Exercices d'application :

1. Soit G un groupe. On appelle centre de G l'ensemble $Z(G) = \{g \in G | \forall h \in G,\ gh = hg\}$. Montrer que $Z(G)$ est un sous-groupe de G.
2. Soit G un groupe dont tous les éléments $\neq e$ sont d'ordre 2. Montrer que G est commutatif.
3. Donner un exemple de groupe infini dont tous les éléments sont d'ordre fini.
4. Montrer que l'ensemble des bijections continues de $\mathbb{R}$ dans $\mathbb{R}$ est un sous-groupe de $\mathrm{Bij}(\mathbb{R})$.
5. Les bijections dérivables de $\mathbb{R}$ dans $\mathbb{R}$ forment-elles un sous-groupe de $\mathrm{Bij}(\mathbb{R})$?
6. Quels sont les sous-groupes finis de $\mathbb{C}^*$?
7. Soit G un groupe et A une partie finie non vide de G stable par produit. Montrer que A est un sous-groupe de G. (On pourra considérer la suite $(g^n)_{n\in\mathbb{N}^*}$.)
8. Soit A une partie du groupe G et $\varphi : G \to G'$ un morphisme de groupes. Montrer que $\langle \varphi(A)\rangle = \varphi(\langle A\rangle)$.
9. Caractériser les groupes finis d'ordre premier.
10. Soit $s \in S_n$ un cycle. À quelle condition sur $d \in \mathbb{Z}$ s^d est-il un cycle ?
11. Caractériser les groupes G dont les seuls sous-groupes sont G et $\{e_G\}$.
12. Le groupe $\mathbb{Q}$ admet-il une partie génératrice finie ?
13. Soit $(G, *)$ un groupe, H un ensemble et $f : G \to H$ une bijection. Montrer que la loi $\bullet$ sur H définie par $h_1 \bullet h_2 = f(f^{-1}(h_1) * f^{-1}(h_2))$ est une loi de groupe sur H, et que f est alors un isomorphisme de groupes. Application : Montrer que la loi sur $]-1, 1[$ donnée par $x * y = \dfrac{x+y}{1+xy}$ est une loi de groupe commutative.
14. L'ensemble $\mathbb{D}$ des nombres décimaux est-il un sous-anneau de $\mathbb{Q}$? Un sous-corps de $\mathbb{Q}$?
15. Soit A un anneau commutatif intègre et non nul.
    (a) Montrer que si A est fini, A est un corps.
    (b) Montrer que si A n'a qu'un nombre fini d'idéaux, A est un corps. (Considérer $x^n A$.)
16. Soit A un anneau commutatif et I un idéal de A. On appelle radical de I le sous-ensemble de A défini par $\sqrt{I} = \{x \in A | \exists n \in \mathbb{N}, x^n \in I\}$.
    (a) Montrer que $\sqrt{I}$ est un idéal de A.
    (b) Déterminer $\sqrt{\sqrt{I}}$.
    (c) Montrer que si J est aussi un idéal de A, alors $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ et $\sqrt{I+J} \supset \sqrt{I} + \sqrt{J}$.
    (d) Si $A = \mathbb{Z}$, $I = 720\mathbb{Z}$, déterminer $\sqrt{I}$.
17. Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$?
18. Soit E un $\mathbb{F}_3$-espace vectoriel de dimension 5. Combien il y a-t-il de couples $(u, v) \in E^2$ libres ? Combien y a-t-il de bases d'un plan fixé de E ? Combien l'espace vectoriel $\mathbb{F}_3^5$ contient-il de plans ?
19. Déterminer les polynômes irréductibles de $\mathbb{Z}/2\mathbb{Z}[X]$ de degré $\leqslant 5$.
20. Soit $S_p = \sum_{k=1}^{n} a_k^p$. Exprimer S_2 et S_3 en fonction des fonctions symétriques élémentaires en les a_k.
21. Sous la dynastie des Tang, au 7^e siècle en Chine, l'empereur voulut connaitre le nombre exact des ses soldats. Bien qu'il en eût un nombre presque innombrable, il savait qu'il en avait moins d'un million. Il fit alors ranger ses soldats en carrés de 29 personnes de côté. Il en resta 180. Il les fit alors se ranger en carrés de 35 personnes de côté. Il en resta alors 1120.
    Combien de soldats avait l'armée de l'empereur ?

Exercice 1 :

1. Soit G un groupe et g un élément de G. Soit φ_g l'application de G dans G définie par $h \longmapsto ghg^{-1}$. Montrer que φ_g est un automorphisme de groupes. Si le groupe G est commutatif, que vaut φ_g ?
2. Soit $\mathrm{Aut}(G)$ l'ensemble des automorphismes de groupes de G. Montrer que $\mathrm{Aut}(G)$ est un groupe pour $\circ$.
3. Soit $\varphi : G \to \mathrm{Aut}(G)$ définie par $\varphi(g) = \varphi_g$. Montrer que φ est un morphisme de groupes. À quelle condition sur le centre $Z(G)$ de G est-il injectif ?

Exercice 2 : Soit $n \in \mathbb{N}^*$ et $\tau \in S_n$. Déterminer les permutations qui commutent à τ (c'est le centralisateur de τ dans S_n). En déduire le centre de S_n.

Exercice 3 ** : À quelle condition les groupes $\mathbb{Z}^n$ et $\mathbb{Z}^p$ sont-ils isomorphes ?

Exercice 4 * – Un théorème de Cayley : Soit G un groupe fini. Pour tout $g \in G$, on note $L_g : G \to G$ l'application $h \mapsto gh$. Soit L l'application $g \mapsto L_g$.

1. Montrer que L est un morphisme injectif de groupes de G vers S_G.
2. En déduire que tout groupe fini est isomorphe à un sous-groupe d'un groupe S_n.
3. Montrer que tout groupe fini est isomorphe à un sous-groupe de $O_n(\mathbb{R})$ (et même $SO_n(\mathbb{R})$) pour un certain $n \in \mathbb{N}^*$.

Exercice 5 * – Groupe dérivé : Soit G et H deux groupes et $\varphi : G \to H$ un morphisme de groupes. Pour tous $a, b \in G$, on note $[a,b] = aba^{-1}b^{-1}$, appelé commutateur de a et b. Soit $\mathcal{D}(G)$ l'ensemble des produits de commutateurs d'éléments de G.

1. Montrer que $\mathcal{D}(G)$ est un sous-groupe de G. Montrer que G est commutatif si et seulement si $\mathcal{D}(G) = \{e_G\}$.
2. Montrer que $\operatorname{Ker}\varphi$ contient $\mathcal{D}(G)$ si et seulement si $\operatorname{Im}\varphi$ est commutatif.
3. Montrer que $D(G)$ est un sous-groupe distingué de G, *i.e.* pour tout $g \in G$ et tout $x \in D(G)$, $gxg^{-1} \in D(G)$.
4. Déterminer le groupe dérivé de S_n où $n \geqslant 3$. (Indication : montrer que $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ appartient à $D(S_n)$ et utiliser la question précédente.)
5. Déterminer le groupe dérivé de $GL_n(\mathbb{C})$. (On pourra admettre que $SL_n(\mathbb{C})$ est engendré par les transvections $T_{i,j}(\lambda)$.)

Exercice 6 * : Soit $n \in \mathbb{N}^*$. On munit S_n de la probabilité uniforme et on note p_n la probabilité qu'une permutation aient tous ses cycles sont de longueur $\leqslant n/2$ dans la décompostion en produit de cycles à support disjoints. Calculer p_n et étudier sa limite.

Exercice 7 * : Montrer que $\mathbb{Z}$, $\mathbb{Z}^2$, $\mathbb{Q}$ et $\mathbb{Q}_+^*$ ne sont pas isomorphes en tant que groupes.

Exercice 8 * – Autres générateurs de S_n :

1. Soit $n \geqslant 2$ et $\tau_i = (i\ i+1) \in S_n$ avec $1 \leqslant i \leqslant n-1$. Montrer que toute permutation $s \in S_n$ s'écrit comme produit des τ_i.
2. Montrer que S_n est engendré par $\begin{pmatrix}1 & 2\end{pmatrix}$ et le n-cycle $\begin{pmatrix}1 & 2 & \cdots & n\end{pmatrix}$.

Exercice 9 * : Soit $n \geqslant 2$.

1. Déterminer tous les morphismes de groupes $\varphi : S_n \to \mathbb{Z}$.
2. Déterminer tous les morphismes de groupes $\varphi : S_n \to \mathbb{C}^*$.

Exercice 10 * : Le n-cycle $\begin{pmatrix}1 & 2 & \cdots & n\end{pmatrix}$ admet-il une racine carrée dans S_n ?

Exercice 11 * : On munit $E = \mathbb{R}^n$ de son produit scalaire usuel et G un sous-groupe de $GL_n(\mathbb{R})$. On suppose qu'il existe $k \in]0,2[$ tels que toute matrice M de G vérifie $|||M - I_n||| < k$.

1. Montrer que toute valeur propre complexe de M est de module 1.
2. Montrer qu'il existe un entier p tel que toute matrice M de G vérifie $M^p = I_n$.

Exercice 12 * : Soit G un groupe fini de cardinal n. Montrer qu'il existe une partie génératrice S de G telle que $\operatorname{Card} S \leqslant \log_2(n)$.

Exercice 13 – Homographies : Soit $\mathbb{H} = \{z \in \mathbb{C} \,/\, \operatorname{Im} z > 0\}$. Pour tout $M = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in SL_2(\mathbb{R})$, on considère l'application φ_M

$$\begin{cases} \varphi_M : \mathbb{H} & \longrightarrow & \mathbb{H} \\ z & \longmapsto & \dfrac{az+b}{cz+d}. \end{cases}$$

Une telle application s'appelle une *homographie*. On note G l'ensemble des homographies, *i.e.*

$$G = \{\varphi_M \,/ M \in SL_2(\mathbb{R})\}.$$

1. Soit $M \in SL_2(\mathbb{R})$. Montrer que l'application φ_M est bien définie et vérifie $\varphi(MN) = \varphi_M \circ \varphi_N$ pour tous $M, N \in SL_2(\mathbb{R})$.
2. En déduire que G est un groupe pour la composition $\circ$, que $M \mapsto \varphi_M$ est un morphisme de groupe. Montrer que φ_M est bijective et donner une expression de sa réciproque.
3. Montrer que G est engendrée par les fonctions de la forme

$$z \mapsto -\frac{1}{z}, \qquad z \mapsto z + t, \qquad z \mapsto kz$$

où $t \in \mathbb{R}$ et $k > 0$.

4. Pour $\theta \in \mathbb{R}$, on pose $R_\theta = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$ et $r_\theta = \varphi_{R_\theta}$. Montrer que l'application $\varphi : \mathbb{R} \to G$ donnée par $\theta \mapsto r_\theta$ est un morphisme de groupes. Déterminer son noyau.

Exercice 14 : Quels sont les deux derniers chiffres décimaux de $7^{7^{7^{7^{7^{7}}}}}$?

Exercice 15 * – Théorème de Wilson : Montrer qu'un entier $p \geqslant 2$ est premier si et seulement si $(p-1)! + 1 \equiv 0 \mod p$.

Exercice 16 : Soient $m, n \in \mathbb{N}$. Montrer que $mn(m^{60} - n^{60})$ est divisible par 56786730.

Exercice 17 – Nombres de Fermat, de Mersenne et d'Euclide :

1. Soit $2^n - 1$ un nombre premier. Montrer que n est premier. (Les nombres premiers de cette forme sont appelés nombres de Mersenne. Quelle est la particularité de leur développement en base 2 ?)

2. On appelle nombre d'Euclide e_n les nombres définis par récurrence par $e_1 = 2$ et $e_{n+1} = e_1 e_2 \cdots e_n + 1$. Montrer que deux nombres d'Euclide distincts sont premiers entre eux. En combien d'étape l'algorithme d'Euclide appliqué à deux nombres d'Euclide termine-t-il ? En déduire qu'il existe une infinité de nombres premiers.
3. Soit $2^n + 1$ un nombre premier. Montrer que n est une puissance de 2.
   On appelle nombre de Fermat F_n les nombres de la forme $2^{2^n} + 1$. Montrer que deux nombres de Fermat distincts sont premiers entre eux.

Exercice 18 – Critère de primalité de Fermat : Montrer que n est composé si et seulement s'il existe un entier a tel que $1 < a < n$ et $a^{n-1} \neq 1 \mod n$. (Un tel a s'appelle un *témoin de Fermat*. Il fournit un certificat de non-primalité pour n.)

Exercice 19 : Une fonction $f : \mathbb{N} \to \mathbb{R}$ est dite *multiplicative* si pour tout couple (m, n) d'entiers premiers entre eux, $f(mn) = f(m)f(n)$.

1. Montrer que f est multiplicative si et seulement si $m \mapsto g(m) = \sum_{d|m} f(d)$ est multiplicative.
2. En déduire que les fonctions φ (indicatrice d'Euler), S (somme des diviseurs) et τ (nombre de diviseurs) sont multiplicatives.

Exercice 20 *– Nombres parfaits pairs : Pour $n \in \mathbb{N}^*$, on note $S(n)$ la somme des diviseurs dans $\mathbb{N}^*$ de n. Un nombre est parfait si $S(n) = 2n$.

1. Montrer que S est multiplicative, *i.e.* si m et n sont premiers entre eux, alors $S(mn) = S(m)S(n)$.
2. Soit $p \in \mathbb{N}$ tel que $2^p - 1$ est premier. Montrer que $2^{p-1}(2^p - 1)$ est parfait (théorème d'Euclide).
3. Soit n parfait et pair. Montrer que n s'écrit $n = 2^{p-1}(2^p - 1)$ où $(2^p - 1)$ est premier (théorème d'Euler).

Exercice 21 :

1. On note $\mathcal{D}(n)$ l'ensemble des diviseurs (positifs) de l'entier n. Soient $a, b \in \mathbb{N}^*$ premiers entre eux et $n = ab$. Montrer que l'application $\mathcal{D}(a) \times \mathcal{D}(b) \longmapsto \mathcal{D}(ab)$ définie par $(k, l) \mapsto kl$ est une bijection.
2. Soit $S(n)$ (resp. $\tau(n)$) la somme des diviseurs (resp. le nombre de diviseurs) de l'entier n. Montrer que si n et m sont premiers entre eux, $S(nm) = S(n)S(m)$ et $\tau(nm) = \tau(n)\tau(m)$.

Exercice 22 * : Soient $a, b \in \mathbb{Z}$.

1. À quelle condition nécessaire et suffisante portant sur a et b a-t-on $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ cyclique ?
2. Déterminer tous les morphismes de $\mathbb{Z}/a\mathbb{Z}$ vers $\mathbb{Z}/b\mathbb{Z}$.

Exercice 23 * : Soit $P \in \mathbb{R}[X]$. Montrer l'équivalence entre :

1. Pour tout $x \in \mathbb{R}$, $P(x) \geqslant 0$;
2. Il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + B^2$.

Exercice 24 * :

1. Soit $P \in \mathbb{R}[X]$ scindé. Montrer que P' est scindé.
2. Soit $P \in \mathbb{R}[X]$ scindé. Montrer que pour tout $\alpha \in \mathbb{R}$, $\alpha P + P'$ est scindé sur $\mathbb{R}$.

Exercice 25 * :

1. Montrer que les automorphismes de la $\mathbb{K}$-algèbre $\mathbb{K}[X]$ sont exactement les applications $P \mapsto P(aX + b)$ où $(a, b) \in \mathbb{K}^* \times \mathbb{K}$.
2. (**) Montrer que les automorphismes de la $\mathbb{K}$-algèbre $\mathbb{K}(X)$ sont exactement les applications $F \mapsto F\left(\dfrac{aX + b}{cX + d}\right)$ où $a, b, c, d \in \mathbb{K}$ avec $ad - bc \neq 0$.

Exercice 26 * :

1. Comment déterminer si un polynôme de $\mathbb{C}[X]$ admet une racine multiple ? (On ne sait pas déterminer les racines en général.)
2. Soit $P \in \mathbb{Q}[X]$ irréductible. Montrer que P n'a pas de racine multiple dans $\mathbb{C}$.
3. Soit $P \in \mathbb{Q}[X]$ de degré 5 admettant une racine multiple dans $\mathbb{C}$. Montrer que P admet une racine dans $\mathbb{Q}$.

Exercice 27 ** : Soient $P, Q \in \mathbb{R}[X]$.

1. On suppose que P et Q sont scindés à racines simples et que leurs racines sont entrelacées, *i.e.* entre deux racines de l'un, il y a une racine de l'autre. Montrer que pour tous $\lambda, \mu \in \mathbb{R}$ le polynôme $\lambda P + \mu Q$ est scindé à racines simples.
2. Montrer que si pour tous $\lambda, \mu \in \mathbb{R}$, le polynôme $\lambda P + \mu Q$ est scindé à racines simples, alors les racines de P et Q sont entrelacées.

Exercice 28 * :

1. Soit $P \in \mathbb{C}[X]$. Étudier l'injectivité et la surjectivité de $P : \mathbb{C} \to \mathbb{C}$.
2. Soit $F \in \mathbb{C}(X)$ non constant. Montrer que $F(\mathbb{C})$ est soit $\mathbb{C}$, soit $\mathbb{C}$ privé d'un point.

Exercice 29 ** : Soit $n \in \mathbb{N}^*$ et $E = \mathbb{R}_n[X]$.

1. Soient $h_0, h_1, ..., h_n$ des réels distincts. Montrer que la famille $((X+h_i)^n)_{0\leqslant i\leqslant n}$ est une base de E. On notera $\theta_h : P \mapsto P(X+h)$.
2. Soit $\mathcal{A} = \{\phi \in \mathcal{L}(E) \,|\, \forall h \in \mathbb{R}, \forall P \in E, \phi(P(X+h)) = (\phi(P))(X+h)\}$. Montrer que $\mathcal{A}$ est une sous-algèbre de dimension $n+1$ de $\mathcal{L}(E)$.

Exercice 30 * :

1. Montrer l'existence et l'unicité d'un $P_n \in \mathbb{R}[X]$ tel que pour tout $t \in \left]0, \frac{\pi}{2}\right[$:
$$P_n(\cot^2 t) = \frac{\sin(2n+1)t}{\sin^{2n+1} t}.$$
2. Déterminer les racines de P_n, leur multiplicité et leur somme.
3. Établir que pour tout $t \in \left]0, \frac{\pi}{2}\right[$ $\sin t \leqslant t \leqslant \tan t$ et $\cot^2 t \leqslant \frac{1}{t^2} \leqslant 1 + \cot^2 t$.
4. En déduire $\displaystyle\sum_{k=1}^{+\infty} \frac{1}{k^2}$.

Exercice 31 : Soit $E = \mathbb{R}_n[X]$ et $(P \mid Q) = \displaystyle\int_{t=0}^{1} P(t)Q(t)\,dt$.

1. Montrer que E muni de $(\ |\ )$ est un espace euclidien.
2. Soit $K = \mathbb{R}_{n-1}[X]^\perp$ et $P \in K \setminus \{0\}$. Quel est le degré de P ?
3. Soit Φ : $x \mapsto \displaystyle\int_{t=0}^{1} P(t)t^x\,dt$. Montrer que Φ est une fonction rationnelle.
4. Trouver Φ à une constante multiplicative près.
5. En déduire les coefficients de P.
6. En déduire une base orthogonale de E.

Exercice 32 * : Soit $M \in \mathcal{M}_n(\mathbb{C})$. On rappelle que $\mathbb{C}[M]$ désigne l'algèbre des polynômes en M.

1. Caractériser les inversibles de l'anneau $\mathbb{C}[M]$.
2. Caractériser les diviseurs de zéro de $\mathbb{C}[M]$. (Un diviseur de 0 d'un anneau commutatif A est un élément non nul a pour lequel il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.)
3. Caractériser les éléments nilpotents de $\mathbb{C}[M]$.

Exercice 33 ** : Montrer que les algèbres $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$ et $\mathcal{C}^1(\mathbb{R}, \mathbb{R})$ ne sont pas isomorphes.

Exercice 34 : Soit A un anneau commutatif.

1. Soit I un idéal de A et $\mathcal{R}$ la relation sur A définie par $x\mathcal{R}y$ si et seulement si $x - y \in I$. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Soit $\mathcal{R}$ un relation d'équivalence sur A compatible avec la somme et le produit. Montrer que la classe d'équivalence de 0 est un idéal.

Exercice 35 * : Soit K un corps fini commutatif. Montrer que $\operatorname{Card} K$ est de la forme p^n où p est premier et $n \in \mathbb{N}^*$. (Indication : montrer que K est un espace vectoriel sur son sous-corps premier.)

Exercice 36 ** : Une algèbre de Boole A est une anneau tel que $x^2 = x$ pour tout $x \in A$.

1. Montrer que $(\mathbb{Z}/2\mathbb{Z})^n$ est une algèbre de Boole.
2. Montrer que tout élément est son propre opposé.
3. On suppose que A est une algèbre de Boole intègre. Montrer que A est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ en tant qu'algèbre.
4. Montrer qu'une algèbre de Boole est naturellement munie d'un structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. En déduire le cardinal d'une algèbre de Boole finie.
5. Déterminer le nombre d'idéaux d'une algèbre de Boole finie.

Exercice 37 * : Existe-t-il un sous-corps $\mathbb{K}$ de $\mathbb{R}$ tel que $\mathbb{R}$ soit un $\mathbb{K}$-espace vectoriel de dimension 2 ?

Exercice 38 ** : Montrer que $\alpha \in \mathbb{C}$ est algébrique si et seulement si $\mathbb{Q}[\alpha]$ est une $\mathbb{Q}$-algèbre de dimension finie. Montrer que l'ensemble $\overline{\mathbb{Q}}$ des nombres algébriques est un sous-corps de $\mathbb{C}$.

Exercice 39 : Soit H une partie finie non-vide de $GL(n, \mathbb{R})$ stable par multiplication.

1. Soit $M \in H$. Montrer que la suite $k \mapsto M^k$ n'est pas injective. En déduire que H est un sous-groupe de $GL(n, \mathbb{R})$.
2. Soit $q = \operatorname{Card} H$ et $P = \frac{1}{q}\displaystyle\sum_{M\in H} M$. Montrer que pour tout $M \in H$, $MP = PM = P$. En déduire que $P^2 = P$.
3. Trouver un supplémentaire dans $\mathbb{R}^n$ de $\displaystyle\bigcap_{M\in H} \ker(M - I_n)$ stable par tous les éléments de H.

Exercice 40 ** : Soit $M \in \mathcal{M}_n(\mathbb{R})$ à coefficients entiers, avec $[M]_{i,i}$ impair pour tout i et $[M]_{i,j}$ pair pour tous $i \neq j$. Montrer que M est inversible.

Travaux dirigés 1 – Indicatrice d'Euler

1. Déterminer $\mathrm{Card}\,(\mathbb{Z}/n\mathbb{Z})^*$.
2. Quels sont les deux derniers chiffres décimaux de 3^{2020} ?
3. * Déterminer $\sum_{k|n} \varphi(k)$. (Indication : on pourra considérer l'ensemble $\{k/n | 1 \leqslant k \leqslant n\}$ et regrouper les éléments selon les dénominateurs.)
4. * Montrer que $\lim \varphi(n) = +\infty$. (Indication : on pourra considérer l'équation $\varphi(n) = k$ d'inconnue n.)
5. ** Établir que pour tout $n \in \mathbb{N}^*$,

$$n \geqslant \varphi(n) \geqslant \frac{n}{\frac{\ln(n)}{\ln(2)} + 1}.$$

Travaux dirigés 2 – Sous-groupe multiplicatif d'un corps fini

Soit G un groupe fini commutatif. Pour tout $x \in G$, on note $O(x)$ l'ordre de x.

1. Soient $x, y \in G$, $m = O(x)$, $n = O(y)$. On suppose que m et n sont premiers entre eux. Montrer que $O(xy) = mn$. Peut-on ôter l'hypothèse sur m et n ?
2. Soient $m, n \in \mathbb{N}^*$. Montrer l'existence de $p, q \in \mathbb{N}^*$ tels que $p|m$, $q|n$, $p \wedge q = 1$ et $ppcm(m, n) = pq$.
3. Montrer qu'il existe $z \in G$ dont l'ordre est le *ppcm* des ordres des éléments de G.
4. Soit K un corps et G un sous-groupe fini du groupe K^*. Montrer que G est cyclique.

Travaux dirigés 3 – Matrices de permutations

Soit n un entier positif. On note $(e_1, e_2, \ldots, e_n)$ la base canonique de $\mathbf{R}^n$ et $\mathcal{M}(n, \mathbf{R})$ l'ensemble des matrices carrées $n \times n$ à coefficients réels. On note S_n le groupe symétrique d'ordre n.

On définit l'application : $\left\{ \begin{array}{c} \Phi : S_n \longrightarrow \mathcal{M}(n, \mathbf{R}) \\ \sigma \longmapsto M_\sigma \end{array} \right.$ par $M_\sigma(e_i) = e_{\sigma(i)}$. Les M_σ s'appellent matrices de permutations.

1. Ecrire les matrices M_σ lorsque σ appartient à S_2 et S_3.
2. Montrer que l'application $\sigma \mapsto M_\sigma$ du groupe $(S_n, \circ)$ dans le groupe $GL(n, \mathbb{Q})$ est un morphisme injectif.
3. Montrer que la signature ε sur S_n est égale à $\det \circ \Phi$.
4. Soit $s \in S_n$. Déterminer le polynôme caractéristique et minimal de M_s en fonction de la décomposition en produit de cycles à supports disjoints de s. Quelles sont les matrices de permutations diagonalisables sur $\mathbb{C}$?
5. Quelles sont les matrices de permutations diagonalisables sur $\mathbb{R}$?

Travaux dirigés 4 – Un théorème de Cauchy

Soit p un nombre premier et G un groupe fini de cardinal n divisible par p. Soit

$$A = \{(x_1, \ldots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = 1_G\}.$$

On considère les indices $1, \ldots, p$ comme des éléments de $\mathbb{Z}/p\mathbb{Z}$.

1. Déterminer le cardinal de A.
2. Montrer que l'application $f : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Bij}(A)$ définie par $f(k)(x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{p+k})$ est un morphisme de groupes. (On dit que $\mathbb{Z}/p\mathbb{Z}$ "opère" sur l'ensemble A. Si $x = (x_1, \ldots, x_p)$, on note en général $k \cdot x$ à la place de $f(k)(x)$.)
3. Montrer que les orbites n'ont que deux cardinaux possibles.
4. Soit $\mathrm{Stab}(x)$ le stabilisateur de x dans $\mathbb{Z}/p\mathbb{Z}$, à savoir $\{k \in \mathbb{Z}/p\mathbb{Z} \mid k \cdot x = x\}$. Montrer "l'équation aux classes" :

$$|A| = \sum_{x \in \Omega} \frac{p}{|\mathrm{Stab}(x)|}$$

où Ω désigne un ensemble de représentant de chaque orbite.

5. En déduire que G contient un élément d'ordre p.

Travaux dirigés 5 – Complexité de l'algorithme d'Euclide

On rappelle que la suite de Fibonacci $(F_n)_n$ est l'unique suite vérifiant $F_0 = 0$, $F_1 = 1$ et pour tout entier naturel n, $F_{n+2} = F_{n+1} + F_n$.

1. Déterminer les racines réelles de $X^2 - X - 1$. On désignera par φ la plus grande et $\widehat{\varphi}$ la plus petite. Montrer que les suites $(\varphi^n)_n$ et $(\widehat{\varphi}^n)_n$ vérifie la même relation de récurrence que F_n.
2. Déterminer deux réels λ et μ tels que pour tout entier n, $F_n = \lambda\varphi^n + \mu\widehat{\varphi}^n$. En déduire que $F_n = \lfloor \frac{1}{\sqrt{5}}\varphi^n + \frac{1}{2} \rfloor$.
3. Soit $n \geqslant 2$. Montrer que le calcul du *pgcd* de F_{n+1} et F_n par l'algorithme d'Euclide nécessite exactement $n - 1$ divisions euclidiennes (*i.e.* le premier reste nul est obtenu à la $(n-1)^{\mathrm{e}}$ division). Quel est ce *pgcd* ?
4. Démontrer le théorème de Lamé :

Théorème de Lamé *Soient a et b deux entiers tels que $0 < b < a$ et de pgcd d. Montrer que si l'algorithme d'Euclide s'arrête au bout de $n - 1$ divisions, on a*

$$a \geqslant dF_{n+1}, \qquad b \geqslant dF_n.$$

5. Soit $N(a,b)$ le nombre de divisions euclidiennes à effectuer pour déterminer le *pgcd* de a et b par l'algorithme d'Euclide. En déduire qu'il existe deux constantes réelles (à préciser) α et β telles que pour tous les entiers $a, b \in \mathbb{N}^*$ avec $a > b > 0$, $N(a,b) \leqslant \alpha \ln b + \beta$.

Travaux dirigés 6 – Le grand théorème de Fermat pour les polynômes

Soit P un polynôme non-nul de $\mathbb{C}[T]$ et $\mathcal{A}$ l'ensemble des racines complexes de P (comptées sans multiplicités). On définit le *radical* de P par $\operatorname{rad} P = 1$ si $\deg P = 0$ et $\operatorname{rad} P = \prod_{\alpha \in \mathcal{A}} (T - \alpha)$ sinon. Soit $r(P)$ le nombre de racines distinctes complexes de P. On considère trois polynômes non-nuls P, Q, R de $\mathbb{C}[T]$.

1. Montrer que $r(P) = \deg \operatorname{rad} P$ et $r(PQR) \leqslant \deg P + \deg Q + \deg R$.
2. On cherche à montrer le théorème de Mason : Si P, Q, R sont trois polynômes premiers entre eux dans leur ensemble dans $\mathbb{C}[T]$ et non-constants tels que $P + Q + R = 0$ alors
$$\max(\deg P, \deg Q, \deg R) \leqslant r(PQR) - 1.$$
On suppose dans cette question que P, Q, R sont comme dans l'énoncé du théorème.
   (a) Soit $\Delta = PQ' - P'Q$. Montrer que Δ est non-nul et que $\Delta = R'Q - RQ' = P'R - PR'$.
   (b) On écrit $P = \lambda \prod_{1 \leqslant i \leqslant p} (T - \alpha_i)^{l_i}$. Montrer que $\prod_{1 \leqslant i \leqslant p} (T - \alpha_i)^{l_i - 1}$ divise Δ.
   (c) Montrer que $(\deg P - p) + (\deg Q - q) + (\deg R - r) \leqslant \deg P + \deg Q - 1$.
   (d) En déduire que $\deg R \leqslant r(PQR) - 1$, puis le théorème de Mason.
3. En déduire le théorème de Liouville (Fermat pour les polynômes) : pour tout entier $n \geqslant 3$, l'équation
$$X^n + Y^n = Z^n$$
n'admet aucune solution dans $\mathbb{C}[T]$ avec X, Y, Z non-constants et premiers entre eux.

Travaux dirigés 7 – Congruences modulo un polynôme

Soit $Q \in \mathbb{K}[X]$ un polynôme de degré $n \geqslant 2$. Soit E_Q le sous-espace de $\mathbb{K}[X]$ formé des polynômes de degrés strictement inférieur à n.

On dit que $P_1, P_2 \in \mathbb{K}[X]$ sont congrus *modulo* Q si Q divise $P_1 - P_2$ et on note alors $P_1 \equiv P_2 \mod Q$. On note Φ l'application de $\mathbb{K}[X]$ dans lui-même qui associe à P son reste dans la division euclidienne par Q.

1. (a) Montrer que la relation "$\equiv \mod Q$" est une relation d'équivalence.
   (b) Soient $A, B \in \mathbb{K}[X]$. Montrer que $\Phi(A) = B$ si et seulement si $A \equiv B \mod Q$ et $\deg B < n$.
   (c) Montrer que Φ est un endomorphisme. Déterminer son image et son noyau. Montrer que $\operatorname{Ker} \Phi$ et $\operatorname{Im} \Phi$ sont supplémentaires.
   (d) L'application Φ est-elle un morphisme de $\mathbb{K}$-algébres ?
2. *L'anneau* $\mathbb{K}[X]/(Q) = E_Q$. On pose pour tous $A, B \in E_Q$: $A \star B = \Phi(AB)$.
   (a) Montrer que $(E_Q, +, \star)$ est une $\mathbb{K}$-algébre commutative.
   (b) Montrer que si Q est irréductible sur $\mathbb{K}$, alors E_Q est un corps.
   (c) Montrer que si Q n'est pas irréductible sur $\mathbb{K}$, alors E_Q n'est pas intégre.
   (d) Soit $A \in E_Q$. Déterminer l'image de l'endomorphisme $f_A : P \mapsto A \star P$ de E_Q. *(Difficile.)*
3. Exemple 1. On suppose $\mathbb{K} = \mathbb{R}$ et $Q = X^2 + 1$. Montrer que E_Q est isomorphe en tant que corps à $\mathbb{C}$.
4. Exemple 2. On suppose $\mathbb{K} = \mathbb{Q}$. On se propose de construire sans utiliser $\mathbb{R}$ ou $\mathbb{C}$ un corps qui contient $\mathbb{Q}$ et une racine de tout polynôme Q à coefficients rationnels. Ceci permet de faire du calcul exact sur les nombres algébriques uniquement en manipulant des entiers. C'est par exemple ce que font Maple et Sage. On prend ici l'exemple $Q = X^3 + X + 1$.
Montrer que E_Q est un corps qui contient $\mathbb{Q}$ et dans lequel le polynôme $T^3 + T + 1$ a une racine.
5. Exemple 3. Montrer qu'il existe un corps à 16 et 32 éléments. (Prendre $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$.)

Travaux dirigés 8 – Groupes linéaires sur un corps fini

1. Soit $\varphi : G \to G'$ un morphisme de groupes où G est un groupe fini. Montrer que $\operatorname{Card}(\operatorname{Ker} \varphi) \operatorname{Card}(\operatorname{Im} \varphi) = \operatorname{Card} G$.
2. Soit $\varphi : G \to G$ un morphisme de groupes où G est un groupe fini. Montrer que $\operatorname{Ker} \varphi = \operatorname{Ker} \varphi^2$ si et seulement si $\operatorname{Im} \varphi = \operatorname{Im} \varphi^2$.
3. Soit K un corps de cardinal q. Calculer $\operatorname{Card} GL(n, K)$ et $\operatorname{Card} SL(n, K)$. Reconnaitre le groupe $GL(2, \mathbb{F}_2)$.
4. Soit $P(K^n)$ l'ensemble des droites vectorielles de K^n. Déterminer son cardinal. Déterminer de même le nombre de sous-espaces vectoriels de dimension p.
5. Soit H le groupe des bijections de $P(K^n)$. Montrer que l'application Φ : $GL(n, K) \to H$ définie par $\Phi(g)(d) = g(d)$ (où $g \in GL(n, K)$ et $d \in P(K^n)$) est un morphisme de groupe. Si G est un sous-groupe de $GL(n, K)$, on note PG son image. Reconnaitre les groupes $PGL(2, \mathbb{F}_p)$ et $PSL(2, \mathbb{F}_p)$ pour $p = 2, 3, 5$.

Travaux dirigés 9 – Sous-groupes de Frattini

Soit G un groupe fini. Si A est une partie de G, on note $\langle A\rangle$ le groupe engendré par A. Un élément $g \in G$ est *mou* si pour toute partie $A \subset G$ contenant g, $\langle A\rangle = G$ implique $\langle A \setminus \{g\}\rangle = G$. On Frat$(G)$ l'ensemble des éléments mous de G.

1. Montrer que Frat(G) est un sous-groupe de G. (On pourra remarquer qu'ajouter un élément mou à une partie non génératrice ne la rend pas génératrice.)
2. Vérifier que Frat(G) est l'intersection des sous-groupes propres maximaux pour l'inclusion de G.
3. Déterminer Frat(G) lorsque $G = S_n$. (On commencera par trouver suffisamment de sous-groupes maximaux de S_n.)
4. Déterminer Frat(G) lorsque $G = \mathbb{Z}/n\mathbb{Z}$.

Indications

Exercice 3. Si et seulement si $n = p$: considérer une partie génératrice minimale.

Exercice 5. 4. Se rappeler que les 3-cycles engendrent A_n.
5. La réponse est $SL_n(\mathbb{C})$; il suffit d'écrire toute transvection comme un commutateur.

Exercice 6. $s \in S_n$ a au plus un cycle de longueur $> n/2$.

Exercice 7. Certains éléments de $\mathbb{Q}_+^*$ n'admettent pas de racines carrées.

Exercice 9. 1. $\operatorname{Im}\varphi$ est un sous-groupe de $\mathbb{Z}$.
2. Montrer que toute transposition est de la forme $s \circ (1\ 2) \circ s^{-1}$ où $s \in S_n$.

Exercice 12. Utiliser la caractérisation interne d'une partie génératrice.

Exercice 15. Regrouper chaque élément de $(\mathbb{Z}/p\mathbb{Z})^*$ avec son inverse.

Exercice 17. 1. Utiliser une identité remarquable $a^n - b^n = \ldots$.
2. Pour l'existence d'une infinité de nombres premiers, considérer un diviseur premier de chaque e_i.
3. Utiliser encore une identité remarquable. Puis regarder *modulo* un diviseur des deux.

Exercice 21. 1. On pourra montrer que $\operatorname{pgcd}(uv, uw) = u\operatorname{pgcd}(v, w)$ ou utiliser la décomposition en facteurs premiers.

Exercice 22. 1. Déterminer l'ordre d'un élément $(\bar{k}, \bar{l})$.
2. Considérer l'image du morphisme, qui est un sous-groupe de $\mathbb{Z}/b\mathbb{Z}$.

Exercice 23. Commencer par regarder deux cas particuliers : P scindé sur $\mathbb{R}$ et P sans racines réelles.

Exercice 24. 1. Considérer les multiplicités puis appliquer le lemme de Rolle.
2. Multiplier par $e^{\alpha t}$.

Exercice 25. 1. Un tel morphisme est déterminé par l'image de X.
2. Montrer qu'un tel automorphisme Φ est de la forme $F \mapsto F \circ G$ et considérer un antécédent de X.

Exercice 27. 1. Utiliser le théorème des valeurs intermédiaires.
2. Commencer par montrer que P et Q n'ont pas de racine commune, puis raisonner comme précédemment.

Exercice 29. 1. Écrire le déterminant de la famille dans la base canonique.
2. On pourra remarquer que $\phi \in \mathcal{A}$ est uniquement déterminée par l'image de X^n.

Exercice 31. Utiliser pleinement le cours sur les fractions rationnelles.

Exercice 33. Comparer les carrés.

Exercice 37. La réponse est non ; choisir une bonne base.

Exercice 38. Vérifier que $\operatorname{Vect}((\alpha+\beta)^k)_{k\in\mathbb{N}}$ et $\operatorname{Vect}((\alpha\beta)^k)_{k\in\mathbb{N}}$ sont des $\mathbb{Q}$-espaces vectoriels.

Exercice 40. Réduire modulo 2.

Solutions

Exercice 3. Montrons par l'absurde que si $n \neq p$, alors il n'existe pas d'isomorphisme de groupe f de $\mathbb{Z}^n$ dans $\mathbb{Z}^p$. On peut supposer $n < p$. On introduit la base canonique $(e_i)_{1\leqslant i\leqslant n}$ de $\mathbb{R}^n$. Soit $g \in \mathcal{L}(\mathbb{R}^n, \mathbb{R}^p)$ l'unique application linéaire telle que $g(e_i) = f(e_i)$ pour tout i ; g existe car $(e_i)_{1\leqslant i\leqslant n}$ est une base. Puisque f est un morphisme surjectif de groupe, f et g coïncident sur $\mathbb{Z}^n$. En particulier, l'image de g contient une base de $\mathbb{Z}^p$. On a trouvé une application linéaire surjective d'un espace de dimension n vers un espace de dimension p, ce qui contredit la formule du rang.

Exercice 16. On $56786730 = 2\times3\times5\times7\times11\times13\times31\times61$. Pour chaque facteur premier, on a $\varphi(p)|60$.

Exercice 20. 3. On écrit $n = 2^{p-1}q$ avec $p \geqslant 2$ et q impair. Alors $2^p q = 2n = S(n) = S(2^{p-1})S(q) = (2^p-1)S(q)$. Donc $S(q) = \dfrac{2^p}{2^p-1}q = q + \dfrac{q}{2^p-1}$. Mais alors, $2^p - 1$ divise q. Puisque q et $\dfrac{q}{2^p-1}$ sont deux diviseurs distincts de q, ce sont les seuls et q est premier et vaut $2^p - 1$.

Exercice 21. 1. (Sans utiliser la décomposition en facteurs premiers.) On sait que $\mathrm{pgcd}(uv, uw) = u\mathrm{pgcd}(v, w)$. Notons $f : (k, l) \mapsto kl$ et $g : m \mapsto (a \wedge m, b \wedge m)$. Si m divise ab, on a

$$\begin{aligned} f\circ g(m) &= (a\wedge m)(b\wedge m) = \big(b(a\wedge m)\big) \wedge \big((m(a\wedge m)\big) \\ &= \big((ba)\wedge(bm)\big) \wedge \big((ma)\wedge(m^2)\big) = m[\big((ab/m)\wedge b\big)\wedge\big(a\wedge m\big)] = m \end{aligned}$$

car un diviseur commun de $(ab/m) \wedge b$ et $a \wedge m$ divise a et b donc 1. D'autre part, $g \circ f(k, l) = ((kl) \wedge a)((kl) \wedge b)$. Or, $(kl) \wedge a = k(l \wedge a/k) = a$ car un diviseur commun à l et a/k est un diviseur commun de a et b donc 1.

Exercice 1. 1. $\mathrm{Card}\,(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$ d'après le cours.

2.

3.

4.

5. Il s'agit de vérifier que la fonction définie sur $\mathbb{N}^*$ par $n \mapsto \ln_2 n + 1 - \dfrac{n}{\varphi(n)}$ est positive. Si n admet comme décomposition en facteurs premiers $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, alors $n/\varphi(n) = m/\varphi(m)$ où $p_1\cdots p_r$. Il suffit donc de la prouver quand tous les facteurs premiers de n sont de valuation 1. Montrons par récurrence sur r nombre de facteurs premiers de n.

   Initialisation. La fonction $p \mapsto \ln_2 p + 1 - \dfrac{1}{1-1/p}$ est croissante et vaut 0 en $p = 2$.

   Hérédité. On suppose le résultat pour r. Soit m produit de r facteurs premiers et p premier à m. Soit $n = mp$. Alors

$$\ln_2 n + 1 - \frac{n}{\varphi(n)} = \ln_2 m + 1 - \frac{m}{\varphi(m)} + \ln_2 p - \frac{m}{\varphi(m)}\frac{1}{p-1}.$$

   Par hypothèse de récurrence et croissance de $p \mapsto \ln_2 p - \dfrac{m}{\varphi(m)}\dfrac{1}{p-1}$ (qui vaut 0 en $p = 2$), c'est gagné.

Exercice 9. TD 9

1. Pour montrer que l'ensemble des éléments mous est un sous-groupe de G, on remarque qu'un élément g de G est mou si pour toute partie B non génératrice de G, la partie $B\cup\{g\}$ reste non génératrice. Soit g, h deux éléments mous de G et B une partie non génératrice de G. Alors $B \cup \{g\}$ n'est pas génératrice, et $B \cup \{g, h\}$ non plus. Or

$$\big\langle B\cup\{gh^{-1}\}\big\rangle \subset \langle B\cup\{g,h\}\rangle \neq G$$

   donc gh^{-1} est mou. Pour conclure, le neutre est évidemment un élément mou.

2. Si g est un élément mou de G et H un sous-groupe maximal de G, comme H n'est pas génératrice, $H\cup\{g\}$ ne l'est pas non plus, donc $H \subset \langle H\cup\{g\}\rangle \neq G$, ce qui, par maximalité de H, impose $H = \langle H\cup\{g\}\rangle$, c'est à dire $g \in H$.

   Réciproquement, si un élément g de G appartient à l'intersection des sous-groupes maximaux de G, si B est une partie de G non génératrice, $\langle B\rangle$ est un sous-groupe propre de G donc est contenu dans un sous-groupe maximal, disons H et alors la partie $B\cup\{g\}$ est encore contenue dans H donc n'est toujours pas génératrice.

3. On peut ainsi trouver les éléments mous du groupe $(S_n, \circ)$ des permutations de $[\![1, n]\!]$. Il suffit pour cela de montrer que pour $i \in [\![1, n]\!]$, le stabilisateur de i

$$\mathrm{Stab}(i) = \{\sigma \in S_n \,|\, \sigma(i) = i\}$$

   est un sous-groupe maximal de S_n. Le seul élément mou de S_n, devant laisser fixe chaque $i \in [\![1, n]\!]$, est bien $id_{[\![1,n]\!]}$. Fixons donc $i \in [\![1, n]\!]$ et montrons que $\mathrm{Stab}(i)$ est un sous-groupe maximal. Prenons $\sigma \in S_n - \mathrm{Stab}(i)$, posons $j = \sigma(i) \neq i$ et montrons que le sous-groupe $H = \langle \mathrm{Stab}(i)\cup\{\sigma\}\rangle$ contient S_n. Pour $p \in [\![1, n]\!] - \{i, j\}$, la permutation $(p, j)\circ\sigma$ envoie i sur p. Puisque (p, j) laisse fixe i, la permutation $(p, j)\circ\sigma$ appartient à H. On peut ainsi

trouver dans H un élément qui envoie i sur n'importe quel élément de $[\![1,n]\!]$. Maintenant, si φ est une permutation quelconque de $[\![1,n]\!]$, notons $p=\varphi(i)$ et prenons $\tau\in H$ envoyant i sur p. Alors $\tau^{-1}\circ\varphi$ envoie i sur i donc $\tau^{-1}\circ\varphi$ appartient à $\mathrm{Stab}(i)$ et φ appartient à H.

4. On étudie les éléments mous de $(\mathbb{Z}/n\mathbb{Z},+)$ pour $n\geqslant 2$. Soit $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ la décomposition de n en produit de facteurs premiers. Soit $a\in\mathbb{Z}$ et $\overline{a}$ la classe de a modulo n. On va montrer que $\overline{a}$ est mou si et seulement si $p_1\dots p_k$ divise a. En particulier, $\overline{0}$ est le seul élément mou de $(\mathbb{Z}/n\mathbb{Z},+)$ si et seulement si n est sans facteur carré.

   Si a est divisible par $p_1\dots p_k$, si B est une partie non génératrice de $\mathbb{Z}/n\mathbb{Z}$, le sous-groupe engendré par B admet un générateur $\overline{b}$ où b est un diviseur de n autre que ±1. Dans ce cas, $\langle B\cup\{\overline{a}\}\rangle=\left\langle\{\overline{d}\}\right\rangle$ où d est le pgcd de a et b. Comme d est divisible par l'un des p_i, $\langle B\cup\{\overline{a}\}\rangle\neq\mathbb{Z}/n\mathbb{Z}$ et $\overline{a}$ est mou.

   Si a n'est pas divisible par $p_1\dots p_k$, a est par exemple premier avec p_1 et alors $\{\overline{a},\overline{p_1}\}$ est génératrice de $\mathbb{Z}/n\mathbb{Z}$ tandis que $\{\overline{p_1}\}$ ne l'est pas. Donc $\overline{a}$ n'est pas mou.

   En utilisant les sous-groupes maximaux, on pouvait aussi écrire :

   Les sous-groupes de $(\mathbb{Z}/n\mathbb{Z},+)$ sont les $d\mathbb{Z}/n\mathbb{Z}$ pour d divisant n. Pour d,d' divisant n, l'inclusion $d\mathbb{Z}/n\mathbb{Z}\subset d'\mathbb{Z}/n\mathbb{Z}$ équivaut à la divisibilité de d' par d. Les sous-groupes maximaux de $(\mathbb{Z}/n\mathbb{Z},+)$ sont donc les $p\mathbb{Z}/n\mathbb{Z}$ pour p premier divisant n. Si l'on note $p_1,\dots,p_k$ les facteurs premiers de n, l'intersection des sous-groupes maximaux de $(\mathbb{Z}/n\mathbb{Z},+)$ est donc $r\mathbb{Z}/n\mathbb{Z}$ où $r=p_1\dots p_k$ est le radical de n.