TD1 : Généralités sur les groupes

Exercice 1.

1. Soit E un ensemble. Décrire le quotient de E par la relation d'égalité, puis le quotient de E par la relation $R = E \times E$.
2. Soit E un ensemble, R une relation sur E, et P la conjonction d'une ou plusieurs des propriétés suivantes : "réflexive", "symétrique", "transitive". Démontrer qu'il existe une plus petite relation sur E contenant R et vérifiant P. En particulier, il existe une plus petite relation d'équivalence contenant R : c'est la *relation d'équivalence engendrée* par R.
3. Soit E un ensemble et $\leq$ une relation d'ordre totale sur E. Identifier le quotient de E par la relation $\leq$.
4. Sur l'ensemble $\mathbb{Z}$ des entiers relatifs, on définit une relation R comme suit : xRy si et seulement s'il existe un nombre premier p tel que $y = px$. Identifier la plus petite relation réflexive et transitive sur $\mathbb{Z}$ contenant R, ainsi que la relation d'équivalence sur $\mathbb{Z}$ engendrée par R. Décrire le quotient de $\mathbb{Z}$ par la relation R.

Solution

1. Les classes d'équivalence pour la relation $=$ sont les singletons $\{x\}$ avec $x \in E$. L'ensemble $E/=$ est donc $\{\{x\}|x \in E\}$, qui mis en bijection avec E par l'application $x \mapsto \{x\}$. Pour la relation $R = E \times E$, il n'y a qu'une seule classe d'équivalence, de sorte que E/R est un singleton.
2. Soit F l'ensemble des relations sur E contenant R et vérifiant P ; on a $F \neq \emptyset$ puisque $E \times E \in F$. Soit R' l'intersection des éléments de F. C'est une relation sur E contenant R, et on vérifie que R' satisfait P. On conclut en remarquant que R' est contenue dans toute autre relation sur E contenant R et vérifiant P.
3. Pour tous $x, y \in E$, on a ou bien $x \leq y$, ou bien $y \leq x$. Dans tous les cas, x et y ont la même image dans $E/\leq$, de sorte que $E/\leq$ est un singleton.
4. Soit $s : \mathbb{Z} \to \{-1, 0, 1\}$ l'application qui envoie 0 sur 0, et tout entier relatif non nul sur son signe, et soit $R' = \{(x, y) \in \mathbb{Z}^2 | s(x) = s(y), \text{ et } x|y\}$. La relation R' est réflexive, transitive, et contient R. Si R'' est un autre relation réflexive, transitive, contenant R, alors pour tout $(x, y) \in R'$, ou bien $x = y = 0$, au quel cas $(x, y) \in R''$, ou bien x et y sont non nuls, auquel cas y/x est un entier strictement positif, que l'on peut alors écrire
$$\frac{y}{x} = \prod_{0 \leq i < N} p_i,$$
avec $N \geq 0$, et les $(p_i)_i$ sont des nombres premiers. Si on pose $x_j = x \prod_{0 \leq i < j} p_i$, alors on a $x_0 = x, x_N = y$ et $x_j R'' x_{j+1}$ pour tout $j < N$ (car $x_{j+1} = p_j x_j$). Puisque R'' est réflexive et transitive, on a $xR''y$. On en déduit que R' est la plus petite relation réflexive et transitive sur $\mathbb{Z}$ contenant R.
Soit $\sim_R = \{(x, y) \in \mathbb{Z}^2 | s(x) = s(y)\}$. La relation $\sim_R$ est une relation d'équivalence contenant R et R'. Si R'' est un autre relation d'équivalence contenant R (et contenant donc R'), alors pour tout $(x, y) \in \sim_R$, on a que $(x, x|y|) \in R'$ et $(y, x|y|) \in R'$, et donc que $(x, y) \in R''$. On en déduit que R' est la plus petite relation d'équivalence et transitive sur $\mathbb{Z}$ contenant R.

Exercice 2.

Soit E un ensemble muni d'une loi de composition, associative, avec élément neutre e, et telle que tout élément de E possède un inverse à gauche. Démontrer que tout élément de E possède un inverse à droite qui coïncide avec son inverse à gauche. En déduire que E est un groupe.

Solution
Soit $g \in E$. Par hypothèse, il existe $h \in E$ tel que $h \cdot g = e$.
De même, il existe $k \in E$ tel que $k \cdot h = e$. L'associativité assure alors que $g = (k \cdot h) \cdot g = k \cdot (h \cdot g) = k$, donc $g \cdot h = e$, donc h est aussi inverse à droite de g.
Par conséquent, tout élément de E admet un inverse (à droite et à gauche), donc E est un groupe.

Exercice 3.

Soit G un groupe tel que $g^2 = e$ pour tout $g \in G$. Démontrer que G est abélien.

Solution
Pour tous $g, h \in G$, on a $(g \cdot h)^2 = e$, i.e. $g \cdot h \cdot g \cdot h = e$, donc en multipliant à droite par $h \cdot g$, on a $g \cdot h = h \cdot g$, i.e. G est commutatif.

Exercice 4.

Soit G un groupe et soit H un sous-ensemble fini non vide de G stable pour la loi de composition du groupe G.

1. Démontrer que H est un sous-groupe de G.
2. Trouver un exemple d'un groupe G et d'un sous-ensemble non vide de G stable pour la loi de composition du groupe G qui ne soit pas un sous-groupe de G.

Solution

1. Soit $h \in H$. Comme H est fini et $h^n \in H$ pour tout $n \in \mathbb{N}$, il existe deux entiers $n > m \geq 0$ tels que $h^n = h^m$. Or h admet un inverse dans G, donc on en déduit l'égalité suivante de G : $h^{n-m} = e$. Or H est stable par multiplication, donc $e \in H$ et $h^{-1} = h^{n-m-1} \in H$, donc H est stable par inverse. Cela assure que H est un sous-groupe de G.
2. On peut prendre $G = (\mathbb{Z}, +)$ et $H = \mathbb{N}$.

Exercice 5.

Démontrer qu'il n'existe pas de morphisme de groupes surjectif de $(\mathbf{Q}, +)$ dans $(\mathbf{Q}_+^*, \times)$.

Solution

Soit $\phi : (\mathbf{Q}, +) \to (\mathbf{Q}_+^*, \times)$ un morphisme surjectif. Alors $2 \in \mathbf{Q}_+^*$ admet un antécédent x par φ. Alors $y := \frac{x}{2} \in \mathbf{Q}$ vérifie que $2y = x$, donc $\varphi(y)^2 = \varphi(x) = 2$. Par conséquent, on a construit un rationnel $\varphi(y) \in \mathbf{Q}_+^*$ tel que $\varphi(y)^2 = 2$, ce qui contredit l'irrationnalité de $\sqrt{2}$.

Exercice 6.

Donner la liste de tous les groupes (à isomorphisme près) de cardinal inférieur ou égal à 7.

Solution

- le seul groupe de cardinal 1 est le groupe trivial.
- si p est un nombre premier et si G est de cardinal p, alors tout élément $g \in G$ distinct de l'élément neutre est d'ordre p, ce qui assure que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Il y a donc un unique groupe de cardinal p (qui est $\mathbb{Z}/p\mathbb{Z}$) pour $p = 2, 3, 5, 7$.
- Soit G un groupe d'ordre 4. Si G admet un élément d'ordre 4, G est isomorphe à $Z/4\mathbb{Z}$. Sinon, tous ses éléments sont d'ordre 1 ou 2. Donc G est abélien, et le choix de deux éléments distincts (non neutres) g et h de G fournit un isomorphisme entre G et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il y a donc exactement deux groupes d'ordre 4.
- Soit G un groupe d'ordre 6. Si G est commutatif, G admet nécessairement un élément d'ordre 2 et un élément d'ordre 3 (sinon tous les éléments de G sont d'ordre divisant 2, auquel cas G contient $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ce qui n'est pas possible, ou tous les éléléments de G sont d'ordre divisant 3, auquel cas G contient $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, ce qui n'est pas possible non plus). Alors le produit de ces deux éléments est d'ordre 6, ce qui assure que G est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.
  Si G n'est pas commutatif : alors G contient un élément d'ordre 3, noté a, et aussi un élément b d'ordre 2 (sinon on montre que G aurait au moins 7 éléments). Nécessairement, a et b ne commutent pas, et ils engendrent G. Les éléments de G sont donc $e, a, a^2, b, a \cdot b, b \cdot a$. Donc néssairement on a $a^2 \cdot b = b \cdot a$ et $b \cdot a^2 = a \cdot b$, ce qui détermine complétement la table de multiplication de G. Il y a donc au plus un groupe non commutatif d'ordre 6. Or $\mathfrak{S}_3$ en est un, donc c'est le seul.
  Il y a donc exactement deux groupes d'ordre 6 : $\mathbb{Z}/6\mathbb{Z}$ et $\mathfrak{S}_3$.

Exercice 7.

On dit qu'un groupe G est d'exposant e si e est le plus petit entier $n \geq 1$ tel que pour tout $g \in G$, on a $g^n = 1$. Pour quels entiers e un groupe d'exposant e est-il nécessairement commutatif ?

Solution

On a déjà vu que $e = 2$ convenait. Et $e = 1$ aussi évidemment. Montrons que ce sont les entiers convenables. Supposons que e soit divisible par 4. Alors le groupe $G = \mathbb{Z}/e\mathbb{Z} \times H$, où H est le groupe des quaternions d'ordre 8, est d'exposant e et n'est pas commutatif (car H ne l'est pas).

Supposons $e \geq 3$ non divisible par 4. Alors e admet un facteur premier impair p. On considère alors le groupe $G = \mathbb{Z}/e\mathbb{Z} \times U(p)$, où $U(p)$ est le sous-groupe de $\mathrm{GL}_p(\mathbb{F}_p)$ formés des matrices triangulaires supérieures avec des 1 sur la diagonale. On voit facilement que G est d'exposant e et n'est pas commutatif, car $U(p)$ n'est pas commutatif.

Exercice 8.

1. Démontrer que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.
2. Démontrer que les sous-groupes non denses de $\mathbb{R}$ sont les $a\mathbb{Z}$, avec $a \in \mathbb{R}$.

Solution

1. Soit G un sous-groupe de $\mathbb{Z}$ non réduit à $\{0\}$. Alors $G \cap \mathbb{N}^*$ admet un plus petit élément noté n. Soit alors $x \in G$. Écrivons la divisions euclidienne de x par n : il existe $q, r \in \mathbb{N}$ tel que $x = nq + r$, avec $0 \leq r < n$. Comme $x, n \in G$ et $r = x - nq$, on a $r \in G \cap \mathbb{N}$ et $r < n$. Donc la minimalité de n assure que $r = 0$, donc $x = nq \in n\mathbb{Z}$. Cela prouve que $G = n\mathbb{Z}$.
2. Soit G un sous-groupe de $\mathbb{R}$ distinct de $\{0\}$ et non dense. Montrons que 0 est un point isolé de G : supposons par l'absurde que tout intervalle ouvert contenant 0 contienne un élément non nul de G. Soit $x \in G$ et I un intervalle ouvert contenant x. Alors $I - x$ est un intervalle ouvert contenant 0. Donc par hypothèse, il existe $y \neq 0 \in G \cap (I - x)$. Alors $y + x \in G \cap I$ et $y + x \neq x$. Donc G est dense dans $\mathbb{R}$, ce qui est exclu. Donc 0 est un point isolé de G. Notons alors $a := \inf G \cap \mathbb{R}_+^*$. On sait donc que $a > 0$. Montrons que $a \in G$. Par définition, il existe une suite (x_n) dans $G \cap \mathbb{R}_+^*$ convergeant vers a. Comme 0 est un point isolé de G, la suite $(x_{n+1} - x_n)$ (à valeurs dans G et convergeant vers 0) est stationnaire à 0, donc la suite (x_n) est stationnaire, donc $a \in G$.
   Soit alors $x \in G \cap \mathbb{R}_+^*$. En considérant la partie entière n de $\frac{x}{a}$, on voit que $na \leq x < (n+1)a$. Alors $0 \leq x - na < a$ et $x - na \in G$, donc la minimalité de a assure que $x - na = 0$, donc $x = na$.
   Cela assure que $G = a\mathbb{Z}$.

Exercice 9.

Soit G un groupe et soit H un sous-groupe de G d'indice 2. Démontrer que H est distingué dans G.

Solution
Les classes à gauche de G modulo H sont $\{H, G \setminus H\}$. Donc les classes à droite de G modulo H sont $\{H, G \setminus H\}$. Si $g \notin H$, on a donc $g \cdot H = G \setminus H = H \cdot g$, ce qui assure le résultat.

Exercice 10.

Soit S un sous-ensemble non vide d'un groupe fini G. Soient $N(S) := \{g \in G \mid gSg^{-1} = S\}$ et $C(S) := \{g \in G \mid \forall s \in S\,, gsg^{-1} = s\}$ le normalisateur et le centralisateur de S dans G. Montrer que :

1. $N(S) < G$ et $C(S) \lhd N(S)$.
2. $N(S) = G$ si et seulement si $S = \bigcup_{g \in G} gSg^{-1}$.
3. Si $H \lhd G$, alors $C(H) \lhd G$.
4. Si $H < G$, alors $N(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.

Solution

1. On a $e \in N(S)$. Soient $g, h \in N(S)$. Alors on a $(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S$, donc $gh \in N(S)$. Si $g \in N(S)$, on a $gSg^{-1} = S$, donc en multipliant à gauche et à droite par g^{-1} et g respectivement, on a $S = g^{-1}Sg$, donc $g^{-1} \in N(S)$. Donc $N(S)$ est un sous-groupe de G. De même, il est clair que $C(S)$ est un sous-groupe de G contenu dans $N(S)$. Montrons qu'il est distingué dans $N(S)$. Soit $g \in C(S)$ et $h \in N(S)$. Soit $s \in S$. Alors
$$(hgh^{-1})s(hgh^{-1})^{-1} = hg(h^{-1}sh)g^{-1}h^{-1}\,,$$
   et comme $h \in N(S)$, on a $h^{-1}sh \in S$, donc comme $g \in C(S)$, $g(h^{-1}sh)g^{-1} = h^{-1}sh$, donc finalement $(hgh^{-1})s(hgh^{-1})^{-1} = h(h^{-1}sh)h^{-1} = s$, donc $hgh^{-1} \in C(S)$, donc $C(S) \lhd N(S)$.
2. On suppose $N(S) = G$. Alors pour tout $g \in G$, on a $gSg^{-1} = S$, donc $S = \bigcup_{g \in G} gSg^{-1}$. Réciproquement, si on suppose $S = \bigcup_{g \in G} gSg^{-1}$, pour tout $g \in G$, on a donc $g^{-1}Sg \subset S$, donc en multipliant par g et g^{-1} à gauche et à droite respectivement, on a $S \subset gSg^{-1} \subset S$, ce qui assure que $gSg^{-1} = S$, donc $g \in N(S)$, donc $G = N(S)$.
3. On suppose H distingué dans G. Soit $g \in G$ et $c \in C(H)$. Soit enfin $h \in H$. On calcule $(gcg^{-1})h(gcg^{-1})^{-1} = gc(g^{-1}hg)c^{-1}g^{-1}$: puisque H est distingué dans G, on sait que $g^{-1}hg \in H$. Or $c \in C(H)$, donc $c(g^{-1}hg)c^{-1} = g^{-1}hg$, donc finalement $(gcg^{-1})h(gcg^{-1})^{-1} = g(g^{-1}hg)g^{-1} = h$, ce qui assure que $gcg^{-1} \in C(H)$. Donc $C(H)$ est distingué dans G.
4. Par définition et via la question a), il est clair que $N(H)$ est un sous-groupe de G contenant H, et que H est distingué dans $N(H)$. Soit maintenant K un sous-groupe de G contenant H tel que $H \lhd K$. Alors par définition, pour tout $k \in K$, on a $kHk^{-1} = H$, donc $k \in N(H)$, donc $K \subset N(H)$, ce qui assure la maximalité de $N(H)$ parmi les sous-groupes de G concernés.

Exercice 11.

Soit G un groupe et soit $H \lhd G$ un sous-groupe distingué.

1. Décrire les sous-groupes distingués de G/H en fonction de ceux de G.
2. Soit K un sous-groupe de G.
   (a) Si K est distingué dans G et contient H, montrer que l'on a un isomorphisme $(G/H)/(K/H) \cong G/K$.
   (b) Démontrer que HK est un sous-groupe de G égal à KH.

(c) Démontrer que H est distingué dans HK.

(d) Démontrer que l'on a un isomorphisme $K/(K \cap H) \cong (HK)/H$.

Solution

1. On note $\pi : G \to G/H$ la projection canonique. On sait que la correspondance $K \mapsto \pi(K)$ établit une bijection entre l'ensemble des sous-groupes de G contenant H est l'ensemble des sous-groupes de G/H, dont la réciproque est donnée par $\overline{K} \mapsto \pi^{-1}(\overline{K})$. On vérifie immédiatemment que cette bijection induit une bijection entre les sous-groupes distingués de G contenant H et les sous-groupes distingués de G/H.
2. (a) Le morphisme $\pi : G \to G/H$, composé avec la projection $\pi' : G/H \to (G/H)/(K/H)$, induit un morphisme surjectif $q : G \to (G/H)/(K/H)$. Par construction, un élément $g \in G$ est dans $\mathrm{Ker}(q)$ si et seulement si $\pi(g) \in \mathrm{Ker}(\pi') = K/H$ si et seulement si $g \in K$. Donc $\mathrm{Ker}(q) = K$. Le théorème de factorisation assure alors que q induit un isomorphisme $\overline{q} : G/K \xrightarrow{\simeq} (G/H)/(K/H)$.

   (b) Soient $h, h' \in H$ et $k, k' \in K$. Comme H est distingué dans G, il existe $h'' \in H$ tel qu'on ait $k \cdot h' = h'' \cdot k$, donc $(h \cdot k) \cdot (h' \cdot k') = (h \cdot h'') \cdot (k \cdot k') \in HK$, donc HK est un sous-groupe de G.
   Puisque pour tous $h \in H$ et $k \in K$, il existe $h' \in H$ tel que $h \cdot k = k \cdot h'$, on voit que $HK \subset KH$. De même, pour tous $h \in H$ et $k \in K$, il existe $h' \in H$ tel que $k \cdot h = h' \cdot k$, donc $HK = KH$.

   (c) C'est évident.

   (d) L'inclusion $K \to HK$ induit un morphisme $p : K \to (HK)/H$. Montrons que p est surjectif : si $h \in H$ et $k \in K$, on voit que la classe $(h \cdot k)H = kH$ est l'image de k par p, donc p est surjectif. En outre, un élément $k \in K$ est dans $\mathrm{Ker}(p)$ si et seulement si il est dans H, donc $\mathrm{Ker}(p) = K \cap H$. Le théorème de factorisation permet de conclure.

Exercice 12.

Soit G un groupe fini.

1. Démontrer qu'il existe $n \in \mathbb{N}$ tel que G soit (isomorphe à) un sous-groupe de $\mathfrak{S}_n$.
2. Démontrer qu'il existe $n \in \mathbb{N}$ tel que G soit (isomorphe à) un sous-groupe de $\mathfrak{A}_n$.
3. Démontrer qu'il existe $n \in \mathbb{N}$ tel que G soit (isomorphe à) un sous-groupe de $\mathrm{GL}_n(k)$, pour tout corps k.

Solution

1. On considère l'action de G sur lui-même par translation à gauche. Autrement dit, on regarde le morphisme de groupes $\varphi : G \to \mathfrak{S}(G)$ défini par $\varphi(g)(h) := g \cdot h$. Comme G est de cardinal n, on sait que $\mathfrak{S}(G)$ est isomorphe à $\mathfrak{S}_n$. Il suffit donc de montrer que le morphisme φ est injectif. Soit $g \in \mathrm{Ker}(\varphi)$. Alors pour tout $h \in G$, on a $g \cdot h = h$, ce qui assure (en prenant $h = e$ par exemple) que $g = e$. Donc φ st injective.
2. Au vu de la question précédente, il suffit de plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$. Remarquons d'abord que l'on dispose d'un morphisme injectif naturel $\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+2}$ obtenu en prolongeant une bijection de $\{1, \ldots, n\}$ en une bijection de $\{1, \ldots, n+2\}$ par l'identité sur les éléments $n+1$ et $n+2$. On définit alors l'application $\psi : \mathfrak{S}_n \to \mathfrak{A}_{n+2}$ de la façon suivante : si $\sigma \in \mathfrak{A}_n$, on pose $\psi(\sigma) := \iota(\sigma)$, et si $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$, on pose $\psi(\sigma) := \iota(\sigma) \circ (n, n+1)$. On vérifie facilement que ψ est un morphisme de groupes injectif, ce qui conclut la preuve.
3. Au vu de la première question, il suffit de construire un morphisme de groupes injectif de $\mathfrak{S}_n$ dans $\mathrm{GL}_n(k)$. On utilise pour cela les matrices de permutations. On a en effet une application

$$\varphi : \mathfrak{S}_n \to \mathrm{GL}_n(k)$$

   définie par $\varphi(\sigma) := P_\sigma$. Il est classique que φ est un morphisme de groupes, et il est clair que celui-ci est injectif. Cela conclut la preuve.

Exercice 13.

Déterminer les classes de conjugaison dans $\mathfrak{S}_n$. Et dans $\mathfrak{A}_n$?

Solution

Soit $c = (a_1, \ldots, a_k)$ un k-cycle dans $\mathfrak{S}_n$. Il est clair que pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)) .$$

Comme toute permutation se décompose de façon unique en produit de cycles à supports disjoints, on trouve immédiatemment que les classes de conjugaisons dans $\mathfrak{S}_n$ sont paramétrée par les partitions de l'entiers n. On rappelle qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que $m_1 \leq \cdots \leq m_r$ et $\sum m_i = n$. La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

La description des classes de conjugaison dans $\mathfrak{A}_n$ est un peu plus subtile. On remarque d'abord que puisque $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$, la classe de conjugaison dans $\mathfrak{S}_n$ d'un élément de $\mathfrak{A}_n$ est contenue dans $\mathfrak{A}_n$. Comme $\mathfrak{A}_n$ est d'indice 2 dans $\mathfrak{S}_n$, pour tout $\sigma \in \mathfrak{A}_n$, la classe de conjugaison de σ dans $\mathfrak{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathfrak{A}_n$, soit réunion de deux classes de conjugaison dans $\mathfrak{A}_n$ (celle de σ et une autre).
Montrons alors que l'on est dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition.
En effet, si σ admet un cycle c de longueur paire, pour tout $\tau \in \mathfrak{S}_n$, on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ coïncident. Si σ admet deux cycles $c = (a_1, \dots, a_{2k+1})$ et $c' = (a'_1, \dots, a'_{2k+1})$ de même longueur impaire, alors si on note $d := (a_1 a'_1) \dots (a_{2k+1} a'_{2k+1})$ (permutation impaire), on a pour tout $\tau \in \mathfrak{S}_n$, $\tau\sigma\tau^{-1} = (\tau d)\sigma(\tau d)^{-1}$, ce qui assure que les classes de conjugaison dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ coïncident.
Réciproquement, si σ n'a que des cycles de longueurs impaires deux-à-deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ, et on voit facilement que $(ij) \circ \sigma \circ (ij)$ n'est pas conjuguée à σ dans $\mathfrak{A}_n$ alors qu'elle l'est dans $\mathfrak{S}_n$.

Exercice 14.

Démontrer que si $n \geq 2$, $\mathfrak{S}_{n+2}$ a deux sous-groupes non conjugués isomorphes à $\mathfrak{S}_n$.

Solution
On a vu à l'exercice que l'on disposait d'un morphisme injectif canonique $\iota : \mathfrak{S}_n \to \mathfrak{S}_{n+2}$ (prolongement des bijections par l'identité sur les éléments $n+1$ et $n+2$) compatible avec la signature, i.e. tel que pour tout $\sigma \in \mathfrak{S}_n$, on a $\epsilon(\iota(\sigma)) = \epsilon(\sigma)$, et d'un morphisme injectif canonique $\psi : \mathfrak{S}_n \to \mathfrak{A}_{n+2}$. Puisque deux permutations conjuguées ont même signature, et puisqu'il existe dans $\mathfrak{S}_n$ des permutations impaires, on voit donc que les deux sous-groupes $\iota(\mathfrak{S}_n)$ et $\psi(\mathfrak{S}_\mathfrak{n})$ de $\mathfrak{S}_{n+2}$ sont isomorphes à $\mathfrak{S}_n$ et ne sont pas conjugués.

Exercice 15.

Soit $f : G_1 \to G_2$ un morphisme de groupes et soit x un élément de G_1 d'ordre fini. Démontrer que l'ordre de $f(x)$ divise l'ordre de x.

Solution
On note n l'ordre de x. On a $x^n = e$, donc $f(x)^n = f(x^n) = e$, donc l'ordre de $f(x)$ divise n.

Exercice 16.

Soit G un groupe. Vrai ou faux ?

1. Si tout sous-groupe H de G est distingué dans G, alors G est abélien.
2. Si $H \triangleleft G$ et $K \triangleleft H$, alors $K \triangleleft G$.
3. Soient x et $y \in G$ d'ordre fini. Alors xy est nécessairement d'ordre fini.
4. Si G a un nombre fini de sous-groupes, alors G est fini.

Solution

1. Faux. On considère par exemple le groupe H des quaternions, d'ordre 8. Ce groupe est définit de la façon suivante : l'ensemble H est
$$H = \{\pm 1, \pm i, \pm j, \pm k\} ,$$
et la loi de groupe est définie par
$$\begin{aligned}&(-1)^2 = 1 \, , \, i^2 = j^2 = k^2 = -1 \, , \\ &(-1) \cdot i = i \cdot (-1) = -i \, , \, (-1) \cdot j = j \cdot (-1) = -j \, , \, (-1) \cdot k = k \cdot (-1) = -k \, , \\ &i \cdot j = -j \cdot i = k \, .\end{aligned}$$
On voit que les sous-groupes de H sont les suivants :
— le sous-groupe trivial $\{1\}$, qui est distingué.
— le sous-groupes de cardinal 2 engendré par -1, qui est distingué car contenu dans le centre de H.
— les sous-groupes de cardinal 4 sont d'indice 2 dans H, donc distingué.
— le sous-groupe H entier, qui est distingué.
Donc les sous-groupes de H sont tous distingués, alors que H n'est pas commutatif.
2. Faux. On peut prendre $G = \mathfrak{S}_4$ ou $\mathfrak{A}_4$, $H = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $K = \{\mathrm{id}, (12)(34)\} \cong \mathbb{Z}/2\mathbb{Z}$.

3. Faux. Pour avoir un contre-exemple, il faut nécessairement que le groupe G soit infini et non commutatif. On peut prendre par exemple le groupe libre sur deux générateurs a et b d'ordre 2, i.e. l'ensemble des mots finis formés des lettres a et b sans répétition, avec la loi de concaténation des mots (avec simplification éventuelle des mots aa et bb apparaissant). Dans ce groupe, les éléments a et b sont d'ordre 2, alors que leur produit $a \cdot b = ab$ est d'ordre infini.

   Pour un exemple plus concret, on peut prendre $G = \mathrm{GL}_2(\mathbf{Q})$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Alors x est d'ordre 2, y est d'ordre 3 et $x \cdot y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ est d'ordre infini.
4. Vrai. Il est clair que tout élément de G est d'ordre fini : si $g \in G$ est d'ordre infini, alors le sous-groupe engendré par g est isomorphe à $\mathbb{Z}$, et il contient donc une infinité de sous-groupes distincts. Or G a un nombre fini de sous-groupes cycliques, noté $\langle g_1 \rangle, \dots, \langle g_n \rangle$. Donc pour tout $g \in G$, il existe i tel que $\langle g \rangle = \langle g_i \rangle$, donc g est une puissance de g_i, ce qui assure que le cardinal de G est borné par la somme des ordres des g_i, donc G est fini.

Exercice 17.

Soit G un groupe fini.

1. Démontrer que des éléments conjugués dans G sont de même ordre.
2. Deux éléments de même ordre dans G sont-ils toujours conjugués ?
3. Trouver tous les groupes abéliens finis G pour lesquels la question précédente a une réponse positive. Un exemple non abélien ?

Solution

1. Si $g, h \in G$ et $n \in \mathbb{N}$, on a $(h \cdot g \cdot h^{-1})^n = h \cdot g^n \cdot h^{-1}$, donc $(h \cdot g \cdot h^{-1})^n = e$ si et seulement si $g^n = e$, ce qui assure le résultat.
2. Non. Par exemple, dans le groupe commutatif $G = \mathbb{Z}/3\mathbb{Z}$, on a deux éléments d'ordre 3 qui ne sont pas conjugués.
3. Dans un groupe abélien fini, les classes de conjugaison sont réduites à un élément. Donc la question précédente a une réponse positive dans un groupe abélien fini G si et seulement si tous les éléments de G ont des ordres distincts. Or si un groupe admet un élément g d'ordre $n \geq 3$, alors il admet d'autres éléments d'ordre n, par exemple g^{-1}. Donc les seuls groupes abéliens convenables sont le groupe trivial et le groupe $\mathbb{Z}/2\mathbb{Z}$.

   Si $G = \mathfrak{S}_3$, alors les éléments d'ordre 2 dans G sont les transpositions $(12), (13), (23)$ qui sont bien conjuguées, et les éléments d'ordre 3 sont les 3-cycles (123) et (132), qui sont également conjugués. Donc G est un exemple de groupe non abélien convenable.

Exercice 18.

Soit N un entier naturel.

1. Démontrer qu'il n'y a qu'un nombre fini (à isomorphisme près) de groupes de cardinal au plus N.
2. Démontrer qu'il n'y a qu'un nombre fini (à isomorphisme près) de groupes abéliens finis possédant au plus N automorphismes.
3. Démontrer qu'il n'y a qu'un nombre fini (à isomorphisme près) de groupes finis possédant au plus N automorphismes.

Solution

1. Un groupe de cardinal n est déterminé à isomorphisme près par sa table de multiplication, de taille $n \times n$, chacune des cases étant étiquetées par l'un des n éléments de G. Il y a donc au plus n^{n^2} groupes de cardinal n (à isomorphisme près) .
2. Rappelons (cela sera revu en cours) que tout groupe abélien fini est isomorphe à un groupe de la forme

$$\prod_{q \in S} (\mathbb{Z}/q\mathbb{Z})^{d_q},$$

   où S est une partie finie de l'ensemble des puissances de nombres premiers divisant $|G|$, et $d_q \geq 1$ pour chaque $q \in S$. On a donc

$$N \geq |\mathrm{Aut}(G)| \geq |\mathrm{GL}_{d_q}(\mathbb{Z}/q\mathbb{Z})|,$$

   pour chaque $q \in S$. Par ailleurs, si q est la puissance d'un nombre premier p, alors

$$|\mathrm{GL}_d(\mathbb{Z}/q\mathbb{Z})| = q^{d^2} \prod_{r=1}^{d} (1 - p^{-r}) \geq \frac{q^{d^2}}{4}.$$

   On a donc $q^{d_q^2} \leq 4N$ pour chaque $q \in S$, de sorte que $q \leq 4N$ et $d_q^2 \leq \log_2(4N)$. Ceci démontre qu'il n'y a qu'un nombre fini de classes d'isomorphismes parmi les groupes abéliens finis possédant au plus N automorphismes.

3. Soit G un groupe fini de centre Z, et soit $I = G/Z$. On suppose que G admet exactement N automorphismes. Le morphisme

$$\begin{aligned} G &\to \mathrm{Aut}(G) \\ g &\mapsto (x \mapsto gxg^{-1}) \end{aligned}$$

est de noyau exactement Z, de sorte que I est isomorphe à un sous-groupe de $\mathrm{Aut}(G)$. En particulier, le cardinal de I divise N, et lui est donc inférieur ou égal. Soit K le sous-groupe de $\mathrm{Aut}(Z)$ constitué des restrictions à Z des automorphismes de G qui induisent l'identité sur I. On a bien sûr $|K| \leq N$, et on se propose de majorer le cardinal de $\mathrm{Aut}(Z)/K$.

— Soit $\pi : G \to I$ la projection canonique, et soit $\sigma : I \to G$ une application telle que $\pi \circ \sigma = \mathrm{id}_I$. Tout élément de G admet une unique écriture sous la forme $z\sigma(x)$ avec $(z, x) \in Z \times I$, ce que l'on va utiliser pour construire des automorphismes de G. Considérons l'application

$$\begin{aligned} c : I \times I &\to Z \\ (x, y) &\mapsto \sigma(x)\sigma(y)\sigma(xy)^{-1}. \end{aligned}$$

Si $\varphi \in \mathrm{Aut}(G)$ induit l'identité sur I, alors on a

$$(\varphi \circ c)(x, y) = f_\varphi(x) f_\varphi(y) f_\varphi(xy)^{-1} c(x, y),$$

où $f_\varphi : I \to Z$ est donnée par $x \mapsto \varphi(\sigma(x))\sigma(x)^{-1}$. Ainsi, si on note $d : Z^I \to Z^{I \times I}$ le morphisme

$$d : f \mapsto ((x, y) \mapsto f(x)f(y)f(xy)^{-1}),$$

alors on dispose d'une application

$$\begin{aligned} \gamma : \mathrm{Aut}(Z)/K &\to Z^{I \times I}/\mathrm{Im}(d) \\ \varphi &\mapsto \varphi \circ c. \end{aligned}$$

Cette application est injective : en effet, si φ_1 et φ_2 sont des automorphismes de Z tels que

$$\varphi_1 \circ c = d(f)\varphi_2 \circ c,$$

alors on peut définir un automorphisme ψ de G dans lui-même par la formule

$$\forall (z, x) \in Z \times I, \psi(z\sigma(x)) = \varphi_2^{-1}(f(x)\varphi_1(z))\sigma(x).$$

avec $z \in Z$. On a $\varphi_1 = \varphi_2 \circ \psi_{|Z}$, et $\psi_{|Z} \in K$, d'où l'injectivité de γ. En particulier,

$$|\mathrm{Aut}(Z)/K| \leq |Z|^{N^2}.$$

Puisque $|K| \leq N$, on obtient

$$|\mathrm{Aut}(Z)| \leq N|Z|^{N^2}.$$

— On démontre ensuite que si $\varphi \in \mathrm{Aut}(Z)$ vérifie $\varphi(x) = a(x)^N x$ pour un certain morphisme $a : Z \to Z$, alors $\varphi \in K$. Il suffit pour cela de démontrer que $\gamma(\varphi) = c$. C'est bien le cas, puisque alors $\varphi \circ c = d(f)c$, avec

$$f : x \in I \mapsto \left(\prod_{y \in I} a \circ c(x, y) \right)^{\frac{N}{|I|}}.$$

— Comme dans la question précédente, on écrit

$$Z \simeq \prod_{q \in S} (\mathbb{Z}/q\mathbb{Z})^{d_q}.$$

On va démontrer que le nombre de possibilités pour S est borné en fonction de N.
Tout d'abord, si $q = p^r \in S$, soit φ_k l'automorphisme de Z qui agit par élévation à la puissance k sur le facteur $(\mathbb{Z}/q\mathbb{Z})^{d_q}$, et comme l'identité sur les autres facteurs, avec $0 < k < p$. Alors $\varphi_k \in K$ par le point précédent, ce qui produit $p - 1$ éléments distincts de K. En particulier $p - 1 \leq N$.
Ensuite, si $M = N \prod_{p \leq N+1} p$, alors pour tout $h \in [|0, N|]$, l'automorphisme $z \mapsto z^{1+Mh}$ de Z appartient à K par le point précédent, de sorte que le principe des tiroirs assure l'existence d'entiers h, h' avec $0 \leq h < h' \leq N$ tels que $z^{1+Mh} = z^{1+Mh'}$ pour tout $z \in Z$. En particulier, on a $z^{N!M} = 1$ pour tout $z \in Z$. Ainsi, chaque $q \in S$ divise l'entier $R = N!M$.

— Soit $q \in S$ tel que $q^{d_q} \geq |Z|^{|S|^{-1}}$. Puisque $q \leq R$, on a

$$d_q \geq \frac{\log |Z|}{|S| \log R}.$$

Par ailleurs, on a

$$N|Z|^{N^2} \geq |\mathrm{Aut}(Z)| \geq |\mathrm{GL}_{d_q}(\mathbb{Z}/q\mathbb{Z})| \geq \frac{q^{d_q^2}}{4} \geq 2^{d_q^2-2},$$

d'où

$$d_q^2 \leq 2 + \frac{\log(N)}{\log(2)} + N^2 \log |Z|.$$

On en déduit une inégalité de la forme $(\log |Z|)^2 \leq a(N) + b(N) \log |Z|$, ce qui démontre que le cardinal de Z (et donc celui de G) est borné en fonction de N. On conclut ensuite à l'aide de la question 1.

Exercice 19

Soit k un corps fini à q éléments. Démontrer que les cardinaux de $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$ et $\mathrm{PGL}_n(k)$ sont des fonctions polynomiales en q, que l'on explicitera.

Solution

Le cardinal de $\mathrm{GL}_n(k)$ est égal au nombre de bases de k^n, c'est-à-dire de familles $(e_i)_{i=1}^n$ dans k^n, telles que e_i n'appartient pas au k-espace vectoriel engendré par $(e_j)_{j<i}$. Il y a $q^n - 1$ choix pour e_1, puis $q^n - q$ choix pour e_2, etc. On a donc

$$|\mathrm{GL}_n(k)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}).$$

On dispose d'un morphisme surjective $\det : \mathrm{GL}_n(k) \to k^\times$, de noyau $\mathrm{SL}_n(k)$, de sorte que

$$|\mathrm{SL}_n(k)| = \frac{|\mathrm{GL}_n(k)|}{|k^\times|} = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})}{q - 1}.$$

Par ailleurs $\mathrm{PGL}_n(k)$ est le quotient de $GL_n(k)$ par un sous-groupe de cardinal $q-1$, et est donc de même cardinal que $\mathrm{SL}_n(k)$.

Exercice 20

Soit $k = \mathbb{Z}/p\mathbb{Z}$ et soit n un entier naturel.

(a) Déterminer le groupe des automophismes du groupe additif k^n.

(b) Combien y a-t-il de sous-groupes de cardinal p dans k^2 ? Plus généralement, combien y a-t-il de sous-groupes de cardinal p^m (avec $m \leq n$) dans k^n ?

(c) Expliciter une bijection entre la droite projective sur k et l'ensemble des sous-groupes de cardinal p dans k^2, telle que l'action de $\mathrm{Aut}(k^2)$ sur ce dernier ensemble corresponde à une action par homographies sur la droite projective.

Solution

(a) Puisque $k = \mathbb{Z}/p\mathbb{Z}$, tout automorphisme du groupe abélien k^n est k-linéaire. Ainsi, $\mathrm{Aut}(G)$ est isomorphe à $\mathrm{GL}_n(k)$.

(b) Il y a autant de sous-groupes de cardinal p^m dans k^n que de sous-k-espaces vectoriels de k^n de dimension m. Chacun de ces sous-espaces admet exactement $(p^m - 1)(p^m - p) \dots (p^m - p^{m-1})$ bases (cf. exercice 19), et le nombre de familles libres à m éléments dans k^n est $(p^n - 1)(p^n - p) \dots (p^n - p^{m-1})$. Le nombre de ces sous-espaces est donc

$$\frac{(p^n - 1)(p^n - p) \dots (p^n - p^{m-1})}{(p^m - 1)(p^m - p) \dots (p^m - p^{m-1})}.$$

Pour le nombre de droites dans k^2, on obtient $\frac{p^2-1}{p-1} = p + 1$.

(c) Il suffit d'associer à $x \in k$ la droite engendrée par $(x, 1)$, et à ∞ la droite engendrée par $(1, 0)$.

Exercice 21

Soit G un groupe fini de cardinal $n \geq 1$.

(a) Démontrer l'existence d'un système de générateurs $(a_i)_{i=1}^k$ de G tels que pour tout $i \in [|1, k|]$, l'élément a_i n'appartient pas au sous-groupe de G engendré par $(a_j)_{j<i}$.

(b) Démontrer que G possède au plus $n^{\log_2(n)}$ endomorphismes.

Solution

(a) Le groupe G étant fini, il admet une partie génératrice finie. Soit $(a_i)_{i=1}^k$ un famille génératrice de G, de cardinal k, avec k minimal. Si on avait un $i \in [|1,k|]$ tel que a_i appartient au sous-groupe enendré par les $(a_j)_{j<i}$, alors la famille $(a_j)_{j\neq i}$ serait également génératrice, mais de cardinal $< k$, ce qui est impossible.

(b) Soit $(a_i)_{i=1}^k$ comme dans la question précédente. L'application qui à un endomorphisme f de G associe l'élément $(f(a_i))_i$ de G^k est injective, de sorte que G possède au plus n^k endomorphismes.
Il suffit de démontrer que $k \leq \log_2(n)$. On considère pour cela le sous-groupe H_i engendré par $(a_j)_{j<i}$. La suite $(H_i)_i$ est strictement croissante pour l'inclusion, et H_{i-1} est donc d'indice au moins 2 dans H_i. Ainsi, $H_0 = \{1\}$ est d'indice au moins 2^k dans $H_k = G$. En particulier, on a $2^k \leq n$, comme voulu.

Exercice 22

Soit G un groupe tel que le quotient par son centre est monogène. Démontrer que G est abélien.

Solution
On rappelle que le centre $Z(G)$ de G est distingué. On considère le morphisme quotient $\pi : G \to G/Z(G)$. Par hypothèse, $G/Z(G)$ est engendré par un élément $\overline{g_0}$. Comme π est surjective, il existe $g_0 \in G$ tel que $\pi(g_0) = \overline{g_0}$. Soient alors $g, h \in G$. Il existe des entiers $n, m \in \mathbb{Z}$ tels que $\pi(g) = \overline{g_0}^n$ et $\pi(h) = \overline{g_0}^m$. Donc $\pi(g\cdot g_0^{-n}) = \pi(h\cdot g_0^{-m}) = e$, donc $y = g \cdot g_0^{-n}$ et $z = h \cdot g_0^{-m}$ sont dans $Z(G)$.
Alors

$$g \cdot h = y \cdot g_0^n \cdot z \cdot g_0^m = y \cdot z \cdot g_0^{n+m} = z \cdot g_0^m \cdot y \cdot g_0^n = h \cdot g\,,$$

donc G est commutatif.
Exercice 23

Quel est le nombre minimal de transpositions nécessaires pour engendrer le groupe $\mathfrak{S}_n$?

Solution
Montrons que ce nombre vaut $n-1$. Il est clair qu'il existe une famille de $n-1$ transpositions engendrant $\mathfrak{S}_n$ (par exemple les transpositions de la forme $(1i)$, avec $2 \leq i \leq n$).
Montrons que l'on ne peut pas faire mieux. Soit $E \subset \mathfrak{S}_n$ un ensemble de transpositions. On considère le graphe fini Γ dont les sommets sont les entiers $1, 2, \dots, n$, de sorte que deux sommets distincts i et j sont reliés par une arète si et seulement si $(ij) \in E$. Supposons la partie E génératrice. Alors il est clair que le graphe Γ est connexe.
Il suffit donc de montrer, par récurrence sur n, qu'un graphe connexe à n sommets possède au moins $n-1$ arêtes : le cas $n = 2$ est évident. Montrons l'hérédité : soit donc un tel graphe Γ, connexe à $n+1$ sommets. On a l'alternative suivante :
— soit chaque sommet a au moins deux voisins. Alors le nombre total d'arêtes est au moins égal à $\frac{1}{2}(n+1)\cdot 2 = n+1$.
— soit il existe un sommet s ayant un unique voisin. On considère alors le graphe Γ' dont les sommets sont les sommets de Γ autres que s et les arêtes celles de Γ autres que celle contenant s. Alors il est clair que Γ' est un grpahe connexe à n sommets, donc il admet au moins $n-1$ arêtes, donc Γ a au moins n arêtes.
Cela conclut la preuve par récurrence.
Exercice 24

Soit G un groupe de type fini (i.e. engendré par un nombre fini d'éléments).

(a) Un sous-groupe H de G est-il nécessairement de type fini ?

(b) Même question en supposant de plus que le cardinal de G/H est fini.

Solution

(a) Non. Un contre-exemple est donné par le sous-groupe G de $\mathrm{GL}_2(\mathbf{Q})$ engendré par les matrices $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, et le sous-groupe H de G formé des matrices de G avec des 1 sur la diagonale. Supposons que H soit de type fini. Alors il existe un entier $N \geq 1$ tel que H soit contenu dans le sous-groupe de $\mathrm{GL}_2(\mathbf{Q})$ formé des matrices de la forme $\begin{pmatrix} 1 & \frac{a}{N} \\ 0 & 1 \end{pmatrix}$. Or $A^{-N} \cdot B \cdot A^N = \begin{pmatrix} 1 & \frac{1}{2^N} \\ 0 & 1 \end{pmatrix}$ est dans H, ce qui est contradictoire puisque $2^N > N$, donc H n'est pas de type fini, alors que G l'est

(b) On suppose G/H fini. Alors on peut trouver un nombre fini déléments $g_1 = e, \dots, g_n$ de G tels que $G/H = \{g_1H, \dots, g_nH\}$. Puisque G est de type fini, on dispose de $h_1, \dots, h_m \in G$ tels que tout éléments de G est produit des h_i. Alors pour tout i, j, il existe $1 \leq k \leq n$ et $h_{i,j} \in H$ tels que $h_i \cdot g_j = g_k \cdot h_{i,j}$.

Montons alors que les $h_{i,j}$ engendrent H. Soit $h \in H$. On sait qu'il existe des entiers $i_1, \dots, i_r$ tels que $h = h_{i_1} \dots h_{i_r}$. On a donc $h_{i_r} = h_{i_r} \cdot e = h_{i_r} \cdot g_1 = g_{k_r} \cdot h_{i_r,1}$, donc finalement

$$h = h_{i_1} \cdot \dots \cdot h_{i_{r-1}} \cdot g_{k_r} \cdot h_{i_r,1} \,.$$

De même, $h_{i_{r-1}} \cdot g_{k_r} = g_{k_{r-1}} \cdot h_{i_{r-1},k_r}$, donc

$$h = h_{i_1} \cdot \dots \cdot h_{i_{r-2}} \cdot g_{k_{r-1}} \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,.$$

Donc par récurrence, on trouve

$$h = g_{k_1} \cdot h_{i_1,k_2} \cdot \dots \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,.$$

Enfin, h et les $h_{i,j}$ sont dans H, donc $g_{k_1} \in H$, donc $k_1 = 1$ et donc

$$h = h_{i_1,k_2} \cdot \dots \cdot h_{i_{r-1},k_r} \cdot h_{i_r,1} \,,$$

ce qui conclut la preuve.

Exercice 25

Démontrer que tout sous-groupe d'indice n dans $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$. On admettra que pour $n \geq 5$ les sous-groupes distingués de $\mathfrak{S}_n$ sont $\{1\}$, $\mathfrak{A}_n$, et $\mathfrak{S}_n$ lui-même.

Solution

— On suppose $n \geq 5$. On note $G = \mathfrak{S}_n$ et H un sous-groupe de G d'indice n. On note enfin $X := G/H$ l'ensemble quotient de cardinal n. On dispose d'un morphisme de groupes

$$\psi : G \to \mathfrak{S}(X) \cong \mathfrak{S}_n \,,$$

donné par $g \mapsto (xH \mapsto gxH)$. Montrons que c'est un isomorphisme : son noyau est un sous-groupe distingué de $G = \mathfrak{S}_n$, d'indice minoré par le cardinal de l'image de ψ, elle-même minorée par n. Ce sous-groupe distingué n'est donc égal ni à $\mathfrak{S}_n$, ni à $\mathfrak{A}_n$: il doit donc s'agir du sous-groupe trivial. Ainsi, ψ est injective, donc par cardinalité, c'est un isomorphisme.
On peut restreindre ψ au sous-groupe H. Or le point $x := H \in X$ est clairement un point fixé par les éléments de $\psi(H)$, donc on en déduit que les éléments de $\psi(H)$ préservent $X' := X \setminus \{x\}$. D'où un morphisme

$$\varphi : H \to \mathfrak{S}(X') \cong \mathfrak{S}_{n-1} \,.$$

Ce morphisme φ est injectif car ψ l'est, donc par cardinalité, c'est un isomorphisme, d'où la conclusion.

— Si $2 \leq n \leq 4$, on montre le résultat à la main : si $n = 2$ ou 3, le résultat est évident. Si $n = 4$, on utilise l'exercice pour savoir qu'un sous-groupe d'indice 4 dans $\mathfrak{S}_4$ est isomorphe à $\mathbb{Z}/6\mathbb{Z}$ ou $\mathfrak{S}_3$. Or $\mathfrak{S}_4$ ne contient aucun élément d'ordre 6, donc ce sous-groupe est bien isomorphe à $\mathfrak{S}_3$.