Université Claude Bernard Lyon I — 2nd semestre 2009/2010
Master 1 — Introduction à la Logique

Théorie des ensembles
Correction du DM5.

Exercice I.

1. Considérons $x \in G$. L'ensemble des éléments de la forme $(x^{\pm 1})^{z_1} \dots (x^{\pm 1})^{z_m}$ est le plus petit sous-groupe normal de $\mathcal{G}$ qui contient x : en effet, c'est un sous-groupe normal, et tout sous-groupe normal contenant x doit contenir tous les produits de conjugués de x et x^{-1}.
Si $\mathcal{G}$ est simple, alors pour tout $x \in G \setminus \{1\}$ le plus petit sous-groupe normal contenant x doit être $\mathcal{G}$ tout entier, ce qui donne une des deux implications demandées par l'énoncé. Réciproquement, si $\mathcal{G}$ satisfait la condition de l'énoncé et $\mathcal{H}$ est un sous-groupe de $\mathcal{G}$ non réduit à $\{1\}$ alors, si on considère $x \in H \setminus \{1\}$, H doit contenir le plus petit sous-groupe normal qui contient x, par conséquent la condition de l'énoncé impose que $H = G$. Autrement dit, $\mathcal{G}$ est simple.

2. Supposons $\mathcal{G}$ simple, considérons $\mathcal{H}$ une sous-structure élémentaire de $\mathcal{G}$ (en particulier, c'est un sous-groupe) et fixons $h_1, h_2 \in \mathcal{H}$. D'après la question précédente, il doit exister $z_1, \dots, z_m \in G$ et $\epsilon_1, \dots, \epsilon_m \in \{-1, 1\}$ tels que $y = (x^{\epsilon_1})^{z_1} \dots (x^{\epsilon_m})^{z_m}$. Autrement dit, $\mathcal{G} \models \phi(h_1, h_2)$, où $\phi(x, y)$ est la formule

$$\exists z_1 \dots z_m \quad y = (x^{\epsilon_1})^{z_1} \dots (x^{\epsilon_m})^{z_m} \ .$$

Puisque $\mathcal{H}$ est une sous-structure élémentaire de $\mathcal{G}$, on doit aussi avoir $\mathcal{H} \models \phi(h_1, h_2)$, et cela prouve (d'après la question précédente) que H est simple.
Remarque. On n'a pas prétendu que « être un groupe simple »s'exprime par une formule du premier ordre : ci-dessus, il a fallu commencer par fixer m avant d'obtenir une formule du premier ordre... C'est ce qui explique le fait que dans la suite on va construire un groupe simple dont une extension élémentaire n'est pas simple.

3. On a $A_{\mathbb{N}} = \bigcup_{n \in \mathbb{N}} A_n$, par conséquent si $x, y \in A_{\mathbb{N}}$ avec $x \neq 1$ alors il doit exister un certain entier n (supérieur ou égal à 5 si l'on veut) tel que $x, y \in A_n$. Comme $\mathcal{A}_n$ est simple, le résultat de la question 1 nous dit qu'il existe m, $z_1, \dots, z_m \in A_n$ et $\epsilon_1, \dots, \epsilon_m \in \{-1, 1\}$ tels que $y = (x^{\epsilon_1})^{z_1} \dots (x^{\epsilon_m})^{z_m}$. Ceci est donc encore vrai dans $A_{\mathbb{N}}$, et on en déduit (toujours par la caractérisation obtenue en 1) que $\mathcal{A}_{\mathbb{N}}$ est simple.

4. Comme d'habitude, il nous faut construire un modèle du diagramme élémentaire de $\mathcal{A}_{\mathbb{N}}$ avec une bonne propriété ; ici, on rajoute deux symboles de constante c_x, c_y à notre langage et on considère l'ensemble d'énoncés

$$\Sigma = Th(\mathcal{A}_{\mathbb{N}}, A_{\mathbb{N}}) \cup \{\forall z_1 \dots z_m \ c_y \neq (c_x^{\epsilon_1})^{z_1} \dots (c_x^{\epsilon_m})^{z_m}\},$$

où les ϵ_i sont quelconques dans $\{-1, 1\}$ [1] . Un modèle $\mathcal{M}$ de Σ serait une extension élémentaire de $\mathcal{A}_{\mathbb{N}}$ (en particulier, ce serait un groupe), et les interprétations dans $\mathcal{M}$ de c_x, c_y témoigneraient du fait que $\mathcal{M}$ n'est pas simple. Il nous faut donc simplement montrer que Σ est consistant ; pour cela, on doit montrer, par compacité, que tout fragment fini de Σ est consistant. Comme qui peut le plus peut le moins, il nous suffit de montrer que pour tout $M \in \mathbb{N}$ l'ensemble d'énoncés

$$\Sigma_M = Th(\mathcal{A}_{\mathbb{N}}, A_{\mathbb{N}}) \cup \{\forall z_1 \dots z_m \ c_y \neq (c_x^{\epsilon_1})^{z_1} \dots (c_x^{\epsilon_m})^{z_m}\}_{m \leq M}$$

est consistant (encore une fois, les ϵ_i peuvent prendre des valeurs quelconques dans $\{-1, 1\}$, et pour chaque choix de ϵ_i on obtient un énoncé différent.).
Pour trouver un modèle de Σ_M, on prend comme univers $A_{\mathbb{N}}$, on interprète chaque $\sigma \in A_{\mathbb{N}}$ par lui-même, et bien sûr on interprète les opérations de groupe par celles de $\mathcal{A}_{\mathbb{N}}$. Ensuite, on peut par exemple interpréter c_x par un 3-cycle quelconque ; comme l'inverse et les conjugués d'un 3-cycle sont aussi des

1. i.e pour tout m et tout choix de $\varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\}$ on inclut un énoncé dans notre famille

3-cycles, un produit d'au plus M conjugués d'un 3-cycle fixé et de son inverse doit avoir un support [2] de cardinal au plus $3M$. Il nous suffit donc pour conclure d'interpéter c_y par une permutation paire dont le support est de cardinal strictement supérieur à $3M$, par exemple un $6M+1$-cycle.

Exercice II.

1. Le troisième axiome de la liste nous dit que f est injective, tandis que le deuxième axiome dit que f n'est pas surjective (il existe exactement un point qui n'est pas dans l'image de f). Comme une fonction d'un ensemble fini dans lui-même est injective ssi elle est surjective, on en déduit immédiatement que tout modèle de T est infini.
2. C'est immédiat (0 est le seul entier qui n'est le successeur d'aucun autre entier, etc, etc).
3. Si T était finiment axiomatisable alors (par compacité) un sous-ensemble fini des énoncés donnés dans le sujet suffirait à axiomatiser T. Sans perte de généralité, un tel ensemble d'énoncés dit que f est injective, qu'il existe exactement un élément qui n'est pas dans l'image de f, et que pour tout $n \in \{1, \dots, N\}$ on a pour tout x $f^n(x) \neq x$. Considérons l'ensemble $X = \mathbb{N} \sqcup \{0, \dots, N\}$ où on munit $\mathbb{N}$ de la fonction successeur et $\{0, \dots, N\}$ de la fonction successeur modulo N. Ceci induit une fonction f sur X qui satisfait tous les énoncés de notre ensemble fini ; pourtant $\langle X, f\rangle$ n'est pas un modèle de notre théorie, puisque pour tout élément $a \in \{0, \dots, N\}$ on a $f^{N+1}(a) = a$.
4. (a) Il est immédiat que $\sim$ est réflexive et symétrique. Pour voir qu'elle est transitive, supposons qu'on ait $\mathcal{M} \models (f^n(x) = f^m(y))$ et $\mathcal{M} \models (f^p(y) = f^q(z))$ avec $n, m, p, q \in \mathbb{N}$. Alors, on a $\mathcal{M} \models (f^{p+n}(x) = f^{q+m}(z))$, autrement dit $\sim$ est transitive.

   (b) Pour voir que chaque $\sim$-classe est une sous-structure de $\mathcal{M}$, il nous suffit de montrer que toute $\sim$-classe est stable par f.
   Pour cela, supposons que $z \sim x$; alors il existe n, m tels que $\mathcal{M} \models (f^n(x) = f^m(z))$, par conséquent $\mathcal{M} \models (f^{n+1}(x) = f^m(f(z)))$ et on a bien $x \sim f(z)$.

   (c) Appelons m_0 l'unique élément de M qui n'est pas dans l'image de f, et E_0 sa $\sim$-classe d'équivalence. On doit montrer que $\langle E, f_{|E}\rangle$ est isomorphe à $\langle \mathbb{N}, s\rangle$, et que pour tout $m \in M \setminus E_0$, si l'on note E_m la $\sim$-classe de m alors $\langle E_m, f_{|E_m}\rangle$ est isomorphe à $\langle \mathbb{Z}, s\rangle$. Commençons par traiter le cas de E_0. Si $y \in E_0$ alors on a $p, q \in \mathbb{N}$ tels que $f^p(y) = f^q(m_0)$ [3] ; si $q < p$ alors ceci donne (en utilisant l'injectivité de f) $f^{p-q}(y) = m_0$, ce qui est impossible puisque m_0 n'est pas dans l'image de f. On a donc nécessairement $p \leq q$, et alors on a (toujours grâce à l'injectivité de f) $f^{q-p}(m_0) = y$. On vient de montrer que pour tout $y \in E$ il existe $r \in \mathbb{N}$ (nécessairement unique puisque f est injective et n'a pas de points périodiques) tel que $y = f^r(x)$. Il est alors immédiat de vérifier que l'application $F_0 \colon \mathbb{N} \to E_0$ définie par $F_0(n) = f^n(x)$ est un isomorphisme de $\langle \mathbb{N}, s\rangle$ sur $\langle E_0, f_{|E_0}\rangle$.
   Reste à traiter le cas de E_m quand $m \notin E_0$. Alors $f_{|E_m} \colon E_m \to E_m$ est bijective, et pour tout $y \in E_m$ il existe $k \in \mathbb{Z}$ tel que $y = (f_{|E_m})^k(x)$. Comme f n'a pas de points périodiques, ce k est nécessairement unique, et on en déduit que l'appplication $F_m \colon \langle \mathbb{Z}, s\rangle \to \langle E_m, f_{|E_m}\rangle$ est un isomorphisme.
   Ceci suffit à conclure la démonstration.
5. On a fait tout le travail dans la question précédente : Si l'on appelle $\mathcal{E}$ l'ensemble formé par les $\sim$-classes isomorphes à $\langle \mathbb{Z}, s\rangle$, et E_0 la classe isomorphe à $\langle \mathbb{N}, s\rangle$ alors on doit avoir pour tout modèle $\mathcal{M}$ de T que

$$M = E_0 \sqcup \bigsqcup_{E \in \mathcal{E}} E \ .$$

   Si l'on suppose que le modèle est de cardinal $\kappa > \aleph_0$, et qu'on appelle λ le cardinal de E alors on obtient (comme les classes sont deux à deux disjointes) $\kappa = \aleph_0 + \aleph_0.\lambda$. En particulier, λ doit alors être infini (sans quoi M serait dénombrable), et on obtient $\kappa = \aleph_0.\lambda$, autrement dit $\max(\aleph_0, \lambda) = \kappa > \aleph_0$. On en déduit

2. i.e l'ensemble des x tels que $\sigma(x) \neq x$.
3. Pour être rigoureux il faudrait ajouter des $\mathcal{M} \models \dots$ aux bons endroits, mais comme il n'y a pas vraiment de confusion possible j'allège un peu les notations...

que $\lambda = \kappa$. On vient de montrer que dans un modèle de cardinal $\kappa > \aleph_0$ il y a toujours une $\sim$-classe isomorphe à $\langle \mathbb{N}, s\rangle$ et κ $\sim$-classes isomorphes à $\langle \mathbb{Z}, s\rangle$. Il est alors facile de prouver que deux modèles de même cardinal $\kappa > \aleph_0$ sont isomorphes, i.e T est κ-catégorique pour tout cardinal $\kappa > 0$.

6. Une conséquence élémentaire, et vue en cours, du théorème de Löwenheim-Skolem est qu'une théorie dans un langage dénombrable qui est κ-catégorique pour un cardinal infini κ doit être complète. Par conséquent T est complète, autrement dit pour tout modèle $\mathcal{M}$ de T on a $T = Th(\mathcal{M})$. En particulier, on a $T = Th(\langle \mathbb{N}, s\rangle)$.
7. Un raisonnement similaire à celui de la question 5 nous dit que deux modèles de T sont isomorphes ssi ils ont le même nombre de classes isomorphes à $\langle \mathbb{Z}, s\rangle$. Si on ne considère que les modèles dénombrables, le cardinal de l'ensemble des classes isomorphes à $\langle \mathbb{Z}, s\rangle$ peut prendre comme valeurs tous les élements de $\omega + 1$ (autrement dit : tous les cardinaux finis, ainsi que $\aleph_0$). Il y a donc exactement $\aleph_0$ possibilités, ce qui prouve que T a exactement $\aleph_0$ modèles dénombrables.
8. Considérons la structure $\mathcal{M}$ d'univers $\mathbb{N} \sqcup \mathbb{Z} = \mathbb{N} \times \{0\} \cup \mathbb{Z} \times \{1\}$ et telle que $f^{\mathcal{M}}(n, 0) = (n + 1, 0)$ pour tout $n \in \mathbb{N}$ et $f^{\mathcal{M}}(m, 1) = (m + 1, 1)$ pour tout $m \in \mathbb{Z}$. L'ensemble $\mathbb{N} \times \{1\}$, muni de la restriction de $f^{\mathcal{M}}$, est une sous-structure $\mathcal{M}'$ de $\mathcal{M}$. Cette sous-structure n'est pas élémentaire : en effet,

$$\mathcal{M} \models (\exists x\ (0, 1) = f(x))\ ,\ \text{tandis que}\ \mathcal{M}' \models\ \forall x\ ((0, 1) \neq f(x))\ .$$

   On en déduit immédiatement que T n'élimine pas les quanteurs : en effet, si une théorie T élimine les quanteurs alors tout plongement entre modèles de T est élémentaire, puisqu'un plongement préserve les valeurs de vérité des formules sans quanteurs et que toute formule est équivalente à une formule sans quanteurs. En particulier, dès que $\mathcal{M}'$ est une sous-structure de $\mathcal{M}$ et que $\mathcal{M}$, $\mathcal{M}'$ sont deux modèles d'une théorie complète T qui élimine les quanteurs, $\mathcal{M}'$ est une sous-structure élémentaire de $\mathcal{M}$.
9. Dans notre nouveau langage, et avec notre nouvel axiome, on a nommé l'unique élément qui n'est pas dans l'image de f. Le même raisonnement que précédemment permet de voir que T' est κ-catégorique pour tout cardinal κ non dénombrable, et donc T' est complète.
   Pour voir que T' élimine les quanteurs, on peut par exemple penser aux modèles saturés. On vérifie facilement les faits suivants :
   - Tout modèle dénombrable de T' a une extension élémentaire dénombrable ayant une $\sim$-classe isomorphe à $\langle \mathbb{N}, s\rangle$ et $\aleph_0$ $\sim$-classes isomorphes à $\langle \mathbb{Z}, s\rangle$ (par compacité, il existe une extension élémentaire avec une infinité de $\sim$-classes isomorphes à $\langle \mathbb{Z}, s\rangle$ et, par Löwenheim-Skolem descendant, il doit alors en exister une qui est dénombrable).
   - Deux modèles dénombrables ayant chacun une $\sim$-classe isomorphe à $\langle \mathbb{N}, s\rangle$ et $\aleph_0$ $\sim$-classes isomorphes à $\langle \mathbb{Z}, s\rangle$ sont isomorphes (on l'a vu plus haut).
   - Dans un modèle comme à l'item précédent (appelons-le provisoirement « riche »), deux éléments qui ont le même type sans quanteurs peuvent être envoyés l'un sur l'autre par un isomorphisme : en effet, le type sans quanteurs d'un élément dit s'il est dans la $\sim$-classe isomorphe à $\langle \mathbb{N}, s\rangle$ (et, si oui, à quelle distance il est de 0) et on peut par va-et-vient envoyer deux uplets qui ont le même type sans quanteurs (dans T') l'un sur l'autre.

   Montrons maintenant que deux uplets $\bar{x}$,$\bar{y}$ ayant le même type sans quanteurs ont nécessairement le même type. Pemièrement, notons que $\bar{x}$, $\bar{y}$ sont réalisés dans des modèles dénombrables de T' ; quitte à passer à des extensions élémentaires, on peut supposer que ces modèles sont riches. Deux modèles riches dénombrables étant isomorphes, on voit ainsi que $\bar{x}$ et $\bar{y}$ sont réalisés dans un même modèle dénombrable riche $\mathcal{M}$. Mais alors on a vu qu'il existe un isomorphisme de $\mathcal{M}$ qui envoie $\bar{x}$ sur $\bar{y}$, par conséquent $\bar{x}$ et $\bar{y}$ ont le même type.
   On a donc prouvé que deux uplets ayant le même type sans quanteurs ont nécessairement le même type, autrement dit la théorie T' élimine les quanteurs.
10. Considérons un modèle $\mathcal{M}$ de T, étendons-le en un modèle de T' en appelant $c^{\mathcal{M}}$ l'unique élément de M qui n'est pas dans l'image de $f^{\mathcal{M}}$. Alors la $\sim$-classe $\mathcal{M}'$ de $c^{\mathcal{M}}$ est isomorphe (en tant que $L \cup \{c\}$-structure) à $\langle \mathbb{N}, s, 0\rangle$ et est une sous-structure (élémentaire puisque T' élimine les quanteurs) de $\mathcal{M}$.
    Notons encore $\mathcal{M}'$ la L-structure correspondant à la $\sim$-classe de $c^{\mathcal{M}}$.
    Si $\bar{x}, \bar{y} \in (M')^k$ on peut vérifier que $\bar{x}, \bar{y}$ ont le même T-type ssi ils ont le même T'-type. Par conséquent, les T-types obtenus en voyant un uplet $\bar{x} \in (M')^k$ dans $\mathcal{M}$ et dans $\mathcal{M}'$ sont égaux (puisque leurs T'-types le sont), ce qui revient à dire que $\mathcal{M}'$ est une sous-structure élémentaire de $\mathcal{M}$.