Exercices

action, monoïdes, groupes

Axiome de l'infini. Soit f une fonctionnelle (définie sur la classe de tous les ensembles). Soit o un ensemble. On étudier l'indépendance des trois conditions (1) "f injective", (2) "o n'est pas atteint par f" et (3) "f n'a pas de point fixe".

1. *Montrer que (2) n'est pas impliquée par (1) et (3).* (hint : $\left\{ \begin{array}{ccc} a \neq \mathfrak{P}(\emptyset) & \longmapsto & \mathfrak{P}(a) \\ \mathfrak{P}(\emptyset) & \longmapsto & \emptyset \end{array} \right.$)
2. *Montrer que (1) n'est pas impliquée par (2) et (3).* (hint : $\left\{ \begin{array}{ccc} a \neq \{\{\emptyset\}\} & \longmapsto & \{a\} \\ \{\{\emptyset\}\} & \longmapsto & \{\emptyset\} \end{array} \right.$)
3. *Montrer que (3) est impliquée par (1) et (2) à condition de restreindre la recherche des points fixes à une plus petite partie contenant o et stable par f.* (hint : montrer par induction $f(n) = n \Longrightarrow f(o) = o$)

Logique. On donne comme langage un symbole de loi binaire (sous-entendu), un symbole $^{-1}$ de loi singulaire et un symbole 1 d'objet distingué. On note :

- AS l'énoncé $\forall a, b, c,\ a(bc) = (ab)c$;
- $\left\{ \begin{array}{l} NEU_d \text{ l'énoncé } \forall a,\ a1 = a \\ NEU_g \text{ l'énoncé } \forall a,\ 1a = a \end{array} \right.$; NEU la conjonction de NEU_d et NEU_g ;
- $\left\{ \begin{array}{l} INV_d \text{ l'énoncé } \forall a,\ aa^{-1} = 1 \\ INV_g \text{ l'énoncé } \forall a,\ a^{-1}a = 1 \end{array} \right.$; INV la conjonction de INV_d et INV_g.

1. *Que définit la conjonction de AS et NEU ? celle de AS, NEU et INV ? Est-ce que la première peut prouver la seconde ?*
2. *Est-ce que les axiomes d'un groupe peuvent prouver l'énoncé de commutativité ?*
3. *Montrer que le système formé des énoncés AS, NEU_g et INV_d est strictement plus faible que celui AS, NEU et INV. On pourra munir $\mathbf{R}^*$ de la loi $(a, b) \mapsto |a| b$.*
4. *Montrer que NEU et INV ne peuvent prouver AS. On pourra considérer un alphabet contenant au moins trois lettres distinctes 1, a et b que l'on munira d'une loi constamment égale à 1 sauf sur les couples contenant 1.*
5. *Montrer que AS, NEU_g et INV_g (ou AS, NEU_d et INV_d) prouvent AS, NEU et INV.*

Monoïdes et groupes.

1. Soit $f : M \longrightarrow N$ un morphisme de monoïdes. *Montrer qu'il y a une unique application $f^\times : M^\times \longrightarrow N^\times$ faisant commuter le diagramme* $\begin{array}{ccc} M & \xrightarrow{f} & N \\ \uparrow \cup & & \uparrow \cup \\ M^\times & \xrightarrow{f^\times} & N^\times \end{array}$ *où les flèches $\uparrow \cup$ sont des inclusions canoniques.*
2. Soient $M \xrightarrow{f} N \xrightarrow{g} O$ deux morphismes de monoïdes. *Montrer l'égalité $[g \circ f]^\times = g^\times \circ f^\times$ et que le diagramme suivant commute* $\begin{array}{ccccc} M & \xrightarrow{f} & N & \xrightarrow{g} & O \\ \uparrow \cup & & \uparrow \cup & & \uparrow \cup \\ M^\times & \xrightarrow{f^\times} & N^\times & \xrightarrow{g^\times} & O^\times \end{array}$.

Groupe algébrique. *Montrer que les automorphismes du $\mathbf{Q}$-espace vectoriel $\mathbf{Q} + \mathbf{Q}\sqrt[3]{7} + \mathbf{Q}\sqrt[3]{49}$ qui préservent la multiplication forment un groupe que l'on déterminera.*

Commutant. Soit G un groupe. Soit $A \subset G$. *Montrer l'inclusion*

$$A \subset \mathrm{Comm}(\mathrm{Comm}(A)) \text{ avec égalité ssi } A \text{ est de la forme } \mathrm{Comm}(B).$$

Sous-groupes denses. *Montrer que les sous-groupes de* $\mathbf{U}$ *autres que les* $\mathbf{U}_n$ *sont denses dans le cercle unité.*

Composé de sous-groupes. Soit G un groupe. Soient A et B deux sous-groupes de G. On note $AB := \{ab \ ; \ a \in A \text{ et } b \in B\}$ (idem dans l'autre sens).

1. On suppose que A et B sont en produit direct et commutent, *i. e.* que $A \cap B = \{1\}$ et $\forall\, (a,b) \in A \times B,\ ab = ba$. *Montrer que* AB *est un sous-groupe isomorphe au groupe produit* $A \times B$.
   (bonus sagittal) *Montrer l'unicité d'un tel isomorphisme sous la condition de faire commuter le diagramme* $\begin{array}{ccccc} & \hookrightarrow & A \times B & \hookleftarrow & \\ A & & \simeq & & B \\ & \subset & AB & \supset & \end{array}$.
2. On suppose $G = GL_2\left(\mathbf{Z}/n\right)$ où n est un entier impair et que A et B sont engendrés respectivement par les matrices $a := \begin{pmatrix} 1 & 1 \\ \cdot & 1 \end{pmatrix}$ et $b := \begin{pmatrix} 1 & \cdot \\ \cdot & 2 \end{pmatrix}$. *Montrer* $\forall p, q \in \mathbf{N},\ a^p b^q = b^q \left(a^p\right)^{2^q}$. *En déduire* $ab \neq ba$ *et* $AB = BA$.
3. *Montrer que* AB *est un sous-groupe ssi* $AB = BA$. *Ces conditions équivalent-elles à* $\forall\, (a,b) \in A \times B,\ ab = ba$ *?*

Ordres. Soit G un groupe dont l'ordre de tous les éléments fait sens et est ≤ 2. *Montrer que* G *est abélien.* **Bonus** : *montrer que* G est *isomorphe au sous-groupe* $\mathbf{F}_2^{(I)}$ *du groupe puissance* $\mathbf{F}_2^I$ *formée des familles à support fini.*

Exposant d'un groupe abélien fini. Soit G un groupe abélien fini. On veut montrer qu'il contient un élément d'ordre maximal pour la divisibilité.

1. *Légitimer pour tout premier* p *la définition* $\alpha_p := \max\{n \in \mathbf{N} \ ; \ \exists g \in G,\ \omega(g) = p^n\}$.
   Soit $(a_p) \in G^{(\mathbf{P})}$ tel que $\forall p \in \mathbf{P},\ \omega(a_p) = p^{\alpha_p}$.
2. Soit $g \in G$. Notons $\prod_{p \in \mathbf{P}} p^{\gamma_p}$ son ordre. *En considérant les* $\left(\prod_{p \neq p_0} p^{\gamma_p}\right)$*-ièmes itérés de* g *(où* p_0 *varie) montrer que* $\omega(g) \mid \omega\left(\prod a_p\right)$ *et conclure.*
3. Soit K un corps fini (commutatif). *Montrer que* K^* *est cyclique.*

Isomorphismes.

1. Soit A un ensemble. On munit $\mathfrak{P}(A)$ d'une des trois lois $\cap$, $\cup$ ou Δ. *Parmir les trois monoïdes obtenus, lesquels sont isomorphes ?*
2. Soit $n \in \mathbf{N}$. *Les monoïdes monogènes d'ordre* n *sont-ils tous isomorphes ?*
3. *Donner un groupe de référence isomorphe à* $\left\{ \begin{pmatrix} 1 & a & b \\ \cdot & 1 & c \\ \cdot & \cdot & 1 \end{pmatrix} \ ; \ a, b, c \in \mathbf{F}_2 \right\}$.
4. *Décrire la structure de* $\left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ ; \ a, b \in \mathbf{Z}[i] \text{ et } |a|^2 + \left|b^2\right| = 1 \right\}$.
5. *Déterminer lesquels groupes sont isomorphes parmi* $\mathbf{R}$, $\mathbf{Z}$, $\mathbf{Q}$ *et* $\mathbf{Z}^2$.

Automorphismes intérieurs. Soit G un groupe. (On pourrait tout faire avec un monoïde.)

1. Soit $\varphi \in \operatorname{Aut} G$. On note $G_\varphi := G \times \mathbf{Z}$ muni de la loi $\left(\begin{pmatrix} g \\ a \end{pmatrix}, \begin{pmatrix} h \\ b \end{pmatrix}\right) \mapsto \begin{pmatrix} g\ \varphi^a(h) \\ a + b \end{pmatrix}$.
   (a) *Vérifier que* G_φ *est un groupe. Expliciter le neutre et l'inversion.*
   (b) *Montrer que* G *se plonge dans* G_φ via *le plongement de* G *dans le groupe produit* $G \times \mathbf{Z}$.

(c) *Prouver l'identité* $\forall\,(g,a)\in G\times\mathbf{Z},\ \begin{pmatrix}\varphi^a(g)\\0\end{pmatrix}=\binom{1}{a}\binom{g}{0}\binom{1}{a}^{-1}$.

(d) *Exhiber un automorphisme* c *intérieur de* G_φ *faisant commuter le diagramme* $\begin{array}{ccc}G&\hookrightarrow&G_\varphi\\ \varphi\downarrow\simeq&&\simeq\downarrow c\\ G&\hookrightarrow&G_\varphi\end{array}$. *Interpréter.*

2. On note $G^\lozenge:=G\times\operatorname{Aut}G$ muni de la loi $\left(\binom{g}{\alpha},\binom{h}{\beta}\right)\mapsto\binom{g\ \alpha(h)}{\alpha\circ\beta}$. On définit $j:\left\{\begin{array}{ccc}\operatorname{Aut}G&\longrightarrow&\operatorname{Int}G^\lozenge\\ \alpha&\longmapsto&\underset{(1,\alpha)}{\operatorname{int}}\end{array}\right.$.

(a) *Montrer que* $G^\lozenge$ *est un groupe dont on précisera le neutre et l'inversion.*

(b) *Montrer que* G *se plonge dans* $G^\lozenge$ *et (***bonus***) ce d'une unique manière faisant commuter le diagramme* $\begin{array}{ccc}G&\hookrightarrow&\\ \|&&G^\lozenge\\ G&\twoheadleftarrow&\end{array}$. On appelle i un tel plongement.

(c) *Montrer que* j *est un plongement.*

(d) *Montrer la commutativité du digramme* $\begin{array}{ccc}G\times\operatorname{Aut}G&\overset{i\times j}{\hookrightarrow}&G^\lozenge\times\operatorname{Int}G^\lozenge\\ \downarrow\acute{e}v&&\downarrow\acute{e}v\\ G&\overset{i}{\hookrightarrow}&G^\lozenge\end{array}$ *où les flèches* $\downarrow\acute{e}v$ *sont des évaluations* $(g,\alpha)\mapsto\alpha(g)$. *Interpréter et faire le lien avec les groupes* G_φ.

Quotients. Soit G un groupe.

1. Soient $N\subset M$ deux monoïdes (pour la même loi) finis. *Est-ce que* $|N|$ *divise* $|M|$ *? A-t-on* $|M|=\left|{}^M\!/_N\right||N|$ *ou* $|M|=|N|\left|{}_N\backslash^M\right|$ *?*
2. Soit $A\subset G$. *Montrer que l'ensemble* $\{gA\ ;\ g\in G\}$ *partitionne* G *ssi* A *le translaté d'un sous-groupe. Peut-on alors parler de quotient ?*
3. Soit $\varphi:G\longrightarrow H$ un morphisme de groupes. *Montrer qu'il y a un unique isomorphisme de groupes* ${}^G\!/_{\operatorname{Ker}\varphi}\simeq\operatorname{Im}\varphi$ *faisant commuter le diagramme* $\begin{array}{ccc}H&\hookleftarrow&\operatorname{Im}\varphi\\ \uparrow\varphi&&\uparrow\simeq\\ G&\twoheadrightarrow&{}^G\!/_{\operatorname{Ker}\varphi}\end{array}$.
4. Soit H un sous-groupe de G. *Montrer que la loi* $\overline{a}\,\overline{b}:=\overline{ab}$ *munit l'ensemble* ${}^G\!/_H$ *d'une structure de groupe ssi* $\forall a\in G,\ aHa^{-1}=H$. *Traduire cette dernière condition en termes de morphismes. Que dire de* ${}_H\backslash^G$ *? Vérifier le cas où* H *est le noyau d'un morphisme.*
5. Soit A un sous-groupe de G stable par conjugaison. Soit $\mathcal{H}$ un sous-groupe de ${}^G\!/_A$. *Montrer que* $H:=\cup\mathcal{H}$ *est un sous-groupe de* G *et que* $\mathcal{H}$ *est égal à* ${}^H\!/_A$.
6. Soit H un sous-groupe de G stable par conjugaison. *Montrer que* G *est isomorphe à* ${}^G\!/_H\times H$ *s'il y a un endomorphisme de* G *d'image* H *fixant ce dernier. Exemples ? **Étudier la réciproque.*

Actions. Soit G un groupe fini. Soit p un premier divisant $|G|$.

1. **(Cauchy bis)** On veut prouver le lemme de Cauchy à l'aide d'une action de groupe.
   On note $\mathbf{F}_p:={}^{\mathbf{Z}}\!/_p$ et $F:=\left\{f\in G^{\mathbf{F}_p}\ ;\ \prod_{a\in\mathbf{F}_p}f(a)=1\right\}$. On fait agir le groupe additif $\mathbf{F}_p$ sur F en définissant
   $$\forall\ (a,f)\in\mathbf{F}_p\times F,\ a\cdot f:\overline{n}\mapsto f(a+\overline{n}).$$
   (a) *Montrer que la partie* $\Phi:=\{f\in F\ ;\ \operatorname{Fix}f=\mathbf{F}_p\}$ *est formée des fonctions constantes de valeur une racine* p*-ième de* 1. *En déduire qu'il suffit de montrer que* p *divise* $|\Phi|$.
   (b) *Pour tout* $f\in F$, *montrer ou bien* $f\in\Phi$ *ou bien* $p\mid\#\operatorname{Orb}f$.
   (c) *Montrer* $|F|=|G|^{p-1}$ *et conclure.*
2. **(Sylow 2)** On appelle p-(sous-)groupe (de G) tout sous-groupe (de G) d'ordre une puissance de p. Un p-Sylow (de G) est défini comme étant un p-groupe maximal. On veut montrer que *tous les* p*-Sylow sont conjugués* (c'est le **deuxième théorème de Sylow**). On va montrer plus généralement que tout p-groupe est inclus dans le conjugé d'un p-Sylow fixé.
   Soit H un p-groupe. Soit S un p-Sylow. On fait agir H sur ${}^G\!/_S$ par composition. *Montrer modulo* p *l'égalité* $\left|{}^G\!/_S\right|=\#\{\overline{g}\ ;\ \operatorname{Fix}\overline{g}=H\}$. *En déduire la non-vacuité de* $\#\{\overline{g}\ ;\ \operatorname{Fix}\overline{g}=H\}$ *et conclure.*