UNIVERSITÉ GRENOBLE-ALPES Prépa Agreg

Enseignant : Rémi Molinier
remi.molinier@univ-grenoble-alpes.fr

Exercices sur les groupes

Merci beaucoup à Vincent Beck pour presque l'entièreté des exercices de cette longue liste.

1 Les inexcusables.

Exercice 1 – Classification des groupes d'ordre 1 à 7
Il est **impératif** de connaître cette classification et surtout de savoir la faire vite. Pour les groupes d'ordre 8 à 11, il faut connaître la classification.

Exercice 2 – Classification des groupes d'ordre p^2

1) **Lemme 1.** Montrer que le centre d'un p-groupe non trivial est non réduit à l'élément neutre (voir l'exercice 15).

2) **Lemme 2.** Soit G un groupe et H un sous-groupe du centre de G. Montrer que $H \lhd G$. On suppose de plus que G/H est un groupe monogène (fini ou infini). Montrer que G est commutatif.

3) Montrer qu'un groupe d'ordre p^2 est commutatif.

4) En déduire qu'un groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou $(\mathbb{Z}/p\mathbb{Z})^2$ (distinguer suivant l'existence ou non d'un élément d'ordre p^2).

5) Que dire du centre d'un groupe G d'ordre p^3 ? Et de son groupe dérivé ? à quel groupe est isomorphe G/ZG

6) **Complément.** Soit G un groupe **non abélien** d'ordre pq (où p et q sont des nombres premiers distincts). Déterminer le centre de G.

2 Rappel généraux sur les groupes : le cours

Exercice 3 – Groupe quotient
Soit G un groupe, H un sous-groupe de G. On définit les relations d'équivalences sur G $\mathscr{R}_H$ et $\mathscr{R}'_H$ par

$$x\mathscr{R}_H y \iff x^{-1}y \in H \qquad et \qquad x\mathscr{R}'_H y \iff xy^{-1} \in H\,.$$

Les ensembles quotients correspondant se note G/H et $H\backslash G$ (plutôt que $G/\mathscr{R}_H$ et $\mathscr{R}'_H\backslash G$).

1) Décrire la classe de x pour $\mathscr{R}_H$ (classe à gauche modulo H) et $\mathscr{R}'_H$ (classe à droite modulo H).

2) Montrer l'équivalence des propositions suivantes

(i) $\mathscr{R}_H = \mathscr{R}'_H$;
(ii) $\forall x \in G, \quad xHx^{-1} = H$;
(iii) $\forall x \in G, \quad xHx^{-1} \subset H$;
(iv) $\forall x \in G, \quad H \subset xHx^{-1}$;
(v) $\forall x \in G, \quad xH = Hx$;
(vi) $\forall x \in G, \quad xH \subset Hx$;
(vii) $\forall x \in G, \quad Hx \subset Hx$;

(viii) toute classe à gauche modulo H est une classe à droite modulo H ;

(ix) toute classe à droite modulo H est une classe à gauche modulo H ;

(x) il existe un groupe G' et $f : G \to G'$ un morphisme de groupes tel que $\ker f = H$;

(xi) il existe un groupe G' et $f : G \to G'$ un morphisme surjectif de groupes tel que $\ker f = H$;

(xii) il existe sur G/H une structure de groupes telle que la surjection canonique $\pi : G \to G/H$ soit un morphisme de groupes (une telle structure est alors unique) ;

(xiii) il existe sur G/H une structure de groupes telle que la surjection canonique $\pi : G \to H\backslash G$ soit un morphisme de groupes (une telle structure est alors unique) ;

(xiv) $\mathscr{R}_H$ est compatible avec la loi de G ;

(xv) $\mathscr{R}'_H$ est compatible avec la loi de G.

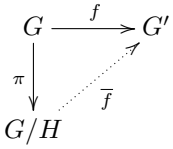
Un sous-groupe H vérifiant ces propriétés est appelé sous-groupe *distingué* dans G.

3) Trouver un exemple de triplet (G, H, x) avec G groupe, H sous-groupe de G et $x \in G$ tel que $xHx^{-1} \subsetneq H$ (on pourra penser au cas où H est le sous-groupe engendré par une transvection dans $GL(V)$).

4) Soit $\mathscr{R}$ une relation d'équivalence sur un groupe G. Montrer qu'il existe sur $G/\mathscr{R}$ une structure de groupe telle que la surjection canonique π soit un morphisme de groupes (cette structure étant alors unique) si et seulement si $\mathscr{R}$ est compatible avec la loi de G. De plus, montrer que si ces conditions sont vérifiées, il existe un sous-groupe distingué H de G tel que $\mathscr{R} = \mathscr{R}_H$.

5) Propriété universelle du quotient. Soient G un groupe, H un sous-groupe distingué de G et $\pi : G \to G/H$ la surjection canonique. On considère un groupe G' et $f : G \to G'$ un morphisme de groupes. Montrer l'équivalence des trois propriétés suivante

(i) Il existe une application $\overline{f} : G/H \to G'$ telle que $f = \overline{f} \circ \pi$ i.e. telle que le diagramme suivant soit commutatif



(ii) $H \subset \ker f$

(iii) $f(H) = \{1_G\}$.

Montrer que lorsque ces conditions sont vérifiées, l'application $\overline{f}$ est uniquement définie et que c'est un morphisme de groupes. Vérifier que $\operatorname{Im} \overline{f} = \operatorname{Im} f$ et $\ker \overline{f} = \ker f/H$ et que $\overline{f}$ est donnée par $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in G$ (où $\overline{x} = \pi(x)$ désigne la classe de x dans G/H).

Morale (à retenir) : *se donner un morphisme de groupes issu d'un quotient, c'est la même chose que de se donner un morphisme trivial sur le groupe par lequel on veut quotienter. C'est donc très facile de construire des morphismes issus de quotient.*

6) Montrer que l'application

$$\begin{aligned} \operatorname{Hom}_{\text{gr.}}(G/H, G') &\longrightarrow \operatorname{Hom}_{\text{gr.}}(G, G') \\ \varphi &\longmapsto \varphi \circ \pi \end{aligned}$$

est une application injective dont on déterminera l'image. Pour un élément de l'image, on décrira l'unique antécédent.

7) Premier théorème d'isomorphisme. Soit $f : G \to G'$ un morphisme de groupes. Montrer que f induit un isomorphisme de groupes $\varphi : G/\ker f \to \operatorname{Im} f$ donné par $\varphi(g \ker f) = f(g)$ pour tout $g \in G$. Qu'obtient-on lorsque f est surjectif ?

8) Soient G et G' deux groupes finis et $f : G \to G'$ un morphisme de groupes. Montrer que $|\operatorname{Im} f| \mid |G|$ et $|\operatorname{Im} f| \mid |G'|$. En déduire que si $\operatorname{pgcd}(|G|, |G'|) = 1$ alors f est le morphisme trivial.

Exercice 4 – Quelques exemples de sous-groupes distingués

1) $GL_m^+(\mathbb{R})$ est un sous-groupe distingué de $\mathrm{GL}_m(\mathbb{R})$.

2) Montrer que si T est un sous-groupe de $k^\times$ alors $G_T = \det^{-1}(T)$ est un sous-groupe distingué de $\mathrm{GL}_n(k)$.

3) Montrer que les sous-groupes distingués de $\mathrm{GL}_n(k)$ sont les G_T et les $T\,\mathrm{Id}$ pour T parcourant les sous-groupes de $k^\times$ (sauf si $k = \mathbb{F}_2, \mathbb{F}_3$ et $n = 2$).

4) Montrer que si $H \leq ZG$ alors $H \trianglelefteq G$: tous les sous-groupes du centre sont distingués.

5) Si $n \neq 4$, montrer que les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $1, \mathfrak{A}_n$ et $\mathfrak{S}_n$. Que se passe-t-il pour $n = 4$?

6) Montrer que tout sous-groupe d'un groupe abélien est distingué. La réciproque est-elle vraie ? (penser au groupe $\mathbb{H}_8$)

7) Montrer que si $D(G) = [G, G] \leq H$ alors H est distingué dans G et que G/H est commutatif.

8) Si $H \leq G$. Montrer qu'il existe un plus groupe sous-groupe de G dans lequel H est distingué (nommé *normalisateur de G dans H*) et noté $N_G(H)$. Montrer que $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

9) Montrer que $H \trianglelefteq G$ si et seulement si $N_G(H) = G$.

10) Montrer qu'un sous-groupe d'indice 2 est distingué.

11) On suppose que G est fini. On note p le plus petit diviseur premier de $|G|$ et H un sous-groupe d'indice p de G (un tel sous-groupe n'existe pas forcément). Montrer que $H \lhd G$.

12) Montrer que $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$.

Exercice 5 – Théorème de correspondance

Soient G et H deux groupes et $f : G \to H$ un morphisme **surjectif** de groupes. On note $K = \ker f$, $\mathscr{G}$ (resp. $\mathscr{G}_K$) l'ensemble des sous-groupes de G (resp. contenant K), $\mathscr{H}$ l'ensemble des sous-groupes de H.

1) Montrer que l'application

$$\begin{aligned} \alpha\colon \mathscr{G} &\longrightarrow \mathscr{H} \\ G' &\longmapsto f(G') \end{aligned}$$

est bien définie.

2) Montrer que l'application

$$\begin{aligned} \beta\colon \mathscr{H} &\longrightarrow \mathscr{G} \\ H' &\longmapsto f^{-1}(H') \end{aligned}$$

est bien définie et à valeurs dans $\mathscr{G}_K$.

3) Pour $H' \in \mathscr{H}$ et $G' \in \mathscr{G}$, calculer $\alpha \circ \beta(H')$ et $\beta \circ \alpha(G')$. En déduire que β est injective, α est surjective et β et α sont des bijections réciproques l'une de l'autre entre $\mathscr{G}_K$ et $\mathscr{H}$.

4) Montrer que ces bijections induites par α et β conservent les inclusions, les intersections (attention, ce n'est pas purement formel), les sous-groupes distingués, l'indice.

5) Deuxième théorème d'isomorphisme. Soit H' (resp. G') un sous-groupe distingué de H (resp. G contenant K). Construire un isomorphisme de groupes entre $G/\beta(H')$ et H/H' (resp. entre G/G' et $H/\alpha(G')$).

6) Application. On considère un groupe G, K un sous-groupe distingué de G et $f : G \to G/K$ la surjection canonique. Décrire des bijections respectant les inclusions, les intersections, les sous-groupes distingués et l'indice entre les sous-groupes de G contenant K et les sous-groupes de G/K. Déduire de la question e, l'isomorphisme $G/H \cong_{gr.} (G/K)/(H/K)$ pour tout sous-groupe H distingué dans G et contenant K.

7) **Application.** Rappeler la description des sous-groupes de $\mathbb{Z}$. à quelle condition a-t-on $n\mathbb{Z} \subset d\mathbb{Z}$? Soit $n \in \mathbb{N}^*$. Déduire de ce qui précède que pour tout diviseur d de n, il existe un unique sous-groupe d'**indice** d de $\mathbb{Z}/n\mathbb{Z}$ et un unique sous-groupe d'**ordre** d de $\mathbb{Z}/n\mathbb{Z}$. Montrer que ces sous-groupes sont cycliques et donnez-en un générateur (attention au piège !) En déduire que tout sous-groupe d'un groupe cyclique (i.e. monogène et fini) est encore un groupe cyclique.

Soit $k \in \mathbb{Z}$. Quel est le cardinal du sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de k ?

8) **Application.** Soit G un groupe et $D(G)$ son groupe dérivé. Montrer que tout sous-groupe H contenant $D(G)$ est distingué dans G et que le quotient G/H est commutatif.

Exercice 6 – Centralisateur

Soient G un groupe, S une partie de G et $H \leq G$. On note

$$Z_H(S) = \{g \in H \mid \forall\, s \in S,\ sg = gs\}\,.$$

1) Montrer que $Z_H(S)$ est un sous-groupe de H.

2) On suppose $S \subset T$. Comparer $Z_H(S)$ et $Z_H(T)$.

3) On suppose $H' \leq H$. Comparer $Z_{H'}(S)$ et $Z_H(S)$.

4) En déduire que $Z_H(S) = Z_G(S) \cap H$.

5) On note $Z(G)$ plutôt que $Z_G(G)$. On dit que c'est le *centre de* G. à quelle condition a-t-on $Z(G) = G$?

6) Montrer que $Z(G)$ est distingué dans G et que tout sous-groupe de $Z(G)$ est distingué dans G.

7) Relier $Z(G)$ au noyau du morphisme de groupes

$$\begin{aligned} \mathrm{Int}\colon G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto (c_g : x \mapsto gxg^{-1})\,. \end{aligned}$$

8) Calculer le centre d'un groupe d'ordre pq non abélien (où p et q sont deux nombres premiers distincts, voir 2).

9) Soient G et H deux groupes. Calculer $Z(G \times H)$.

10) Calculer $Z(\mathfrak{S}(X))$, $Z(\mathfrak{A}(X))$, $Z(GL(V))$, $Z(SL(V))$, $Z(B)$ où B désigne le groupe des matrices triangulaires inversibles.

11) Si V est un espace vectoriel euclidien, calculer $Z(O(V))$, $Z(SO(V))$.

Exercice 7 – Groupe dérivé

Soit G un groupe. Pour $x, y \in G$, on note $[x, y] = xyx^{-1}y^{-1}$ le *commutateur* de x et y et on définit $D(G)$ (parfois noté $[G, G]$) le sous-groupe engendré par les commutateurs.

1) Montrer que tout élément de $D(G)$ est un produit de commutateurs.

2) Donner une condition nécessaire et suffisante pour que $D(G) = 1$.

3) Soient G, H deux groupes et $\varphi : G \to H$ un morphisme de groupes. Montrer que φ induit un morphisme de groupes de $D(G)$ dans $D(H)$ (surjectif (resp. injectif, bijectif) si φ l'est).

4) En déduire que $D(G)$ est un sous-groupe caractéristique de G et donc un sous-groupe distingué de G.

5) Déduire de la question c que si tout morphisme de groupes $\varphi : G \to H$ induit un morphisme de groupes $\widetilde{\varphi} : G/D(G) \to H/D(H)$ (surjectif (resp. bijectif) si φ l'est). Donner un exemple où φ est injectif et $\widetilde{\varphi}$ ne l'est pas.

6) Montrer que si H est commutatif et $\varphi : G \to H$ un morphisme de groupes alors $D(G) \subset \ker \varphi$.

7) Montrer que $G/D(G)$ est commutatif et que tout sous-groupe de G contenant $D(G)$ est un sous-groupe distingué de G.

8) Soit A un groupe abélien. Montrer que tout morphisme de groupes de G dans A se factorise de façon unique par la surjection canonique $\pi : G \to G/D(G)$.

9) En déduire que

$$\begin{aligned} \mathrm{Hom}_{\mathrm{gr.}}(G/D(G), A) &\longrightarrow \mathrm{Hom}_{\mathrm{gr.}}(G, A) \\ \varphi &\longmapsto \varphi \circ \pi \end{aligned}$$

est un isomorphisme de groupes (au fait, c'est quoi la structure de groupes sur $\mathrm{Hom}_{\mathrm{gr.}}(G, A)$ et si A n'est pas commutatif, est-ce que $\mathrm{Hom}_{\mathrm{gr.}}(G, A)$ est un groupe ?).

10) Soit A un groupe abélien et $\varphi : G \to A$ un morphisme de groupes de G dans A tel que φ induise (par factorisation) un isomorphisme entre $G/D(G)$ et A. Montrer que tout morphisme de groupes de G dans un groupe abélien B se factorise de façon unique par φ.

11) Calculer le groupe dérivé d'un groupe non abélien d'ordre pq (où p, q sont des nombres premiers distincts).

12) Soit G et H deux groupes. Calculer $D(G \times H)$.

13) Déterminer le sous-groupe dérivé de $\mathfrak{S}_n$, $\mathfrak{A}_n$ et de $\mathrm{GL}(V)$, $\mathrm{SL}(V)$ où V est un espace vectoriel de dimension finie. Calculer le sous-groupe dérivé de B le groupe des matrices triangulaires supérieures.

Exercice 8 – Construction de morphismes

Soit G un groupe. Pour $n \in \mathbb{N}$, on note $G_n = \{x \in G, x^n = 1_G\}$ l'ensemble des éléments de G dont l'ordre divise n.

1) Montrer que les applications suivantes sont bien définies et des bijections réciproques l'un de l'autre

$$\begin{aligned} \mathrm{Hom}_{\mathrm{gr.}}(\mathbb{Z}, G) &\longrightarrow G \\ \varphi &\longmapsto \varphi(1) \end{aligned} \qquad et \qquad \begin{aligned} G &\longrightarrow \mathrm{Hom}_{\mathrm{gr.}}(\mathbb{Z}, G) \\ x &\longmapsto (n \mapsto x^n) \end{aligned}$$

Morale (à retenir) : *se donner un morphisme de groupes issu de $\mathbb{Z}$, c'est la même chose que se donner un élément du groupe.*

2) Montrer que les applications suivantes sont bien définies et des bijections réciproques l'un de l'autre

$$\begin{aligned} \mathrm{Hom}_{\mathrm{gr.}}(\mathbb{Z}/n\mathbb{Z}, G) &\longrightarrow G_n \\ \varphi &\longmapsto \varphi(\overline{1}) \end{aligned} \qquad et \qquad \begin{aligned} G_n &\longrightarrow \mathrm{Hom}_{\mathrm{gr.}}(\mathbb{Z}/n\mathbb{Z}, G) \\ x &\longmapsto (n \mapsto x^k) \end{aligned}$$

où $\overline{1}$ désigne la classe de 1 modulo n.

Morale (à retenir) : *se donner un morphisme de groupes issu de $\mathbb{Z}/n\mathbb{Z}$, c'est la même chose que se donner un élément du groupe d'ordre divisant n.*

On pourra remarquer que les bijections des deux questions ci-dessus dépendent du "choix" d'un générateur de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$.

3) D'après la propriété universelle du quotient, $\mathrm{Hom}_{\mathrm{gr.}}(\mathbb{Z}/n\mathbb{Z}, G)$ s'identifie à un sous-ensemble de $\mathrm{Hom}_{\mathrm{gr.}}\, \mathbb{Z}G$ (lequel ?). Montrer que cette identification est compatible aux bijections ci-dessus i.e. montrer que le diagramme suivant est commutatif

$$\begin{array}{ccc} \mathrm{Hom}_{\mathrm{gr.}}(\mathbb{Z}/n\mathbb{Z}, G) & \longrightarrow & G_n \\ {\scriptstyle \circ\pi}\downarrow & & \downarrow \\ \mathrm{Hom}_{\mathrm{gr.}}(\mathbb{Z}, G) & \longrightarrow & G \end{array}$$

4) à quel sous-ensemble de G s'identifie les morphismes injectifs de $\mathbb{Z}$ dans G, les morphismes injectifs de $\mathbb{Z}/n\mathbb{Z}$ dans G.

5) Soit G un groupe. Dénombrer les morphismes injectifs de $\mathbb{Z}/2\mathbb{Z}$ dans G. Qu'obtient-on si $G = \mathfrak{S}_n$?

6) Soit G un groupe. Dénombrer les morphismes surjectifs de G dans $\mathbb{Z}/2\mathbb{Z}$ puis les morphismes surjectifs de G dans $\mathbb{Z}/p\mathbb{Z}$ pour p un nombre premier. Plus généralement, soit G et H deux groupes. Dénombrer les morphismes surjectifs de G dans H dont le noyau est fixé. Étudier le cas $G = \mathfrak{S}_4$ et $H = \mathfrak{S}_3$.

7) Soient H et K deux groupes. On note $p_1 : H \times K \to H$ la projection sur la première coordonnée et $p_2 : H \times K \to K$. Montrer que les applications suivantes sont bien définies et des bijections réciproques l'un de l'autre

$$\begin{aligned} \mathrm{Hom}_{\mathrm{gr.}}(G, H \times K) &\longrightarrow \mathrm{Hom}_{\mathrm{gr.}}(G, H) \times \mathrm{Hom}_{\mathrm{gr.}}(G, K) \\ \varphi &\longmapsto (p_1 \circ \varphi, p_2 \circ \varphi) \end{aligned}$$

$$\begin{aligned} \mathrm{Hom}_{\mathrm{gr.}}(G, H) \times \mathrm{Hom}_{\mathrm{gr.}}(G, K) &\longrightarrow \mathrm{Hom}_{\mathrm{gr.}}(G, H \times K) \\ (\varphi_1, \varphi_2) &\longmapsto (x \mapsto (\varphi_1(x), \varphi_2(x))) \,. \end{aligned}$$

Morale (à retenir) : *se donner un morphisme de groupes à valeurs dans un groupe produit, c'est la même chose que se donner un morphisme à valeurs dans chacun des facteurs.*

8) Soit G un groupe. Pour $g \in G$, montrer que l'application

$$\begin{aligned} c_g \colon G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

est un automorphisme de groupes. Décrire l'automorphisme inverse. On dit que c_g est l'*automorphisme intérieur de G associé à g.*

9) Montrer que l'application

$$\begin{aligned} \mathrm{Int} \colon G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto c_g \end{aligned}$$

est un morphisme de groupes. En déduire une action de G sur lui-même appelée *action de G par conjugaison*. L'image de ce morphisme est l'ensemble des automorphismes intérieurs et noté $\mathrm{Int}(G)$. Quel est le noyau de $\mathrm{Int}(G)$?

10) Montrer que $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$. On note $\mathrm{Out}(G)$ le quotient correspondant. Montrer que l'on a une suite exacte courte

$$1 \longrightarrow ZG \longrightarrow G \xrightarrow{\mathrm{Int}} \mathrm{Aut}(G) \longrightarrow \mathrm{Out}(G) \longrightarrow 1$$

Remarque : *Il arrive que tout automorphisme d'un groupe soit intérieur. C'est le cas du groupe $\mathfrak{S}_n$ pour $n \neq 6$ ou encore du groupe $SO_n(\mathbb{R})$ pour $n \neq 8$ (pour lequel on a $Aut(SO_8(\mathbb{R}))/Int(SO_8(\mathbb{R}))$).*

11) Soit $N \lhd G$ un sous-groupe distingué. Vérifier que par restriction, l'automorphisme intérieur de G associé à g définit un automorphisme de N **qui n'est plus nécessairement un automorphisme intérieur de N** (considérer le cas d'une transposition de $\mathfrak{S}_3$ agissant sur $\mathfrak{A}_3$). Ainsi, on a un morphisme de groupes de $\mathrm{Int}(G)$ dans $\mathrm{Aut}(N)$ et même un morphisme de groupes de G dans $\mathrm{Aut}(N)$. Quel est le noyau ?

3 Quelques grands classiques.

Exercice 9 – Produit et intersection
Soient G un groupe fini, H et K deux sous-groupes de G.

1) Que dire de $H \cap K$ si $\mathrm{pgcd}(|H|, |K|) = 1$?

2) Montrer que

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}$$

où $HK = \{hk,\ h \in H,\ k \in K\}$ (comparer au calcul du cardinal de la réunion de deux ensembles).

Exercice 10 – Un calcul très utile
Soient G et G' deux groupes, H un sous-groupe de G et $f : G \to G'$ un morphisme de groupes.

1) Calculer le noyau de la restriction de f à H.

2) On suppose que f est surjectif. Donner une condition nécessaire et suffisante pour que la restriction de f à H soit injective (resp. surjective, bijective).

Exercice 11 – Partie génératrice
Soient G un groupe fini de cardinal n. Montrer que G a une partie génératrice ayant au plus $\log_2(n)$ éléments. Cette borne est-elle optimale ?

Exercice 12 – Exposant d'un groupe abélien
Soit G un groupe abélien fini et $a, b \in G$. Si $g \in G$, on note $\mathrm{o}(g)$ son ordre. On note $\mathrm{Exp}(G)$ le plus petit entier n tel que $g^n = 1$ pour tout $g \in G$.

1) Soit $a \in G$ et soit $r \in \mathbb{N}^*$. Que vaut $\mathrm{o}(a^r)$?

2) Montrer que si $\mathrm{pgcd}(\mathrm{o}(a), \mathrm{o}(b)) = 1$ alors $\mathrm{o}(ab) = \mathrm{o}(a)\mathrm{o}(b)$.

3) Montrer qu'il existe $g \in G$ tel que $\mathrm{o}(g) = \mathrm{ppcm}(\mathrm{o}(a), \mathrm{o}(b))$.

4) Montrer que $\mathrm{Exp}(G)||G|$. Montrer qu'il existe $g \in G$ tel que $\mathrm{o}(g) = \mathrm{Exp}(G)$. En déduire que si $\mathrm{Exp}(G) = |G|$ alors G est cyclique.

5) Montrer que tout sous-groupe fini de k^* (k un corps commutatif) est cyclique.

Exercice 13 – Sous-groupe de $\mathbb{Z}$

1) Soient $m, n \in \mathbb{Z}$. Le groupe $\langle m, n\rangle$ engendré par m et n est un sous-groupe de $\mathbb{Z}$ donc de la forme $k\mathbb{Z}$. Exprimer k en fonction de m et n.

2) Même question avec $m\mathbb{Z} \cap n\mathbb{Z}$.

Exercice 14 – Sous-groupe d'un groupe
Montrer que l'ensemble $\mathscr{G} = \{H \leq G\}$ est sous-groupe de G est un treillis pour la relation d'inclusion.

4 Les p-groupes.

Exercice 15 – Action de groupes et p-groupes
Cet exercice propose des applications ultra-classiques de la question b.

1) Soient G un groupe et X un G-ensemble (i.e. un ensemble muni d'une action de G). On dit que $x \in X$ est un point fixe sous G si $gx = x$ pour tout $g \in G$. On note X^G l'ensemble des points fixes sous G. Vérifier que les points fixes sont les éléments de X dont l'orbite sous G est ponctuelle ou encore les éléments de X dont le stabilisateur est G tout entier.

2) Soient G un **p-groupe** et X un G-ensemble. Montrer que $|X| = |X^G|\,[p]$ (indication : dans l'équation aux classes, séparer orbites ponctuelles et non ponctuelles).

3) Se convaincre que le résultat de la question b est évident lorsque $p = 2$ et $G = \mathbb{Z}/2\mathbb{Z}$.

4) Déduire de la question b que le centre d'un p-groupe non trivial est non trivial. Et même plus précisément, soit G un p-groupe et $\{1\} \neq N$ un sous-groupe distingué de G alors $N \cap ZG \neq \{1\}$. En déduire qu'un p-groupe a des sous-groupes distingués de tous les ordres possibles et même qu'il existe une suite $(G_i)_{1\leq i\leq r}$ de sous-groupes distingués dans G vérifiant

$$G_0 = \{1\} \subsetneq G_1 \subsetneq \cdots \subsetneq G_{r-1} \subsetneq G_r = G$$

et $|G_i| = p^i$. Montrer que tout p-groupe G non cyclique admet un sous-groupe distingué N tel que $G/N \cong_{gr.} (\mathbb{Z}/p\mathbb{Z})^2$ (utiliser l'exercice 2).

5) **Lemme de Cauchy.** Soit G un groupe dont l'ordre est divisible par p (avec p premier). On va montrer que G admet un élément d'ordre p. On considère $X = \{(x_1, \dots, x_p) \in G^p \mid x_1 \cdots x_p = 1_G\}$. Déterminer $|X|$, faire agir $\mathbb{Z}/p\mathbb{Z}$ sur X et déterminer $X^{\mathbb{Z}/p\mathbb{Z}}$ et son cardinal, conclure.

6) Démontrer que $\binom{p^s}{k} = 0\,[p]$ pour tout $0 < k < p^s$ et $s \in \mathbb{N}$ (faire agir un groupe à p^s éléments (au fait, il en existe bien un ?) sur l'ensemble de ses parties à k éléments).

7) On considère $n = mp^r$ avec $\mathrm{pgcd}(m, p) = 1$ et $r \in \mathbb{N}$. Démontrer la congruence

$$\binom{n}{p^r} = m\,[p]$$

(considérer l'action d'un groupe S d'ordre p^r sur l'ensemble $S \times T$ où T est un ensemble à m éléments donnée par $(s, (s', t)) \mapsto (ss', t)$). Une autre méthode consiste à regarder le coefficient en $X^{(m-1)p^r}Y^{p^r}$ dans le polynôme $(X+Y)^{mp^r} = (X^{p^r} + Y^{p^r})^m \in \mathbb{F}_p[X, Y]$.

8) Le résultat de la question b est utilisé dans la plupart des démonstrations des théorèmes de Sylow.

Definition 1 (Élément maximal)**.** Soit $(X, \leq)$ un ensemble ordonné. Un élément $x \in X$ est un *élément maximal de* X si pour tout $y \in X$ vérifiant $x \leq y$, on a $x = y$ (i.e. si x n'a pas d'élément strictement plus grand que lui dans X).

Soit G un groupe et H un sous-groupe de G. On dit que H est maximal si c'est un élément maximal de l'ensemble ordonné (pour l'inclusion) des sous-groupes de G distincts de G. Autrement dit, un sous-groupe H de G est maximal si les seuls sous-groupes de G contenant H sont H et G, i.e. si pour tout G' vérifiant $H \leq G' \leq G$, on a $G' = H$ ou $G' = G$.

Exercice 16 – Sous-groupes maximaux

1) Soit G un groupe et H un sous-groupe d'indice p premier. Montrer que H est un sous-groupe maximal de G.

2) Soit G un p-groupe et H un sous-groupe maximal de G. Montrer que $H \lhd G$ et $(G : H) = p$ (on pourra démontrer, par récurrence sur le cardinal, que dans un p-groupe, le seul sous-groupe égal à son normalisateur est le groupe tout entier).

3) En déduire que dans un p-groupe, les sous-groupes maximaux sont exactement les sous-groupes d'indice p et qu'ils sont tous distingués.

4) Soit G un groupe. On considère $\Phi(G)$ le *sous-groupe de Frattini* qui est défini comme l'intersection des sous-groupes maximaux de G. Montrer que $\Phi(G)$ est distingué dans G.

5) Soit G un p-groupe. Montrer que $G/\Phi(G)$ est abélien et que tous ses éléments (sauf 1) sont d'ordre p.

6) Soit G un groupe fini (ou même simplement de type fini, ou encore plus généralement tel que tout sous-groupe (distinct de G) soit contenu dans un sous-groupe maximal). Montrer qu'une partie S de G engendre G si et seulement si son image dans $G/\Phi(G)$ engendre $G/\Phi(G)$.

5 Les théorèmes de Sylow.

Théorème 1 (Les théorèmes de Sylow)**.** *Soit G un groupe fini d'ordre $n = mp^r$ avec $r \in \mathbb{N}$ et* $\mathrm{pgcd}(m, p) = 1$. *Alors*

(i) G admet un p-Sylow i.e. un sous-groupe d'ordre p^r ;

(ii) pour tout p-sous-groupe H de H et tout p-Sylow S de G, il existe $g \in G$ tel que $H \subset gSg^{-1}$; en particulier,

(a) deux p-Sylow de G sont conjugués ;

(b) tout p-sous-groupe de G distingué dans G est contenu dans tous les p-Sylow ;

(c) si G a p-Sylow qui est distingué alors il est unique ;

(iii) Le nombre s_p de p-Sylow de G est congru à 1 modulo p et divise m. De plus, on a $s_p = [G : N_G(S)]$ où S est un p-Sylow de G.

Exercice 17 – Une démonstration des théorèmes de Sylow dans le cas abélien
Soit G un groupe abélien fini.

1) Montrer que H_p l'ensemble des éléments de G dont l'ordre est une puissance de p est un sous-groupe de G.

2) Montrer que H_p est un p-groupe (c'est le lemme de Cauchy).

3) Montrer que l'ordre de G/H_p n'est pas divisible par p (c'est le lemme de Cauchy). Au fait, pourquoi G/H_p a-t-il bien une structure de groupe ?

4) Montrer que H_p est un p-Sylow de G et que c'est le seul.

Exercice 18 – Une démonstration des théorèmes de Sylow
La question difficile dans les théorèmes de Sylow est celle de l'existence. Les autres propriétés sont plus élémentaires.

1) On suppose que le point (i) des théorèmes de Sylow est vérifié et on va montrer (ii). Montrer que H agit sur G/S par translation à gauche. En déduire que $|(G/S)^H| \neq 0[p]$ (voir l'exercice 15). En déduire que $(G/S)^H \neq \emptyset$. Conclure.

2) On suppose que le point (i) des théorèmes de Sylow est vérifié et on va montrer (ii). Montrer que G agit par conjugaison sur $\mathscr{S} = \{p-\text{Sylow de } G\}$ et donc que S agit aussi sur $\mathscr{S}$ par conjugaison. Montrer, en utilisant le point (iii) du point (ii) des théorèmes de Sylow que $\mathscr{S}^S = \{S\}$. En déduire que $|\mathscr{S}| = 1[p]$ (voir l'exercice 15). Montrer que $|\mathscr{S}| = [G : N_G(S)]$ pour tout $S \in \mathscr{S}$. Conclure.

3) Passons à la démonstration du point (i). On fait agir G par translation à gauche sur l'ensemble des parties à p^r éléments de G. Montrer qu'il existe un ensemble E dont le cardinal de l'orbite n'est pas divisible par p (utiliser la congruence de la question g de l'exercice 15). Montrer que le stabilisateur G_E de E est un sous-groupe d'indice premier à p. Montrer que $|G_E| \leq p^r$ (on pourra montrer que $G_E \subset Ee^{-1}$ pour $e \in E$). Conclure.

4) Donnons une deuxième démonstration du point (i). On raisonne par récurrence sur le cardinal du groupe. On distingue deux cas. Premier cas : on suppose que $Z(G) = 0[p]$. Montrer qu'il existe un élément x d'ordre p dans $Z(G)$ et appliquer l'hypothèse de récurrence dans le groupe (pourquoi en est-ce un ?) $G/\langle x\rangle$. Deuxième cas : on suppose que $Z(G) \neq 0[p]$. En appliquant l'équation aux classes (à l'action de conjugaison de G sur lui-même), montrer qu'il existe $x \in G$ tel que le stabilisateur G_x de x (qui s'appelle aussi le centralisateur de x) soit distinct de G et d'indice premier à p. Appliquer l'hypothèse de récurrence dans G_x.

Exercice 19 – Une démonstration des théorèmes de Sylow (c'est celle du Perrin)
Cet exercice propose une autre démonstration des théorèmes de Sylow. Il s'agit donc d'obtenir les résultats sans se servir des théorèmes de Sylow.

1) Soit G un groupe. On suppose que G admet un p-Sylow. On va montrer que tout sous-groupe de G admet aussi un p-Sylow. Pour cela, faire opérer H sur G/S (par translation à gauche) et calculer le stabilisateur de aS pour tout $a \in G$. Montrer que ces stabilisateurs sont des p-groupes et montrer qu'il en existe un dont l'indice est premier à p. Conclure : on obtiendra en particulier qu'il existe $a \in G$ tel que $aSa^{-1} \cap H$ est un sous-groupe de Sylow de H.

2) Montrer que tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$ (penser au morphisme de Cayley) puis que $\mathfrak{S}_n$ est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ (penser aux matrices de permutations). En déduire que tout groupe fini admet un p-Sylow.

3) Retrouver le résultat de la question a en une ligne en utilisant les théorèmes de Sylow.

Definition 2. Soit G un groupe (pas nécessairement fini) et $H \leq G$. On dit que H est *sous-groupe caractéristique de* G si $\varphi(H) = H$ pour tout $\varphi \in \mathrm{Aut}(G)$ ou encore si $\varphi(H) \subset H$ pour tout $\varphi \in \mathrm{Aut}(G)$.

Un sous-groupe caractéristique est toujours distingué (penser aux automorphismes intérieurs). La réciproque est fausse.

Par exemple, $\{1\}$, G, $D(G)$ et $Z(G)$ sont des sous-groupes caractéristiques.

Exercice 20 – Sous-groupes caractéristiques

1) Soit G un groupe ayant un seul sous-groupe H d'ordre (resp. d'indice) d. Montrer que H est un sous-groupe caractéristique.

2) Soit G un groupe fini. Montrer les équivalences

(i) il existe un unique p-Sylow dans G ;

(ii) tous les p-Sylow sont caractéristiques ;

(iii) tous les p-Sylow sont distingués ;

(iv) il existe un p-Sylow distingués.

Dans quelles implications se sert-on des théorèmes de Sylow ?

Exercice 21 – p-Sylow, sous-groupe, quotient

1) Soit $H \leq G$ et S' un p-Sylow de H. Montrer qu'il existe S un p-Sylow de G tel que $S' = S \cap H$. Montrer que ce n'est pas vrai pour tous les p-Sylow de G.

2) Soit $H \leq G$, S' un p-Sylow de H et S_1 un p-Sylow de G. Montrer qu'il existe $g \in G$ tel que $S' = gSg^{-1} \cap H$ (comparer avec l'exercice 19).

3) Soit $H \trianglelefteq G$ et S un p-Sylow de G. Montrer que $S \cap H$ est un p-Sylow de H.

4) Soit $H \trianglelefteq G$ et $\pi : G \to G/H$ la surjection canonique. Montrer que $\pi(S)$ est un p-Sylow de G/H et que, pour tout p-Sylow S' de G/H, il existe un p-Sylow de G tel que $\pi(S) = S'$. Montrer qu'un tel que S est unique si, de plus, H est un p-groupe ou $H \subset Z(G)$.

Exercice 22 – Théorèmes de Sylow et Wilson

1) Déterminer les éléments d'ordre p dans $\mathfrak{S}_p$. En particulier, combien y en a-t-il ?

2) Déterminer le nombre de p-Sylow de $\mathfrak{S}_p$.

3) En déduire le théorème de Wilson : $(p-1)! = -1\,[p]$.

Exercice 23 – Théorème de Sylow et petit groupe symétrique

1) Déterminer les 2-Sylow et les 3-Sylow de $\mathfrak{S}_3$ et leur normalisateur.

2) Déterminer (le nombre et leur forme) les 2-Sylow et les 3-Sylow de $\mathfrak{S}_4$ et $\mathfrak{A}_4$ (pour les 2-Sylow, on pourra utiliser le fait que le sous-groupe formé par l'identité et les 3 double-transpositions est distingué dans $\mathfrak{S}_4$ et que tout élément dont l'ordre est une puissance de 2 est dans un 2-Sylow) ainsi que leur normalisateur.

3) Déterminer (le nombre et leur forme) les 2-Sylow, les 3-Sylow et les 5-Sylow de $\mathfrak{S}_5$ et $\mathfrak{A}_5$ ainsi que les normalisateurs.

Exercice 24 – Théorème de Sylow et groupe linéaire
Soit k un corps fini. On note $q = p^n$ son cardinal.

1) Montrer que le groupe U des matrices triangulaires supérieures unipotentes (i.e. avec des 1 sur la diagonales) est un p-Sylow de $\mathrm{GL}_r(k)$ **à SAVOIR ABSOLUMENT**. Cela sert dans l'exercice 19.

2) Déterminer le normalisateur de U.

3) En déduire le nombre de p-Sylow de $\mathrm{GL}_r(k)$.

Exercice 25 – Lemme de Cauchy et théorème de Sylow
Dans l'une des preuves des théorèmes de Sylow (laquelle au fait ?), on s'est servi du lemme de Cauchy et pas dans les autres (c'est sûr ?). Retrouver le lemme de Cauchy à l'aide des théorèmes de Sylow et de la question d de l'exercice 15.

Exercice 26 – Normalisateur de p-Sylow
Soient G un groupe fini et S, S' deux p-Sylow de G.

1) Montrer que si $S' \subset N_G(S)$ alors $S' = S$.

2) En déduire que si $N_G(S) = N_G(S')$ alors $S = S'$ (l'application qui à un p-Sylow associe son normalisateur est injective).

3) Montrer que $N_G(N_G(S)) = N_G(S)$.

4) Plus généralement, montrer que si H contient S alors $N_G(H) = H$.

5) **L'argument de Frattini.** On suppose que $N \trianglelefteq G$ alors $G = N_G(S)N$.

6 Action de groupes.

Exercice 27 – Le cours
Une action du groupe G sur l'ensemble X est une application

$$\begin{aligned} m\colon G \times X &\longrightarrow X \\ (g,x) &\longmapsto m(g,x) := g \cdot x \end{aligned}$$

vérifiant $1_G \cdot x = x$ pour tout $x \in X$ et $(gg') \cdot x = g \cdot (g' \cdot x)$ pour tous $g, g' \in G$ et $x \in X$.

1) Soit $g \in G$. Montrer que l'application $\alpha_g : X \to X$ définie par $\alpha_g(x) = g \cdot x$ pour tout $x \in X$ est une bijection de X dont on donnera la bijection réciproque.

2) Montrer que l'application

$$\begin{aligned} \varphi\colon G &\longrightarrow \mathfrak{S}(X) \\ g &\longmapsto \alpha_g \end{aligned}$$

est un morphisme de groupes.

3) Inversement, à partir d'un morphisme de groupes $\varphi : G \to \mathfrak{S}(X)$, construire une action de G sur X.

Morale : *une action de groupe de G sur X est la même chose qu'un morphisme de groupes de G dans $\mathfrak{S}(X)$.*

4) Montrer que la relation $x \sim y \iff \exists\, g \in G,\ g \cdot x = y$ est une relation d'équivalence sur X. La classe d'équivalence de x est appelé *l'orbite de x sous G* noté $\mathcal{O}(x)$.

5) Montrer que $G_x = \{g \in G \mid g \cdot x = x\}$ est un sous-groupe de G appelé le *stabilisateur de x*.

6) Montrer que l'application

$$\begin{aligned} \delta_x\colon G/G_x &\longrightarrow \mathcal{O}(x) \\ gG_x &\longmapsto gx \end{aligned}$$

est bien définie et est une bijection G-équivariante.

Exercice 28 – G-morphismes

1) Soit X un G-ensemble. Montrer que Id_X est une application G-équivariante.

2) Montrer que la composée de deux applications G-équivariantes est G-équivariante.

3) Définir la notion d'isomorphisme de G-ensemble. Montrer qu'un morphisme de G-ensemble est un isomorphisme de G-ensembles si et seulement si il est bijectif.

4) Définir la notion de sous-G-ensemble.

5) Définir un produit de G-ensemble et démontrer une propriété universelle du produit.

6) Soit X un G-ensemble et $\mathscr{R}$ une relation d'équivalence sur X. A quelle condition existe-t-il sur $X/\mathscr{R}$ une structure de G-ensemble telle que $\pi : X \to X/\mathscr{R}$ soit G-équivariante. Démontrer alors la propriété universelle du quotient pour les applications G-équivariante $X \to Y$ compatible avec $\mathscr{R}$.

Exercice 29 – Action sur un sous-ensemble

1) Si G agit sur X et $Y \subset X$. A quelle condition G agit sur Y par restriction ?

2) On suppose que G agit sur X. Montrer que G agit sur $X \times X$ et sur $\{(x, y) \in X \times X \mid x \neq y\}$. Montrer que G agit sur $X \times X \times X$ et sur $\{(x, y, z) \in X \times X \mid x \neq y, y \neq z, z \neq x\}$.

3) Exemple (le théorème de Thalès) : soient $\mathscr{D}$ une droite affine et (A, B, C), (A', B', C') deux familles de trois points distincts deux à deux. à quelle condition existe-t-il f une application affine telle que $f(A) = A'$, $f(B) = B'$ et $f(C) = C'$.

Exercice 30
Dans l'action de G sur G/H, quel est le stabilisateur de xH ? quel est celui de H ? Est-ce étonnant ?

Exercice 31 – Algèbre linéaire

1) **La théorie du rang.** Soient $M, N \in \mathrm{Mat}\, n \times mk$. à quelle condition les deux matrices ont-elles la même orbite sous l'action de $\mathrm{GL}_n(k) \times \mathrm{GL}_m(k)$ donnée par $((P, Q), M) = PMQ^{-1}$?

2) Soient $M, N \in \mathrm{Mat}\, n \times mk$. à quelle condition les deux matrices ont-elles la même orbite sous l'action de $\mathrm{GL}_n(k)$ donnée par $(P, M) = PM$?

3) Soient $M, N \in \mathrm{Mat}\, n \times mk$. à quelle condition les deux matrices ont-elles la même orbite sous l'action de $\mathrm{GL}_m(k)$ donnée par $(P, M) = MP^{-1}$?

Exercice 32 – Géométrie affine
Soit $\mathscr{E}$ une espace affine. Montrer que $\mathrm{Aff}(\mathscr{E})$ le groupe des bijections affines de $\mathscr{E}$ agit sur $\mathscr{E}$. Quels sont les orbites et les stabilisateurs ?

Soit $\mathscr{E}$ une espace affine euclidien. Alors $\mathrm{Is}(\mathscr{E})$ le groupe des isométries affines de $\mathscr{E}$ agit sur $\mathscr{E}$. Quels sont les orbites et les stabilisateurs ?

Exercice 33
Soit k un corps. Pour chacune des opérations suivantes, décrire les orbites et les stabilisateurs :

1) $\mathrm{GL}_n(k)$ sur k^n,

2) $\mathrm{O}_n(\mathbb{R})$ sur $\mathbb{R}^n$,

3) $\mathrm{GL}_n(k)$ sur $\mathbb{P}^{n-1}(k)$ (l'ensemble des droites vectorielles de k^n).

4) $\mathrm{GL}_n(k) \times \mathrm{GL}_m(k)$ sur $\mathrm{M}_{n,m}(\mathbb{R})$ (pour l'action $(P, Q).M = PMQ^{-1}$).

5) $\mathrm{GL}_n(\mathbb{R})$ sur l'ensemble des matrices symétriques $n \times n$ par congruence ($P.S = PS\,{}^tP$).

Exercice 34
Soit k un corps. Soit $\mathbb{P}^1$ l'ensemble des droites vectorielles de k^2. On considère l'action naturelle de $GL_2(k)$ sur $\mathbb{P}^1$.

1) Montrer que cette action est transitive. Est-elle 2-transitive ? Est-elle 3-transitive ? Est-elle 4-transitive ?
On appelle *homographie de* $\mathbb{P}^1$ toute application $f\colon \mathbb{P}^1 \to \mathbb{P}^1$ telle qu'il existe $u \in GL_2(k)$ vérifiant $f(a) = u(a)$ pour toute droite a.

2) Montrer que les homographies forment un groupe pour la composition. L'action du groupe des homographies sur $\mathbb{P}^1(k)$ est-elle transitive ? 2-transitive ? 3-transitive ? 4-transitive ?

3) Montrer qu'il existe une bijection $\mathbb{P}^1 \to k \cup \{\infty\}$ qui fait se correspondre $t \in k$ (ou ∞) avec la droite engendrée par $(1, t)$ (ou la droite engendrée par $(0, 1)$, respectivement).

4) Soient $a, b, c \in \mathbb{P}^1$ deux à deux distincts. Montrer qu'il existe une unique homographie $g\colon \mathbb{P}^1 \to \mathbb{P}^1$ telle que $g(a) = \infty$, $g(b) = 0$ et $g(c) = 1$.
Soient $a, b, c, d \in \mathbb{P}^1$ tels que a, b, c sont deux à deux distincts. Soit g l'homographie de la question précédente. On appelle *birapport de* a, b, c, d et on note $[a, b, c, d]$ l'élément $g(d)$ de $\mathbb{P}^1$.

5) Dans le cas où $a, b, c, d \in k \subseteq \mathbb{P}^1$, montrer que $[a, b, c, d] = \frac{d-b}{d-a} / \frac{c-b}{c-a} \in \mathbb{P}^1$ avec les conventions usuelles.

Exercice 35
Soit G un groupe fini opérant sur un ensemble fini X. Démontrer que le nombre d'orbites de X est égal à $\frac{1}{|G|} \sum_{g \in G} |fix(g)|$ où $fix(g) = \{x \in X \mid gx = x\}$.

Exercice 36
Soit G un groupe fini et H un sous-groupe propre de G. Montrer que G n'est pas la réunion des conjugués de H (on pourra s'aider de l'exercice précédent). Qu'est-ce que cela signifie en termes d'actions de groupes ?

7 Le groupe symétrique.

Exercice 37 – Parties génératrices de $\mathfrak{S}_n$

1) Montrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1, 2), (2, 3), \ldots, (n-1, n)$. En déduire une famille génératrice de $\mathfrak{A}_n$.

2) Montrer que $\mathfrak{S}_n$ est engendré par les transpositions $(1, 2), (1, 3), \ldots, (1, n)$. En déduire une famille génératrice de $\mathfrak{A}_n$.

3) Montrer que $\mathfrak{A}_n$ est engendré par les carrés des éléments de $\mathfrak{S}_n$.

Exercice 38
Quels sont les sous-groupes d'indice 2 de $\mathfrak{S}_n$?

Exercice 39
Soit $\sigma \in \mathfrak{S}_n$ et soit $c = (i_1, \ldots, i_l)$ un l-cycle, montrer que $\sigma c \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_l))$. Quel est le stabilisateur de c (pour l'action de conjugaison) ? Quel est le cardinal de ce stabilisateur ?

Exercice 40 – Les groupe $\mathfrak{S}_4, \mathfrak{A}_4$

1) Déterminer tous les éléments de $\mathfrak{S}_4$. Pour chaque élément calculer son centralisateur. Pour chaque type de décomposition en produit de cycles disjoints calculer le nombre de classes de conjugaison. Pour les éléments de $\mathfrak{A}_4$ comparer le centralisateur et les orbites pour l'action de $\mathfrak{S}_4$ avec ceux pour l'action de $\mathfrak{A}_4$.

2) Effectuer le même travail pour les sous-groupes de $\mathfrak{S}_4$.

3) Pour $\mathfrak{S}_4$ et pour $\mathfrak{A}_4$ exhiber la classe d'isomorphie et le nombre de sous-groupes de Sylow.

Exercice 41 – les groupes $\mathfrak{S}_5, \mathfrak{A}_5$

1) Déterminer tous les éléments de $\mathfrak{S}_5$. Pour chaque élément calculer son centralisateur. Pour chaque type de décomposition en produit de cycles disjoints calculer le nombre de classes de conjugaison. Pour les éléments de $\mathfrak{A}_5$ comparer le centralisateur et les orbites pour l'action de $\mathfrak{S}_5$ avec ceux pour l'action de $\mathfrak{A}_5$.

2) Déterminer tous les sous-groupes de $\mathfrak{A}_5$, leur classe de conjugaison, leur normalisateur. Pour les sous-groupes de $\mathfrak{A}_5$, comparer la classe de conjugaison et le normalisateur avec ceux dans $\mathfrak{A}_5$.

3) Pour $\mathfrak{S}_5$ et pour $\mathfrak{A}_5$ exhiber la classe d'isomorphie et le nombre de sous-groupes de Sylow.

Exercice 42
Soit $n \geqslant 3$. Soit $\sigma \in \mathfrak{A}_n$. Trouver une condition nécessaire et suffisante pour que $\mathrm{Stab}_{\mathfrak{A}_n}(\sigma) = \mathrm{Stab}_{\mathfrak{S}_n}(\sigma)$.

Exercice 43 – Sur les groupes simples d'ordre 60

1) Montrer que $\mathfrak{A}_5$ est simple.

2) Soit G un groupe simple d'ordre 60. Montrer que G a 10 3-sous-groupes de Sylow et 6 5-sous-groupes de Sylow. En déduire que G ne contient pas d'élément d'ordre 6 ou 10 et que tout 2-sous-groupe de Sylow est le centralisateur de chacun de ses éléments d'ordre 2. Calculer le nombre de 2-sous-groupes de Sylow de G. Montrer que $G \cong \mathfrak{A}_5$.

3) Soit G un groupe d'ordre 60 qui a exactement 15 éléments d'ordre 2 ; 20 éléments d'ordre 3 ; et 24 éléments d'ordre 5. Montrer que G est isomorphe à $\mathfrak{A}_5$ (on pourra s'aider de la question précédente).

Exercice 44 – Les sous groupes d'indice n de $\mathfrak{S}_n$.
Soit $n \geqslant 2$, on admettra que $\mathfrak{A}_n$ est simple si $n \neq 2, 4$.

1) Soit $n \geqslant 5$, montrer que les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathfrak{A}_n$ et 1.

2) Soit G un sous-groupe d'indice n de $\mathfrak{S}_n$. Montrer que G est isomorphe à $\mathfrak{S}_{n-1}$ (faire opérer $\mathfrak{S}_n$ sur l'ensemble quotient $\mathfrak{S}_n/G$).

3) Montrer que pour $n \geqslant 3$, le groupe $\mathfrak{A}_n$ n'admet aucun sous-groupe isomorphe à $\mathfrak{S}_{n-1}$.

4) Soit $n \geqslant 3$ et soit H un sous-groupe de $\mathfrak{A}_n$ d'indice n.

- Etablir l'existence d'un isomorphisme entre $\mathfrak{A}_n$ et le groupe des permutations paires de l'ensemble $\mathfrak{A}_n/H$.
- En déduire que l'existence d'un isomorphisme $\varphi\colon \mathfrak{A}_n \xrightarrow{\sim} \mathfrak{A}_n$ tel que $\varphi(H) = \{\sigma \in \mathfrak{A}_n \mid \sigma(1) = 1\}$.

5) Soit H un groupe simple d'ordre 60. On veut montrer que $H \cong \mathfrak{A}_5$ (sans utiliser l'Exercice 43). En comptant les sous-groupes de Sylow de H, établir l'existence d'un morphisme injectif $H \hookrightarrow \mathfrak{A}_6$. En déduire que $H \cong \mathfrak{A}_5$.

6) Montrer que $\mathfrak{S}_5$ admet un sous-groupe H d'ordre 20. En faisant opérer $\mathfrak{S}_5$ par translation à gauche sur $\mathfrak{S}_5/H$ exhiber un sous-groupe d'indice 6 de $\mathfrak{S}_6$ qui ne fixe aucun élément de $\{1, \ldots, 6\}$ (une telle situation est exceptionnelle, voir le cours de Perrin).

Exercice 45 – Les automorphismes de $\mathfrak{S}_n$
Étant donné $\sigma \in \mathfrak{S}_n$ on notera $\iota_\sigma\colon \mathfrak{S}_n \to \mathfrak{S}_n$ la conjugaison par σ. On notera que c'est un automorphisme de $\mathfrak{S}_n$. Le groupe des automorphismes de $\mathfrak{S}_n$ est noté $\mathrm{Aut}(\mathfrak{S}_n)$.

1) Montrer que l'application $\mathfrak{S}_n \to \mathrm{Aut}(\mathfrak{S}_n), \sigma \mapsto \iota_\sigma$ est un homorphisme de groupes et que son image est un sous-groupe distingué de $\mathrm{Aut}(\mathfrak{S}_n)$.

Un automorphisme de la forme ι_σ est dit *intérieur*. Un automorphisme qui n'est pas de la forme ι_σ est dit *extérieur*. L'ensemble des automorphismes intérieurs est noté $\mathrm{Int}(\mathfrak{S}_n)$.

2) Soit φ un automorphisme de $\mathfrak{S}_n$. Montrer que $\varphi \in \mathrm{Int}(\mathfrak{S}_n)$ si et seulement si φ transforme toute transposition en une transposition.

3) Soit $\sigma \in \mathfrak{S}_n$. On suppose que la décomposition de σ en produit de cycles à supports disjoints fait apparaître k_1 1-cycles, k_2 2-cycles, etc. jusqu'à k_n n-cycles. Montrer que le cardinal du centralisateur de σ dans $\mathfrak{S}_n$ est égal à $\prod_{i=1}^{n} k_i! i^{k_i}$.

4) Soit $n \neq 6$ et $\varphi \in \mathrm{Aut}(\mathfrak{S}_n)$. Montrer que φ est intérieur (*indication :* étant donnée une permutation σ, on pourra comparer les centralisateurs de σ et de $\varphi(\sigma)$.

5) Soit $n \neq 4$. Montrer que $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_6)$ si et seulement si les sous-groupes d'indice n de $\mathfrak{S}_n$ sont tous conjugués (on pourra exploiter les techniques utilisées à l'Exercice 44).

6) En déduire que $\mathfrak{S}_6$ a un automorphisme extérieur.

7) Soit $\varphi \in \mathrm{Aut}(\mathfrak{S}_6)$ un automorphisme extérieur. Que dire de la décomposition en produit de cycles à supports disjoints de $\varphi(\tau)$, pour une transposition $\tau \in \mathfrak{S}_6$.

8) En déduire que $\mathrm{Int}(\mathfrak{S}_6)$ est d'indice 2 dans $\mathrm{Aut}(\mathfrak{S}_6)$.

9) Montrer qu'il existe un automorphisme extérieur $\varphi \in \mathrm{Aut}(\mathfrak{S}_6)$ d'ordre 2 (*indication :* on pourra d'abord chercher un automorphisme extérieur dont le carré est la conjugaison par un 5-cycle).

10) En déduire que $\mathrm{Aut}(\mathfrak{S}_6)$ est isomorphe à un produit semi-direct de $\mathrm{Int}(\mathfrak{S}_6)$ par $\mathbb{Z}/2\mathbb{Z}$.

8 Groupes linéaires.

Exercice 46
Groupes linéaires sur des corps finis

1) Justifier qu'un corps commutatif fini est de cardinal une puissance d'un nombre premier.

Dans la suite, on fixe q une puissance d'un nombre premier et on suppose que $\mathbb{F}_q$ est un corps (commutatif) fini à q éléments. Soit $n \geqslant 2$ un entier.

2) Montrer que les groupes suivants sont finis et calculer leur cardinal : $GL_n(\mathbb{F}_q), SL_n(\mathbb{F}_q), PGL_n(\mathbb{F}_q)$ et $PSL_n(\mathbb{F}_q)$.

3) Montrer qu'il existe un homomorphisme injectif de groupes $PGL_2(\mathbb{F}_q) \hookrightarrow \mathfrak{S}_{q+1}$.

4) En déduire que chacun des groupes suivants est isomorphe à un sous-groupe bien connu d'un groupe symétrique : $GL_2(\mathbb{F}_2)$, $PGL_2(\mathbb{F}_3)$, $PSL_2(\mathbb{F}_3)$, $PGL_2(\mathbb{F}_4)$, $PGL_2(\mathbb{F}_5)$ et $PSL_2(\mathbb{F}_5)$.

Exercice 47 – Le groupe $SL_2(\mathbb{F}_3)$

1) Quel est le cardinal de $SL_2(\mathbb{F}_3)$? Ce groupe est-il isomorphe à $\mathfrak{S}_4$?

La suite de cet exercice propose de reconstruire le groupe $SL_2(\mathbb{F}_3)$ à partir de groupes qui sont apparus plus haut.

2) Quelle est la classe d'isomorphisme de $D(PSL_2(\mathbb{F}_3))$?

3) En utilisant une suite exacte adéquate, déterminer le cardinal de $D(SL_2(\mathbb{F}_3))$.

4) En déduire la classe d'isomorphisme de $D(SL_2(\mathbb{F}_3))$.

5) Déterminer le groupe $SL_2(\mathbb{F}_3)$ à l'aide d'un produit semi-direct.

Exercice 48 – Les matrices de transvection et les matrices de dilatation
Soit A un anneau euclidien, soient $m, n \in \mathbb{N}$ deux entiers non nuls. On note $GL_n(A)$ le groupe des éléments inversibles de l'anneau $M_n(A)$.

1) Montrer que $M \in M_n(A)$ est dans $GL_n(A)$ si et seulement si $det(M) \in A^\times$. Que devient cette condition si $A = \mathbb{Z}$?

On note $SL_n(A) = \{P \in GL_n(A) \mid det(P) = 1\}$.

2) Justifier que $SL_n(A)$ est un sous-groupe distingué de $GL_n(A)$.

3) Soient $i, j \in \{1, \dots, n\}$ distincts et $a \in A$. On note $T_{i,j}(A)$ la matrice dont tous les coefficients sont nuls sauf les coefficients diagonaux qui valent 1 et le coefficient en ligne i et colonne j qui vaut a. Une telle matrice est appelée une *matrice de transvection*.

(i) Montrer que, pour i, j fixés, l'ensemble $\{T_{i,j}(a) \mid a \in A\}$ est un sous-groupe de $SL_n(A)$.

(ii) Soit $M \in M_{n,m}(A)$. Calculer les coefficients de $T_{i,j}(a)M$ en fonction de ceux de M. Que constate-t-on ?

(iii) Soit $M \in M_{m,n}(A)$. Calculer les coefficients de $MT_{i,j}(a)$ en fonction de ceux de M. Que constate-t-on ?

4) Soit $i \in \{1, \dots, n\}$ et $a \in A^\times$. On note $D_i(a)$ la matrice diagonale dont tous les coefficients diagonaux sont égaux à 1 sauf celui en ligne i qui vaut a. Une telle matrice est appelée une *matrice de dilatation*.

(i) Quel est le sous-groupe de $GL_n(A)$ engendré par l'ensemble des matrices de dilatation ?

(ii) Soit $M \in M_{n,m}(A)$ et $D \in GL_n(A)$ une matrice de dilatation. Calculer les coefficients de DM en fonction de ceux de M. Que constate-t-on ?

(iii) Soit $M \in M_{n,m}(A)$ et $D \in GL_m(A)$ une matrice de dilatation. Calculer les coefficients de MD en fonction de ceux de M. Que constate-t-on ?

5) Soit $M = [a_1, \dots, a_n]^t \in M_{n,1}(A)$ et soit d un pgcd de $a_1, \dots, a_n$. Montrer qu'il existe $P \in GL_n(A)$ tel que $PM = [d, 0, \dots, 0]$. Que peut-on dire de P ?

6) Soit $M \in M_{n,m}(A)$. Montrer qu'il existe $P \in GL_n(A)$ et $Q \in GL_m(A)$ s'écrivant toutes deux comme des produits de matrices de transvection et telles que PMQ est diagonale par blocs $\begin{bmatrix} a_1 & & & \\ & \ddots & & 0 \\ & & a_r & \\ & 0 & & 0 \end{bmatrix}$ où $a_1, \dots, a_r \in A$ sont non nuls et tels que $a_1 | a_2 | \cdots | a_r$. Que constate-t-on lorsque A est un corps ?

7) En déduire que $SL_n(A)$ est engendré par l'ensemble des matrices de transvection et que $GL_n(A)$ est engendré par l'ensemble constitué des matrices de transvection et de celles de dilatation.

8) Montrer que la suite $a_1, \dots, a_r$ est uniquement déterminée par M, à la multiplication prés de chaque a_i par une élément inversible de A (on pourra caractériser le produit $a_1 \cdots a_i$ en fonction de M).

9) *Question subsidiaire :* (à garder éventuellement pour la série d'exercice sur les anneaux) : les résultats précédents s'étendent-ils au cas où A est un anneau principal ?

10) *Application :* soit k un corps et $A = k[X]$. Soit B la matrice $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & -1 & 0 \\ -1 & 0 & 1 & 1 & -1 \\ 0 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 & 0 \end{bmatrix}$. Calculer une suite d'éléments $a_1, \dots, a_r \in A$ (comme ci-dessus) pour la matrice $M = B - X.Id \in M_5(A)$.

9 Classification.

Exercice 49
Donner les classes d'isomorphisme des groupes abéliens finis d'ordre 15 au plus.

Exercice 50
Soit G un groupe tel que $g^2 = 1$ pour tout $g \in G$. Montrer que G est abélien. Montrer que l'ordre de G est une puissance de 2. Montrer que si $|G| = 2^n$ alors $G \cong (\mathbb{Z}/2\mathbb{Z})^n$.

Exercice 51
Soit G un groupe et H un sous-groupe de G d'indice 2 dans G.

1) Soit K un sous-groupe de G. Montrer que : $K \subseteq H$ ou $K \cap H$ est d'indice 2 dans K.

2) En déduire que si H est simple et si $|G| \neq 4$, alors G n'admet aucun autre sous-groupe d'indice 2.

3) En déduire que si $|G| = 2n$ avec n impair, alors G a au plus un sous-groupe d'indice 2.

Exercice 52
Soit G un groupe fini et H un sous-groupe de G contenu dans le centre de G. Montrer que H est distingué. Montrer que si G/H est cyclique, alors G est abélien.

Exercice 53 – Groupes d'ordre $2p$ (p premier impair)
Soit G un groupe d'ordre $2p$. On va montrer qu'il est cyclique ($\mathbb{Z}/2p\mathbb{Z}$) ou diédral (D_{2p}).

1) Montrer que G n'a qu'un seul p-sous-groupe de Sylow noté S.

2) Soit $x \in G$ d'ordre 2 (justifier l'existence).

b1) Monter que $G =< S, x >$.

b2) Montrer que l'automorphisme $S \to S,\ g \mapsto xgx^{-1}$ est soit l'identité soit l'application $g \mapsto g^{-1}$ (Rappel : le groupe des automorphismes de S est cyclique d'ordre $p-1$).

b3) En déduire que G est soit cyclique, soit diédral.

Exercice 54 – Groupes d'ordre pq avec p et q premiers impairs tels que $p < q$ et p ne divise pas $q-1$
Soit G un tel groupe, on va démontrer que G est cyclique. Montrer que G admet un unique q-sous-groupe de Sylow, noté S, isomorphe à $\mathbb{Z}/q\mathbb{Z}$. Soit x un élément de G d'ordre p (justifier l'existence). Montrer que x normalise S. Montrer que x centralise S. En déduire que $G \cong \mathbb{Z}/pq\mathbb{Z}$.

Exercice 55 – Les groupes d'ordre 8
Soit G un groupe non abélien d'ordre 8 et soit $Z(G)$ son centre.

1) Montrer que $Z(G)$ est d'ordre 2 et que $G/Z(G) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

2) Montrer que G contient au moins un élément d'ordre 4.

3) Montrer que tout sous-groupe de G d'ordre 4 est distingué dans G. Soit H un sous-groupe cyclique et d'ordre 4 de G.

1er cas Supposons qu'il existe dans $G \backslash H$ un élément x d'ordre 2. Montrer que $G =< H, x >$. Montrer que l'automorphisme $H \to H, g \mapsto xgx^{-1}$ est égal à $g \mapsto g^{-1}$. En déduire que G est le groupe diédral.

2ème cas Supposons que tout élément de $G \backslash H$ est d'ordre 4. Montrer que G n'a qu'un seul élément d'ordre 2 et qu'il engendre $Z(G)$, on le note -1. Soit i un générateur de H et soit $j \in G \backslash H$. On pose $k = ij$. Montrer que $i^2 = j^2 = k^2 = -1$. On note alors $-i$ pour i^3, $-j$ pour j^3, $-k$ pour k^3. Ecrire la table de multiplication de G. Ce groupe est appelé le groupe des quaternions et noté $\mathbb{H}_8$.

Exercice 56 – Les groupes d'ordre 12
Soit G un groupe d'ordre 12. Soit t (resp. d) le nombre de ses 3-sous-groupes (resp. 2-sous-groupes) de Sylow.

1) Montrer que $t \in \{1,4\}$ et $d \in \{1,3\}$. Montrer que $t = 1$ ou $d = 1$.

2) On suppose que $t = 1$ et $d = 1$. Montrer que G est isomorphe à $\mathbb{Z}/12\mathbb{Z}$ ou à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3) On suppose que $t = 1$ et $d = 3$. Montrer que G est le produit semi-direct non direct de son 3-sous-groupe de Sylow par un de ses 2-sous-groupes de Sylow. Montrer qu'on obtient ainsi 2 classes d'isomorphisme de groupes d'ordre 12 dont l'un d'eux est le groupe diédral.

4) On suppose que $t = 4$ et $d = 1$. En faisant opérer G sur l'ensemble de ses 3-sous-groupes de Sylow trouver la classe d'isomorphisme de G.

10 Quelques idées de développement.

Exercice 57 – Un théorème de Burnside
Soit $n \geqslant 1$ et G un sous-groupe de $GL_n(\mathbb{C})$. On suppose que G est d'exposant fini : il existe $N \in \mathbb{N}^*$ tel que $g^N = 1$ pour tout $g \in G$. Le but de l'exercice est de démontrer que G est fini.

1) Montrer que l'ensemble T des traces des éléments de G est fini.

Étant donnée $g \in G$ on note $\varphi_g \colon G \to T$ l'application définie par $\varphi_g(h) = Tr(gh)$.

2) Soit $g \in G$. Montrer que si $Tr(g) = Tr(1)$, alors $g = 1$.

3) En déduire que l'application $g \mapsto \varphi_g$ est injective.

4) En déduire que G est fini.

Exercice 58 – Le théorème de la base de Burnside
Le but de l'exercice est de démontrer le théorème suivant :
«Soit P un p-groupe fini. Alors toutes les parties génératrices minimales de P ont le même cardinal.»
Soit P un p-groupe fini non nul.

1) Soit Q un sous-groupe propre de P. Notons $N_P(Q)$ son normalisateur défini par :

$$N_P(Q) = \{g \in P \mid gQg^{-1} = Q\}$$

- Soit $y \in P$. Montrer que :
$$\{x \in Q \mid xyQ = yQ\} = Q \cap\ yQy^{-1}$$
- Considérons l'opération de Q sur P/Q par translation à gauche des classes modulo Q. Montrer que les orbites ponctuelles sont celles de la forme yQ avec $y \in N_P(Q)$. En déduire qu'il y a $Card(N_P(Q)/Q)$ orbites ponctuelles.
- En écrivant l'équation aux classes en déduire que $Q \subsetneq N_P(Q)$.

2) déduire de 1) que les sous-groupes propres de P et maximaux pour l'inclusion sont distingués dans P. En déduire que les sous-groupes propres de P et maximaux pour l'inclusion sont exactement les sous-groupes d'indice p dans P.

3) Notons $\Phi(P)$ le **sous-groupe de Frattini de** P, égal à l'intersection des sous-groupes propres de P et maximaux pour l'inclusion. Notons $\pi \colon P \twoheadrightarrow P/\Phi(P)$ la surjection naturelle. Soit Q un sous-goupe distingué de P. Montrer que $\Phi(P) \subseteq Q$ si et seulement si P/Q est isomorphe à un produit de $\mathbb{Z}/p\mathbb{Z}$.

(i) Soient $x_1, \ldots, x_n$ des éléments de P. Montrer que $(x_1, \ldots, x_n)$ engendre P si et seulement si $\pi(x_1), \ldots, \pi(x_n)$ engendrent $P/\Phi(P)$ (*indication : montrer que $x_1, \ldots, x_n$ n'engendrent pas P si et seulement si il existe un sous-groupe propre de P, maximal pour l'inclusion, en contenant $x_1, \ldots, x_n$*).

(ii) Conclure en remarquant que $P/\Phi(P)$ est naturellement muni d'une structure de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel.

(iii) Montrer que le résultat n'est pas toujours vrai lorsque le groupe considéré n'est plus un p-groupe.

Exercice 59 – Une caractérisation des groupes cycliques.
Le but de l'exercice est de démontrer le résultat suivant : *«Soit $n \geqslant 2$ un entier tel que n et $\varphi(n)$ sont premiers entre eux. Alors tout groupe d'ordre n est cyclique.»* La preuve sera faite par l'absurde. Soit G un groupe d'ordre n, où n et $\varphi(n)$ sont premiers entre eux. Supposons que n est minimal pour cette propriété. Rappelons que le groupe des automorphismes de $\mathbb{Z}/p\mathbb{Z}$ est cyclique d'ordre $\varphi(p) = p - 1$.

1) Les entiers concernés. Montrer qu'un entier positif m est premier à $\varphi(m)$ si et seulement si il existe une décomposition $m = p_1 \dots p_r$ en produit d'entiers premiers deux à deux distincts et tels que p_i ne divise pas $p_j - 1$ si $i \neq j$. En déduire que si $d|n$, alors d et $\varphi(d)$ sont premiers entre eux.

2) Les sous-groupes et les quotients de G. Montrer que les sous-groupes propres et les quotients non nuls de G sont cycliques. Montrer que l'indice d'un sous-groupe de G est premier avec son ordre.

3) La simplicité de G. Soit H un sous-groupe distingué de G. Supposons que $1 \subsetneq H \subsetneq G$, et soit $\pi\colon G \to G/H$ la surjection canonique. Soit $y \in G$ tel que $\pi(y)$ engendre G/H, et soit d l'ordre de y dans G. Ainsi il existe un entier e tel que $d = eCard(G/H)$.

- Montrer que y^e est d'ordre $Card(G/H)$ et que $\pi(y^e)$ est d'ordre $Card(G/H)$.
- Montrer que y^e centralise H (comparer l'ordre de y^e avec celui du groupe des automorphismes de H). En déduire que G est le produit direct de H et du sous-groupe engendré par y^e et que donc G est cyclique.

4) Les sous-groupes propres et maximaux de G sont tous conjugués. Soit H un sous-groupe propre de G et maximal pour l'inclusion. Soit K un sous-groupe propre de G. Montrer que :

- $H = N_G(H)$,
- $G =< H, K >$ si $K \not\subseteq H$,
- $K \cap H$ est un sous-groupe distingué de G si $K \not\subseteq H$ (Rappel : un groupe abélien normalise tous ses sous-groupes),
- $K \cap H = 1$ ou $K \subseteq H$.

Si H est un sous-groupe de G, notons $\widehat{G/H}$ un système de représentants dans G des éléments de G/H. Soient H et K deux sous-groupes maximaux non conjugués de G. Montrer que :

- $gHg^{-1} \cap kHk^{-1} = 1$ lorsque $gH \neq kH$, pour tous $g, k \in G$,
- $gHg^{-1} \cap kKk^{-1} = 1$ pour tous $g, k \in G$,
- $\bigcup\limits_{g\in G} (gHg^{-1}\backslash\{1\}) = \coprod\limits_{g\in\widehat{G/H}} (gHg^{-1}\backslash\{1\})$,
- $\bigcup\limits_{g\in G} (gKg^{-1}\backslash\{1\}) = \coprod\limits_{g\in\widehat{G/K}} (gKg^{-1}\backslash\{1\})$,
- $\left(\bigcup\limits_{g\in G} (gHg^{-1}\backslash\{1\})\right) \cap \left(\bigcup\limits_{g\in G} (gKg^{-1}\backslash\{1\})\right) = \emptyset$.

En comptant les éléments de $\left(\bigcup\limits_{g\in G} (gHg^{-1}\backslash\{1\})\right) \cup \left(\bigcup\limits_{g\in G} (gKg^{-1}\backslash\{1\})\right)$ en déduire une contradiction.

5) Conclusion. Soit p un entier premier divisant l'ordre de G. Montrer que tout élément de G d'ordre p est dans un sous-groupe propre maximal de G et en déduire une contradiction.

11 Produit semi-direct et suite exacte.

Exercice 60
Parmi les suites exactes courtes vue en cours et les suivantes (dont on vérifiera qu'elles sont biens des suites exactes), dire lesquels sont scindées. Décrire un scindage et donné l'action associée.

1) $0 \longrightarrow \mathbb{Z} \xrightarrow{[\times 2i\pi]} \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \longrightarrow 1$;

2) $1 \longrightarrow \mathrm{SL}_n(k) \longrightarrow \mathrm{GL}_n(k) \xrightarrow{\det} k^\times \longrightarrow 1$ avec $n \geq 1$;

3) $1 \longrightarrow \mathrm{SO}_n(\mathbb{R}) \longrightarrow O_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\} \longrightarrow 1$ avec $n \geq 1$;

4) $1 \longrightarrow Z(G) \longrightarrow G \longrightarrow \mathrm{Int}(G) \longrightarrow 1$;

5) Soit $\mathscr{E}$ un espace affine de direction E : $0 \longrightarrow E \xrightarrow{T} \mathscr{GA}(\mathscr{E}) \longrightarrow \mathrm{GL}(V) \longrightarrow 1$