CHAPITRE 19

Groupes

I Généralités

Définition I.1.

Soit G un ensemble non vide muni d'une application $\cdot : G \times G \to G$, appelée loi de composition interne.
On dit que $(G, .)$ est un groupe si :

- $\cdot$ est associative : $\forall x, y, z \in G\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- $\cdot$ admet un element neutre : il existe $e \in G$ tel que $\forall x \in G\ x \cdot e = x = e \cdot x$
- Tout élément admet un inverse : $\forall x \in G\ \exists x^{-1} \in G\ x \cdot x^{-1} = e = x^{-1} \cdot x$

Si $\cdot$ est commutative, i.e. $\forall x, y \in G\ x \cdot y = y \cdot x$, on dit alors que $(G, .)$ est un groupe commutatif ou groupe abélien

On note $(G, .)$ un groupe, non nécéssairement commutatif
$(G, +)$ désigne par contre toujours un groupe commutatif

Exercice I.2.

Soit $(G, .)$ un monoide tel que tout element admet un inverse à gauche. Montrer que G est un groupe

Définition I.3.

On dit que $H \subset G$ est un sous-groupe du groupe $(G, .)$ si H est stable par $.$ et $(H, .\big|_{H\times H}^{H}) = (H, .)$ forme un groupe. On notera $H \leq G$.
Ceci est équivalent à demander $H \neq \varnothing$ et $\forall x, y \in H\ xy^{-1} \in H$

Proposition I.4.

$e_H = e_G$ et $\forall h \in H\ h^{-1}$ est le même au sens de $(G, .)$ et $(H, .)$
On a aussi $\forall g, h \in G\ (gh)^{-1} = h^{-1}g^{-1}$

Preuve :
On a $e_H \cdot e_H = e_H$ d'où, en multipliant par son inverse dans G, on obtient $e_H = e_G$.
Soit $a \in H$ et a_H^{-1} son inverse au sens de $(H, .)$. Alors $a_H^{-1} \cdot a = e_H = e_G$ et donc, en multipliant à droite par l'inverse de a au sens de $(G, .)$, on obtient $a_H^{-1} = a_G^{-1}$
Remarquant que $(gh)(h^{-1}g^{-1}) = gg^{-1} = e$ et donc, en multipliant par $(gh)^{-1}$ à gauche, on a $(gh)^{-1} = h^{-1}g^{-1}$

Proposition I.5.

Soit $S \subset G$. Alors il existe un (unique) sous-groupe minimum (pour l'inclusion) de G contenant S qu'on nomme sous groupe engendré par S et note $\langle S \rangle$. On a alors $\langle S \rangle = \bigcap_{H \leq G \ S \subset H} H$

Preuve : Il suffit de vérifier qu'une intersection quelconque de sous-groupes est toujours un sous-groupe. Ceci étant clair, on a alors que $\bigcap_{H \leq G \ S \subset H} H$ est bien un sous-groupe minimum (pour l'inclusion) contenant S et donc on a bien l'existence. L'unicité provient du fait que, dans un ensemble partiellement ordonné, le minimum est toujours unique s'il existe.

Exercice I.6.

Soit H une partie non vide finie de G. Montrer que $H \leq G \iff \forall (x,y) \in H^2 \ xy \in H$

Translations dans une groupe G :

Soit $a \in G$, on note $\gamma_a : \begin{cases} G & \longrightarrow G \\ x & \mapsto ax \end{cases}$ et $\delta_a : \begin{cases} G & \longrightarrow G \\ x & \mapsto xa \end{cases}$

Il s'agit de permutations de G qui ne sont des morphismes que pour $a = e$

Puissances dans une groupe G :

Soit $n \in \mathbb{Z}^*$ et $x \in G$. On définit $x^n := \underbrace{x^\delta \dots x^\delta}_{|n| \text{ fois}}$ où $\delta = \begin{cases} 1 \text{ si } n \geq 1 \\ -1 \text{ si } n \leq -1 \end{cases}$

Pour $n = 0$ on définit $x^0 = e$.

Il est aisé de vérifier que $\forall (n,m) \in \mathbb{Z}^2 \ x^{n+m} = x^n \cdot x^m$

⚠Si la loi est additive on note nx au lieu de x^n

Morphismes de groupes :

Définition I.7.

Soit f une application de G vers H. On dit que f est un (homo)morphisme de $(G, .{}_G)$ vers $(H, .{}_H)$, et on le note $f \in Hom(G,H)$, si $\forall x, y \in G \ f(x._G y) = f(x)._H f(y)$

Exemple :

1. Soit $a \in G$ $j_a : \begin{cases} (\mathbb{Z}, +) & \longrightarrow (G, .) \\ n & \mapsto a^n \end{cases}$ est un morphisme de groupes.
2. Soit $a \in G$ $\sigma_a : \begin{cases} G & \longrightarrow G \\ x & \mapsto axa^{-1} \end{cases}$ est un morphisme bijective, d'inverse $\sigma_{a^{-1}}$. On le nomme automorphisme intérieur associé à a. Il agit par conjugaison.

Preuve : Soit $a, b, g \in G$. Alors $\sigma_a \circ \sigma_b(g) = \sigma_a(bgb^{-1}) = abgb^{-1}a^{-1} = (ab)g(ab)^{-1} = \sigma_{ab}(g)$ d'où $\sigma_{ab} = \sigma_a \circ \sigma_b$ et donc, en particulier, $\sigma_a \circ \sigma_{a^{-1}} = \sigma_e = \mathrm{Id} = \sigma_e = \sigma_{a^{-1}} \circ \sigma_a$

Conjugaison :

On dit que $x, y \in G$ sont conjugués si $\exists a \in G \ y = axa^{-1} = \sigma_a(x)$

Il s'agit en fait d'une relation d'équivalence sur G, qui donc le partitionne (voir la section "Action de conjugaison")

Proposition I.8.

Soit $f \in Hom(G, G')$

1. $f(e) = e' : f(e) = f(e \cdot e) = f(e)^2$ et donc $f(e) = e'$
2. Si $H \leq G$ alors $f(H) \leq G'$. En particulier, $Im(f) = f(G) \leq G'$
3. Si $K \leq G'$ alors $f^{-1}(H) \leq G$. En particulier, $Kerf := f^{-1}(\{e'\}) \leq G$
4. f est injective $\iff Ker(f) = \{e\} \iff Ker(f) \subset \{e\}$
   $\implies : x \in Ker(f) \iff f(x) = e' = f(e) \underset{f \text{ injective}}{\iff} x = e$
   $\impliedby : f(x) = f(y) \iff f(xy^{-1}) = e' \iff xy^{-1} \in Ker(f) \iff xy^{-1} = e \iff x = y$

Proposition I.9.

1. Les homomorphismes de groupes se composent
2. Les isomorphismes (morphismes bijectifs) de G vers G, nommés automorphismes de G et notés $Aut(G)$, forment un groupe
3. s'il existe un isomorphisme entre deux groupes G et G', on notera $G \simeq G'$

Exemple :

$\varphi : \begin{cases} G & \longrightarrow Aut(G) \\ a & \mapsto \sigma_a \end{cases}$ est un morphisme de groupes de noyau $Ker(\varphi) = Z(G) := \{x \in G \ \forall y \in G \ xy = yx\}$

En effet, $a \in Ker(f) \iff \sigma_a = \mathrm{Id} \iff \forall x \in G \ axa^{-1} = x \iff \forall x \in G \ ax = xa$

Exercice I.10.

Soit G un groupe. Montrer que $\varphi : \begin{cases} (G, .) & \longrightarrow (Bij(G), \circ) \\ a & \mapsto \gamma_a \end{cases}$, où $Bij(G)$ désigne l'ensemble des applications bijectives de l'ensemble G dans lui même, est un morphisme injectif de groupes.
En particulier, ceci montre que tout groupe peut être vu comme un sous-groupe d'un groupe symetrique (eventuellement infini) et que donc, si $|G| = n < \infty$, alors G peut être identifié à un sous-groupe de $\mathcal{S}_n$

Sous-groupes distingués (invariants)

Définition I.11.

Soit $H \leq G$. On dit que H est distingué (ou normal), et on le note $H \trianglelefteq G$, lorsque $\forall a \in G \ aHa^{-1} = \sigma_a(H) \subset H$
Dans ce cas, on a alors $aHa^{-1} = H$ et $aH = Ha$
Remarquer que si G est abélien, alors tout sous-groupe $H \leq G$ est distingué.

Exemple : $\{e\}$ et G sont distingués. $Ker(f)$ pour $f \in Hom(G, G')$ aussi. On a d'ailleurs aussi une sorte de réciproque, qu'on présentera comme exercice après

Proposition I.12.

De même, si $S \subset G$, alors il existe un (unique) sous-groupe distingué minimum (pour l'inclusion) de G contenant S qu'on nomme sous groupe distingué (ou normal) engendré par S et note $\langle S \rangle_{norm}$. On a alors $\langle S \rangle_{norm} = \bigcap_{H \trianglelefteq G \ S \subset H} H$

Définition I.13.

HP :
Soit $H \leq G$. Alors on peut définir deux relations d'équivalences $x \sim_g y \iff x^{-1}y \in H$ et $x \sim_d y \iff xy^{-1} \in H$.
Ces deux relations d'équivalences partitionnent G en $G/\sim_g$, appelé quotient de G à gauche par H et aussi noté G/H, et $G/\sim_d$, appelé quotient de G à droite par H et aussi noté $H\backslash G$.

Proposition I.14.

1. Les éléments de $G/\sim_g$ sont de la forme aH avec $a \in G$ (et inversement). Les éléments de $G/\sim_d$ sont de la forme Ha avec $a \in G$ (et inversement)
2. $aH = bH \iff a \sim_g b$ et $Ha = Hb \iff a \sim_d b$.
3. $\gamma_{ba^{-1}}$ est une bijection entre aH et bH. $\delta_{a^{-1}b}$ est une bijection entre Ha et Hb. En particulier, fini ou infini, on a $\forall a \in G \ |aH| = |Ha| = |H|$ et donc, si G est maitenant fini, on a $|H|||G|$ (appelé théorème de Lagrange) et $\dfrac{|G|}{|H|} = |G/H| = |H\backslash G|$. On notera ce nombre $[G : H]$ et on le nommera l'indice de H dans G.
4. G/H et $H\backslash G$ coincident $\iff H \trianglelefteq G$.
   Dans ce cas, on peut munir $G/H = H\backslash G$ d'une loi de composition interne déduite naturellement de G par $aH \cdot bH := (ab)H \iff \overline{a} \cdot \overline{b} := \overline{ab}$.
   Cette loi fait de G/H un groupe et on a un morphisme natural surjectif $\pi : \begin{cases} G & \longrightarrow G/H \\ a & \mapsto aH \end{cases}$ de noyau $Ker(\pi) = H$
5. Soit $H \leq G$. Le point précédent permet de déduire que $H \trianglelefteq G \iff \exists G'$ groupe et $\exists \phi \in Hom(G, G')$ tel que $H = Ker(\phi)$

Preuve : Les preuves étant similaires pour $\sim_g$ et $\sim_d$. On se contentera de traiter la première.
Tout d'abord $\sim_g$ est bien une relation d'équivalence. En effet :

1. $x \sim_g x$ car $x^{-1}x = e \in H$
2. $x \sim_g y \iff x^{-1}y \in H \underset{H \leq G}{\iff} (x^{-1}y)^{-1} \in H \iff y^{-1}x \in H \iff y \sim_g x$
3. Si $x \sim_g y$ et $y \sim_g z$ alors $z^{-1}x = (z^{-1}y)(y^{-1}x) \underset{H \leq G}{\in} H$

Prouvons maintenant les propositions :

1. Soit $a \in G$. Alors $\overline{a} = \{b \in G \ a^{-1}b \in H\} = \{b \in G \ b \in aH\} = aH$
2. $aH = bH \iff \overline{a} = \overline{b} \iff a \sim_g b$
3. Remarquons d'abord que $\gamma_{ba^{-1}}\Big|_{aH}^{bH}$ et $\gamma_{ab^{-1}}\Big|_{bH}^{aH}$ sont bien définies puis qu'elles sont inverse l'un de l'autre.
   Supposons désormais G fini. On a alors $G = \bigsqcup_{\overline{a} \in G/H} \overline{a}$ puis, puisqu'ils sont tous de cardinal $|H|$, $|G| = |G/H| \cdot |H|$

4. $G/H = H\backslash G \iff \forall a \in G\ \overline{a}_{G/H} = \overline{a}_{H\backslash G} \iff \forall a \in G\ aH = Ha \iff \forall a \in G\ aHa^{-1} = H \iff H \trianglelefteq G$
   Supposons désormais $H \trianglelefteq G$.
   - La loi . est bien définie : En effet, soit $a, b \in G$. On a alors dans G (pas G/H pour le moment) $aHbH \underset{H\trianglelefteq G}{=} abHH \underset{H\leq G}{=} abH$.
     Une autre manière de démontrer ceci (qui est équivalente à celle ci-dessus mais peut être plus claire) est de montrer que cette égalité est indépendante du représentant.
     Soit $a, a', b, b' \in G$ tel que $aH = a'H$ et $bH = b'H$. Alors $(ab)^{-1}a'b' = b^{-1}a^{-1}a'b' \in b^{-1}Hb' \underset{H\trianglelefteq G}{=} b^{-1}b'H \subset H$ car $b^{-1}b \in H$ et H est stable. Ainsi $\overline{ab} = \overline{a'b'}$ et . est bien définie
   - $(G/H, .)$ est un groupe :
     - $(G/H, .)$ reste une loi de composition intérieure associative
     - $\overline{a} \cdot \overline{e} = \overline{ae} = \overline{a} = \overline{ae} = \overline{a} \cdot \overline{e}$ et donc $e_{G/H} = \overline{e}$
     - $\overline{a} \cdot \overline{a^{-1}} = \overline{aa^{-1}} = \overline{e} = \overline{a^{-1}a} = \overline{a^{-1}} \cdot \overline{a}$ et donc $\overline{a}^{-1} = \overline{a^{-1}}$
   - Il aisé de vérifier que π est bien défini et est un morphisme de groupe. On a de plus $a \in Ker(\pi) \iff aH = H \iff \overline{a} = \overline{e} \iff a \in \overline{e} = H$
5. On a déja vu que le noyau d'un morphisme est toujours normal. Pour la réciproque, considérer le morphisme π ci-haut.

Proposition I.15.

HP. 1er théorème d'isomorphisme
Soit $f \in Hom(G, G')$. Alors f induit un (unique) morphisme injectif $\overline{f} \in Hom(G/ker(f), G')$ qui vérifie de plus $f = \overline{f} \circ \pi$. En particulier, $G/Ker(f) \simeq Im(f)$
Plus généralement, si $H \trianglelefteq G$ et $H \subset Ker(f)$ alors il existe un (unique) morphisme $f_H \in Hom(G/H, G')$ tel que $f = f_H \circ \pi_H$. De plus, $Ker(f_H) = \pi_H(Ker(f)) = \{y.H,\ y \in Ker(f)\}$
Conséquence direct : Soit $H' \leq G'$, alors $|f^{-1}(H')| = |H' \cap Im(f)| \times |Ker(f)|$

Preuve : Posons $\overline{f} : \begin{cases} G/ker(f) & \longrightarrow G' \\ \overline{x} & \mapsto f(x) \end{cases}$.

- $\overline{f}$ est bien définie. Ceci car si $\overline{x} = \overline{y}$ alors $f(x) = f(yy^{-1}x) = f(y)f(y^{-1}x) \underset{y^{-1}x\in Ker(f)}{=} f(y)$
- $\overline{f}$ est unique vu que $f = \overline{f} \circ \pi$ impose que $\overline{f}(a \cdot Ker(f)) = f(a)$
- Il est asié de vérifier que $\overline{f}$ reste bien un morphisme
- $x \in Ker(\overline{f}) \iff f(x) = 0 \iff x \in Ker(f) \iff \overline{x} = \overline{e}$ et donc $\overline{f}$ est injectif.

$G/Ker(f) \simeq Im(f)$ est une conséquence directe de ce qui précède.
La généralisation à H se fait de la même manière.
Pour l'égalité des cardinaux, appliquer le 1er théorème d'isomorphisme à $f\big|_{f^{-1}(H')}^{H'\cap Im(f)}$
Ajoutons une dernière propriété, qui peut parfois nous aider lorsqu'on a besois de quotienter (par exemple pour se réduire à un groupe fini) mais qu'on ne dispose pas de groupe normal évident

Proposition I.16.

(Coeur d'un sous-groupe) Soit $H \leq G$, alors $N := \bigcap_{g\in G} gHg^{-1} = \bigcap_{g\in G} \sigma_g(H)$ est l'unique sous-groupe de G qui est maximum pour les deux propriétés suivantes :

1. $N \leq H$
2. $N \trianglelefteq G$

De plus, si $m := [G : H] < \infty$, alors $[G : N] < \infty$ et $[G : N] | m!$

Preuve :
$N \trianglelefteq G$ est clair vu que c'est un sous-groupe de G (l'intersection de groupes est un groupe) et est stable par toutes les conjugaisons $(\sigma_g)_{g\in G}$
$N \leq H$ est aussi clair vu que H est l'un des termes dans l'intersection
Pour le caractère maximum de N, remarquer que si N' vérifie les deux propriétés alors $\forall g \in G\ \sigma_{g^{-1}}(N') = N' \subset H$ et donc $\forall g \in G\ N' \subset \sigma_g(H)$ d'où $N' \subset N$. Ce caractère maximum octroie aussi l'unicité.
Montrons maintenat le dernier point : Considérons $\varphi : \begin{cases} G & \longrightarrow Bij(G/H) \\ g & \mapsto (aH \mapsto gaH) \end{cases}$.
ϕ est bien un morphisme. Remarquons maintenant que $N = ker(\varphi)$
En effet, prenons $g \in G$. Alors $g \in Ker(\varphi) \iff \forall a \in G\ aH = gaH \iff \forall a \in G\ a^{-1}gaH = H \iff \forall a \in G\ a^{-1}ga \in H \iff g \in \bigcap\limits_{a\in G} aHa^{-1} = N$
En utilisant maintenant le 1er théorème d'isomorphisme on déduit que $G/N \simeq Im(\varphi) \leq Bij(G/H) \simeq \mathcal{S}_m$ et donc $[G : N] < \infty$ et de plus, par Lagrange, $[G : N] | m!$

Définition I.17.

G est dit simple si $G \neq \{e\}$ et si ses seuls sous-groupes distingués sont $\{e\}$ et G.
Autrement dit, si $G \neq \{e\}$ et $\phi \in Hom(G, G')$ alors soit ϕ est injectif soit $\phi = 0$
C'est aussi équivalent à dire que $G \neq \{e\}$ et $\forall g \in G - \{e\}\ \langle g \rangle_{norm} = G$

Exemple : $\mathbb{Z}/p\mathbb{Z}$ avec p premier

Définition I.18.

Soit G_1 et G_2 deux groupes. $G_1 \times G_2$, muni de la multiplication cordonnée par cordonnée, est un groupe, appelé groupe produit (direct). Les projection $pr_i : G_1 \times G_2 \to G_i$ sont des morphismes.
En particulier, $\{e\} \times G_2$ et $G_1 \times \{e\}$ sont des sous-groupes distingués de $G_1 \times G_2$

Exercice I.19.

Soit $H, K \leq G$

1. Montrer que $HK = KH \iff HK \leq G$
2. Si $H \trianglelefteq G$ alors $HK \leq G$
3. $H \cap K = \{e\} \iff f : \begin{cases} H \times K & \longrightarrow HK \\ (h, k) & \mapsto hk \end{cases}$ est bijective
4. Montrer que si H et K sont distingués et $H \cap K = \{e\}$ alors $\forall (h, k) \in H \times K\ hk = kh$.
5. Montrer que si $H \cap K = \{e\}$ et $\forall (h, k) \in H \times K\ hk = kh$ alors f est un isomorphisme

Exercice I.20.

Produit semi-direct : Remarquons que le défaut de $H \times K$ est qu'il nécéssite la commutation de H et K. Or, on veut tout de même étudier la structure du groupe HK lorsque c'est bien un groupe.
L'exercice qui suit essaie de généraliser l'idée de produit sans nécéssiter cette commutation et permet d'aborder la structure du groupe HK lorsque $H \trianglelefteq G$.
Soit H et K deux groupes et $f \in Hom(K, Aut(H))$. Pour une écriture plus compacte, on notera f_k à la place de $f(k)$. On définit le produit semi-direct $(G := H \rtimes_f K, \cdot)$ par :

- $G = H \times K$ en tant qu'ensemble
- $(h_1, k_1)(h_2, k_2) = (h_1 f_{k_1}(h_2), k_1 k_2)$

1. Verifier que cela définit bien un groupe
2. Montrer que qu'on peut injecter H et K dans G en les identifiant avec $H \times \{e\}$ et $\{e\} \times K$ respectivement. Verifier que $H \cap K = \{e\}$
3. Suposons que f est le morphisme trivial, montrer alors que G est simplement le produit direct usuel

Ce que l'on a présenté ci-haut est la construction d'un produit semi-directe de l'exterieur.
Procédons maintenant à celle interne :
Prenons un nouveau groupe G et $H, K \leq G$ tel que $H \cap K = \{e\}$. On suppose que H est normal.
Considérons $f : \begin{cases} K & \longrightarrow Aut(H) \\ k & \mapsto \sigma_k\big|_H^H \end{cases}$.
Montrer que $\phi : \begin{cases} H \rtimes K & \longrightarrow HK \\ (h,k) & \mapsto hk \end{cases}$ est un isomorphisme

II Le groupe $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 2$. On note $\sim$ la relation d'équivalence sur $\mathbb{Z}$ définie par $a \sim b \iff n|a-b \iff a-b \in n\mathbb{Z}$.
On note finalement $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'equivalences pour $\sim$. Une telle classe s'écrit $\overline{x} = x + n\mathbb{Z}$.
Il est aisé de verifier que $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\} = \{\overline{m}, \dots, \overline{m+n-1}\}$ pour tout m et que ces n éléments sont distincts.

Définition II.1.

Soit X, Y deux classes dans $\mathbb{Z}/n\mathbb{Z}$ et $x \in X$, $y \in Y$. Alors $\overline{x+y}$ ne dépend que de X et Y.
Ceci permet donc de définir une loi $+$ sur $\mathbb{Z}/n\mathbb{Z}$ qui en en fait un groupe abélien et $\pi : \begin{cases} \mathbb{Z} & \longrightarrow \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto \overline{x} \end{cases}$ est un morphisme surjectif de noyau $Ker(\pi) = n\mathbb{Z}$
Finalement, $\varphi : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow \mathbb{U}_n \\ \overline{k} & \mapsto e^{\frac{i2\pi k}{n}} \end{cases}$ est bien définie et constitue un isomorphisme

Preuve :
Remarquer que tout sous-groupe d'un groupe abélien est normal. Il suffit donc d'appliquer ce qui précéde sur $G = \mathbb{Z}$ et $H = n\mathbb{Z}$
Pour φ, on peut soit le vérifier à la main, soit juste considérer $\phi : \begin{cases} \mathbb{Z} & \longrightarrow \mathbb{U}_n \\ k & \mapsto e^{\frac{i2\pi k}{n}} \end{cases}$ qui est bien un morphisme

de groupes puis de remarquer que $Ker(\phi) = n\mathbb{Z}$ et d'utiliser le 1er théorème d'isomorphisme.

III Ordre d'un élément

Soit $a \in G$. Notons $j : \begin{cases} \mathbb{Z} & \longrightarrow \langle a \rangle \\ m & \mapsto a^m \end{cases}$ qui est un morphisme surjectif de groupes. On peut alors écrire $Ker(j) = nZ$ avec $n \geq 0$

- Si $n = 0 (\iff Ker(j) = \{0\})$ alors j est un isomorphisme et on posera $\omega(a) = \infty$
- Si $n \geq 1 (\iff Ker(j) \neq \{0\})$, on note alors $\omega(a) = n$, appelé l'ordre de a

Proposition III.1.

Placons nous dans le cas $Ker(j) \neq \{0\}$ et posons $n := \omega(a)$

1. $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ et ces éléments sont distincts. De plus, $\forall k \in \mathbb{Z}\ a^k = e \iff n|k$
2. $n = min\{m \in \mathbb{N}^*,\ a^m = e\}$
3. $\forall m \in \mathbb{Z}\ \exists! k \in [\![0; n-1]\!]\ a^m = a^k$
4. $\forall m, l \in \mathbb{Z}\ a^m = a^l \iff n|m-l \iff m - l \in \mathbb{Z}/n\mathbb{Z}$
5. $\forall k \in \mathbb{Z}\ \omega(a^k) = \dfrac{n}{n \wedge k}$. Conséqence : si $q|n$ alors $\omega(a^q) = \dfrac{n}{q}$

Preuve :

1. Soit $k \in \mathbb{Z}$. Alors $a^k = e \iff k \in Ker(j) \iff k \in n\mathbb{Z} \iff n|k$. En particulier, $a^n = e$.
   $\supset$: Clair.
   $\subset$: Soit $k \in \mathbb{Z}$. Faisons la division euclidienne de k par n : $k = qn + b$ avec $b \in [\![0; n-1]\!]$. On a alors $a^k = (a^n)^k a^b = e^k a^b = a^b$. Ces éléments sont de plus distincts car si $i \neq j \in [\![0; n-1]\!]$ vérifient $a^i = a^j$ alors $a^{i-j} = e$ et donc $n|i-j$ d'où $i = j$.
2. D'après le point 1, $\forall k \in [\![1; n-1]\!]\ a^k \neq e$. Or, $a^n = e$ d'où le résultat.
3. L'unicité, si existence, provient du point 1. Pour l'existence, faire une divison euclidienne par n comme ci-haut.
4. $a^m = a^l \iff a^{m-l} = e \iff n|m-l \iff m - l \in \mathbb{Z}/n\mathbb{Z}$
5. Soit $k, l \in \mathbb{Z}$. $(a^k)^l = e \iff a^{kl} = e \iff n|kl \iff \dfrac{n}{n \wedge k} \Big| \dfrac{k}{n \wedge k} l \underset{\text{Gauß}}{\iff} \dfrac{n}{n \wedge k} \Big| l$. Et donc $\omega(a^k) = min\{l \in \mathbb{N}^*\ (a^k)^l = e\} = \dfrac{n}{n \wedge k}$

IV Actions de morphismes

Proposition IV.1.

Soit $f \in Hom(G, G')$

1. $\omega(a) < \infty \Longrightarrow \omega(f(a)) | \omega(a)$
2. Si f est injective alors $\omega(a) = \omega(f(a))$
3. Si a et b sont conjugués, alors $\omega(a) = \omega(b)$. En particulier, $\forall x, y \in G,\ \omega(xy) = \omega(yx)$

Preuve :

1. $f(a)^{\omega(a)} = f(a^{\omega(a)}) = f(e) = e'$ et donc $\omega(f(a)) < \infty$ et $\omega(f(a)) | \omega(a)$

2. $\omega(a) = \infty$ donne que $\langle f(a)\rangle = f(\langle a\rangle)$ est infini par injectivité et donc $\omega(f(a)) = \infty$
   Si $\omega(a) < \infty$ alors $f(a)^k = e' \iff f(a^k) = e \underset{f \text{ injectif}}{\iff} a^k = e \iff \omega(a)|k$ et donc $\omega(f(a)) < \infty$ et $\omega(f(a)) = \omega(a)$

3. Pour cela il suffit de se rappeler que la conjugaisons $\sigma_z \in Aut(G)$.
   Pour le second point : $yx = \sigma_y(xy)$

Exercice IV.2.

Mines :
Soit $m, n \geq 1$ tel que $m \wedge n = 1$. Déterminer $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$

Exercice IV.3.

Soit $(a, b) \in G^2$ avec $\omega(a) = m \leq \omega(b) = n < \infty$

1. A-t-on $\omega(ab) < \infty$.
   Indice : Penser à S_θ et $S_{\theta'}$ symetriques
2. On suppose $ab = ba$ et $\omega(a) \wedge \omega(b) = 1$. Montrer que $\omega(ab) = mn$
3. On suppose toujours que $ab = ba$. Montrer qu'il existe $c \in G$ tel que $\omega(c) = n \vee m$
4. On suppose maintenant que G est abelien et $|G| < \infty$.
   Montrer $\exists z \in G\ \forall x \in G\ \omega(x)|\omega(z)$

Proposition IV.4.

Lagrange faible, démonstration dans le cas commutatif.
Soit $a \in G$ avec G un groupe commutatif fini. Alors $\omega(a)||G|$

Preuve : $\gamma_a \in Bij(G)$ et donc $\prod_{g\in G} g = \prod_{g\in G} \gamma_a(g) = \prod_{g\in G} (ag) = a^{|G|} \prod_{g\in G} g$.
En multipliant par l'inverse de $\prod_{g\in G} g$ on obtient $a^{|G|} = e$

V Groupes cycliques

Définition V.1.

Soit G un groupe, On dit qu'il est monogène s'il est engendré par un seul élément. Si de plus G est fini, alors on dit qu'il est cyclique.

Proposition V.2.

Si $G = \langle a \rangle$, alors deux cas se présentent :

1. $\omega(a) = \infty$, auquel cas $j : \begin{cases} \mathbb{Z} & \longrightarrow \langle a \rangle \\ m & \mapsto a^m \end{cases}$ est un isomorphisme
2. $n := \omega(a) < \infty$, auquel cas $G = \{e, a, \dots, a^{n-1}\}$ avec ces elements distincts. De plus $|G| = n$

On suppose désormais G un groupe quelconque et $n \geq 1$

1. G est cyclique de cardinal $n \iff G \simeq \mathbb{Z}/n\mathbb{Z}$.
   De plus, cet isomorphisme est induit en envoyant $\overline{1}$ sur n'importe quel générateur de G

Preuve : 1 et 2 déja faits
Pour la dernière proposition. $\Longleftarrow$: Clair

$\Longrightarrow$: G n'est pas infini et donc $G = \{e, a, \dots, a^{n-1}\}$ par ce qui précède. Posons $\phi : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \longrightarrow G \\ \overline{k} & \mapsto a^k \end{cases}$.
On peut vérifier aisement qu'elle est bien définie et est un morphisme.
De plus, ϕ est bijective vu que $G = \{e, a, \dots, a^{n-1}\}$ et que ces éléments sont distincts.

Exercice V.3.

Soit $G = \langle a \rangle$ un groupe cyclique d'ordre $n := |G|$ et $H \leq G$. Posons $d := |H|$. On rappelle que par Lagrange $d|n$ (G est commutatif, quoique non nécessaire).
Montrer que $H = \langle a^{\frac{n}{d}} \rangle$

Remarque : Soit $n \geq 1$. Alors $D_n = \{k \geq 1 \ k|n\}$ vérifie que $|D_n| \leq 2\sqrt{n} + 1$. En effet, $\varphi : \begin{cases} D_n \cap [\![1; \lfloor \sqrt{n} \rfloor]\!] & \longrightarrow D_n \cap [\![\lfloor \sqrt{n} \rfloor; n]\!] \\ d & \mapsto \dfrac{n}{d} \end{cases}$ est une bijection

Exercice V.4.

Soit $G = \langle a \rangle$ cyclique avec $|G| = n \geq 2$.
Montrer que $G = \langle a^k \rangle \iff k \wedge n = 1$. On posera alors $\varphi(n) := |\{k \in [\![1; n]\!] \ k \wedge n = 1\}|$ nommée l'indicatrice d'euler.
Application : Pour $G = \mathbb{U}_n$, $e^{\frac{i2\pi k}{n}}$ avec $k \wedge n = 1$ s'appelle une racine primitive $n-$ème de l'unité. La théorie des polynomes cyclotomique (et des extensions de Galois cyclotomiques) se base sur ces racines.
Montrer que $\displaystyle\sum_{d|n \ d \geq 1} \varphi(d) = n$

Exercice V.5.

1. Soit G_1 et G_2 deux groupes cycliques. Trouver une condition nécéssaire et suffisante pour que $G_1 \times G_2$ soit cyclique.
2. (Lemme des restes chinois) Soit $a, b \geq 1$. Montrer que $\varphi : \begin{cases} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \overline{x} & \mapsto (\overline{x}, \overline{x}) \end{cases}$
   est bien définie puis que φ est un isomorphisme $\iff a \wedge b = 1$

Exercice V.6.

Soit A un anneau commutatif unitaire.

1. Soit $P, Q \in A[X]$ avec Q de coefficient dominant égal à 1 (i.e. $Q = 1$ ou Q est unitaire). Montrer que l'on peut effectuer "la" division euclidienne de P par Q
2. On suppose que A est intègre et $degP = n \geq 0$. Montrer que P possède au plus n racines distinctes
3. Soit $\mathbb{K}$ un corps et $G \subset \mathbb{K}^*$ un sous-groupe fini de $\mathbb{K}^*$. Montrer que G est cyclique

VI Groupe engendré par une partie

Proposition VI.1.

On rappelle que $\forall A \subset G$, il existe un plus petit sous-groupe $\langle A \rangle$ de G contenant A et appellée sous-groupe engendré par A.
Description externe : $\langle A \rangle = \bigcap_{H \leq G \ A \subset H} H$
Description interne : $\langle A \rangle = \{M \in G \ \exists n \in \mathbb{N} \ \exists a_1, \dots, a_n \in A \ \exists \alpha_1, \dots, \alpha_n \in \mathbb{Z} \ M = a_1^{\alpha_1} \dots a_n^{\alpha_n}\}$

Preuve : L'existence, unicité et formule externe ont déja été faits.
Pour celle interne, remarquer que l'ensemble de droite est bien un sous-groupe contenant A et que donc il contient $\langle A \rangle$.
Réciproquement, montrer, par récurrence sur la longeur n du mot que chaque terme de l'ensemble de droite appartient à $\langle A \rangle$.
L'idée de la propriété ci-dessus est en faite bien généralisable : il s'agissait de considérer la groupe libre sur A (voir bonus).
Vocabulaire : On dit que $S \neq \varnothing$ est générateur (de G) si $G = \langle S \rangle$
Exemple : $\mathcal{S}_n$ est généré par les transposition de la forme $(i \ i+1)$

Exercice VI.2.

Soit $(G, +)$ un groupe fini abélien et p un nombre premier tel que $\forall g \in G \ \omega(g) | p$. Montrer que $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ pour un certain $n \geq 0$

⚠Un $p-$groupe n'est pas forcément abélien
$G = \left\{ \begin{pmatrix} \overline{1} & \overline{a} & \overline{b} \\ 0 & \overline{1} & \overline{c} \\ 0 & 0 & \overline{1} \end{pmatrix} \in SL_3(\mathbb{Z}/p\mathbb{Z}) \right\} \ |G| = p^3$
Pour $|G| = p$ ou $G = |p|^2$ par contre c'est vrai (voir compléments).

Exercice VI.3.

Soit $G \neq \{e\}$ un groupe. Notons $\mathbb{P}$ l'ensemble des nombres premiers.
Montrer que $Sg(G) = \{\{e\}, G\} \iff \exists p \in \mathbb{P} \ G \simeq \mathbb{Z}/p\mathbb{Z} \iff \forall g \in G - \{e\} \ \langle g \rangle = G \iff \exists p \in \mathbb{P} \ |G| = p$

Exercice VI.4.

Soit p un nombre premier. Montrer que $\mathcal{S}_p$ est engendré par n'importe quelle transposition (ij) et grand cycle σ.

VII Compléments :

1. Quotients

Exercice VII.1.

Soit p, q deux nombres premiers distincts et $(G, +)$ un groupe abélien d'ordre $|G| = pq$. Montrer que $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

Exercice VII.2.

Soit G un groupe fini et $H \leq G$ tel que $[G : H] = 2$. Montrer que $H \trianglelefteq G$ et que donc H contient tous les carrés. On le généralisera une fois les actions de groupes vues.

2. Actions de groupes

Définition VII.3.

Soit X un ensemble non vide et G un groupe. Une action de groupe (à gauche) est un morphisme $\phi : G \longrightarrow Bij(X)$. Au lieu de noter $\phi(g)(x)$ on le note plus simplement $g.x$
C'est aussi équivalent de définir une action comme une application $\phi : G \times X \to X$ qui vérifie :

- $\forall x \in X \; e.x = x$
- $\forall g, h \in G \; \forall x \in X \; (gh).x = g.(h.x)$

Exemples : Si $X = G$, $g \mapsto \gamma_g \iff g.x = gx$ et $g \mapsto \sigma_g \iff g.x = gxg^{-1}$ sont des actions de groupes. La première est l'action de translation à gauche et la seconde l'action de conjugaison.
Remarquer que $x \mapsto \delta_x$ ne définit une action à gauche que $\iff G$ est abélien.

Définition VII.4.

On définit $\forall x \in X \; O(x) := \{y \in X \; \exists g \in G \; g.x = y\}$ l'orbite de x (sous ϕ) et $Stab(x) := \{g \in G \; g.x = x\}$ le stabilisateur de x (sous ϕ).

Proposition VII.5.

1. Les orbites partitionnent X i.e. $\forall x, y \in X\ O(x) = O(y)$ ou $O(x) \cap O(y) = \varnothing$ et $\bigcup_{x \in X} O(x) = X$.
   Voici une autre formulation équivalente : Considérons la relation $x \sim y \iff \exists g \in G\ y = g.x \iff y \in O(x)$. Alors $\sim$ est une relation d'équivalence et $X/\sim = \{O(x),\ x \in X\}$. On notera $X/\sim$ par X/G.
2. $Stab(x) \leq G$. De plus, si $y = g.x$ alors $Stab(y) = gStab(x)g^{-1} = \sigma_g(Stab(x))$.
3. Soit $x \in X$. Alors $\phi_x : \begin{cases} G/Stab(x) & \longrightarrow O(x) \\ g & \mapsto g.x \end{cases}$ est bien définie et est une bijection. En particulier, si G est fini, $|G/Stab(x)| = [G : Stab(x)] = \dfrac{|G|}{|Stab(x)|} = |O(x)|$
4. (Fomule des classes) Supposons G et X finis et soit $(x_i)_{i \in X/G}$ un système de représenants de X/G i.e. $\forall i \in S/G\ x_i \in i$ alors $|X| = \sum_{i \in X/G} \dfrac{|G|}{|Stab(x_i)|}$

Preuve :

1. - $x \sim x$ car $x = e.x$
   - $x \sim y \iff \exists g \in G\ y = g \cdot x \iff \exists g \in G\ x = g^{-1} \cdot y \underset{G \text{ groupe}}{\iff} \exists g \in G\ x = g \cdot y \iff y \sim x$
   - $x \sim y$ et $y \sim z \implies \exists g, h \in G\ y = g \cdot x$ et $z = h \cdot y \implies \exists g, h \in G\ z = h \cdot (g \cdot x) = (hg) \cdot x \underset{G \text{ groupe}}{\implies} \exists g \in G\ z = g \cdot x \implies x \sim z$
2. $Stab(x) \leq G$ est clair. Soit $h \in G$, on a alors $h \in Stab(g \cdot x) \iff (hg) \cdot x = h.(g.x) = g.x \iff (g^{-1}hg) \cdot x = x \iff g^{-1}hg \in Stab(x) \iff h \in gStab(x)g^{-1}$ et donc $Stab(g \cdot x) = gStab(x)g^{-1}$
3. Soit $g, h \in G\ g \cdot x = h \cdot x \iff (g^{-1}h) \cdot x = x \iff (g^{-1}h) \in Stab(x) \iff h \in gStab(x) \underset{Stab(x) \leq G}{\iff} gStab(x) = hStab(x)$. Ceci montre que ϕ est bien définie et qu'elle est injective. Elle est de plus clairement surjective par définition de $O(x)$.
4. $X = \bigsqcup_{i \in X/G} i$ et donc $|X| = \sum_{i \in X/G} |i| = \sum_{i \in X/G} |O(x_i)| = \sum_{i \in X/G} \dfrac{|G|}{|Stab(x_i)|}$

Exercice VII.6.

Soit G un groupe fini et $H \leq G$ tel que $[G : H] = p$ où p est le plus petit premier qui divise l'ordre de G. Montrer que $H \trianglelefteq G$ et que donc H contient toutes les puissances $p-$emes

3. Action de conjugaison

Proposition VII.7.

Cette section s'occupe du cas particulier de l'action par conjugaison/automorphisme intérieur sur G fini : $\phi : \begin{cases} G & \longrightarrow Aut(G) \\ x & \mapsto \sigma_x \end{cases}$
On a alors $Stab(a) = C(a) = \{x \in G \ xax^{-1} = a\} = \{x \in G \ ax = xa\}$ et $O(a) = \{xax^{-1} \ x \in G\}$
Remarquons que $a \in Z(G) \iff C(a) = G \iff O(a) = \{a\}$. Par ce qui précède :

1. $\forall a \in G \ C(a) \leq G$ et $G/C(a) \simeq O(a)$
2. $\forall a \in G \ |G| = |C(a)||O(a)|$
3. (Formule des classes) Soit R un ensemble de représentants des classes de conjugaison non réduites à un singleton, alors $|G| = |Z(G)| + \sum_{x \in R} \frac{|G|}{|C(x)|}$

Applications :

1. Soit G un $p-$groupe fini i.e. $|G| = p^n$ avec $n \geq 1$ et p premier. Alors son centre $Z(G)$ est non trivial. En particulier, si $n \leq 2$ alors G est abélien
   Preuve :
   - Appliquons la formule des classes à G. On a alors $|Z(G)| = |G| - \sum_{x \in R} \frac{|G|}{|C(G)|}$. Or, $\forall x \in R$, $C(G) \neq G$ par définition et donc $1 \neq \frac{|G|}{|C(G)|}||G| = p^n$. Or, vu que p est premier, les seuls diviseurs positives de p^n autre que 1 sont de la forme p^k $1 \leq k \leq n$ et donc $\frac{|G|}{|C(G)|} \equiv 0[p]$.
     En particulier, $|Z(G)| \equiv 0[p]$ et donc, vu que ce dernier contient au moins e, c'est alors un sous-groupe strict de G.
   - Supposons $n = 1$ et prenons $x \in G - \{0\} \neq \varnothing$. Alors $\langle x \rangle$ est un sous-groupe strict de G et donc son cardinal, par Lagrange, est un diviseur de p different de 1. Par conséquent, $G = \langle x \rangle$ et donc G est abélien
   - Supposons $n = 2$. On a par ce qui précède $Z(G) \neq \{e\}$. Toujours par Lagrange, $|Z(G)| = p$ ou p^2. Si c'est p^2 on a finit. Sinon, prenons alors $x \in G - Z(G)$. On sait que par Lagrange $\langle \{x\} \cup Z(G) \rangle = G$ (son cardinal ne peut pas être p ou 1 et est donc p^2). Or, tous les éléments de $\{x\} \cup Z(G)$ commutent entre eux deux à deux d'où G est abélien (facile à voir avec la caractérisation interne du sous-groupe engendré.
2. Soit G un groupe fini et p un nombre premier tel que $p|n := |G|$. Alors il existe $x \in G \ \omega(x) = p$
   Preuve :
   Considérons $E = \{(x_1, \ldots, x_p) \in G^p \ x_1 \ldots x_p = e\}$. Il est aisé de voir que $E \simeq G^{p-1}$ comme ensemble (les $p-1$ premières coordonnées peuvent être choisies librement et la dernière est forcement l'inverse du produit des autres) et donc $|E| = n^{p-1}$
   Considérons l'action de permutation circulaire de $\mathbb{Z}/p\mathbb{Z}$ sur E. Plus précisement, $\overline{k} \cdot (x_1, \ldots, x_p) = (x_{\sigma^k(1)}, \ldots, x_{\sigma^k(p)})$ où $\sigma = (1 \ldots p)$ le grand cycle usuel.
   Remarquer que cette action est bien définie et n'est pas triviale car $\omega(\sigma) = p$.
   Notons $Z := \{x \in G \ x^p = e\}$. Soit $X = (x_1, \ldots x_n) \in E$. On sait que $|O(X)|$ est soit p soit 1 car divise $|\mathbb{Z}/p\mathbb{Z}|$.
   Il est aisé de vérifier que $|O(X)| = 1 \iff \exists x \in Z \ X = (x, \ldots, x)$ et donc il y'a autant de X d'orbite triviale que d'éléments de Z.
   Ainsi, si S_1 est un ensemble de représentants des elements d'orbite triviale et X_2 un ensemble de

représenants du reste alors la formule des classes donne que :
$|G| = |S_1| + p|S_2|$ et donc, modulo p, $|S_1| = |Z| \equiv 0\ (modp)$. Ainsi, sachant que $e \in Z$, on a $p||Z|$ et donc, vu que $p \geq 2$, $Z - \{e\}$ est non vide.

Remarquons que pour le cas abélien on dispose d'une preuve plus simple :

Exercice VII.8.

(Inspiré du TD d'Alain Troesch, un de nos professeurs de sup)
Soit G un groupe abélien fini et p un nombre premier

1. Soit $K \trianglelefteq G$. Montrer que s'il existe $x \in G/K$ d'ordre p alors il en existe un aussi d'ordre p dans G
2. On suppose que $p||G|$, montrer qu'il existe $x \in G\ \omega(x) = p$
3. Soit $a \geq 1$. On suppose que $p^a||G|$. Montrer que $\exists H \leq G$ d'ordre p^a
4. en déduire que $\forall n||G|\ \exists H \leq G\ |H| = n$

Groupes abéliens

Proposition VII.9.

On présentera, sans démonstration, deux théorèmes qui peuvent parfois être utile pour mieux visualiser les choses en tête :

1. Soit $\{0\} \neq G \leq \mathbb{R}^n$ un sous-groupe <u>discret</u> de $\mathbb{R}^n$. Alors il admet une $\mathbb{Z}-$base $(e_1, \dots, e_s) \in G^s$ i.e. $\forall g \in G\ \exists!(a_1, \dots, a_s) \in \mathbb{Z}^n\ g = a_1 \cdot e_1 + \dots + a_s \cdot e_s$. De plus, $s = dim(Vect(G))$ et donc, en particulier, $s \leq n$.
2. Soit $G \neq \{0\}$ un groupe <u>abélien</u> de type fini (i.e. engendré par un nombre fini d'éléments). Alors il existe des uniques $r, s \in \mathbb{N}$ et une unique séquence $2 \leq n_1| \dots |n_s$ tel que $G \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_s\mathbb{Z}$
   Par le théorème chinois, on obtient la formulation suivante aussi : Il existe un unique $r \in \mathbb{N}$ et une unique suite, à ordre près, $n_1, \dots_{,n}\ _l$ de puissances de nombres premiers tel que $G \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_l\mathbb{Z}$

VIII Bonus

Cette partie étant bonus, on ne détaillera pas trop les preuves et on se contentera donc de donner les idées clés.

Définition VIII.1.

Soit $S \neq \varnothing$ un ensemble.
Alors on définit $Lib(S)$ comme l'ensemble des mots finis sur l'alphabet $S \coprod S^{-1}$ (i.e. M tel qu'il existe $n \geq 0$ et $a_1, \dots, a_n \in S \coprod S^{-1}$ tel que $M = a_1 \dots a_n$) quotienté par la relation d'équivalence qui identifie $Mxx^{-1}N$ et $Mx^{-1}xN$ avec MN i.e. permet d'enlever toutes les occurences d'éléments et leurs inverses si elle sont consécutives.
$Lib(S)$, avec la concaténation des mots, forme alors un groupe appelé le groupe libre sur S ou, si $n = |S|$ est fini, le groupe libre à n éléments, usuellement noté F_n. Son élément neutre est le mot vide $\varnothing$
$Lib(\varnothing) = \{e\}$

Exercice VIII.2.

(Propriété universelle et adjonction)
Soit $I \neq \varnothing$ un ensemble et $(g_i) \in G^I$ une famille d'élements du groupe G.
Montrer qu'il existe un unique morphisme de groupe $f : Lib(I) \longrightarrow G$ tel que $\forall i \in I\ f(i) = g_i$.
Réciproquement, soit G un groupe et $(g_i) \in G^I$ une famille d'elements de G tel que pour tout groupe H et famille $(h_i) \in H^I$ il existe un unique morphisme $f \in Hom(G, H)$ tel que $\forall i \in I\ f(g_i) = h_i$. Montrer que $G \simeq Lib(S)$
En déduire que tout groupe G est un quotient d'un groupe libre
Notons U "l'application" (c'est en faite un foncteur) qui prend un groupe G et lui associe l'ensemble G, démuni de sa structure de groupe.
Notons F "l'application" qui prend un ensemble S et lui associe le groupe libre sur S.
Soit maintenant S un ensemble non vide et G un groupe.
Montrer qu'il existe une bijection (qui est d'ailleurs même naturelle) entre $U(G)^S$ et $Hom(F(S), G)$

Définition VIII.3.

Soit G, H deux groupes. On définit $G * H$ leur groupe libre comme le groupe libre généré par $G \coprod H$ mais où on identifie deux termes successifs de G ou H avec leur produit et e au mot vide.
Remarquer alors que, même si G et H tous les deux sont abéliens, $G * H$ ne l'est pas en général. Par exemple, $\mathbb{Z} * \mathbb{Z} = F_2$ n'est pas abelien
Remarquer aussi que $G * H$ contient G et H comme des mots de longueurs 1 et que, vus dans $G * H$, $G \cap H = \{e\}$

Exercice VIII.4.

(Propriété universelle) Soit G_1, G_2 deux groupes.
Montrer que pour tout groupe H et $f_i \in Hom(G_i, H)$ morphismes, il existe un unique morphisme de groupe $f : G_1 * G_2 \longrightarrow H$ tel que $\forall g \in G_i\ f(g) = f_i(g)$.
Réciproquement, soit G un groupe un groupe qui satisfait la propriété ci-haut, montrer que $G \simeq G_1 * G_2$

On mentionnera aussi qu'il existe une notion de groupe libre abélien qui est la même que celle ci-haut à la difference près que c'est abélien i.e. que le mot $AabB$ et $AbaB$ sont identifiés.
On peut montrer qu'il s'agit en fait de $Ab(Lib(S))$, l'abélianisé du groupe libre $Lib(S)$.
L'équivalent du produit libre abélien pour les groupes abélien est simplement le produit direct déja vu.
On peut vérifier que les propriétés ci-haut restent valables à condition d'ajouter des "abéliens" partout.
On ajoutera une dernière notion

Définition VIII.5.

Soit G un groupe. On notera $Ab(G)$ l'abélianisé du groupe G. Conceptuellement, il s'agit de G mais en le rendant abélien.
Formellement, $Ab(G) := G/[G : G]$ où $[G : G] := \{ghg^{-1}h^{-1},\ (g, h) \in G^2\}$ est un sous-groupe distingué de G et on a donc une surjection naturelle $\pi : G \longrightarrow Ab(G)$

Exercice VIII.6.

(Propriété universelle)
Soit G un groupe (pas forcement abélien).
Montrer que pour tout groupe abélien H et tout $f \in Hom(G, H)$, il existe un unique $\overline{f} \in Hom(Ab(G), H)$ tel que $f = \overline{f} \circ \pi$
Montrer que si G' est un groupe abélien qui vérifie la même propriété ci-haut de $G' \simeq Ab(G)$

Correction de l'exercice I.2. :

Notons l'inverse à gauche de a par a_g^{-1}.
On a alors $a_g^{-1} \cdot a \cdot a_g^{-1} = e \cdot a_g^{-1} = a_g^{-1}$
Ainsi, $a \cdot a_g^{-1} = e \cdot a \cdot a_g^{-1} = (a_g^{-1})_g^{-1} a_g^{-1} \cdot a \cdot a_g^{-1} = (a_g^{-1})_g^{-1} a_g^{-1} = e$
Et donc a admet aussi un inverse à droite (qui est forcément le même que celui à gauche) et donc G est un groupe.

Correction de l'exercice I.6. :

$\Longrightarrow$: Clair
$\Longleftarrow$: H étant non vide et stable, il suffit de vérifier l'existence des inverses (le neutre vient gratuitement). Soit $a \in H$. H étant fini, on dispose de $1 \leq i < j$ tel que $a^i = a^j$. Si $j = i+1$ alors $a = e$ et donc $a^{-1} = e \in H$. Sinon, $j \geq i+2$ et donc $b = a^{j-i-1} \in H$. Montrons que $b = a^{-1}$.
$ba = a^{j-i-1}a = a^{j-i} = e = aa^{j-i-1} = ab$ d'où le résultat.
Remarquons au passage qu'on avait besoin de vérifier uniquement l'inversion à gauche ou droite et pas forcement les deux.

Correction de l'exercice I.10. :

Le fait que ce soit un morphisme est clair. Montrons alors son injectivité :
Soit $a \in Ker(\varphi)$, alors $\varphi(a)(e) = e$ et donc $a \cdot e = e$ d'où $a = e$.
Ceci permet donc d'identifier G au sous-groupe $Im(\phi)$ de $Bij(G)$.
Supposons désormais $|G| < n$ et prenons une bijection d'ensembles $\phi : G \simeq [\![1; n]\!]$.
on a alors un isomorphisme $f : \begin{cases} Bij(G) & \longrightarrow \mathcal{S}_n \\ \sigma & \mapsto \phi \circ \sigma \circ \phi^{-1} \end{cases}$ qui identifie les 2 (il s'agit juste d'une nouvelle numérotation de $\mathcal{S}_n$ par des éléments de $\mathcal{S}_n$ à la place et donc toutes les structures sont préservés) d'où le résultat.
Remarquer au passage que ce procédé est bien plus général. En effet, si on a un ensemble G muni d'une structure avec des lois internes ou externes. Alors on peut transmettre cette structure sur n'importe quel ensemble S de même cardinalité que G. Il suffit de "lire les lois" dans G.
Pour mieux illustrer l'idée, voici un exemple simple avec par exemple la loi de groupe :
On définit $\forall x, y \in S \; x \cdot y := \phi(\phi^{-1}(x) \cdot \phi^{-1}(y))$ où $\phi : G \simeq [\![1; n]\!]$ une bijection d'ensembles qui, une fois S muni de cette loi, rend S un groupe et ϕ un isomorphisme entre les deux.
Si on y pense, c'est assez intuitive, on ne fait que renomer nos éléments.
Un exemple simple de l'utilisation de cette idée : c'est quasiment comme ceci qu'on généralise la notion de structure différentiable de $\mathbb{R}^n$ à d'autres ensembles, qu'on nomme variétés différentiables.

Correction de l'exercice I.18. :

1. $\Longleftarrow$: $HK \underset{HK \leq G}{=} (HK)^{-1} = K^{-1}H^{-1} \underset{H \text{ et } K \leq G}{=} KH$
   $\Longrightarrow$: $HK \neq \varnothing$ donc il suffit de vérifier que $\forall (h,k,h',k') \in H \times K \times H \times K$ on a $(hk)(h'k')^{-1} \in HK$.
   Pour cela remarquer que $(hk)(h'k')^{-1} = hkk'^{-1}h'^{-1} \underset{K \leq G}{\in} hKh'^{-1} \underset{H \leq G}{\subset} HKH \underset{HK=KH}{=} HHK \underset{H \leq G}{=} HK$
2. Supposons que $H \trianglelefteq G$. Alors $HK = \bigcup_{k \in K} Hk \underset{H \trianglelefteq G}{=} \bigcup_{k \in K} kH = KH$
3. $\Longleftarrow$: Soit $x \in H \cap K$. On a alors $f(x,e) = x = f(e,x)$ et donc, par injectivité, $x = e$
   $\Longrightarrow$: f est surjective par définition. Soit $(h,k,h',k') \in H \times K \times H \times K$.
   On a alors $f(h,k) = f(h',k') \iff hk = h'k' \iff h'^{-1}h = k'k^{-1} \underset{H \cap K = \{e\}}{=} e \iff h = h'$ et $k = k'$ d'où f est bijective.
   Remarquer que sans commutation entre H et K f n'est pas un morphisme
4. Remarquons que $hkh^{-1}k^{-1} \in hKh^{-1}k^{-1} \cap hkHk^{-1} \underset{H \text{ et } K \trianglelefteq G}{=} Kk^{-1} \cap hH \underset{H \text{ et } K \leq G}{=} K \cap H = \{e\}$ et donc $hk = kh$
5. Par ce qui précède f est bijective. C'est de plus désormais un morphisme vu que H et K commutent (facile à vérifier) et donc c'est finalement un isomorphisme

Correction de l'exercice I.19. :

1. Ce sont juste des calculs pas très compliqués, laissés au lecteur
2. $H \times \{e\}$ est un groupe isomorphe à H à travers la projection sur la première coordonée. En effet, $(h,e)\cdot(h',e) = (hf_e(h'), e\cdot e) = (h\ \mathrm{Id}(h'), e) = (hh', e)$.
   Similairement, $\{e\}\times K$ est un groupe isomorphe à K à travers la projection sur la seconde coordonée. En effet, $(e,k)\cdot(e,k') = (ef_h(e), k\cdot k') = (e\cdot e, kk') = (e, kk')$.
   Finalement, $(H\times\{e\})\cap(\{e\}\times K) = \{(e,e)\} = \{e_G\}$
3. Si f est le morphisme trivial, alors $(h,k)\cdot(h',k') = (hf_k(h'), kk') = (h\,\mathrm{Id}(h'), kk') = (hh', kk')$ et donc $G \simeq H\times K$

Par $I.18$. $HK \leq G$ vu que $H \trianglelefteq G$.
f est bien un morphisme. En effet, on sait déja que les σ_k se composent comme des morphismes. Il suffit alors de vérifier qu'ils stabilisent H.
Or, ceci est vrai vu que H est normal.
Ainsi, $H \rtimes_f K$ est bien défini comme groupe par ce qui précède. Il reste à verifier que ϕ est un isomorphisme.

1. ϕ est un morphisme : $\phi((h,k)(h',k')) = \phi((h\sigma_k(h'), kk')) = h\sigma_k(h')kk' = hkh'k^{-1}kk' = hkh'k' = \phi((h,k))\phi((h',k'))$
2. ϕ est surjectif par définition de HK
3. Soit $(h,k)\in ker(\phi)$, alors $hk = e$ i.e. $h = k^{-1} \in H\cap K = \{e\}$ et donc $h = k^{-1} = e$ d'où $h = k = e$ et donc ϕ est injectif.

On déduit finalement que ϕ est un isomorphisme.

Correction de l'exercice IV.2. :

Soit $f \in Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$
On sait que $f(1) \in \mathbb{Z}/n\mathbb{Z}$ et donc $nf(1) = 0$.
En particulier, $\omega(f(1))|n$.
De même, $\omega(f(1))|\omega(1_{\mathbb{Z}/m\mathbb{Z}}) = m$ et donc $\omega(f(1))|m\wedge n = 1$ i.e. $f(1) = 0$.
Ainsi $f = 0$

Correction de l'exercice IV.3. :

1. Rappelons nous que $S(\theta)S(\theta') = R(\theta-\theta')$ où $S(\theta)$ désigne la symetrie par rapport à la droite d'angle θ avec $x = 0$ (dans le sens direct) dans $\mathbb{R}^2$ et $R(\theta)$ désigne la rotation d'angle θ (dans le sens direct) dans $\mathbb{R}^2$

   En particulier, si on prend θ et θ' vérifiant $\dfrac{\theta-\theta'}{\pi} \in \mathbb{R}-\mathbb{Q}$ alors $S(\theta)$ et $S(\theta')$ sont d'ordre deux mais leur produit est d'ordre infini.
2. Tout d'abord, ab admet un ordre et $l := \omega(ab)|mn$ car $(ab)^m n = (a^m)^n(b^n)^m = e$.
   Remarquons maintenant que $(ab)^l = e$ et donc $(ab)^{lm} = e = (a^m)^l b^{lm} = b^{lm}$ d'où $n|ml$ et donc, par Gauß vu que $m\wedge n = 1$, $n|l$.
   De même, on peut montrer similairement que $m|l$ et que donc, vu que $v\wedge n = 1$, $mn|l$.
   Conclusions : $l = \omega(ab) = mn$
3. Prenons p un nombre premier, il a une valuation (eventuellement nulle) dans m et n. Si sa valuation dans m est plus grande que dans n on le supprime de la décomposition de n sinon on le supprime dans celui de m. Dans tous les cas, après un nombre fini d'étapes (plus exactement après avoir traité tous les premiers dans la décomposition de mn) on se retrouve avec m' et n' tel que $1 \geq m'|m$ et $1 \leq n'|n$ et $m'\wedge n' = 1$ et $m'n' = m\vee n$.
   On finit en utilisant la question précédente à $a^{\frac{m}{m'}}$, d'ordre m', et $b^{\frac{n}{n'}}$, d'ordre n'.
4. Posons $S := \{\omega(x)\ x\in G\}$. Puis, vu que S est fini non vide, $s := \bigvee_{m\in S} m$. On a forcement que $s\in S$ car S est fini et stable par prise de ppcm finie et donc on dispose de $x\in G$ tel que $\omega(x) = s$ qui répond au problème.

Correction de l'exercice V.3. :

Quoique on peut faire sans, on sait qu'on dispose de $\phi : \mathbb{Z}/n\mathbb{Z} \simeq G$ avec $\phi(1) = a$.
On peut soit faire l'exercice à la main grâce à la division euclidienne, soit juste remarquer que $n\mathbb{Z} = \pi^{-1}(\{0\}) \leq \pi^{-1}(H') \leq \mathbb{Z}$ où $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique.
Ainsi, $\pi^{-1}(H') = (kZ)$ pour un certain $1 \leq k | n$.
En effet, l'écriture $\pi^{-1}(H') = (kZ)$ pour un certain $k \geq 1$ vient du fait que c'est un sous-groupe de $\mathbb{Z}$ et le fait que $k|n$ vient du fait qu'il contient $n\mathbb{Z}$

Ainsi, $G \underset{\pi \text{ surjective}}{=} \pi(k\mathbb{Z}) = k\mathbb{Z}/n\mathbb{Z} = \{\overline{k \times 0}, \dots, \overline{k \times \left(\frac{n}{k} - 1\right)}\}$ et son cardinal est exactement $\frac{n}{k} = d$ (les elements précédents sont distincts).
Ainsi, on conclue que $H' = k\mathbb{Z}/n\mathbb{Z}$ où $m = \frac{n}{d}$ et donc $H = \langle a^{\frac{n}{d}} \rangle$

Correction de l'exercice V.4. :

$G = \langle a^k \rangle \iff \omega(a) = n \iff k \wedge n = 1$

$$n = |[\![1; n]\!]| = \left| \bigsqcup_{d|n \ d\geq 1} \{k \in [\![1; n]\!] \ k \wedge n = d\} \right| = \sum_{d|n \ d\geq 1} |\{k \in [\![1; n]\!] \ k \wedge n = d\}| = \sum_{d|n \ d\geq 1} |\{k \in d \times [\![1; \frac{n}{d}]\!] \ \frac{k}{d} \wedge \frac{n}{d} = 1\}|$$

$$= \sum_{d|n \ d\geq 1} |\{k \in [\![1; \frac{n}{d}]\!] \ k \wedge \frac{n}{d} = 1\}| = \sum_{d|n \ d\geq 1} \varphi\left(\frac{n}{d}\right) = \sum_{d|n \ d\geq 1} \varphi(d)$$

Dans la dernière égalité, on a utilisé que $k \mapsto \frac{n}{k}$ constitue une bijection de $\{k \ k|n \ k \geq 1\}$ dans lui même.

Correction de l'exercice V.5. :

1. Notons $n := |G_1|$ et $m := |G_2|$ et a, b des générateurs de G_1 et G_2 respectivement.
   - Cas 1 : $n \wedge m = 1$: Posons $z = (a, b) = (a, 0) + (0, b)$. D'après *IV.3.* $\omega(z) = ab$ et donc, vu que $|G_1 \times G_2| = ab$, alors $G_1 \times G_2 = \langle z \rangle$ et ce dernier est cyclique
   - Cas 2 : $n \wedge m \neq 1$: Posons alors $l = a \vee b$. Il est clair que $\forall z \in G_1 \times G_2 \ z^l = (e, e)$ et donc $G_1 \times G_2$ ne peut pas être cyclique
2. On peut vérifier que φ est bien définie de plusieurs manières. En voici 3 par exemple : soit vérifier à la main que la définition est indépendante du représentant, soit remarquer $ab\mathbb{Z} \ker \phi$ où ϕ est l'application définie cette fois de $\mathbb{Z}$, soit simplement remarquer que $ab\mathbb{Z} \subset a\mathbb{Z}$ et $ab\mathbb{Z} \subset b\mathbb{Z}$.
   $\implies$: $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est en particulier cyclique et donc, par ce qui précède, $a \wedge b = 1$
   : la preuve ci haut nous donne que $(1, 1)$ est d'ordre ab ($\overline{1}$ génère $\mathbb{Z}/a\mathbb{Z}$ et $\overline{1}$ génère $\mathbb{Z}/b\mathbb{Z}$ et $a \wedge b = 1$) et donc φ est surjective. Par cardinalité ($|\mathbb{Z}/ab\mathbb{Z}| = |\mathbb{Z}/a\mathbb{Z}| \cdot |\mathbb{Z}/b\mathbb{Z}| = ab$) φ est aussi injective.
   Remarquer aussi que cette utilisation du cardinal n'était pas vraiment nécéssaire. En effet, on avait $G_1 \times G_2 = \langle z \rangle$ et $\omega(z) = ab$ d'où $\varphi(k) = z^k$ constitue un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et G (proposition *V.2.*).

Correction de l'exercice V.6. :

1. Pour l'existence, faire une récurrence forte sur le degré de P en remarquant que 1 est inversible et que donc, si $P = \sum_0^n a_k X^k$ avec $a_n \neq 0$, alors soit $deg(P) < deg(Q)$, soit $deg(P - a_n Q) < deg(P)$
   Pour l'unicité, si $P = QR_1 + S_1 = QR_2 + S_2$ où $deg(S_1), deg(S_2) < deg(Q)$, alors $Q(R_1 - R_2) = S_1 - S_2$ imposerait que $deg(Q(R_1 - R_2)) < deg(Q)$ (le degré se comporte bien lorsque le coefficient dominant d'un des polynomes est inversible ou même, plus généralement, n'est pas un diviseur de zero. Developper la formule du produit pour le voir) imposerait, vu que 1 est inversible, que $Q(R_1 - R_2) = 0 = S_1 - S_2$. Ceci impose alors, toujours parce que 1 est inversible (ou plutot, la même raison qu'avant), que $R_1 - R_2 = S_1 - S_2 = 0$.
2. C'est exactement la même demonstration que pour un corps donc on ne la refera pas ici. Remarquer

aussi qu'on peut même passer par le corps de fraction $Frac(A)$ et là c'est du cours vu que ce dernier est un corps.

3. G étant commutatif et fini, on dispose alors de $g \in G$ tel que $\forall x \in G\ \omega(x)|n := \omega(g)$ (IV.3.) et donc $\forall x \in G\ x^n = e$. Notons $H = \langle g \rangle$. On a , $H \subset G$ et $|H| = n$ d'où $|G| \geq n$.
Réciproquement, $X^n - 1$ admet au plus n racines distinctes par ce qui précède et donc $|G| \leq n$.
On conclue donc que $|G| = n$ et $G = H = \langle g \rangle$ est cyclique.

Correction de l'exercice VI.2. :

On a $\forall x \in G\ p.x = 0$ et donc on peut voir G comme $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel.
En particulier, comme espace vectoriel (et donc a fortioti comme groupe abélien) $G \simeq (\mathbb{Z}/p\mathbb{Z})^n$ où $n := dim_{\mathbb{Z}/p\mathbb{Z}}(G)$.

Correction de l'exercice VI.3. :

$(i) \Longrightarrow (ii)$: Soit $x \in G - \{e\}$. Alors $\langle x \rangle = G$ et donc G est cyclique d'ordre $\omega(x) \geq 2$. Si $\omega(x)$ n'est pas premier alors, en prenant $2 \leq d|n$ un diviseur strict de n, on a que $\langle x^d \rangle$ est un sous-groupe strict car de cardinal $2 \leq \dfrac{n}{d} \leq n - 1$. Ainsi, $\omega(x) = p$ et donc G est cyclique de cardinal premier p d'où $G \simeq \mathbb{Z}/p\mathbb{Z}$
$(ii) \Longrightarrow (iii)$: Soit $g \in G - \{e\}$, alors $\langle g \rangle$ est un sous-groupe de cardinal different de 1 et divisant le premier p par Lagrange. Ainsi, $|\langle g \rangle| = p$ et $\langle g \rangle = G$.
$(iii) \Longrightarrow (iv)$: G est monogène. Ainsi il est soit infini isomorphe à $\mathbb{Z}$, chose impossible vu que $2 \neq 0$ n'engendre pas $\mathbb{Z}$ entier, soit cyclique fini de cardinal n et donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Or, si n n'est pas premier, alors tout diviseur strict $2 \leq d|n$ engendre un groupe strict de G. Ainsi, n est premier.
$(iv) \Longrightarrow (i)$: La question est équivalente à ce que tout element non nul engendre G tout entier.
Prenons alors $x \in G - \{e\}$. Exactement comme avant, $H = \langle x \rangle$ est de cardinal un diviseur du premier p autre que 1 et donc $|H| = p$ et $H = G$ d'où le résultat

Correction de l'exercice VI.4. :

Correction de l'exercice VII.1. :

Si G admet un element d'ordre pq alors on finit grace au lemme chinois.
Sinon, par Lagrange (abélien), tout element non nul est d'ordre p ou q.
Si on a un element d'ordre p et un autre d'ordre q alors leur produit est d'ordre pq par $IV.3$. (G abélien et $p \wedge q = 1$). Ainsi, sans perte de généralité, tout élement non nul est d'ordre p et donc tout élément est d'ordre un diviseur de p.
On conclue en utilisant l'exercice $VI.2$. et en trouvant l'absurdité dans l'imposibilité de l'égalité $|G| = p^n = pq$ vu que q est un nombre premier distinct de p.

Correction de l'exercice VII.2. :

$[G : H] = 2$ d'où les classes à gauche sont $\{H, aH\}$ pour un certain $a \in G - H$.
Remarquons au passage que n'importe quel $a \in G - H$ convient vu qu'il donnerait une classe aH differente de H et qu'il en existe que 2.
Aussi, vu qu'il y a que deux classes, on a alors que $aH = G - H$ et donc les classes à gauche sont $\{H, G - H\}$
Par un raisonnement similaire, les classes à droite sont aussi $\{H, G - H\}$ et donc H est distingué.
Considérons maintenant $\pi : G \longrightarrow G/H$ la surjection canonique.
Alors $\forall x \in G\ \pi(x^2) = \pi(x)^2 = e_{G/H}$ (par Lagrange) i.e. $\forall x \in G\ x^2 \in H$. Remarquons que cette seconde démonstration (les carrés) marche pour tout $[G : H]$ (quand $H \trianglelefteq G$) et pas seulement 2.

Correction de l'exercice VII.6. :

Pour la déduction sur les puissances p-emes, voir $VII.2$.
On démonstera ce résultats par deux méthodes :

1. (HP) : Considérons $N \leq H$ le coeur du sous-groupe H. Alors $N \trianglelefteq G$ et, vu que $[G : H] = p$, vérifie que $[G : N]|p!$.
Or, $[G : N]||G|$ par Lagrange et donc, vu que p est le plus petit nombre premier divisant l'ordre de G, on a alors que $[G : N] = 1$ ou $[G : N] = p$.

Le premier cas est exclu car implique que $G = N$ ce qui en claire contradiction avec $N \subset H \subsetneq G$ le 2eme cas implique alors, vu que $N \leq H$, que $H = N$ et donc H est normal

2. Action de groupes : Considérons l'action de H sur G/H définie par $h \cdot aH = haH$. Notre but est de montrer que cette action agit trivialement i.e. $\forall (h, a) \in H \times G \; h \cdot aH = aH$. Supposons que ce n'est pas le cas, prenons alors a tel que l'action sur aH n'est pas triviale. En particulier, $|O(aH)| \neq 1$. Or, $|O(aH)|||H|||G|$ et donc, vu que p est le plus petit premier disant l'ordre de G, on a $|O(aH)| \geq p$. Remarquons maintenant que $O(H) = \{H\}$ (et donc en particulier est une orbite distincte de celle de aH) et donc la formule des classes nous donne que $|G/H| = p \geq |O(H)| + |O(aH)| \geq 1 + p$ ce qui est absurde.
Ainsi, l'action est triviale et on a donc que $\forall h \in H \; \forall a \in G \; h.aH = aH$ i.e. $\forall h \in H \; \forall a \in G \; (a^{-1}ha)H = H$ et donc $\forall h \in H \; \forall a \in G \; a^{-1}ha \in H$ et donc H est normal.

Correction de l'exercice VII.8. :

1. Prenons $x \in G$ tel que $\omega(\pi(x)) = p$. Alors (x est d'ordre fini et) $p = \omega(\pi(x))|\omega(x)$. On a alos que $\frac{\omega(x)}{p} \cdot x \in G$ est d'ordre p.
2. Par récurrence forte sur l'ordre de G : Prenons $x \in G - \{e\}$. Si $p|\omega(x)$ alors $\frac{\omega(x)}{p} \cdot x$ convient. Sinon considérons $H := \langle x \rangle \neq \{e\}$.
On a alors que $p||G/H| = \dfrac{|G|}{|H|}$ vu que p est premier, $p||G|$ et $p \nmid |H|$. Ainsi, par récurrence forte ($|G/H| < |G|$), G/H possède un élément d'ordre p et on conclue grace à la question 1
3. Par récurrence forte sur a. Pour $a = 1$ on l'a déja démontré.
Posons $m := v_p(|G|)$ et supposons le résultat pour $1 \leq a - 1 \leq m - 1$ et prenons $H \leq G$ tel que $|H| = p^{a-1}$. Alors $p||G/H|$ et donc on peut prendre un sous groupe $M \leq G/H$ d'ordre p.
Finalement, $L := \pi^{-1}(M)$ convient. En effet, $|L| = |M \cap Im(\pi)| \cdot |Ker(\pi)| \underset{\pi \text{ surjectif}}{=} |M| \cdot |H| = p \cdot p^{a-1} = p^a$.
4. La réponse est une conséquence directe de la question 3 et de l'exercice *IV.*3.

Correction de l'exercice VIII.2. :

1. L'unicité, si existence, est claire vu que I engendre $Lib(I)$
Pour l'existence, définissons $f(a_1^{\delta_1} \dots a_n^{\delta_n}) = g_1^{\delta_1} \dots g_n^n$ où les $\delta_i \in \{-1, 1\}$. Il n'est pas compliqué de vérifier que f ainsi est bien défini et que c'est un morphisme de groupe.
2. Réciproquement, prenons un tel G. Par la propriété universelle (le point démontré ci-haut) on dispose d'un unique $f \in Hom(Lib(S), G)$ tel que $\forall i \in I \; f(i) = g_i$.
Définissons de même, toujours par la propriété universelle, l'unique $h \in Hom(G, Lib(S))$ tel que $\forall i \in I \; h(g_i) = i$.
Ainsi, $f \circ h \in Hom(G, G)$ vérifie $\forall i \in I \; f \circ h(g_i) = g_i$. Par unicité d'un tel morphisme (prop univ) et le fait que Id_G vérifie ceci, on obtient que $f \circ h = \mathrm{Id}$
De la même manière on vérifie que $h \circ f = \mathrm{Id}_{Lib(I)}$ et donc les deux groupes sont isomorphes.
En théorie des catégories, beaucoup de notions sont définies par des propriétés universelles. Les preuves d'unicité à isomorphisme près pour les propriétés universelles se ressemblent en général : on prend deux éléments A et B vérifiant nos propriétés. On applique la propriété universelle de A à B (de manière convenable) puis l'inverse puis on étudie les composition pour en déduire que ce sont des isomorphismes (pour le lecteur intéréssé, on peut formaliser ceci par le fait que les fleches universelles constitue des objects initiaux/terminaux dans une certaine catégorie, appelée Comma category)
3. Soit G un groupe. Définissons $f \in Hom(Lib(G), G)$ par $\forall g \in G \; f(g) = g$.
Par définition G est surjective et, par le 1er théorème d'isomorphisme, on a $G \simeq Lib(G)/Ker(f)$
4. Posons $\phi : U(G)^S \longrightarrow Hom(F(S), G)$ par $\phi(f)$ l'unique morphisme qui vérifie $\forall s \in S \; \phi(f)(s) = f(s)$.

Inversement, définissons $\psi : Hom(F(S), G) \longrightarrow U(G)^S$ par $\psi(f) = f\Big|_S$.
Il est aisé de vérifier que ψ et ϕ sont inverses l'un de l'autre
Toujours pour le lecteur curieux : ce genre de relation est ce qu'on appelle adjonction en théorie des catégories.

Correction de l'exercice VIII.4. :

L'unicité de f, si existence, est conséquence du fait que $G_1 * G_2$ est engendré par $G_1 \bigcup G_2$.
Pour l'existence, posons $f(g_{1,1}g_{1,2}\dots g_{n,1}g_{n,2}) = f_1(g_{1,1})f_2(g_{1,2})\dots f_1(g_{n,1})f_2(g_{n,2})$.
Il n'est pas compliqué de vérifier que f ainsi est bien définie. Soit le faire à la main soit passer par le groupe libre sur $G_1 \coprod G_2$ puis remarquer que le noyau de cette nouvelle application contient le groupe N qui identifie les produits dans G_i et que donc l'application passe au quotient $Lib(G_1 \coprod G_2)/\langle N\rangle_{norm} = G_1 * G_2$
Voir la recette donnée en $VIII.2.$ pour l'isomorphisme

Correction de l'exercice VIII.6. :

Remarquer que π est surjective et donc $\overline{f}$ est unique si elle existe.
Pour l'existence, on peut soit le définir à la main et montrer que c'est bien défini comme on a fait à maintes reprises ci-haut, ou opter pour le quotient.
Présentons cette deuxième methode alors :
H est abélien et donc $\forall x, y \in G\ f(xyx^{-1}y^{-1}) = f(x)f(x)^{-1}f(y)f(y)^{-1} = e_H$. Ainsi $\forall x, y \in G\ xyx^{-1}y^{-1} \in Ker(f)$. En particulier, $N := \langle xyx^{-1}y^{-1},\ x, y \in G\rangle \leq Ker(f)$. De plus, N étant clairement distingué, on a alors l'existence de $\overline{f} : G/N = Ab(G) \longrightarrow H$ qui vérifie la propriété voulue.
Voir la recette donnée en $VIII.2.$ pour l'isomorphisme

* *
*

Document compilé par Issam Tauil le 23/05/2022 pour cpge-paradise.com. Ceci est une version incomplète du cours, elle risque donc de contenir des imprécisions et/ou des erreurs.