TD8

Exercice 1.
Ecrire les arbres de preuve pour les propriétés suivantes :

1. $(P \to \neg Q) \leftrightarrow \neg(P \wedge Q)$
2. $((P \vee Q) \to R) \leftrightarrow (P \to R) \wedge (Q \to R)$
3. $\forall x \neg A \leftrightarrow \neg(\exists x A)$
4. $(\exists x A \vee \exists x B) \leftrightarrow \exists x(A \vee B)$
5. $\exists x(A \wedge B) \leftrightarrow (\exists x A \wedge \exists x B)$ si $x \notin FV(B)$

Exercice 2.
Un groupe abélien $(G, +, 0)$ est dit **ordonnable** si et seulement s'il existe sur G une relation d'ordre totale $\leq$ **compatible** avec l'operation $+$, c'est-à-dire telle que, pour tous éléments x, y et z de G, si $x \leq y$, alors $x + z \leq y + z$.
Un groupe abélien $(G, +, 0)$ est dit **sans torsion** si et seulement si, pour tout élément x de G, distinct de 0, et pour tout entier naturel non nul n, x^n est différent de 0.
Un groupe abélien $(G, +, 0)$ est dit **de type fini** si et seulement s'il est engendré par une partie finie de G (ce qui veut dire qu'il existe une partie finie $X \subset G$ telle que le plus petit sous-groupe de G contenant X soit G lui-même).

1. Soit $(G, +, 0)$ un groupe abélien. Définir un ensemble $\mathcal{A}(G)$ de formules du calcul propositionnel qui soit satisfiable si et seulement si le groupe G est ordonnable.
2. Montrer que, pour qu'un groupe abélien soit ordonnable, il faut et il suffit que tous ses sous-groupes de type fini soient ordonnables.
3. Montrer qu'un groupe abélien soit ordonnable si et seulement s'il est sans torsion.
   Aide : On peut utiliser le théoreme d'algèbre suivant :

   > Pour tout groupe abélien de type fini sans torsion $(G, +, 0)$ non réduit à l'élément neutre, il existe un entier p tel que $(G, +, 0)$ soit isomorphe au groupe $(\mathbb{Z}^p, +, 0)$.

Exercice 3.
On fixe le langage égalitaire $\mathcal{L} = \{R^2, =\}$ où R est un prédicat binaire.

1. Existe t-il une théorie des relations d'équivalence n'ayant que des classes finies, i.e., une théorie dont l'ensemble des modèles soit exactement l'ensemble des ensembles munis d'une relation d'équivalence n'ayant que des classes finies ?
2. Existe t-il une théorie des relations d'équivalence n'ayant qu'un nombre fini de classes ?
3. Donner une axiomatisation de la théorie $T_\equiv$ des relations d'équivalences ayant sont une infinité de classes qui sont toutes infinies.
4. Une théorie T est finiment axiomatisable s'il existe une théorie finie T_1 telle que $T \vdash T_1$ et $T_1 \vdash T$. Montrer que si T est finiment axiomatisable, alors il existe un sous-ensemble fini T' de T tel que $T' \vdash T$.
5. La théorie $T_\equiv$ est-elle finiment axiomatisable ?
6. La théorie $T_\equiv$ est elle complète ?

Exercice 4.

1. On définit la fonction β de Gödel de la manière suivante :

$$\beta(i, a, b) = \text{ le reste de la division euclidienne de } b \text{ par } a(i+1)+1$$

   Montrer que la fonction β est représentable.

2. Soit $(n_1, \ldots, n_k)$ une suite d'entiers. Soit $m \geq k$ un entier tel que $a = m!$ satisfait $a > n_i$ pour chaque $i \in \{1, \ldots, k\}$. Montrer que les nombres $a(i+1)+1$, pour $i \in \{1, \ldots, k\}$, sont premiers entre eux deux à deux. Montrer qu'il existe un entier b tel que b est congru à n_i modulo $a(i+1)+1$ pour chaque $i \in \{1, \ldots, k\}$.

   Indice : Utiliser le théorème de restes chinois qui implique que, pour tout ensemble $\{a_1, \ldots, a_k\}$ d'entiers distincts et premiers deux à deux et tout k-uple $(n_1, \ldots, n_k)$ tel que $0 \leq n_i < a_i$ $\forall i \in \{1, \ldots, k\}$, il existe un entier x tel que $x \equiv n_i \pmod{a_i}$ $\forall i \in \{1, \ldots, k\}$.

3. En déduire que, pour chaque $i \in \{1, \ldots, k\}$, on a $\beta(i, a, b) = n_i$.

4. Montrer que la fonction exponentielle $f_m(n) = m^n$ est représentable.

5. Donner une formule qui exprime le théorème de Fermat : pour tout $n > 2$, l'équation $x^n + y^n = z^n$ n'admet par de solution entière non-triviale (i.e., où $x \neq 0$, $y \neq 0$ et $z \neq 0$).

6. On pourrait penser que n'importe quel codage de suites finies d'entiers convient. Par exemple, considérons celui beaucoup plus simple défini de la manière suivante : la suite $(i_1, \ldots, i_n)$ est codée par l'entier $2^{1+i_1} \cdot 3^{1+i_2} \cdots p_n^{1+i_n}$, où p_n est le n-ème nombre premier. Pourquoi celà ne marche-t-il pas ?