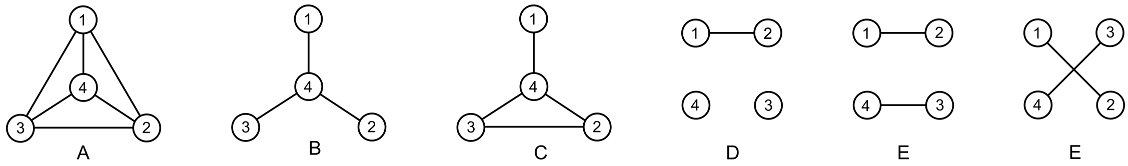
Partiel du cours d'Algèbre 1, ENS Ulm, Mardi 7 Novembre 2023

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 $\Gamma \subset \mathrm{P}(\{1,\ldots,n\})$ constitué de parties à 2 éléments de $\{1,\ldots,n\}$. Ces parties seront aussi appelées* arêtes *du graphe Γ. 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 Γ un n-graphe. Pour $i \in \{1,\ldots,n\}$ on pose $\mathrm{V}_\Gamma(i) = \{j \in \{1,\ldots,n\} \mid \{i,j\} \in \Gamma\}$ (ensemble des voisins *de i dans Γ) et $\mathrm{v}_\Gamma(i) = |\mathrm{V}_\Gamma(i)|$. Enfin, on définit le* groupe de symétries de Γ *comme étant*

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

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

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

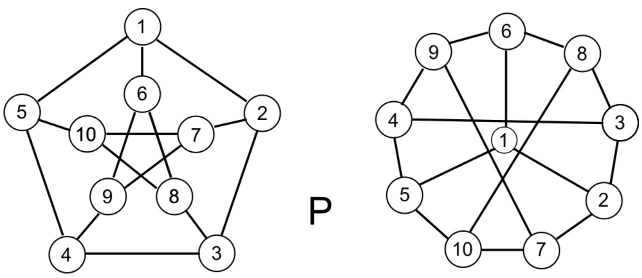
(iii) Pour chacun des cinq 4-graphes Γ ci-dessus, donner sans démonstration un groupe isomorphe à $\mathrm{G}(\Gamma)$ dans la liste suivante : 1, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, S_3, D_8, H_8, S_4.

(iv) (suite) Pour deux graphes Γ de votre choix parmi ces cinq, justifier votre réponse. On pourra expliciter la fonction $\mathrm{v}_\Gamma : \{1,2,3,4\} \to \mathbb{N}$ et lister les éléments de $\mathrm{G}(\Gamma)$.

Dans la suite du problème, on s'intéresse au graphe de Petersen. *C'est le 10-graphe 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 $\mathrm{G}(\mathrm{P}) \simeq \mathrm{S}_5$. Comme tout sous-groupe de S_{10}, le groupe $\mathrm{G}(\mathrm{P})$ agit naturellement sur $\{1,\ldots,10\}$. Pour $I \subset \{1,\ldots,n\}$ on pose $\mathrm{G}(\mathrm{P})_I = \{g \in \mathrm{G}(\mathrm{P}) \mid g(i) = i,\ \forall i \in I\}$.

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

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 $\mathrm{E} = \{\{1,2\},\{3,4\}\}$.

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

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

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

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

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*).*

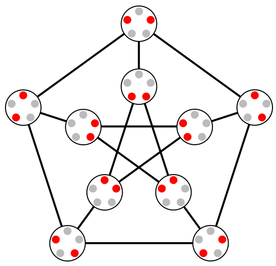
(x) Vérifier qu'il existe exactement deux tétrades T *et* T' *contenant* 1*, et que l'on a* $T \cap T' = \{1\}$.

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

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

(xiii) Conclure.

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



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*

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

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* α *bien choisi.*

Partie I : Le cas des groupes abéliens

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

(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.*

(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* $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

(iv) En déduire une classification, à isomorphisme près, des groupes abéliens finis sous-cycliques.

---

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

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.*

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

(iii) *On admet qu'un groupe sous-abélien fini 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.*

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 $H[n] = \{h \in H \mid h^n = 1\}$ est un sous-groupe caractéristique de H, et que tout nombre premier divisant $|H[n]|$ divise l'entier n.*

(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 $|B| = b$.*

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

(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 $G \to G/H$.*

(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 $n \geq 1$.*

(ix) *Conclure.*

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 ≥ 1 et $G = \langle x \rangle \langle y \rangle$, ainsi que $k \in \mathbb{Z}$ avec $yxy^{-1} = x^k$ et $k \not\equiv 1 \bmod p^m$.*

(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 $\langle x^p \rangle\,\langle y \rangle$.*

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

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

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

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

---

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

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

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

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

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

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

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

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

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