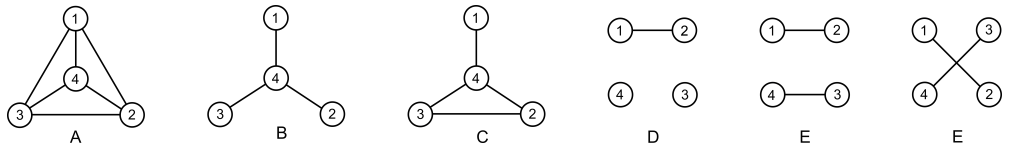
PARTIEL DU COURS D'ALGÈBRE 1, ENS ULM, MARDI 7 NOVEMBRE 2023

Aucun document n'est autorisé. Temps de composition : 2h. Il n'est pas du tout nécessaire de traiter toutes les questions pour avoir le maximum des points. On soignera la rédaction.

**Problème 1.** *Soit $n \geq 1$ un entier. Nous appellerons* $n$-graphe *la donnée d'un sous-ensemble $\Gamma \subset \mathrm{P}(\{1,\dots,n\})$ constitué de parties à 2 éléments de $\{1,\dots,n\}$. Ces parties seront aussi appelées* arêtes *du graphe $\Gamma$. Par exemple, les six figures suivantes définissent*[1] *cinq 4-graphes (les deux derniers étant égaux), dans lesquels les arêtes sont représentées par des traits :*




*Soit $\Gamma$ un $n$-graphe. Pour $i \in \{1,\dots,n\}$ on pose $\mathrm{V}_\Gamma(i) = \{j \in \{1,\dots,n\} \mid \{i,j\} \in \Gamma\}$ (ensemble des* voisins *de $i$ dans $\Gamma$) et $\mathrm{v}_\Gamma(i) = |\mathrm{V}_\Gamma(i)|$. Enfin, on définit le* groupe de symétries de $\Gamma$ *comme étant*

$$\mathrm{G}(\Gamma) := \{g \in \mathrm{S}_n \mid \forall i,j \in \{1,\dots,n\},\ \{i,j\} \in \Gamma \implies \{g(i),g(j)\} \in \Gamma\}.$$

*(i) Vérifier que $\mathrm{G}(\Gamma)$ est bien un sous-groupe de $\mathrm{S}_n$.*

*On a clairement $1 \in \mathrm{G}(\Gamma)$. Soient $g,h \in \mathrm{G}(\Gamma)$. Pour $\{i,j\} \in \Gamma$, on a $\{h(i),h(j)\} \in \Gamma$ car $h \in \mathrm{G}(\Gamma)$, puis $\{g(h(i)),g(h(j))\} = \{gh(i),gh(j)\} \in \Gamma$ car $g \in \mathrm{G}(\Gamma)$, et donc $gh \in \mathrm{G}(\Gamma)$. Reste à voir $g^{-1} \in \mathrm{G}(\Gamma)$. Méthode 1. Observer $g^{-1} = g^{n-1}$ avec $n = \operatorname{ord} g \geq 1$, et donc $g^{-1} \in \mathrm{G}(\Gamma)$ par ce qui a déjà été montré. Méthode 2. L'application $\Gamma \to \Gamma, X \mapsto g(X)$, est bien définie pour $g \in \mathrm{G}(\Gamma)$, et injective car $g(X) = g(Y)$ implique $X = Y$ en appliquant $g^{-1} \in \mathrm{S}_n$. Comme $\Gamma$ est fini, elle est bijective, et donc $g(\Gamma) = \Gamma$, puis $g^{-1}(\Gamma) = \Gamma$.*

*(ii) Soient $i \in \{1,\dots,n\}$ et $g \in \mathrm{G}(\Gamma)$. Vérifier $g(\mathrm{V}_\Gamma(i)) = \mathrm{V}_\Gamma(g(i))$ et $\mathrm{v}_\Gamma(i) = \mathrm{v}_\Gamma(g(i))$.*

*Pour $j \in \mathrm{V}_\Gamma(i)$ on a $\{g(i),g(j)\} \in \Gamma$ et donc $g(j) \in \mathrm{V}_\Gamma(g(i))$. On en déduit $g(\mathrm{V}_\Gamma(i)) \subset \mathrm{V}_\Gamma(g(i))$. Appliqué à $g^{-1} \in \mathrm{G}(\Gamma)$, on a aussi $g^{-1}(\mathrm{V}_\Gamma(g(i)) \subset \mathrm{V}_\Gamma(g^{-1}g(i)) = \mathrm{V}_\Gamma(i)$, puis l'autre inclusion $\mathrm{V}_\Gamma(g(i)) \subset g(\mathrm{V}_\Gamma(i))$. On conclut en prenant le cardinal.*

*(iii) Pour chacun des cinq 4-graphes $\Gamma$ ci-dessus, donner sans démonstration un groupe isomorphe à $\mathrm{G}(\Gamma)$ dans la liste suivante : $1$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathrm{S}_3$, $\mathrm{D}_8$, $\mathrm{H}_8$, $\mathrm{S}_4$.*

*On a $\mathrm{G}(\mathrm{A}) = \mathrm{S}_4$, $\mathrm{G}(\mathrm{B}) \simeq \mathrm{S}_3$, $\mathrm{G}(\mathrm{C}) \simeq \mathbb{Z}/2\mathbb{Z}$, $\mathrm{G}(\mathrm{D}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{G}(\mathrm{E}) \simeq \mathrm{D}_8$.*

*(iv) (suite) Pour deux graphes $\Gamma$ de votre choix parmi ces cinq, justifier votre réponse. On pourra expliciter la fonction $\mathrm{v}_\Gamma : \{1,\dots,n\} \to \mathbb{N}$ et lister les éléments de $\mathrm{G}(\Gamma)$.*

(A) *Le graphe A contient tous les $\{i,j\}$ avec $1 \leq i < j \leq 4$. On a donc $\mathrm{G}(\Gamma) = \mathrm{S}_4$.*

(B) *On a $\mathrm{v}_\mathrm{B}(i) = 1$ pour $i = 1,2,3$ et $\mathrm{v}_\mathrm{B}(4) = 3$. Par le (ii), pour $g \in \mathrm{G}(\mathrm{B})$ on a donc $g(4) = 4$ et $g(\{1,2,3\}) = \{1,2,3\}$). Comme n'importe quelle permutation $\sigma \in \mathrm{S}_4$ fixant 4 permute $\{1,4\}$, $\{2,4\}$ et $\{3,4\}$, on constate que $G$ est l'ensemble des $\sigma \in \mathrm{S}_4$ avec $\sigma(4) = 4$. Il est naturellement isomorphe à $\mathrm{S}_3$. Par exemple, l'application $\mathrm{G}(B) \to \mathrm{S}_{\{1,2,3\}}, \sigma \mapsto \sigma_{|\{1,2,3\}}$, est un morphisme bijectif.*

1. Concrètement, il faut comprendre $\mathrm{A} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$, $\mathrm{B} = \{\{1,4\},\{2,4\},\{3,4\}\}$, $\mathrm{C} = \{\{1,4\},\{2,4\},\{2,3\},\{3,4\}\}$, $\mathrm{D} = \{\{1,2\}\}$ et $\mathrm{E} = \{\{1,2\},\{3,4\}\}$.

(C) *On a* $\mathrm{v_C}(1)=1$, $\mathrm{v_C}(4)=3$ *et* $\mathrm{v_C}(i)=2$ *pour* $i=2,3$ *D'après le (ii),* $\mathrm{G(C)}$ *fixe* $1$, $4$, *et préserve* $\{2,3\}$. *Ses seuls éléments possibles sont donc* $1$ *et* $(2\,3)$, *qui conviennent manifestement. On a donc* $\mathrm{G(C)}=\langle(2\,3)\rangle\simeq\mathbb{Z}/2\mathbb{Z}$.

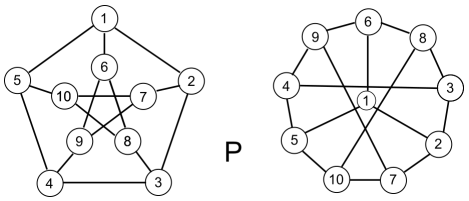
(D) *Pour le graphe* $\mathrm{D}=\{\{1,2\}\}$ *on a* $g\in\mathrm{G(D)}\iff\{g(1),g(2)\}=\{1,2\}$. *On a donc* $\mathrm{G(D)}=\{1,(12),(34),(12)(34)\}$. *Ce groupe est isomorphe au groupe* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. *En effet, l'application* $\mathrm{G(D)}\to\mathrm{S}_{\{1,2\}}\times\mathrm{S}_{\{3,4\}}, g\mapsto(g_{|\{1,2\}},g_{|\{3,4\}})$, *est un morphisme bijectif, et on a* $\mathrm{S}_X\simeq\mathbb{Z}/2\mathbb{Z}$ *pour* $|X|=2$.

(E) *Plus difficile car on a* $\mathrm{v_\Gamma}(i)=2$ *pour tout* $i$. *Par définition, on a* $g\in\mathrm{G(E)}\iff g$ *préserve ou échange* $\{1,2\}$ *et* $\{3,4\}$. *Le sous-groupe des* $g\in\mathrm{G(E)}$ *préservant* $\{1,2\}$ *est le groupe* $\mathrm{G(D)}$ *déterminé ci-dessus. On a donc* $\mathrm{G(E)}=\mathrm{G(D)}\cup(1\,4)(2\,3)\mathrm{G(D)}$, *puis* $|\mathrm{G(E)}|=8$. *On reconnaît que* $\mathrm{G(E)}$ *est un conjugué de* $\mathrm{D}_8$ *dans* $\mathrm{S}_4$ *: les éléments* $(1\,3\,2\,4)$ *et* $(1\,4)(2\,3)$ *sont dans* $\mathrm{G(E)}$ *et l'engendrent pour des raisons de cardinal.*

*Dans la suite du problème, on s'intéresse au* graphe de Petersen. *C'est le* $10$*-graphe* $\mathrm{P}$ *défini par*

$$\mathrm{P}=\{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{1,5\},\{6,8\},\{8,10\},\{7,10\},\{7,9\},\{6,9\},\{1,6\},\{2,7\},\{3,8\},\{4,9\},\{5,10\}\}.$$

*Les deux figures suivantes en donnent deux représentations :*




*On se propose de montrer que l'on a* $\mathrm{G(P)}\simeq\mathrm{S}_5$. *Comme tout sous-groupe de* $\mathrm{S}_{10}$, *le groupe* $\mathrm{G(P)}$ *agit naturellement sur* $\{1,\dots,10\}$. *Pour* $I\subset\{1,\dots,n\}$ *on pose* $\mathrm{G(P)}_I=\{g\in\mathrm{G(P)}\mid g(i)=i,\ \forall i\in I\}$.

(v) *À l'aide des figures, donner un élément d'ordre* $3$ *et un élément d'ordre* $5$ *dans* $\mathrm{G(P)}$.

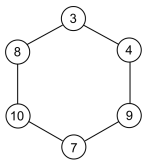
*La figure de gauche étant invariante par la rotation centrale d'angle* $2\pi/5$ *(sens horaire), on constate que l'élément* $c=(1\,2\,3\,4\,5)(6\,7\,8\,9\,10)$ *est dans* $\mathrm{G(P)}$. *Il est d'ordre* $5$. *En considérant de même, la rotation centrale d'angle* $2\pi/3$ *de la figure de droite, l'élément* $t=(2\,5\,6)(3\,10\,9)(8\,7\,4)$ *est dans* $\mathrm{G(P)}$ *et il est d'ordre* $3$.

(vi) *Montrer que* $\mathrm{G(P)}$ *agit transitivement sur* $\{1,\dots,10\}$.

*Regardons l'orbite de* $1$ *sous* $\mathrm{G(P)}$. *Elle contient les* $c^i(1)$, $i\in\mathbb{Z}$, *et donc* $1,2,3,4,5$. *Elle contient donc aussi* $t(5)=6$, *puis les* $c^j(6)$, $j\in\mathbb{Z}$, *i.e.* $6,7,8,9,10$. *On a montré* $\mathrm{O}_1=\{1,\dots,10\}$ *: l'action est transitive.*

(vii) *Montrer que* $\mathrm{G(P)}_{\{1,2,5,6\}}$ *est engendré par l'élément* $(3\,7)(4\,10)(8\,9)$.

*L'élément* $d:=(3\,7)(4\,10)(8\,9)$ *fixe* $1,2,5,6$, $\{1,2\}$, $\{1,5\}$, $\{1,6\}$, *et permute* $\{5,4\}$ *et* $\{5,10\}$, $\{6,8\}$ *et* $\{6,9\}$, *et* $\{2,3\}$ *et* $\{2,7\}$. *Les* $6$ *arêtes restantes forment le "sous-graphe" dont* $d$ *est*




*la symétrie centrale, ce qui montre* $d\in\mathrm{G(P)}$. *Réciproquement, soit* $g\in\mathrm{G(P)}_{\{1,2,5,6\}}$. *Par le*

*(ii), $g$ permute les 3 voisins $1, 4, 10$ de $5 = g(5)$, et comme il fixe 1, on a $g(\{4, 10\}) = \{4, 10\}$. Quitte à remplacer $g$ par $dg$ on peut supposer $g(4) = 4$ et $g(10) = 10$. Comme 3 et l'unique voisin commun à 2 et 4, on a alors $g(3) = 3$, et on constate de même que $g$ fixe 9 (unique voisin de 4 et 6), 8 (unique voisin de 3 et 10) et 7 (unique voisin de 2 et 10). On a donc $g = 1$, puis $\mathrm{G(P)}_{\{1,2,5,6\}} = \{1, d\}$.*

(viii) *Montrer que l'on a une suite exacte courte* $1 \to \mathrm{G(P)}_{\{1,2,5,6\}} \to \mathrm{G(P)}_{\{1\}} \to \mathrm{S}_{\{2,5,6\}} \to 1$.

*Par la question (ii), le groupe $\mathrm{G(P)}_{\{1\}}$ agit naturellement sur l'ensemble $\{2, 5, 6\}$ des voisins de 1, ce qui définit donc un morphisme $f : \mathrm{G(P)}_{\{1\}} \to \mathrm{S}_{\{2,5,6\}}$. Par définition, on a $\ker f = \mathrm{G(P)}_{\{1,2,5,6\}}$. Il ne reste qu'à montrer que $f$ est surjective. Mais on a vu $f(t) = (2\,5\,6)$. En considérant la symétrive verticale $s$ de la figure de droite, on a aussi $s \in \mathrm{G(P)}$ et $s = (8\,9)(3\,4)(2\,5)(7\,10)$, et donc $f(s) = (2\,5)$. On conclut car $(2\,5)$ et $(2\,5\,6)$ engendrent $\mathrm{S}_{\{2,5,6\}}$.*

(ix) *En déduire* $|\mathrm{G(P)}| = 120$.

*Par la formule orbite-stabilisateur, on a $|\mathrm{G(P)}| = |\mathrm{G(P)}_{\{1\}}||\mathrm{O}_1|$. On a vu $|\mathrm{O}_1| = 10$ au (vi). On a aussi $|\mathrm{G(P)}_{\{1\}}| = |\mathrm{Im}\, f||\ker f|$ avec $|\mathrm{Im}\, f| = |\mathrm{S}_3| = 6$ par le (viii) et $|\ker f| = |\mathrm{G(P)}_{\{1,2,5,6\}}| = 2$ par le (vii). On a donc bien $|\mathrm{G(P)}| = 10 \cdot 6 \cdot 2 = 120$.*

*Appelons* tétrade *de* P *tout sous-ensemble $T \subset \{1, 2, \ldots, 10\}$ avec $|T| = 4$ et vérifiant $\forall i, j \in T$, $\{i,\ j\} \notin \mathrm{P}$ (autrement dit, $T$ ne contient pas de couple de voisins dans* P*).*

(x) *Vérifier qu'il existe exactement deux tétrades $T$ et $T'$ contenant 1, et que l'on a $T \cap T' = \{1\}$.*

*Soit $T$ une tétrade contenant 1. Elle ne contient donc aucun voisin de 1 (i.e. 2, 5 et 6), et encore 3 éléments parmi $\{8, 3, 9, 4, 7, 10\}$. Comme $\{8, 3\}$, $\{9, 4\}$ et $\{7, 10\}$ sont dans* P*, $T$ contient un et un seul élément de chacune de ces 3 paires. Si $T$ contient 8, elle ne contient pas son voisin 10, et donc 7, et donc pas 9, et donc 4 : on a $T = \{1, 8, 7, 4\}$, qui convient bien. Dans l'autre cas, on a de même $T' = \{1, 3, 9, 10\}$. On a bien $T \cap T' = \{1\}$.*

(xi) *En déduire que* P *contient exactement* 5 *tétrades.*

*Le groupe* G(P) *préserve l'ensemble $\mathcal{T}$ des tétrades. Comme il agit transitivement sur $\{1, \ldots, 10\}$, on déduit du (viii) que tout $i \in \{1, \ldots, 10\}$ est dans exactement 2 tétrades. Il y a donc exactement $2 \cdot 10 = 20$ paires $(T, i)$ avec $T \in \mathcal{T}$ et $i \in \{1, \ldots, 10\}$. Comme chaque tétrade a 4 éléments, on a donc aussi $20 = |\mathcal{T}| \cdot 4$, ce qui conclut.*

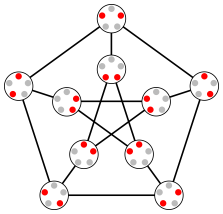
(xii) *Montrer qu'il existe un morphisme de groupes injectif* $\mathrm{G(P)} \longrightarrow \mathrm{S}_5$.

*Le groupe* G(P) *agit naturellement sur l'ensemble des parties à 4 éléments de $\{1, \ldots, 10\}$ en préservant les 5 tétrades. Soit $\varphi : \mathrm{G(P)} \to \mathrm{S}_{\mathcal{T}}$ le morphisme associé. Soit $i \in \{1, \ldots, 10\}$. Par le (vi) et le (x), il existe exactement deux tétrades $T_i$ et $T_i'$ contenant $i$, avec en outre $T_i \cap T_i' = \{i\}$. Pour $g \in \ker \varphi$, on a $g(T_i) = T_i$ et $g(T_i') = T_i'$, et donc $g(i) = i$, pour tout $i$, et donc $g = 1$. On conclut en composant $\varphi$ avec un isomorphisme $\mathrm{S}_{\mathcal{T}} \simeq \mathrm{S}_5$.*

(xiii) *Conclure.*

*On a vu $|\mathrm{G(P)}| = 120 = |\mathrm{S}_5|$ au (ix), donc le morphisme injectif du (xii) est un isomorphisme.*

(xiv) *Démontrer l'existence d'un morphisme injectif* $\mathrm{S}_5 \to \mathrm{G(P)}$ *sans utiliser les questions précédentes, mais en contemplant l'égalité* $\binom{5}{2} = 10$ *et la figure suivante :*



*Soit $C$ un ensemble a 5 éléments (« 5 points gris ») et $D$ l'ensemble des parties à 2 éléments de $C$ ( « 2 points rouges parmi les 5 »). On a $|D| = \binom{5}{2} = 10$. Superposant la figure de l'énoncé et la figure gauche de* P*, on constate (Oh !) une bijection $b : D \xrightarrow{\sim} \{1, 2, \ldots, 10\}$ telle que*

$$\forall X, Y \in D \text{ avec } X \neq Y, \text{ on a } X \cap Y = \emptyset \iff \{b(X), b(Y)\} \in \mathrm{P}.$$

*Le groupe $\mathrm{S}_C$ agit naturellement sur $D$, donc sur $\{1, \ldots, 10\}$ via $b$. Le morphisme induit $\psi : \mathrm{S}_C \to \mathrm{S}_{10}$ a son image dans* G(P)*, car pour $\sigma \in \mathrm{S}_C$ et $X, Y \subset C$, on a $X \cap Y = \emptyset \iff \sigma(X) \cap \sigma(Y) = \emptyset$. Pour conclure l'assertion d'injectivité, il suffit donc de voir que $\mathrm{S}_C$ agit fidèlement sur $D$. Supposons que $\sigma \in \mathrm{S}_C$ préserve toutes les parties à deux éléments de $C$. Soit $i \in C$. Choisissons $j, k \in C$ distincts et distincts de $i$. On a $\sigma(\{i, j\}) = \{i, j\}$, $\sigma(\{i, k\}) = \{i, k\}$, donc $\sigma(i) \in \{i, j\} \cap \{i, k\} = \{i\}$.*

**Problème 2.** (Le théorème de Miller-Moreno) *Un groupe $G$ sera dit* sous-cyclique *si tout sous-groupe strict*[2] *de $G$ est cyclique. On se propose de montrer le théorème suivant, dû à Miller et Moreno : si $G$ est un groupe fini sous-cyclique, alors soit $G$ est isomorphe à l'un des groupes*

$$\mathbb{Z}/n\mathbb{Z} \ \ (n \geq 1), \ \ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \ \ (p \text{ premier}), \ \ \mathrm{H}_8,$$

*soit on a $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$ avec $n \geq 1$, $p$ et $q$ premiers vérifiant $q \,|\, p - 1$, et $\alpha$ bien choisi.*

## Partie I : Le cas des groupes abéliens

*(i) Rappeler brièvement pourquoi tout groupe cyclique est sous-cyclique.*

*D'après le cours, si $G$ est cyclique d'ordre $n$ engendré par $g$, les sous-groupes de $G$ sont les $G^{(d)} = \langle g^d \rangle$ avec $d$ divisant $n$. Ce groupe $G^{(d)}$ est cyclique d'ordre $n/d$.*

*(ii) Montrer que pour $p$ premier, le groupe $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ est sous-cyclique et non cyclique.*

*Un groupe d'ordre $p^2$ avec $p$ premier est sous-cyclique. En effet, si $H$ est un sous-groupe strict de $G$ on a $H = \{1\}$ ou $|H| = p$ par Lagrange, et donc $H$ cyclique d'ordre $p$ (cours). Le groupe (additif) $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ n'est pas cyclique, car on a $px = 0$ pour tout $x \in G$, et donc ses éléments sont d'ordre $\leq p$.*

*(iii) Montrer que si $G$ est un groupe abélien fini non cyclique, il existe un nombre premier $p$ tel que $G$ contienne un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

*Par le théorème de structure on a un isomorphisme $f : G \xrightarrow{\sim} \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \mathbb{Z}/a_n\mathbb{Z}$ avec $a_1 | a_2 | \cdots | a_n$ et $a_1 > 1$. Comme $G$ n'est pas cyclique, on a $n \geq 2$. Soit $p$ premier divisant $a_1$, et donc $a_2$. Pour $i = 1, 2$ le groupe cyclique $\mathbb{Z}/a_i\mathbb{Z}$ contient un sous-groupe cyclique $C_i$ d'ordre $p$, engendré par la classe de $a_i/p$. Le sous-groupe $H = C_1 \times C_2 \times \{0\}^{n-2}$ de $\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \mathbb{Z}/a_n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, et $f^{-1}(H)$ convient.*

2. Un sous-groupe $H$ d'un groupe $G$ est dit strict si on a $H \neq G$.

*(iv) En déduire une classification des groupes abéliens finis sous-cycliques.*

*Ce sont les groupes cycliques et ceux isomorphes à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ avec $p$ premier. En effet, ces groupes conviennent par (i) et (ii). Réciproquement, si $G$ est abélien sous-cyclique non cyclique, il contient un sous-groupe $H$ avec $H \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Ce groupe est non cyclique par le (ii), donc non strict, i.e. $H = G$.*

## Partie II : Quelques propriétés des groupes sous-abéliens

*Un groupe $G$ sera dit* sous-abélien *si tout sous-groupe strict de $G$ est abélien.*

*(i) Soient $G$ un groupe sous-abélien et $H$ un sous-groupe distingué de $G$. Montrer que les groupes $H$ et $G/H$ sont sous-abéliens.*

*Un sous-groupe strict de $H$ est un sous-groupe strict de $G$, donc abélien, et $H$ est sous-abélien. Soit $\pi : G \to G/H$ la projection canonique (un morphisme de groupes). Si $K$ est un sous-groupe strict de $G/H$ alors par le cours $\pi^{-1}K$ est un sous-groupe strict de $G$, donc abélien, et on a $\pi(\pi^{-1}K) = K$. Comme l'image d'un groupe abélien par un morphisme de groupes est abélien, donc $K$ est abélien.*

*(ii) Montrer que tout groupe abélien fini non trivial possède un sous-groupe d'indice premier.*

*Par le théorème de structure on a un isomorphisme $f : G \xrightarrow{\sim} G'$ avec $G' = \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$, $a_1|a_2|\cdots|a_n$, $n \geq 1$ et $a_1 > 1$. Soit $p$ premier divisant $a_1$. Le groupe cyclique $\mathbb{Z}/a_1\mathbb{Z}$ possède un sous-groupe cyclique $C$ d'ordre $a_1/p$ (engendré par $p$). Ainsi, $H := C \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \mathbb{Z}/a_n\mathbb{Z}$ est un sous-groupe d'ordre $|G|/p$ de $G'$, et le sous-groupe $f^{-1}(H)$ de $G$ convient.*

*(iii) On admet qu'un groupe sous-abélien non abélien n'est pas simple.* [3] *En déduire que tout groupe sous-abélien fini non trivial possède un sous-groupe distingué d'indice premier.*

*Soit $G$ sous-abélien fini non trivial. On procède par récurrence sur $|G|$, le cas $|G| = 1$ étant vide. Si $G$ est abélien, on conclut par le (ii). Sinon, par le résultat admis $G$ possède un sous-groupe distingué $H$ avec $\{1\} \neq H \neq G$. Par le (i), le groupe $G/H$ est sous-abélien, et on a $1 < |G/H| = |G|/|H| < |G|$. Ainsi, $G/H$ admet un sous-groupe distingué $K$ d'indice premier $p$. Considérons le morphisme surjectif $\pi : G \to G/H$, dont les fibres sont de cardinal $|H|$. Par le cours, on a $\pi^{-1}(K) \triangleleft G$ et $|\pi^{-1}(K)| = |H||K| = |H|\frac{1}{p}|G/H| = |G|/p$.*

*On se propose maintenant de démontrer que si $G$ est un groupe sous-abélien fini non abélien, il existe deux sous-groupes $P$ et $Q$ de $G$ tels que :* (a) *$G = PQ$,* (b) *$P$ est distingué dans $G$ et d'ordre $p^m$ avec $p$ premier et $m \geq 0$, et* (c) *$Q$ est d'ordre $q^n$ avec $q$ premier $\neq p$ et $n \geq 1$.*

*(iv) Soient $H$ un groupe abélien fini et $n \geq 1$. Montrer que le sous-groupe $H[n] = \{h \in H \mid h^n = 1\}$ est caractéristique dans $H$, et que tout nombre premier divisant $|H[n]|$ divise l'entier $n$.*

*Soit $\alpha \in \operatorname{Aut} H$ et $h \in H[n]$. On a $h^n = 1$ donc $1 = \alpha(h^n) = \alpha(h)^n$ puis $\alpha(h) \in H[n]$. Cela montre que $H[n]$ est caractéristique dans $H$. Soit $p$ premier divisant $|H[n]|$. Par Cauchy, il existe $h \in H[n]$ d'ordre $p$. Mais alors $h^n = 1$ implique $p \mid n$.*

3. Ce résultat, admis dans tout le problème, avait fait l'objet du second problème du partiel 2021-2022.

(v) *(suite) On suppose $|H| = ab$ avec $a$ et $b$ premiers entre eux, et pose $A = H[a]$ et $B = H[b]$. Montrer $H = AB$ et $A \cap B = \{1\}$, puis $|A| = a$ et $|B| = b$.*

*Par Bezout, il existe $u, v \in \mathbb{Z}$ avec $1 = au + bv$. Pour $h \in H$ on a donc $h = (h^b)^v (h^a)^u$. On en déduit d'abord $A \cap B = \{1\}$ car $h^a = h^b = 1$ implique $h = 1$. On en déduit aussi $H = AB$ car par Lagrange, on a $h^b \in H[a]$ et $h^a \in H[b]$. Ainsi, $A$ et $B$ sont complémentaires dans $H$, et donc $|H| = |A||B|$. Par le (v), les diviseurs premiers de $|A|$ (resp. $|B|$) divisent $a$ (resp. $b$), on a donc nécessairement $|A| = a$ et $|B| = b$.*

(vi) *Soient $A$ et $B$ deux sous-groupes finis d'un groupe $H$ avec $A \triangleleft H$. Montrer que $AB$ est un sous-groupe de $H$ d'ordre divisant $|A|\,|B|$.*

*On a $1 = 1.1 \in AB$, $AB = BA$ car $A$ est distingué dans $H$, et donc $ABAB = AABB = AB$, puis $(AB)^{-1} = (BA)^{-1} = A^{-1}B^{-1} = AB$. Ainsi, $AB$ est un sous-groupe de $H$. D'après le cours, son ordre est $\frac{|A||B|}{|A \cap B|}$, donc divise $|A||B|$.*

(vii) *Soient $G$ un groupe et $H$ un sous-groupe distingué de $G$ d'indice premier $q$. Montrer qu'il existe $z \in G$ d'ordre une puissance de $q$ et vérifiant $G = H\langle z \rangle$. On pourra considérer la projection canonique $G \to G/H$.*

*Par hypothèse, le groupe $G/H$ est cyclique d'ordre premier $q$. Soit $z \in G$ tel que $\pi(z)$ est générateur de $G/H$. Écrivons $d = \operatorname{ord} z = q^n k$ avec $k$ premier à $q$ et $n \geq 0$. Alors $\pi(z^k) = \pi(z)^k$ engendre $G/H$ (car $k$ est premier à $q$) et $z^k$ est d'ordre $d/k = q^n$. Ainsi, pour tout $g \in G$ il existe $j \in \mathbb{Z}$ avec $\pi(g) = \pi(z)^j$, puis $gz^{-j} \in H$, et donc $g \in H\langle z \rangle$. On a montré $G = H\langle z \rangle$.*

(viii) *(suite) On suppose en outre $G$ sous-abélien. Montrer que l'on a $G = H'Q$ avec $H'$ un sous-groupe abélien distingué de $G$ d'ordre premier à $q$, et $Q$ un sous-groupe de $G$ d'ordre $q^n$ avec $n \geq 1$.*

*Écrivons $|H| = aq^m$ avec $a$ premier à $q$. Par le (v) on a $H = H[a]\,H[q^m]$ avec $|H[a]| = a$ et $|H[q^m]| = q^m$. On pose $H' = H[a]$ et $Q = H[q^m]\langle z \rangle$. Par le (vii) on a $G = H\langle z \rangle = H'Q$. Par le (iv), les $H[n]$ sont distingués dans $G$ car on a $H \triangleleft G$ et $H[n]$ caractéristique dans $H$. Par le (vi), on a $|Q| = q^n$ avec $n \geq 0$. On a $n \geq 1$ car $z \in Q$ est non trivial (car non dans $H$).*

(ix) *Conclure.*

*Soit $G$ sous-abélien fini non abélien. Partons de l'écriture $G = H'Q$ donnée par (iii) et (viii). Si $|H'|$ n'est pas une puissance d'un nombre premier, on peut écrire $|H'| = ab$ avec $a, b > 1$ premiers entre eux. On a vu $H' = AB$ avec $A = H'[a]$ d'ordre $a$ et $B = H'[b]$ d'ordre $b$. D'après le (vi), $AQ$ et $BQ$ sont des sous-groupes stricts de $G$, donc abéliens. Cela implique que les éléments de $A$, $B$ et $Q$ commutent deux à deux, puis que $G = ABQ$ est abélien.*

## Partie III : Les groupes de Miller-Moreno

*Dans cette partie, on s'intéresse aux groupes finis sous-cycliques $G$ non abéliens tels que $|G|$ admette au moins deux diviseurs premiers distincts (« groupes de Miller-Moreno »). Soit $G$ un tel groupe.*

(i) *Montrer qu'il existe des éléments $x$ et $y$ de $G$ d'ordres respectifs $p^m$ et $q^n$, avec $p, q$ premiers distincts, $m, n$ entiers $\geq 1$ et $G = \langle x \rangle \langle y \rangle$, ainsi que $k \in \mathbb{Z}$ avec $yxy^{-1} = x^k$ et $k \not\equiv 1 \bmod p^m$.*

*D'après le (ix) de la partie II, on a $G = PQ$ avec $P$ sous-groupe distingué d'ordre $p^m$, $Q$ sous-groupe d'ordre $q^n$, $p, q$ premiers distincts et $n \geq 1$. On a $P \cap Q = \{1\}$ par Lagrange et donc $|G| = p^m q^n$, puis $m \geq 1$ par hypothèse. Comme $G$ est sous-cyclique, on a $P = \langle x \rangle$,*

*$Q = \langle y \rangle$. Enfin, comme $P$ est distingué, on a $yxy^{-1} \in \langle x \rangle$. On a donc $yxy^{-1} = x^k$ pour un certain $k \in \mathbb{Z}$. On a $k \not\equiv 1 \bmod p^m$ sinon $x$ et $y$ commutent et $G$ est abélien.*

*(ii)* Montrer $x\,y^q = y^q\,x$ et $x^p\,y = y\,x^p$. On pourra considérer $\langle x \rangle\,\langle y^q \rangle$ et $\langle x^p \rangle\,\langle y \rangle$.

*Le sous-groupe $P^{(p)} = \langle x^p \rangle$ de $P$ est d'ordre $p^{m-1}$ et distingué dans $G$ car $yx^py^{-1} = (x^p)^k$, ainsi $P^{(p)}Q$ est d'ordre divisant $p^{m-1}q^n$ par la partie II (vi), donc strict. Il est donc cyclique, en particulier abélien, et donc $y$ et $x^p$ commutent. De même, $PQ^{(q)}$ est un sous-groupe strict de $G$, donc abélien, et $y^q$ et $x$ commutent.*

*(iii)* En déduire $k^q \equiv 1 \bmod p^m$ et $k \equiv 1 \bmod p^{m-1}$.

*Par le (i) et (ii) on a $x = y^qxy^{-q} = y(y(...(yxy^{-1})...)y^{-1})y^{-1} = x^{k^q}$, puis $k^q \equiv 1 \bmod p^m$ car $x$ est d'ordre $p^m$. De même, on a $x^p = yx^py^{-1} = (yxy^{-1})^p = x^{kp}$, donc $kp \equiv p \bmod p^m$, puis $k \equiv 1 \bmod p^{m-1}$.*

*(iv)* Montrer $m = 1$ et $q \,|\, p-1$. On rappelle que pour $r \in p\mathbb{Z}$ on a $(1+r)^p \equiv 1 \bmod pr$.

*Si on a $m > 1$ alors $k \equiv 1 \bmod p^{m-1}$ implique $k^p \equiv 1 \bmod p^m$ par le rappel. Ainsi, l'ordre de $k$ modulo $p^m$ divise $p$ et $q$ : c'est donc $1$ et on a $k \equiv 1 \bmod p^m$, en contradiction avec le (i). On a montré $m = 1$ et que l'ordre de $k \bmod p$ est $q$. On a donc $q \,|\, p-1 = |(\mathbb{Z}/p\mathbb{Z})^\times|$.*

*(v)* Montrer qu'il existe un morphisme de groupes $\alpha : \mathbb{Z}/q^n\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$ envoyant $\overline{1}$ sur $z \mapsto \overline{k}z$.

*Soit $a$ l'automorphisme de $\mathbb{Z}/p\mathbb{Z}$ défini par $a(z) = \overline{k}z$ pour $z \in \mathbb{Z}/p\mathbb{Z}$. On a $a^q = \mathrm{id}$ car $k^q \equiv 1 \bmod p$. On a un morphisme de groupes $f : \mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}, i \mapsto \alpha^i$. On a $f(q^n) = a^{q^n} = 1$ car $a^q = 1$. Par propriété universelle des groupes quotients, $f$ se factorise en un morphisme de groupes $\alpha : \mathbb{Z}/q^n\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^\times$ vérifiant $\alpha(\overline{i}) = a^i$ pour tout $i \in \mathbb{Z}$.*

*(vi)* En déduire $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$.

*Le groupe $G$ est produit semi-direct interne de $Q$ par $P$ (question (i)). Soit $a : \mathbb{Z}/p\mathbb{Z} \to P$ et $b : \mathbb{Z}/q^m\mathbb{Z} \to Q$ les isomorphismes envoyant respectivement $\overline{1}$ sur $x$ et $\overline{1}$ sur $y$. On a $yxy^{-1} = x^k$ et donc $a \circ \mathrm{int}_{b(\overline{1})} \circ a^{-1} = \alpha(\overline{1})$. Par suivi des isomorphismes $a$ et $b$ on a donc $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\alpha \mathbb{Z}/q^n\mathbb{Z}$.*

*(vii)* Réciproquement, montrer que pour $p$ et $q$ premiers avec $q \,|\, p-1$, et $n \geq 1$, il existe un morphisme $\beta : \mathbb{Z}/q^n\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$ tel que $\mathbb{Z}/p\mathbb{Z} \rtimes_\beta \mathbb{Z}/q^n\mathbb{Z}$ est sous-cyclique et non abélien.

*Par hypothèse, et Gauss ou Cauchy, il existe $k \in \mathbb{Z}$ tel que $\overline{k}$ est d'ordre $q$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$. On peut donc définir un morphisme $\beta : \mathbb{Z}/q^n\mathbb{Z} \to \operatorname{Aut} \mathbb{Z}/p\mathbb{Z}$ comme au (v), envoyant $\overline{1}$ sur $\overline{k}$. On pose $G = \mathbb{Z}/p\mathbb{Z} \rtimes_\beta \mathbb{Z}/q^n\mathbb{Z}$. Par construction, on a $G = PQ$ avec $P = \langle x \rangle$ distingué d'ordre $p$, $Q = \langle y \rangle$ d'ordre $q^n$, et $yxy^{-1} = x^k$. Comme $k \not\equiv 1 \bmod p$, $x$ et $y$ ne commutent pas : $G$ n'est pas abélien. Montrons qu'il est sous-cyclique.*

*Soit $\pi : G \to G/P$ la projection canonique. Elle induit un isomorphisme $Q \simeq G/P$ (cyclique d'ordre $q^m$). Soit $H$ un sous-groupe strict de $G$. Si on a $H \cap P = \{1\}$ on a $H \simeq \pi(H)$, et $\pi(H)$ est cyclique car sous-groupe du groupe cyclique $G/P$. Sinon, on a $P \subset H$ cap $|P|$ est premier, et $\pi(H)$ est un sous-groupe strict du groupe cyclique $G/P$ (d'ordre $q^n$), donc inclus dans $(G/P)^{(q)}$. Mais alors $H$ est inclus dans $\pi^{-1}((G/P)^{(q)}) = \langle x, y^q \rangle$. Mais on a $y^qxy^{-q} = x^{k^q} = x$, donc $x$ et $y^q$ commutent. Comme ils sont d'ordre $p$ et $q^{n-1}$, le sous-groupe engendré $\langle x, y^q \rangle$ est cyclique d'ordre $pq^{n-1}$ engendré par $xy$ (Cauchy), donc $H$ est cyclique.*

## Partie IV : (Bonus) le cas des $p$-groupes

On suppose enfin $G$ sous-cyclique non abélien d'ordre $p^n$ avec $p$ premier et $n \geq 2$. On se donne un sous-groupe cyclique distingué $H = \langle x \rangle$ d'ordre $p^{n-1}$, on fixe $y \in G \smallsetminus H$.

(i) Montrer $y^p \in \langle x^p \rangle$ et $yx^p = x^p y$.

Comme $H$ est d'indice $p$ dans $G$ on a $y^p \in H$. Mais tout élément de $H$ est soit d'ordre $p^{n-1}$ (= générateur), soit engendre un sous-groupe strict, de la forme $\langle x^{p^i} \rangle$ avec $1 \leq i \leq n-1$, et en particulier est inclus dans $\langle x^p \rangle$. Mais $y^p$ n'est pas d'ordre $p^{n-1}$, sinon $y$ serait d'ordre $p^n$ et $G$ serait cyclique. Enfin, le sous-groupe $\langle x^p, y \rangle = \cup_{i=0}^{p-1} y^i \langle x^p \rangle$ est d'ordre $\leq pp^{n-2}$, donc strict, puis cyclique et donc abélien.

(ii) Montrer $yxy^{-1} = x^k$ avec $k \in \mathbb{Z}$, $k \equiv 1 \bmod p^{n-2}$ et $n \geq 3$.

On a $\langle x \rangle \triangleleft G$ donc il existe $k \in \mathbb{Z}$ avec $yxy^{-1} = k$. Par le (i) on a $yx^p = x^p y$ et $y^p x = xy^p$. Comme au (iii) partie III cela implique $k \equiv 1 \bmod p^{n-2}$ et $k^p \equiv 1 \bmod p^{n-1}$. Pour $n = 2$ cette seconde congruence implique $k \equiv 1 \bmod p^{n-1}$ donc $G$ commutatif : absurde.

(iii) Montrer que quitte à remplacer $y$ par $x^i y$ pour $i \in \mathbb{Z}$ bien choisi, on peut supposer $y^{2p} = 1$.

La seule chose supposée sur $y \in G$ est $y \notin \langle x \rangle$, ce qui est encore le cas pour $x^i y$ pour tout $i \in \mathbb{Z}$. On a $k = 1 + up^{n-2}$ avec $u \in \mathbb{Z}$ et $y^p = x^{pv}$ avec $v \in \mathbb{Z}$ par le (i). Pour $i \in \mathbb{Z}$ on a

$$(x^i y)^{2p} = x^i (yx^i y^{-1})(y^2 x^i y^{-2}) \cdots (y^{2p-1} x^i y^{-q+1}) y^{2p} = x^{(\sum_{j=0}^{2p-1} ik^j) + 2v}.$$

On a $k^j \equiv 1 + ju \bmod p^{n-1}$ et $\sum_{j=0}^{2p-1} j = p(2p-1)$, donc $\sum_{j=0}^{2p-1} k^j \equiv 2p \bmod p^{n-1}$. On a donc $(x^{-v} y)^{2p} = 1$.

(iv) En considérant le sous-groupe $\langle t, y \rangle$ de $G$ avec $t = x^{p^{n-2}}$, montrer $p = 2$ et $y^2 = t$.

Par le (i) le sous-groupe $K := \langle t, y \rangle$ est abélien. Il est donc strict (car $G$ non abélien), donc cyclique, et annulé par $2p$. Comme $t \in K$ est d'ordre $p$, on a soit $K = \langle t \rangle$ et $|K| = p$, soit $K$ d'ordre $2p$. Le premier cas est exclus car il entraîne $y \in \langle x \rangle$. Dans le second cas, on a $2p \,|\, p^n$ par Lagrange, et puis $p = 2$, $K = \langle y \rangle$ d'ordre 4 et $y^2 = t$.

(v) En déduire $G \simeq \mathrm{H}_8$, puis terminer la démonstration du théorème de Miller-Moreno.

Soit $z = x^{2^{n-3}}$. On a $z$ d'ordre 4, $z^2 = t = y^2$ et $yzy^{-1} = z^k$ avec $k \equiv \pm 1 \bmod 4$. Le cas $k \equiv 1 \bmod 4$ implique que $M := \langle z, y \rangle$ est commutatif, donc strict et cyclique, et d'exposant 4, donc cyclique d'ordre 4, puis $M = \langle x \rangle = \langle y \rangle$ : absurde. On a donc $yzy^{-1} = z^{-1}$, $M$ non commutatif, puis $M = G$. On a reconnu le groupe $\mathrm{H}_8$ (envoyer $I$ sur $z$ et $J$ sur $y$).