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 un 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 : $\mathbb{Z}/2\mathbb{Z}=\{\overline{0},\overline{1}\}$ 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.

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.

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 $(\mathbb{C}^*,\times)$.

4 **Oral ENS** Soit $(G,*)$ un groupe, Aut(G) l'ensemble de ses automorphismes.

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

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 $[a,b]$, i.e. 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 $\forall g\in G,\quad g\,D_G=D_G\,g$.
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 $(xD_G,yD_G)\longmapsto(xy)D_G$ est convenablement définie et munit $\mathcal{Q}_G$ d'une structure de groupe, puis montrer que $x\longmapsto xD_G$ est un morphisme de G dans $\mathcal{Q}_G$.
   (c) Montrer que $\mathcal{Q}_G$ est abélien.

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^km. 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

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

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.

2. Anneaux et idéaux, corps

7 Soit $D=\{x\in\mathbb{Q},\ \exists n\in\mathbb{Z},\quad x\cdot10^n\in\mathbb{Z}\}$ l'anneau des nombres décimaux. Montrer qu'il est principal.

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

Commencer par traiter le cas où ab est nilpotent pour se donner des idées.

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 $(a)\cap(b)$.

10 **Anneau sans idéal non premier** Soit A un anneau commutatif dont tout idéal I est premier ($xy\in I\Longrightarrow x\in I$ ou $y\in I$).
Montrer que A est un corps.

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.

3. Arithmétique entière

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

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) $v(x+y) \geqslant \min(v(x), v(y))$;

(iii) $v(x) = +\infty \iff x = 0$.

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

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 : $n = a_0 + a_1 p + \cdots + a_r p^r$ et on pose $x = a_0 + \cdots + a_r$. Montrer que $v_p(n!) = \dfrac{n-s}{p-1}$.
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 $D(x) \geqslant 0$ pour tout $x \in \mathbb{R}^+$ et en déduire que
$$\frac{(30n)!n!}{(15n)!(10n)!(6n)!} \in \mathbb{N}$$
pour tout $n \in \mathbb{N}$.

15 **Encadrement de Tchebychev**

On note $\mathscr{P}_n$ 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 $\pi(n) \sim \dfrac{n}{\ln n}$.

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

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

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

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

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

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

16 **Théorème de Kurschak** Pour quelles valeurs entières $n \geqslant m$ a-t-on $\displaystyle\sum_{k=m}^{n} \frac{1}{i} \in \mathbb{N}$?

Utiliser la valuation 2-adique.

17 **Probabilité que deux entiers soient premiers entre eux**

Pour $n \geqslant 1$, 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 $\mu : \mathbb{N}^* \to \mathbb{Z}$ 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 $r_n = \dfrac{1}{n^2} \displaystyle\sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^2$.
2. Calculer $\displaystyle\sum_{d \mid n} \mu(d)$.
3. Montrer que $r_n \xrightarrow[n \to +\infty]{} \dfrac{6}{\pi^2}$.