$ est un groupe.
2. Déterminer les groupes finis tels que $\text{Aut}(G)$ soit réduit à un élément.

Solution de 4 : Oral ENS

La première question est simple, c'est une entrée en matière dans laquelle il faut montrer clarté et précision. Soit G un groupe fini tel que $\text{Aut}(G)$ soit réduit à un élément. Alors, pour tout $g \in G$,

$$\phi_g : h \longmapsto ghg^{-1}$$

étant dans $\text{Aut}(G)$, est égal à Id_G . On en déduit que G est commutatif.

Mais alors $x \longmapsto x^{-1}$ est aussi dans $\text{Aut}(G)$, et donc est égal à Id_G . On en déduit que $(G, *)$ est un groupe fini tel que pour tout $g \in G$, $g^2 = e$.

Il existe alors des éléments $g_1, \dots, g_m$ de G tels que, en notant $\langle g_1, \dots, g_k \rangle$ le sous-groupe engendré par $\{g_1, \dots, g_k\}$ (i.e. le plus petit sous-groupe contenant $g_1, \dots, g_k$), on ait

$$\forall k \in \llbracket 2, m \rrbracket \quad g_k \notin \langle g_1, \dots, g_{k-1} \rangle$$

et $G = \langle g_1, \dots, g_m \rangle$ (sinon, on pourrait construire par récurrence une suite $(g_n)_{n \geq 1}$ d'éléments de G tels que

$$\forall k \geq 2 \quad g_k \notin \langle g_1, \dots, g_{k-1} \rangle$$

ce qui contredirait la finitude de G). On vérifie alors que

$$(h_1, \dots, h_m) \longmapsto h_1 \dots h_m$$

est un isomorphisme de $\langle g_1 \rangle \times \dots \times \langle g_m \rangle$ sur $(G, *)$ où $\langle g \rangle = \{e, g\}$ est le sous-groupe engendré par g . Ou encore, tout élément de G s'écrit de manière unique sous la forme

$$g_1^{\epsilon_1} \dots g_m^{\epsilon_m}$$

où les ϵ_k sont dans $\{0, 1\}$. On a en fait revu G comme $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel de dimension finie, comme dans l'exercice 1, $(g_1, \dots, g_m)$ en est une base. L'application

$$g_1^{\epsilon_1} \dots g_m^{\epsilon_m} \longmapsto g_1^{\epsilon_2} g_2^{\epsilon_2} \dots g_m^{\epsilon_m}$$

définit alors un automorphisme de G autre que Id si $m \geq 2$. Les seuls groupes finis ayant un seul automorphisme sont donc $\{e\}$ et $\{e, g\}$ avec $g^2 = e$.

5 Oral X – Groupe dérivé Soit G un groupe. Pour $(a, b) \in G^2$, on note $[a, b] = aba^{-1}b^{-1}$. On note D_G le sous-groupe de G engendré par les éléments de la forme $[a, b]$, ie le plus petit sous-groupe de G contenant les éléments de la forme $[a, b]$.

1. Montrer que $\forall g \in G, \quad gD_Gg^{-1} = D_G$.
2. Montrer que $\forall g \in G, \quad gD_G = D_Gg$.
3. On pose $\mathcal{Q}_G = \{xD_G; x \in G\}$.
 - (a) Montrer que $\mathcal{Q}_G$ est une partition de G .
 - (b) Montrer que la fonction $(xD_G, yD_G) \mapsto (xy)D_G$ est convenablement définie et munit $\mathcal{Q}_G$ d'une structure de groupe, puis montrer que $x \mapsto xD_G$ est un morphisme de G dans $\mathcal{Q}_G$.
 - (c) Montrer que $\mathcal{Q}_G$ est abélien.

Solution de 5 : Oral X – Groupe dérivé

1. Soit $(a, b) \in G^2$. Alors

$$g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gagg^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gagg^{-1}, gbg^{-1}]$$

L'application $h \mapsto ghg^{-1}$ est un automorphisme du groupe G ; elle transforme les sous-groupes de G en sous-groupes de G . Elle laisse invariant $A = \{[a, b]; (a, b) \in G^2\}$. Elle transforme donc les sous-groupes contenant A en les sous-groupes contenant A . Et comme elle préserve l'inclusion, elle transforme le plus petit d'entre eux, D_G , en lui-même. On a donc $gD_Gg^{-1} = D_G$.

2. Facile conséquence de ce qu'on a fait précédemment.
3. (a) Supposons $xD_G \cap yD_G \neq \emptyset$; il existe alors h_1, h_2 dans D_G tels que

$$xh_1 = yh_2$$

Mais alors, si $h \in D_G$,

$$xh = y \underbrace{h_2h_1^{-1}}_{\in D_G} h \in yD_G$$

d'où $xD_G \subset yD_G$ et, symétriquement, $yD_G \subset xD_G$, donc xD_G et yD_G sont, s'ils ne sont pas la même partie de G , deux parties disjointes de G .

- (b) Pour la définition convenable, il s'agit de s'assurer que si $xD_G = x'D_G$ et $yD_G = y'D_G$ alors $xyD_G = x'y'D_G$. Ou encore, de manière équivalente, on doit montrer que si $x^{-1}x'$ et $y^{-1}y'$ sont dans D_G , alors $(xy)^{-1}x'y' \in D_G$. Mais...

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = \underbrace{y^{-1}y'}_{\in D_G} y'^{-1} \left(\underbrace{x^{-1}x'}_{\in D_G} \right) y'$$

et il suffit d'appliquer 1. pour conclure.

Il est clair qu'on définit ainsi une loi interne sur $\mathcal{Q}_G$.

Cette loi est associative, la vérification en est très formelle : avec des notations évidentes,

$$xD_G(yD_G zD_G) = xD_G(yzD_G) = x(yz)D_G = (xy)zD_G = (xy)D_G zD_G = (xD_G yD_G)zD_G$$

L'élément $D_G = eD_G$ de $\mathcal{Q}_G$ est neutre. Et l'élément $x^{-1}D_G$ est symétrique de l'élément xD_G . La propriété de morphisme demandée est alors très simple à écrire, elle découle de la définition.

- (c) Il s'agit de montrer que, pour tous x, y dans G ,

$$(xy)D_G = (yx)D_G$$

ou encore que $(xy)^{-1}yx \in D_G$ ce qui est bien simple vu la définition de D_G .

6 Oral X-ENS – Théorème de Sylow

Soit p un nombre premier et k un entier naturel non nul. Soit G un groupe de cardinal $p^k m$ avec $p \nmid m$. Il s'agit de montrer que G a un sous-groupe de cardinal p^k .

1. Traiter le cas $m = 1$ puis le cas où G est cyclique.

On définit $M = \{A \subset G, |A| = p^k\}$.

2. Montrer que p ne divise pas le cardinal de M .

On définit une relation d'équivalence $\sim$ sur M en posant pour A_1, A_2 dans M

$$A_1 \sim A_2 \iff \exists g \in G, A_1 = gA_2.$$

3. Montrer qu'il existe une classe d'équivalence de cardinal non divisible par p .

On prend A un représentant de cette classe, et on pose $H = \{g \in G, gA = A\}$.

4. Montrer que H est un sous-groupe de G de cardinal p^k .

Solution de 6 : Oral X-ENS – Théorème de Sylow

FGN 1 1.24

1. Si $m = 1$, $|G| = p^k$ et G lui-même convient.

Si G est cyclique, engendré par x , considérons $\langle x^m \rangle$. Son cardinal est l'ordre de x^m . Or, comme G est cyclique engendré par x , le plus petit n tel que $(x^m)^n = e$ est $n = p^k$. Donc $\langle x^m \rangle$ est d'ordre p^k .

2. Avec la formule de Legendre (voir exercice 14),

$$\begin{aligned} v_p(|M|) &= v_p\left(\binom{p^k m}{p^k}\right) = v_p((p^k m)!) - v_p((p^k)!) - v_p((p^k(m-1))!) \\ &= \sum_{\ell=1}^k \left(\left\lfloor \frac{p^k m}{p^\ell} \right\rfloor - \left\lfloor \frac{p^k}{p^\ell} \right\rfloor - \left\lfloor \frac{p^k(m-1)}{p^\ell} \right\rfloor \right) \\ &= \sum_{\ell=1}^k (p^{k-\ell} m - p^{k-\ell} - p^{k-\ell}(m-1)) \\ &= 0 \end{aligned}$$

Sans la formule de Legendre, en remarquant que $v_p(p^k m - \ell) = v_p(\ell)$ pour $\ell \in \llbracket 1, p^k - 1 \rrbracket$,

$$v_p\left(\binom{p^k m}{p^k}\right) = \sum_{\ell=0}^{p^k-1} v_p(p^k m - \ell) - v_p((p^k)!) = k + \sum_{\ell=1}^{p^k-1} v_p(\ell) - v_p((p^k)!) = 0.$$

En effet, comme $p \nmid m$ et $1 \leq \ell \leq p^k - 1$, donc la plus grande puissance de p qui divise $p^k m - \ell$ est la même que la plus grande puissance qui divise ℓ .

3. Comme la somme des cardinaux des classes est égale à $|M|$ qui n'est pas divisible par p , c'est aussi le cas du cardinal d'au moins une classe.
4. On vérifie facilement que H est un sous-groupe de G .

Comme dans la démonstration du théorème de Lagrange, en utilisant le relation d'équivalence sur A

$$a \sim b \iff a^{-1}b \in H,$$

on peut écrire A comme réunion disjointe de classes d'équivalences de la forme Ha donc toutes de cardinal $|H|$, on obtient que $|H|$ divise $|A| = p^k$ et donc $|H| = p^\ell$ avec $\ell \leq k$.

Enfin, on vérifie avec $f : g \in G \mapsto gA \in \text{cl}(A)$ (classe de la relation d'équivalence de la question 3) que pour tout $g \in G$, $f^{-1}(gA) = gH$, ce qui par lemme des bergers, nous dit que $|G| = |H| \times |\text{cl}(A)|$ et comme $p \nmid |\text{cl}(A)|$, $|H| = p^k$.

2. Anneaux et idéaux, corps

7 Soit $\mathbb{D} = \{x \in \mathbb{Q}, \exists n \in \mathbb{Z}, x \cdot 10^n \in \mathbb{Z}\}$ l'anneau des nombres décimaux. Montrer qu'il est principal.

Solution de 7 :

FGN 1 2.12

C'est facilement un sous-anneau de $(\mathbb{Q}, +, \times)$. Ses éléments s'écrivent de manière unique $2^\alpha 5^\beta p$ avec $p \in \mathbb{Z}$ premier avec 10 et $\alpha, \beta \in \mathbb{Z}$.

Comme dans $\mathbb{Z}$, soit I un idéal non réduit à 0 de $\mathbb{D}$ et $x = 2^\alpha 5^\beta p$ un élément non nul de I .

Alors $p = 2^{-\alpha} 5^{-\beta} x \in I$ car $2^{-\alpha} 5^{-\beta} \in \mathbb{D}$. Ainsi $|p| \in \mathbb{N}^* \cap I$, partie non vide de $\mathbb{N}$ qui possède un min noté a .

On a déjà $a\mathbb{D} \subset I$.

Si, réciproquement, $x = 2^\alpha 5^\beta p \in I$, alors $p \in I$ et par division euclidienne, $p = aq + r$ avec $r \in I \cap \mathbb{N}$ et $r < a$ donc $r = 0 : p = aq$ et $x = aq 2^\alpha 5^\beta : I \subset a\mathbb{D}$.

8 Soit A un anneau et $(a, b) \in A^2$. On suppose $1 - ab$ inversible. Montrer que $1 - ba$ l'est aussi.

Solution de 8 :

Si $(ab)^n = 0$, $(1 - ab)^{-1} = 1 + ab + \dots + (ab)^{n-1}$.

Alors $(ba)^{n+1} = b(ab)^n a = 0$ et $(1 - ba)^{-1} = 1 + ba + \dots + (ba)^n = 1 + b(1 - ab)^{-1}a$.

On vérifie alors que $1 + b(1 - ab)^{-1}a$ est bien l'inverse de $1 - ba$ dans le cas général.

9 Idéaux principaux Soit A un anneau commutatif. Pour a et b dans A , montrer que si l'idéal $(a) + (b)$ est principal, il en est de même de $(a) \cap (b)$.

Solution de 9 : Idéaux principaux

FGN 1 2.9

On s'inspire du cas de $\mathbb{Z}$ où $m = a \vee b = da'b'$ où $d = a \wedge b$, $a = da'$ et $b = db'$.

On a $(a) + (b) = (d)$ qui contient (a) et (b) donc on a $a', b' \in A$ tels que $a = da'$ et $b = db'$.

Soit $m = da'b'$. On montre que $(a) \cap (b) = (m)$.

On a déjà $(m) \subset (a) \cap (b)$ car $m \in (a)$ et $m \in (b)$.

Réciproquement, si $x \in (a) \cap (b)$, on obtient $x \in (m)$ en utilisant une « relation de Bézout » $d = au + bv$: en écrivant $x = aa' = \beta b$,

$$x = ada' = a(au + bv)a' = xua' + mav = \beta bua' + mav = m(\beta u + av) \in (m).$$

10 Anneau sans idéal non premier Soit A un anneau commutatif dont tout idéal I est premier

$(xy \in I \implies x \in I \text{ ou } y \in I)$.

Montrer que A est un corps.

Solution de 10 : Anneau sans idéal non premier

FGN 1 2.21

Si $x \in A$ non nul, on montre que x est inversible.

Comme (x^2) est premier, $x \in (x^2)$ donc on a $a \in A$ tel que $x = ax^2$.

Or (0) est premier donc A est intègre, donc comme $x \neq 0$, $ax = 1$.

11 Idéaux maximaux Soit A un anneau commutatif et I un idéal strict de A .

1. Montrer que I est maximal pour l'inclusion parmi les idéaux stricts de A si et seulement si pour tout $a \in A \setminus I$, on a $I + aA = A$.

On dit qu'un idéal I est premier si $A \setminus I$ est stable par produit.

2. Montrer que tout idéal maximal est premier.

Solution de 11 : Idéaux maximaux

FGN 2.10

3. Arithmétique entière

12

Montrer que si $n, k \in \mathbb{N}$, $(n!)^k$ divise $(nk)!$.

Solution de 12 :

FGN 1 3.1

$$\frac{(nk)!}{(n!)^k} = \prod_{i=1}^k \binom{in}{n} \in \mathbb{N}$$

13

Valuations sur $\mathbb{Q}$ On appelle valuation sur un anneau A toute application v de A dans $\mathbb{R} \cup \{+\infty\}$

telle que pour tout $(x, y) \in A^2$,

- (i) $v(xy) = v(x) + v(y)$;
- (ii) $v(x + y) \geq \min(v(x), v(y))$;
- (iii) $v(x) = +\infty \iff x = 0$.

1. Donner des exemples de valuations sur $\mathbb{Z}$, sur $\mathbb{Q}$.
2. Déterminer toutes les valuations sur $\mathbb{Q}$.

Solution de 13 : Valuations sur $\mathbb{Q}$

FGN 1 2.27

1. On peut citer les valuations p -adiques sur $\mathbb{Z}$ qui s'étendent à $\mathbb{Q}$ (on fait la différence des valuations p -adiques du numérateur et du dénominateur et on vérifie que le résultat ne dépend pas du représentant choisi du rationnel).

Plus généralement, toutes les λv_p où $\lambda > 0$ et p premier conviennent et on va montrer que ce sont les seules valuations non triviales (ie nulle sur $\mathbb{Q}^*$).

2. Soit v valuation non triviale.

On vérifie alors que $v(1) = 0$ puis $v(-1) = 0$ puis pour tout $x \in \mathbb{Q}^*$, $v(-x) = v(x)$ ie v est paire.

Puis, par récurrence pour tout $n \in \mathbb{N}$, $v(n) \geq 0$.

Enfin, pour tout $x \in \mathbb{Q}$ et $n \in \mathbb{N}$, $v(x^n) = n v(x)$.

Puis $E = \{n \in \mathbb{N}^*, v(n) > 0\}$ est non vide car v non trivial, son plus petit élément p est premier car si $p = ab$ avec $1 < a, b < p$, $v(p) = v(a) + v(b) = 0 + 0 = 0$ ce qui est absurde.

Si q est premier distinct de p , par une relation de Bézout, on montre que $0 = v(1) = v(pu + qv) \geq \min(v(p), v(q))$ donc $v(q) = 0$.

On conclut par décomposition primaire que $v = \lambda v_p$ où $\lambda = v(p) > 0$.

14

Formule de Legendre - Très classique - Oraux divers

1. Exprimer $v_p(n!)$ pour p premier et $n \in \mathbb{N}^*$ sous forme de somme.
2. Combien y a-t-il de zéros à la fin de 2025! ?
3. On écrit n en base p : $n = a_0 + a_1 p + \dots + a_r p^r$ et on pose $s = a_0 + \dots + a_r$. Montrer que $v_p(n!) = \frac{n-s}{p-1}$.

4. Soit $D : x \in \mathbb{R}^+ \mapsto \lfloor x \rfloor - \lfloor x/2 \rfloor - \lfloor x/3 \rfloor - \lfloor x/5 \rfloor + \lfloor x/30 \rfloor$. Montrer que $D(x) \geq 0$ pour tout $x \in \mathbb{R}^+$ et en déduire que

$$\frac{(30n)!n!}{(15n)!(10n)!(6n)!} \in \mathbb{N}$$

pour tout $n \in \mathbb{N}$.

Solution de 14 : Formule de Legendre - Très classique - Oraux divers

Les multiples de q s'écrivent $k = q\ell$ avec $\ell \in \mathbb{Z}$ uniquement déterminé par k et q , et alors $1 \leq k = q\ell \leq n$ si et seulement si $\frac{1}{q} \leq \ell \leq \frac{n}{q}$ si et seulement si $1 \leq \ell \leq \left\lfloor \frac{n}{q} \right\rfloor$ avec $\ell \in \mathbb{Z}$.

Le nombre de multiples de q entre 1 et n est donc $\left\lfloor \frac{n}{q} \right\rfloor$.

Ainsi, la valuation p -adique de $n!$ avec p premier s'obtient en ajoutant les valuations p -adiques des entiers entre 1 et n , d'après la question précédente :

- les $\left\lfloor \frac{n}{p} \right\rfloor$ multiples de p fournissent chacun (au moins) un facteur p ,
- les $\left\lfloor \frac{n}{p^2} \right\rfloor$ multiples de p^2 fournissent chacun (au moins) un facteur p supplémentaire,
- les $\left\lfloor \frac{n}{p^3} \right\rfloor$ multiples de p^3 fournissent chacun (au moins) un facteur p supplémentaire,
- et ainsi de suite.

Le décompte s'arrête car la suite entière $\left(\left\lfloor \frac{n}{p^i} \right\rfloor\right)_{i \in \mathbb{N}^*}$ finit par s'annuler et on obtient la formule de Legendre (avec un nombre fini de termes non nuls) :

$$v_p(n!) = \sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Autre rédaction possible : on peut dénombrer les entiers entre 1 et n ayant une valuation q -adique exactement égale à $i \in \mathbb{N}$: il s'agit des multiples de q^i qui ne sont pas multiples de q^{i+1} et qui sont au nombre de $\left\lfloor \frac{n}{q^i} \right\rfloor - \left\lfloor \frac{n}{q^{i+1}} \right\rfloor$, d'où la formule (les sommes étant toujours faussement infinies)

$$v_p(n!) = \sum_{i=0}^{+\infty} i \cdot \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor \right) = \sum_{i=1}^{+\infty} i \cdot \left\lfloor \frac{n}{p^i} \right\rfloor - \sum_{i=1}^{+\infty} (i-1) \cdot \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=1}^{+\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

15 Encadrement de Tchebychev

On note $\mathcal{P}_n$ l'ensemble des nombres premiers au plus égaux à n et $\pi(n)$ son cardinal.

Le très difficile *théorème des nombres premiers*, démontré par Hadamard et De la Vallée-Poussin dit que $\pi(n) \sim \frac{n}{\ln n}$.

On se contente ici d'un encadrement, dû à Tchebychev.

1. Montrer, en utilisant la formule de Legendre, que pour p premier et $n \in \mathbb{N}^*$, $v_p\left(\binom{2n}{n}\right) \leq \frac{\ln(2n)}{\ln p}$.

En déduire que $\frac{n}{\ln n} = \mathcal{O}(\pi(n))$.

2. Montrer que tout $p \in \mathcal{P}_{2n} \setminus \mathcal{P}_n$ divise $\binom{2n}{n}$, puis que $n^{\pi(2n)-\pi(n)} \leq 2^{2n}$.

En déduire que $\pi(n) = \mathcal{O}\left(\frac{n}{\ln n}\right)$.

On a donc obtenu, avec les notation des informaticiens, que $\pi(n) = \Theta\left(\frac{n}{\ln n}\right)$.

Solution de 15 : Encadrement de Tchebychev

FGN 1 3.50 et 51

16

Théorème de Kurschak

Pour quelles valeurs entières $n \geq m$ a-t-on $\sum_{k=m}^n \frac{1}{k} \in \mathbb{N}$?

Solution de 16 : Théorème de Kurschak

FGN 1 3.32

C'est vrai pour $n = m = 1$ et seulement dans ce cas là.

Si $n \geq 2$, on regarde la valuation 2-adique des entiers entre m et n .

On peut supposer $m < n$ et poser $\alpha \geq 1$ la plus grande valuation 2-adique d'entiers entre m et n .

On vérifie que α est atteinte une et une seule fois, sinon, si $m \leq k = 2^\alpha(2r+1) < k' = 2^\alpha(2s+1) \leq n$, alors $2^\alpha(2r+2)$ est aussi entre m et n et ça contredit la maximalité de α .

Donc, sous forme irréductible, $\sum_{k=m}^n \frac{1}{k} = \frac{A}{2^\alpha B}$ où A et B sont impairs et la somme n'est pas entière.

17

Probabilité que deux entiers soient premiers entre eux

Pour $n \geq 1$, on note r_n la probabilité que deux entiers choisis aléatoirement entre 1 et n soient premiers entre eux.

D'autre part, on définit la fonction de Möbius $\mu : \mathbb{N}^* \rightarrow \mathbb{Z}$ par $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier, $\mu(p_1 \cdots p_r) = (-1)^r$ si les p_i sont des nombres premiers deux à deux distincts.

1. Montrer à l'aide de la formule du crible que $r_n = \frac{1}{n^2} \sum_{d|n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$.
2. Calculer $\sum_{d|n} \mu(d)$.
3. Montrer que $r_n \xrightarrow{n \rightarrow +\infty} \frac{6}{\pi^2}$.

Solution de 17 : Probabilité que deux entiers soient premiers entre eux

FGN 1 3.48

1. Si A_n est l'ensemble des couples (a, b) tels que $a \wedge b = 1$ et U_i l'ensemble des couples (a, b) tels que $p_i | a$ et $p_i | b$, alors A_n est le complémentaire de la réunion des U_i où $p_1, \dots, p_k$ sont les nombres premiers inférieurs à n . En appliquant la formule du crible à cette réunion, on obtient la formule attendue.
2. $\sum_{d|n} \mu(d) = \delta_{n,1}$ comme vu dans le TD précédent.
3. Comme $\frac{1}{n^2} \left\lfloor \frac{n}{d} \right\rfloor^2 \sim \frac{1}{d^2}$, on s'intéresse à

$$\left| r_n - \sum_{d=1}^n \frac{\mu(d)}{d^2} \right| \leq \sum_{d=1}^n \left| \frac{1}{d^2} - \frac{1}{n^2} \left\lfloor \frac{n}{d} \right\rfloor^2 \right| \leq \sum_{d=1}^n \left(\frac{2}{dn} + \frac{1}{n^2} \right) = \mathcal{O}\left(\frac{\ln n}{n}\right) \rightarrow 0$$

en utilisant $H_n \sim \ln n$.

Comme $\frac{6}{\pi^2}$ est l'inverse de $\zeta(2)$, on calcule $\sum_{n=1}^{+\infty} \frac{1}{n^2} \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} = \sum_{p=1}^{+\infty} \sum_{d|p} \frac{\mu(d)}{p^2} = 1$ par sommabilité (due deux fois à la convergence de la série de Riemann) et avec la question précédente, ce qui conclut.