LES GROUPES

EXERCICE 1.1 (École polytechnique).
Soit E un ensemble fini muni d'une loi de composition interne associative.
Montrer qu'il existe $s \in E$ tel que $s^2 = s$

EXERCICE 1.2.
Soit G un sous-groupe de $\mathrm{GL_n}(\mathbb{C})$ constitué d'un nombre fini de matrices $M_1, \cdots, M_r$.
En calculant $\left(\sum_{i=1}^{r} M_i\right)^2$, montrer que $\mathrm{Tr}\left(\sum_{i=1}^{r} M_i\right)$ est un entier divisble par r

EXERCICE 1.3.
Soit $(G, .)$ un groupe et H une partie non vide de G, finie et stable.
Montrer que H est un sous-groupe de $(G, .)$.

EXERCICE 1.4 (Commutant et centre).
Soit $(G, .)$ un groupe multiplicatif. On note $Z(G) = \{a \in G \text{ tel que } \forall\, b \in G, \text{ on a } ab = ba\}$ (*centre de* G), et pour $a \in G$: $C(a) = \{b \in G \text{ tel que } ab = ba\}$ (*commutant de* a).

1. Montrer que $C(a)$ et $Z(G)$ sont des sous-groupes de G.
2. Soit $n \geqslant 2$. Trouver les centres de S_n et $\mathrm{GL}_n(\mathbb{K})$

EXERCICE 1.5 (Sous-groupes de $(\mathbb{R}, +)$).
Soit $(a, b) \in \mathbb{R} \times \mathbb{R}^*$, on pose $H := a\mathbb{Z} + b\mathbb{Z} = \{an + bm \mid (m, n) \in \mathbb{Z}^2\}$.

1. Montrer: $\dfrac{a}{b} \in \mathbb{Q} \Longleftrightarrow \exists \gamma \in \mathbb{R}$ tel que $H = \gamma\mathbb{Z}$
2. Montrer que $(\cos(n))_{n\in\mathbb{N}}$ est dense dans $[-1, 1]$

EXERCICE 1.6 (Groupes dont l'ensemble des sous-groupes est fini).
Caractériser les groupes dont l'ensemble des sous-groupes est fini.

EXERCICE 1.7.
Soit H un sous-groupe strict d'un groupe $(G, \star)$.
Déterminer le groupe engendré par le complémentaire de H dans G.

EXERCICE 1.8 (Ens Ulm).
Trouver les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

EXERCICE 1.9.
Soit G un sous-groupe de $\mathbb{Z}^n$ non réduit à $\{0\}$. Montrer qu'il existe $r \in [\![1, n]\!]$ tel que G soit isomorphe à $\mathbb{Z}^r$

EXERCICE 1.10 (Ordre d'une rotation palne).
Soit $\theta \in \mathbb{R}$, on pose $r = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$.

1. Montrer que r est d'ordre fini si et seulement si $\dfrac{\theta}{2\pi} \in \mathbb{Q}$
2. Si $\dfrac{\theta}{2\pi} = \dfrac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ tels que $p \wedge q = 1$. Déterminer l'ordre de r

EXERCICE 1.11 (Classique).
Soient a et b deux éléments d'un groupe G.

Les groupes

1. Montrer qu'un isomorphisme de groupes conserve l'ordre des éléments.
2. Comparer les ordres de ab et de ba.

Exercice 1.12 (Sous-groupes d'un groupe cyclique)**.**
Soit $n \in \mathbb{N}^*$ et $G = \mathbb{Z}/n\mathbb{Z}$. Soit $k \in \mathbb{Z}$ et $d = k \wedge n$.

1. Déterminer l'ordre de $\overline{k}$ dans $(G, +)$.
2. Montrer que $\overline{k}$ et $\overline{d}$ engendrent le même sous-groupe de G.
3. Quels sont tous les sous-groupes de G ?

Exercice 1.13 (Produit de deux groupes cycliques)**.**
Soient H et K deux groupes notés multiplicativement.

1. Montrer que si h est un élément d'ordre p de H et k un élément d'ordre q de K alors (h, k) est un élément d'ordre $\text{ppcm}(p, q)$ de $H \times K$.
2. On suppose H et K cycliques. Montrer que le groupe produit $H \times K$ est cyclique si, et seulement si, les ordres de H et K sont premiers entre eux.

Exercice 1.14 (Groupe d'"exposant 2)**.**
Soit G un groupe fini tel que : $\forall\ x \in G,\ x^2 = e$.

1. Montrer que G est abélien
2. Soit H un sous-groupe de G et $x \in G \setminus H$. On note $K = H \cup xH$.
   Montrer que K est un sous-groupe de $(G, .)$ et que $\mathbf{Card}K = 2\mathbf{Card}H$.
3. En déduire que $\mathbf{Card}G$ est une puissance de 2.

Exercice 1.15 (Décomposition d'un élément d'ordre fini)**.**
Soit G un groupe multiplicatif et $a \in G$ d'ordre np avec $n \wedge p = 1$.
Montrer qu'il existe $b, c \in G$ uniques tels que: $\begin{cases} b \text{ est d'ordre } n; \\ c \text{ est d'ordre } p; \\ a = bc = cb. \end{cases}$

Exercice 1.16 (Classique)**.**
Soit G un groupe fini de cardinal pair. Montrer qu'il existe un élément d'ordre 2.

Exercice 1.17.
Soit G un groupe fini de cardinal impair. Montrer que : $\forall\ x \in G,\ \exists!\ y \in G$ tel que $x = y^2$.

Exercice 1.18 (Ens Lyon)**.**
Soit G un groupe de cardinal $2p$, avec $p \geqslant 3$ premier. Montrer que G contient un élément d'ordre p.

Exercice 1.19 (Groupe sans sous-groupe non trivial)**.**
Soit G un groupe non trivial qui n'ayant pas de sous-groupe non trivial.
Montrer que G est monogène, fini, et que $\mathbf{Card}(G)$ est un nombre premier.

Exercice 1.20 (Théorème du rang)**.**
Soit $f : G \longrightarrow G'$ un morphisme de groupes où G est un groupe fini.
Montrer que $\mathbf{Card}(\text{Ker}f) \times \mathbf{Card}(\text{Im}f) = \mathbf{Card}(G)$.

Les groupes

Exercice 1.21 (Commutant d'une transposition)**.**

Soit n un entier supérieur à 2, deux entiers $i, j \in [\![1, n]\!]$ tels que $i \neq j$ et $\sigma \in \mathcal{S}_n$.
Montrer que σ et $\tau = \begin{pmatrix} i & j \end{pmatrix}$ commutent si, et seulement si, $\{i, j\}$ est stable par σ.

Exercice 1.22 (Commutant d'un n-cycle)**.**

Montrer que si c et c' sont des n-cycles de S_n commutant entre eux, il existe r tel que $c' = c^r$

Exercice 1.23 (Conjugué d'un cycle)**.**

Soit $n \geqslant 2$, σ une permutation de S_n et $c = \begin{pmatrix} a_1 & a_2 & \dots & a_p \end{pmatrix}$ un p-cycle .
Calculer la permutation $\sigma c \sigma^{-1}$.

Exercice 1.24 (Générateurs de S_n)**.**

Soit n un entier supérieur ou égal à 3. Sachant que le groupe S_n est engendré par l'ensemble des transpositions de $\{1, \cdots, n\}$. Montrer que S_n est engendré par les ensembles suivants de permutations :

1. $\begin{pmatrix} 1 & 2 \end{pmatrix}, \cdots, \begin{pmatrix} 1 & n \end{pmatrix}$;
2. $\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}, \cdots, \begin{pmatrix} n-1 & n \end{pmatrix}$
3. $\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 & \cdots & n \end{pmatrix}$

Exercice 1.25 (Générateurs de A_n)**.**

Soit n un entier. On note A_n le sous-groupe de S_n formé par les permutations paires.

1. Montrer que le produit de deux transpositions distinctes de S_n est un 3-cycle ou un produit de deux 3-cycles. En déduire que A_n est engendré par l'ensemble des 3-cycles de S_n.
2. Montrer que, pour $n \geqslant 3$, A_n est engendré par l'ensemble des 3-cycles : $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, \cdots, \begin{pmatrix} 1 & 2 & n \end{pmatrix}$.

Exercice 1.26 (Centre d'un p-groupe)**.**

Soit G un groupe fini de cardinal p^k où p est un nombre premier et $k \in \mathbb{N}^*$. On note Z le centre de G.

1. En considérant l'action de G sur lui-même par automorphismes intérieurs, montrer que $\mathbf{Card}(Z) \equiv 0[p]$.
2. En déduire que tout groupe d'ordre p^2, p premier, est commutatif et est isomorphe soit à $\mathbb{Z}/p^2\mathbb{Z}$ soit à $(\mathbb{Z}/p\mathbb{Z})^2$.

Exercice 1.27 (Un théorème de Sylow)**.**

Soit G un groupe fini, d'ordre $n = p^\alpha m$ avec p premier et $p \wedge m = 1$.
On note X l'ensemble des parties de G de cardinal p^α, et Y l'ensemble des sous-groupes de G d'ordre p^α.

Le but du jeu est de montrer que $Y \neq \emptyset$, et plus précisément que le nombre de sous-groupes de G d'ordre p^α (*les p-Sylow de G*) est congru à 1 modulo p.

Pour cela, on fait opérer G sur X par translation à gauche : si $g \in G$ et $E \in X$, on pose

$$g \cdot E = gE = \{ga \ ; \ a \in E\} \ .$$

1. Soit $E \in X$. Montrer que son stabilisateur $\mathcal{G}_E = \{g \in G \mid g \cdot E = E\}$ est de cardinal au plus égal à p^α.
2. Soit $E \in X$. Montrer que le cardinal du stabilisateur $\mathcal{G}_E$ est égal à p^α si et seulement si E est une classe à droite modulo un sous-groupe d'ordre p^α (c'est-à-dire $E = H \cdot x$ avec $x \in G$ et $H \in Y$).
3. Montrer que $|X|$ est congru à $m|Y|$ modulo p.
4. Montrer que $|X|$ est congru à m modulo p.
5. Conclure.

Les groupes

Exercice 1.1: Soit a un élément quelconque de E. Comme E est fini la suite $\left(a^{2^n}\right)$ n'est pas injective, donc on peut trouver $n \in \mathbb{N}^*$ et $p > 0$ tels que $a^{2^{n+p}} = a^{2^n}$. On pose $b = a^{2^n}$, alors $b^{2^p} = b$ puis on prend $s = b^{2^p-1}$, on a bien

$$s^2 = b^{2.2^p-2} = b^{2^p}b^{2^p-2} = bb^{2^p-2} = b^{2^p-1} = s$$

Exercice 1.2: Posons $S = \sum_{i=1}^{r} M_i$

1. Soit M_{i_0} un élément de G. L'application de G dans G qui à M associe $M_{i_0}M$ est une bijection. Par suite, on a: $M_{i_0}S = S$ et $S^2 = rS$
2. D'après la relation ci-dessus, on peut écrire: $\left(\frac{S}{r}\right)^2 = \frac{S}{r}$. Par conséquent $\frac{S}{r}$ est un projecteur, sa trace est donc un entier. En conclusion $\mathrm{Tr}\,(S) = \mathrm{Tr}\left(\frac{S}{r}\right) r$ est un entier divisble par r

Exercice 1.3: Il suffit de montrer que l'inverse d'un élément x de H est encore dans H. Puisque H est stable, la suite des itérés $(x^n)_{n\geqslant 1}$ est incluse dans H. Mais puisque H est fini, l'application $n \longmapsto x^n$ ne peut pas être injective. Il existe donc deux entiers n, p, avec $p > n$, tels que $x^n = x^p$. On simplifie par x^n (dans le groupe G) et on trouve $x^{p-n} = e$. Il en découle que e est dans H et que x^{p-n-1} (qui est lui aussi dans H) est l'inverse de x. Conclusion : H est un sous-groupe de G.

Exercice 1.4: Posons e l'élément neutre de G.

1. Commençons par montrer que $C(a)$ est un sous groupe de $(G, .)$.
   - $C(a) \neq \emptyset$ car $ea = ae = a$, donc $e \in C(a)$
   - Soit $x, y \in C(a)$, alors
     $$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$
     Donc $xy \in C(a)$
   - Soit $x \in C(a)$, on a $ax = xa$ et multiplions cette égalité à gauche et à droite par x^{-1}, on obtient donc $x^{-1}a = ax^{-1}$

   Ceci montre bien que $C(a)$ est un sous-groupe de $(G, .)$.
   Il suffit de voir que $Z(G) = \bigcap_{a\in G} C(a)$ est l'intersection d'une famille de sous-groupes de G indexée par un ensemble non vide, donc c'est un sous-groupe.

2. - Déterminons le centre de S_n
     - Si $n = 2$, alors $S_2 = \left\{\mathrm{Id}_{[\![1,2]\!]}, (12)\right\}$ est abélien et donc $Z\left(S_2\right) = S_2$
     - Si $n \geqslant 3$. Montrons que $Z\left(S_n\right) = \left\{\mathrm{Id}_{[\![1,n]\!]}\right\}$.
       Soit $\sigma \in Z\left(S_n\right)$ et $i \in [\![1, n]\!]$. Comme $n \geqslant 3$, il existe deux éléments j, k disrincts de $[\![1, n]\!] \setminus \{i\}$. La permutation σ commute en particulier avec les deux transpositions (i, j) et (i, k). Avec $\sigma(i, j)\sigma^{-1} = (\sigma(i), \sigma(j))$ et d'autre part $\sigma(i, j)\sigma^{-1} = (i, j)$, on tire $\{\sigma(i), \sigma(j)\} = \{i, j\}$. De même $\{\sigma(i), \sigma(k)\} = \{i, k\}$. L'intersection des ensembles $\{i, j\}$ et $\{i, k\}$ est le singleton $\{i\}$, et $\{\sigma(i), \sigma(j)\} \cap \{\sigma(i), \sigma(k)\} = \{\sigma(i)\}$, donc $\sigma(i) = i$
   - Déterminons le centre de $\mathrm{GL_n}\,(\mathbb{K})$.
     Soit $A = (a_{k,l})_{1\leq k,l\leq n} \in \mathrm{GL_n}\,(\mathbb{K})$.
     Si A commute avec toute matrice de $\mathrm{GL_n}\,(\mathbb{K})$, en particulier : $\forall (i, j) \in \{1, ..., n\}^2,\ A(I_n+E_{i,j}) = (I_n+E_{i,j})A$, soit $AE_{i,j} = E_{i,j}A$. Maintenant,

     $$AE_{i,j} = \sum_{k,l} a_{k,\ell}E_{k,\ell}E_{i,j} = \sum_{k=1}^{n} a_{k,i}E_{k,j} \text{ et } E_{i,j}A = \sum_{k,\ell} a_{k,\ell}E_{i,j}E_{k,\ell} = \sum_{\ell=1}^{n} a_{j,l}E_{i,l}.$$

     On note que si $k \neq i$ ou $l \neq j$, $E_{k,j} \neq E_{i,l}$. Puisque la famille $(E_{i,j})_{1\leqslant i,j\leqslant n}$ est libre, on peut identifier les coefficients et on obtient : si $k \neq i$, $a_{k,i} = 0$. D'autre part, le coefficient de $E_{i,j}$ est $a_{i,i}$ dans la première somme et $a_{j,j}$ dans la deuxième. Ces coefficients doivent être égaux.
     Finalement, si A commute avec toute matrice inversible, ses coefficients non diagonaux sont nuls et ses coefficients diagonaux sont égaux. Par suite, il existe un scalaire $\lambda \in \mathbb{K}^*$ tel que $A = \lambda I_n$. Réciproquement, si A est une matrice scalaire non nulle, A commute avec toute matrice inversible.

Les groupes

Exercice 1.5: 1. $\Leftarrow$) Supposons qu'il existe $\gamma \in \mathbb{R}$ tel que $H = \gamma\mathbb{Z}$. Il existe p et q entiers tels que: $a = \gamma.p$ et $b = \gamma.q$. Alors $\frac{a}{b} = \frac{p}{q} \in \mathbb{Q}$

$\Rightarrow$) Réciproquement, si $\frac{a}{b}$ est rationnel, il existe p et q entiers premiers entre eux tels que $\frac{a}{b} = \frac{p}{q}$.
Posons $\gamma = \frac{b}{q}$. On a $a = \gamma p$ et $b = \gamma q$, ce qui prouve que a et b appartiennent à $\gamma\mathbb{Z}$, donc $H \subset \gamma\mathbb{Z}$.
D'autre part, il existe m et n premiers entre eux tels que $mp + nq = 1$. Donc, en multipliant par γ

$$\gamma = mp\gamma + nq\gamma = ma + nb$$

ce qui montre que γ appartient à H, et donc que $\gamma\mathbb{Z}$ est inclus dans H. On a bien l'égalité $H = \gamma\mathbb{Z}$.

2. cos est continue sur $\mathbb{R}$ et $\mathbb{Z} + 2\pi\mathbb{Z}$ est dense dans $\mathbb{R}$, donc par parité et periodicité de cos, la famille $(\cos(n))_{n\in\mathbb{N}}$ est dense dans $\cos(\mathbb{R}) = [-1, 1]$

Exercice 1.6: Les groupes finis vérifient bien sûr la condition. Nous allons montrer que ce sont les seuls.

Soit G un groupe dont l'ensemble des sous-groupes est fini. Tout x de G est d'ordre fini, sinon G contiendrait un sous-groupe isomorphe à $\mathbb{Z}$, qui contiendrait lui-même une infinité de sous-groupes.

Si E' désigne l'ensemble des sous-groupes cycliques de G, alors $G = \bigcup_{H\in E'} H$. Comme E' est par hypothèse fini et que les éléments de E' sont tous des ensembles finis, G est bien fini.

Exercice 1.7: Notons K le complémentaire de H dans G et montrons $< K >= G$.

- On a évidemment $< K > \subset G$.
- Inversement, on a $K \subset < K >$ et il suffit d'établir $H \subset < K >$ pour conclure.
  Puisque H est un sous-groupe strict de G, son complémentaire K est non vide et donc il existe $a \in K$.
  Pour $x \in H$, l'élément $a.x$ ne peut appartenir à H car sinon $a = (a.x)x^{-1}$ serait élément du sous-groupe H.
  On en déduit que $a.x \in K$ et donc $x = a^{-1}.(a.x) \in < K >$. Ainsi $G = H \cup K \subset < K >$ et on peut conclure $< K >= G$.

Exercice 1.8: Soit f un tel morphisme. Son image est un sous-groupe de $\mathbb{Z}$, c'est-à-dire un certain $n\mathbb{Z}$, $n \in \mathbb{N}$.

Si $n \geqslant 1$, soit x un antécédent de n. On a alors $2f(x/2) = f(x) = n$, donc $n/2 = f(x/2) \in n\mathbb{Z}$, ce qui est absurde. On a donc $n = 0$, et f est nul.

Exercice 1.9: Par récurrence sur n :

- Pour $n = 1$: les sous-groupes de $\mathbb{Z}$ sont les $c\mathbb{Z}$, $c \in \mathbb{N}$. G est non nul alors $c \neq 0$, et G est isomorphe à $\mathbb{Z}$, un isomorphisme étant $\mathbb{Z} \longrightarrow c\mathbb{Z},\ x \longmapsto cx$.
- Soit $n \in \mathbb{N}^*$, supposons que pour tout $k \leqslant n-1$, si H est un sous-groupe de $\left(\mathbb{Z}^k, +\right)$, alors il existe $r \in [\![1, k]\!]$ tel que H est isomorphe à $\mathbb{Z}^r$.
  Soit alors H un sous-groupe de $\mathbb{Z}^n$. On considère $f : \mathbb{Z}^n \longrightarrow \mathbb{Z}, (x_1, \cdots, x_n) \longmapsto x_n$, morphisme surjectif de groupe. Alors $f(H)$ est un sous-groupe de $(\mathbb{Z}, +)$; il existe donc $c \in \mathbb{N}$ tel que $f(H) = c\mathbb{Z}$.
  - Si $c = 0$, alors $H \subset \mathrm{Ker}(f) = \mathbb{Z}^{n-1} \times \{0\} \simeq \mathbb{Z}^{n-1}$. Par hypothèse de récurrence, H est donc isomorphe à un certain $\mathbb{Z}^r$ où $r \in [\![1, n-1]\!]$.
  - Si $c > 0$: Soit $v \in H$ tel que $f(v) = c$. Alors, pour $h \in H$, $\frac{f(h)}{c} = \alpha \in \mathbb{Z}$. Ainsi,

    $$f(h - \alpha v) = f(h) - f(\alpha v) = \alpha c - f(\alpha v) = 0$$

    Donc $h - \alpha v \in \mathrm{Ker}(f) \cap H$. Posons $H' = \mathrm{Ker}(f) \cap H$. Alors $H' \sim \mathbb{Z}^r$ pour un certain $r \in [\![1, n-1]\!]$ Considérons maintenant l'application $u : H' \times \mathbb{Z} \longrightarrow H, (h, v) \longmapsto h + nv$. Alors u est un morphisme. u est surjectif : soit $h \in H$. Il existe alors $\alpha \in \mathbb{Z}$ tel que $h - \alpha v \in H'$. Ainsi, si on pose $h' = h - \alpha v$, on a $h = u(h', \alpha)$. u est injectif : si $u(h', n) = 0$, alors $h' + nv = 0$, donc $f(h' + nv) = f(h') + nc = 0$, d?où $n = 0$, puis $h' = 0$. Donc u est un isomorphisme, et H est isomorphe à $\mathbb{Z}^{r+1}$ $(r + 1 \in [\![1, n]\!])$, ce qui achève la récurrence.

Les groupes

Exercice 1.10: 1. Soit $k \in \mathbb{Z}^*$, alors

$$\begin{aligned} r^k = I_2 &\iff \begin{pmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{pmatrix} = I_2 \\ &\iff \begin{cases} \cos k\theta = 1 \\ \sin k\theta = 0 \end{cases} \\ &\iff k\theta \in 2\pi\mathbb{Z} \\ &\iff \exists m \in \mathbb{Z}, \quad k\theta = 2\pi m \end{aligned}$$

r est d'ordre fini s'il existe $(k, m) \in \mathbb{Z}^* \times \mathbb{Z}$ tel que $\dfrac{\theta}{2\pi} = \dfrac{m}{k}$. Autrement-dit si, et seulement, si $\dfrac{\theta}{2\pi} \in \mathbb{Q}$ Si $\dfrac{\theta}{2\pi} \notin \mathbb{Q}$, alors r est d'ordre infini

2. Si $\dfrac{\theta}{2\pi} \in \mathbb{Q}$, alors r est d'ordre fini. Cherchons son ordre n.
On écrit $\dfrac{\theta}{2\pi} = \dfrac{p}{q} \in \mathbb{Q}$, avec $\begin{cases} (p, q) \in \mathbb{Z} \times \mathbb{N}^* \\ p \wedge q = 1 \end{cases}$, alors

$$r^k = I_2 \iff k \in q\mathbb{Z}$$

Donc $\circ(r) = q$

Exercice 1.11: 1. Soient $f : G \to G'$ un isomorphisme de groupes et a un élément de G d'ordre n. Comme $e' = f(e) = f(a^n) = (f(a))^n$, on en déduit que $f(a)$ est d'ordre fini, divisant n.
Si $f(a)^k = e'$, alors $f(a^k) = e'$ donc $a^k = e$ car f injective, d'où n divise k. Il en résulte que $f(a)$ est d'ordre n.

2. $\varphi : G \longrightarrow G, x \longmapsto axa^{-1}$ est un isomorphisme et $ba = \varphi_a(ba)$

Exercice 1.12: Soit n' et k' de $\mathbb{Z}$ tels que $n = dn'$ et $k = dk'$

1. Il s'agit d'un résultat de cours, $\circ\left(\overline{k}\right) = \dfrac{n}{n \wedge k} = \dfrac{n}{d}$

2. On sait déjà que $k = dk'$, donc $\overline{k} = k'\overline{d}$ et $\overline{k} \in < \overline{d} >$, puis l'inclusion $< \overline{k} > \subset < \overline{d} >$. Or $< \overline{d} >$ est d'ordre $\dfrac{n}{d} = \mathbf{Card}\left(< \overline{k} >\right)$, donc l'égalité

3. Soit H un sous groupe additif de $\mathbb{Z}/n\mathbb{Z}$, alors H est cyclique: il existe $k \in \mathbb{Z}$ tel que $H = < \overline{k} >$. On pose $d = n \wedge k$, on a $H = < \overline{d} >$. On conclut donc qu'il existe d diviseur de n tel que $H = < \overline{d} >$.
Inversement si d est un diviseur de n il est clair que $< \overline{d} >$ est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.
Bilan H est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il existe d diviseur de n tel que $H = < \overline{d} >$

Exercice 1.13: 1. Posons $m = \mathbf{ppcm}(p, q)$, alors il existe $a, b \in \mathbb{N}$ tels que $m = ap$ et $m = bq$. Par définition du groupe produit

$$(h, k)^m = (h^m, k^m) = (e_H, e_K)$$

donc (h, k) est d'ordre fini.
Soit $k \in \mathbb{Z}$, on a:

$$\begin{aligned} (h, k)^\alpha = (e_H, e_K) &\iff (h^\alpha, k^\alpha) = (e_H, e_K) \\ &\iff \begin{cases} h^\alpha = e_H \\ k^\alpha = e_K \end{cases} \\ &\iff \begin{cases} p \mid \alpha \\ q \mid \alpha \end{cases} \\ &\iff m \mid \alpha \end{aligned}$$

On conclut donc que $\circ((h, k)) = m$

2. Soit h et k respectivement les générateurs de H et K et p et q sont respectivement leurs ordres

   $\Leftarrow$) Si $p \wedge q = 1$, alors (h,k) est d'ordre pq, avec $(h,k) \in H \times K$ et $\mathbf{Card}\,(H \times K) = pq$, on conclut que $H \times K$ est cyclique de générateur (h,k)

   $\Rightarrow$) Par contraposée, si p et q ne sont pas premiers entre eux, alors tout élément de $H \times K$ est d'ordre inférieur au $\mathbf{ppcm}(p,q) < pq = \mathbf{Card}\,(H \times K) = pq$,

EXERCICE 1.14: 1. Soit x et y deux éléments de G. Alors $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$, donc G est abélien.

2. Montrons que $H \cup xH$ est un sous-groupe de G, plus précisément qu'il est égal au sous-groupe K engendré par x et H.

   - On a clairement $H \cup xH \subset K$.
   - Réciproquement, x étant d'ordre 2, tout élément de K s'écrit $x^{\alpha}h$, avec $\alpha \in \{0,1\}$ et $h \in H$, donc $K \subset H \cup xH$.

   H est disjoint de xH, car sinon il existerait $h \in H$ qui s'écrirait $h = xk$, mais alors $x = k^{-1}h$ serait dans H

3. Montrons par récurrence sur $\mathbf{Card}G$ que $\mathbf{Card}G$ est une puissance de 2.

   Il n'y a rien à vérifier pour $\mathbf{Card}G = 1$.

   Supposons $\mathbf{Card}G \geqslant 2$. On considère les sous-groupes de G distincts de G. Il en existe, par exemple $\{e\}$. Choisissons-en un de cardinal maximal, que l'on notera H. D'après l'hypothèse de récurrence, $\mathbf{Card}H$ est une puissance de 2 (en effet, H vérifie la même propriété que G).

   Soit $a \in G \setminus H$. . Donc $\mathbf{Card}(H \cup aH) = 2\mathbf{Card}H$. De la maximalité du cardinal de H, on déduit alors que $G = H \cup aH$. Donc $\mathbf{Card}G = 2\mathbf{Card}H$ est encore une puissance de 2.

EXERCICE 1.15:
- **Existence:** Comme p et n sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tel que $nu + pv = 1$. Posons alors $b = a^{pv}$ et $c = a^{nu}$. Alors
  - $bc = cb = a^{nu+pv} = a$
  - L'égalité $nu + pv = 1$ montre que $n \wedge v = 1$ et $p \wedge u = 1$ et, par suite, $\circ(b) = \circ(a^{pv}) = \dfrac{np}{np \wedge pv} = n$. De même $\circ(c) = p$
- **Unicité:** Soit $b', c' \in G$ tels que: $\begin{cases} b' \text{ est d'ordre } n; \\ c' \text{ est d'ordre } p; \\ a = b'c' = c'b'. \end{cases}$.

  Montrons que $b = b'$.
  De $a = b'c' = c'b'$ on tire $a^{pv} = b'^{pv}$, puis on utilise $b'^{nu} = e$, on obtient $b' = b'^{pv+nu} = b'^{pv}b'^{nu} = a^{pv} = b$
  En fin de $bc = a = bc'$, on obtient $c = c'$

EXERCICE 1.16: On définit la relation $\mathcal{R}$ sur G par

$$x\mathcal{R}y \Longleftrightarrow y = x \text{ ou } y = x^{-1}$$

La relation est immédiatement est une relation d'équivalence (à vérifier).
S'il n'existe pas dans $(G,.)$ d'élément d'ordre 2, les classes d'équivalence de la relation $\mathcal{R}$ comportent toutes deux éléments sauf celle de e qui ne comporte qu'un élément. Les classes d'équivalence étant disjointes de réunion G, le cardinal de G est alors impair ce qui est contraire aux hypothèses.

EXERCICE 1.18: D'après le théorème de Lagrange, les éléments de G sont d'ordre 1, 2, p ou $2p$. Supposons par l'absurde qu'il n'y a aucun élément d'ordre p. Alors, en particulier, G n'est pas cyclique (car si x engendre G, alors x^2 est d'ordre p), et si $x \in G$, x est d'ordre 1 ou 2. En particulier, $p \geqslant 3$, et pour tout $x \in G$, $x^2 = 1$, alors G est abélien et $\mathbf{Card}G$ est une puissance de 2, donc p est une puissance de 2, ce qui est absurde.

EXERCICE 1.19:
- Soit $a \in G \setminus \{e\}$, alors $< a >$ est un sous-groupe de G autre que $\{e\}$, donc $< a >= G$. Ainsi G est monogène
- Si a n'est pas d'ordre fini, alors le sous-groupe engendré par a^2 est non trivial de G. Absurde

LES GROUPES

- Notons $n = \mathbf{Card}(G) = \circ(a)$. On a bien $n \geqslant 2$. Si n n'est pas premier alors il existe un diviseur propre p de n. On écrit $n = pq$ et on pose $b = a^q$, alors $< b >$ est un sous-groupe de G d'ordre p et donc non trivial. Absurde

EXERCICE 1.20: Le premier théorème d'isomorphisme

EXERCICE 1.21: Si $\{i, j\}$ est stable par σ alors $\{\sigma(i), \sigma(j)\} = \{i, j\}$. On a alors

$$\forall x \notin \{i, j\}, \quad (\sigma \circ \tau)(x) = \sigma(x) = (\tau \circ \sigma)(x)$$

Pour $x = i$ alors $(\sigma \circ \tau)(i) = \sigma(j) = (\tau \circ \sigma)(i)$ et pour $x = j, (\sigma \circ \tau)(j) = \sigma(i) = (\tau \circ \sigma)(j)$. Par suite

$$\sigma \circ \tau = \tau \circ \sigma$$

Inversement, si $\sigma \circ \tau = \tau \circ \sigma$ alors $\sigma(i) = (\sigma \circ \tau)(j) = (\tau \circ \sigma)(j) = \tau(\sigma(j))$. Puisque $\tau(\sigma(j)) \neq \sigma(j)$ on a $\sigma(j) \in \{i, j\}$. De même $\sigma(i) \in \{i, j\}$ et donc $\{i, j\}$ stable par σ.

EXERCICE 1.22: On a $c.c' = c'.c$ où c et c' sont deux cycles d'ordre n. On écrit $c = \begin{pmatrix} 1 & c(1) & \cdots & c^{n-1}(1) \end{pmatrix}$ et $c = \begin{pmatrix} 1 & c'(1) & \cdots & c'^{(n-1)}(1) \end{pmatrix}$.
L'ensemble $\{1, \cdots, n\}$ est égal à $\{1, c(1), \cdots, c^{n-1}(1)\}$. Il existe donc r tel que $c'(1) = c^r(1)$ avec $0 \leqslant r \leqslant n-1$. De plus, si $i \in [\![1, n]\!]$, il existe s tel que $i = c^s(1)$, avec $0 \leqslant s \leqslant n-1$; Donc

$$\begin{aligned} c'(i) &= c' \circ c^s(i) = c^s \circ c'(1) \\ &= c^s \circ c^r(1) = c^r \circ c^s(1) = c^r(i) \end{aligned}$$

Donc $c' = c^r$

EXERCICE 1.23: Soit, pour $1 \leqslant i \leqslant p$, $y_i = \sigma(x_i)$ et $y_{p+1} = y_1$. Alors $\sigma \begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix} \sigma^{-1}(y_i) = y_{i+1}$.
Si $y \notin \{y_1, \cdots, y_p\}$ alors $\sigma \begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix} \sigma^{-1}(y) = y$. Donc

$$\sigma \begin{pmatrix} a_1 & a_2 & \ldots & a_p \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(x_1), \cdots, \sigma(x_p) \end{pmatrix}$$

EXERCICE 1.24:

1. $\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} 1 & i \end{pmatrix} \begin{pmatrix} 1 & j \end{pmatrix} \begin{pmatrix} 1 & i \end{pmatrix}$

2. On prend $i < j$. Supposons $i + 1 < j$. Alors,

$$\begin{pmatrix} i & j \end{pmatrix} = \begin{pmatrix} j-1 & j \end{pmatrix} \begin{pmatrix} i & j-1 \end{pmatrix} \begin{pmatrix} j-1 & j \end{pmatrix} \tag{1}$$

   Si $j - 1 = i + 1$, $\begin{pmatrix} i & j \end{pmatrix} \in \{\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \end{pmatrix}, \cdots, \begin{pmatrix} n-1 & n \end{pmatrix}\}$. Sinon, on applique la formule (1) en remplaçant $\begin{pmatrix} i & j \end{pmatrix}$ par $\begin{pmatrix} i & j-1 \end{pmatrix}$ dans cette formule. Et de proche en proche, on arrive au résultat.

3. Par récurrence sur $i \in [\![2, n]\!]$, on montre

$$\begin{pmatrix} 1 & i \end{pmatrix} = \begin{pmatrix} 2 & 3 & \cdots & n \end{pmatrix}^{i-2} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 & \cdots & n \end{pmatrix}^{2-i}$$

   Ce qui donne la conclusion en utilisant la première question.

EXERCICE 1.25:

1. Soit $i, j, k, \ell \in [\![1, n]\!]$ tels que $\{i, j\} \cap \{k, \ell\} = \emptyset$, alors

$$\begin{aligned} \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} k & \ell \end{pmatrix} &= \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} k & j \end{pmatrix} \begin{pmatrix} k & j \end{pmatrix} \begin{pmatrix} k & \ell \end{pmatrix} \\ &= \begin{pmatrix} i & j & k \end{pmatrix} \begin{pmatrix} j & k & \ell \end{pmatrix} \end{aligned}$$

   Tout élément σ de A_n est le produit d'un nombre pair de transpositions. Donc, σ est produit de 3-cycles. Le sous-groupe de A_n engendré par les 3-cycles contient donc A_n . C'est donc A_n .

2. Soit i, j et k deux à deux distincts et supérieurs ou égaux à 3.

$$\begin{aligned} (ijk) &= (12i)(2jk)(12i)^{-1} \\ (2jk) &= (12j)(12k)(12j)^{-1} \end{aligned}$$

   Donc, $A_n \subset \langle (123), \cdots, (12n) \rangle$, ce qui prouve que $A_n = \langle (123), \cdots, (12n) \rangle$.

Les groupes

Exercice 1.26: 1. Voir le devoir libre 01

2. G est abélien (Voir le devoir libre 01)

   - S'il existe un élément de G d'ordre p^2, alors G est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$
   - Sinon tout élément de $G \setminus \{e\}$ est d'ordre p. Soit alors $a \in G \setminus \{e\}$ et $b \in G \setminus \mathrm{gr}\,(a)$. Le sous-groupe $\mathrm{gr}\,(a,b) = \{a^m b^n \ ,\ m,n \in [\![0,p-1]\!]\}$ est ismorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ et par suite $G = \mathrm{gr}\,(a,b) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Exercice 1.27: 1. Les translations étant des permutations de G, si $E \in X$, on a bien $g \cdot E \in X$, c'est-à-dire $|g \cdot E| = |E| = p^\alpha$. De plus, avec $E \in X$, les égalités $e \cdot E = E$ et $(gh) \cdot E = g \cdot (h \cdot E)$ sont immédiates, on a donc bien une action du groupe G sur l'ensemble X.
Soit $E \in X$, soit $a \in E$ donné ; si $g \in \mathcal{G}_E$, alors $ga \in g \cdot E = E$, donc $g \in Ea^{-1}$. On a donc $\mathcal{G}_E \subset Ea^{-1}$, où a est un élément quelconque de E, d'où $|\mathcal{G}_E| \leqslant |Ea^{-1}| = |E| = p^\alpha$.
Rappelons que le stabilisateur $\mathcal{G}_E$ d'un élément E de X est un sous-groupe de G (vérification immédiate).

2. • Si $E = Hx$ avec $H \in Y$, alors

$$g \in \mathcal{G}_E \iff gE = E \iff gHx = Hx \iff gH = H$$

mais, H étant un sous-groupe, cette dernière condition équivaut à $g \in H$. On a alors $\mathcal{G}_E = H$, d'où $|\mathcal{G}_E| = p^\alpha$.
• Si $|\mathcal{G}_E| = p^\alpha$, alors $\mathcal{G}_E$ est un sous-groupe d'ordre p^α, posons $H = \mathcal{G}_E \in Y$. Si on se donne $a \in E$, on a $H \subset Ea^{-1}$ d'après la question **1.**, d'où $H = Ea^{-1}$ (égalité des cardinaux), donc $E = Ha$: E est une classe à droite modulo a.

3. Les éléments de X de la forme Hx avec $H \in Y$ et $x \in G$ sont au nombre de $m|Y|$: chaque sous-groupe d'ordre p^α, s'il en existe, définit m classes à droite distinctes et deux sous-groupes distincts ne peuvent engendrer une même classe à droite (supposons $H_1x_1 = H_2x_2$, alors $x_1 = ex_1 \in H_2x_2$, donc $x_1x_2^{-1} \in H_2$ puis $x_2x_1^{-1} = (x_1x_2^{-1})^{-1} \in H_2$ et enfin $H_1 = H_2x_2x_1^{-1} = H_2$).
Les autres éléments E de X ont un stabilisateur $\mathcal{G}_E$ dont le cardinal est strictement inférieur à p^α, mais divise $p^\alpha m$ (car les stabilisateurs sont des sous-groupes de G), donc $|\mathcal{G}_E|$ est de la forme $p^k d$, avec $0 \geqslant k \geqslant \alpha - 1$ et $d \mid m$. Ils ont donc une orbite dont le cardinal (qui est l'indice du stabilisateur), $[G : \mathcal{G}_E] = p^{\alpha-k}\dfrac{m}{d}$, est multiple de p.
Les orbites de X sous l'action de G par translation à gauche étant deux à deux disjointes, on déduit $|X| \equiv m|Y|$ modulo p.

4. Le cardinal de X ne dépend que de l'ordre du groupe G et non de sa structure : c'est le nombre de parties à p^α éléments d'un ensemble à $n = p^\alpha m$ éléments. On peut donc supposer ici que $G = \mathbb{Z}/n\mathbb{Z}$. Dans ce cas, G, cyclique d'ordre $p^\alpha m$, admet un unique sous-groupe d'ordre p^α, donc $|Y| = 1$ et $|X| \equiv m$ modulo p.
Cette question est d'ordre purement combinatoire : il s'agit de prouver que, pour p premier, $\alpha \in \mathbb{N}$ et $m \wedge p = 1$, on a $C_{p^\alpha m}^{p^\alpha} \equiv m$ modulo p. Si quelqu'un a une démonstration élémentaire de ce résultat, je suis preneur...

5. On a $m|Y| \equiv m$ modulo p d'après les questions **3.** et

4. Comme m et p sont premiers entre eux, on peut simplifier cette congruence : il reste $|Y| \equiv 1$ modulo p, ce que l'on voulait prouver et, en particulier, $|Y| \neq 0$.