Théorie des ensembles
Correction du DM4.

Exercice 1.

1. (a) Par symétrie, il suffit de montrer que si θ est un énoncé de la forme $\forall x_1 \dots x_n\ \phi(x_1, \dots, x_n)$ avec ϕ sans quantificateurs alors $(T_1 \vdash \theta) \Rightarrow (T_2 \vdash \theta)$. Pour cela, supposons que $T_1 \vdash \theta$ et considérons un modèle $\mathcal{M}_2$ de T_2. Par hypothèse, $\mathcal{M}_2$ se plonge dans un modèle $\mathcal{M}_1$ de T_1 ; notons σ un plongement de $\mathcal{M}_2$ dans $\mathcal{M}_1$. On doit avoir

$$\mathcal{M}_1 \models \forall x_1 \dots x_n \phi(x_1, \dots, x_n)$$

Considérons $m_1, \dots, m_n$ dans $\mathcal{M}_2$; puisque $(\sigma(m_1), \dots, \sigma(m_n)) \in \mathcal{M}_1$ on a $\mathcal{M}_1 \models \phi(\sigma(m_1), \dots, \sigma(m_n))$. Or, le fait que σ soit un plongement et que ϕ soit sans quantificateurs entraîne que

$$(\mathcal{M}_1 \models \phi(\sigma(m_1), \dots, \sigma(m_n))) \Leftrightarrow (\mathcal{M}_2 \models \phi(m_1, \dots, m_n)) \ .$$

Par conséquent, on doit avoir $\mathcal{M}_2 \models \forall x_1 \dots x_n\ \phi(x_1, \dots, x_n)$, ceci étant vrai pour tout modèle de T_2. On vient de prouver que $T_2 \vdash \theta$.

(b) Posons

$$\Sigma = T_2 \cup \{\varphi(\bar{m}) \colon \mathcal{M} \models \phi(\bar{m}),\ \phi \text{ formule sans quantificateurs}\} \ .$$

Pour montrer que Σ est consistant, il nous suffit (par compacité) de prouver que tout fragment fini de Σ est consistant, et pour cela il suffit d'établir que chaque ensemble d'énoncés de la forme $T_2 \cup \{\psi(m_1, \dots, m_k)\}$, où ψ est une formule sans quantificateurs et $(m_1, \dots, m_k) \in M^k$, est consistant. Notons que si dans tout modèle $\mathcal{M}_2$ de T_2 on avait $\mathcal{M}_2 \models \forall x_1 \dots x_k \neg\psi(x_1, \dots, x_k)$ alors $\forall x_1 \dots x_k \neg\psi(x_1, \dots, x_k)$ serait une conséquence universelle de T_2, donc aussi de T_1, donc on aurait aussi $\mathcal{M}_1 \models \forall x_1 \dots x_k \neg\psi(x_1, \dots, x_k)$, ce qui contredit le choix de ψ. Par conséquent, il existe un modèle $\mathcal{M}_2$ de T_2 et $a_1, \dots, a_k \in M_2$ tels que $\mathcal{M}_2 \models \psi(a_1, \dots, a_k)$; en interprétant $m_1, \dots, m_k$ par $a_1, \dots, a_k$ on voit que notre ensemble d'énoncés est bien consistant.
Pour conclure, il suffit de noter que si $\mathcal{N}$ est un modèle de Σ alors le réduit de $\mathcal{N}$ au langage commun à T_1, T_2 est un modèle de T_2, et l'application $\sigma \colon m \mapsto m^{\mathcal{N}}$ est un plongement de $\mathcal{M}$ dans $\mathcal{N}$.

(c) = (a) et (b) .

2. (a) Suivons l'indication de l'énoncé ; le fait que $2\mathbb{Z}$ soit d'indice 2 dans $\mathbb{Z}$ s'exprime par l'énoncé

$$\exists x\, \forall y\, ((\exists z\ y = z + z) \vee (\exists z\ y = z + z + x)) \ .$$

Cet énoncé n'est pas vrai dans $(\mathbb{Z} \times \mathbb{Z}, 0, +)$: supposons que $x = (x_0, x_1)$ satisfasse la condition ci-dessus. Alors avec $y = (0, 1)$ on voit que x_0 est pair tandis que x_1 est impair ; de même, en considérant $y = (1, 0)$ on voit que x_0 est impair alors que x_1 est pair.

(b) Il est bien clair que $(\mathbb{Z}, 0, +)$ se plonge dans $(\mathbb{Z}\times\mathbb{Z}, 0, +)$ (par exemple via $n \mapsto (n, 0)$) par conséquent le raisonnement de la question 1.(a) implique immédiatement le résultat demandé par l'énoncé.

(c) Comme d'habitude, ajoutons à notre langage un symbole de constante n pour chaque entier $n \in \mathbb{Z}^*$ ainsi que deux symboles de constante a et b, puis considérons l'ensemble d'énoncés dans ce nouveau langage

$$\Sigma = Th((\mathbb{Z}, 0, +), \mathbb{Z}) \cup \{ia \neq jb\}_{i,j \in \mathbb{Z}^*} \ .$$

(On a bien sûr utilisé la notation ia comme abréviation de $\underbrace{a + \dots + a}_{i \text{ fois}}$)

On a besoin de montrer que Σ est consistant, par compacité il suffit de le vérifier pour un fragment

fini, et il suffit de traiter les fragments de la forme $Th((\mathbb{Z},0,+),\mathbb{Z}) \cup \{ia \neq jb\}_{i,j\neq 0 \text{ et } |i|,|j|\leq N}$. Un modèle de cette théorie est obtenu en considérant $\mathbb{Z}$, dans lequel on interprète chaque entier par lui-même, l'addition est l'addition usuelle, et on interprète a par 1 et b par $N+1$.
Notre théorie est donc bien consistante, et un modèle de cette théorie est exactement ce que recherche l'énoncé.

(d) L'application $\sigma\colon (i,j) \mapsto (ia^{\mathcal{G}}, jb^{\mathcal{G}})$ est un isomorphisme sur son image par construction de $\mathcal{G}$; autrement dit on a $\sigma(0,0) = 0$ et $\sigma((i_1,j_1)+(i_2,j_2)) = \sigma(i_1,j_1)+\sigma(i_2,j_2)$, ce qui revient à dire que σ est un plongement de $(\mathbb{Z}\times\mathbb{Z},0,+)$ dans $\mathcal{G}$.

(e) Soit θ un énoncé universel vrai dans $(\mathbb{Z},0,+)$. Alors θ est vrai dans $\mathcal{G}$, qui est une extension élémentaire de $(\mathbb{Z},0,+)$. Puisque $(\mathbb{Z}\times\mathbb{Z},0,+)$ se plonge dans $\mathcal{G}$, on en déduit que θ est aussi vrai dans $(\mathbb{Z}\times\mathbb{Z},0,+)$. Par conséquent un énoncé universel vrai dans $(\mathbb{Z},0,+)$ est vrai aussi dans $(\mathbb{Z}\times\mathbb{Z},0,+)$; ajouté au résultat de 2(b), cela nous permet de voir que les théories de $(\mathbb{Z},0,+)$ et $(\mathbb{Z}\times\mathbb{Z},0,+)$ (qui sont complètes) sont compagnes l'une de l'autre.

Exercice 2.

1. Appelons T la théorie dans le langage des corps qui dit « le corps est algébriquement clos ». Alors la théorie des corps algébriquement clos de caractéristique nulle est égale à $T \cup \{p.1 \neq 0\}_{p\in\mathbb{P}}$, où $\mathbb{P}$ désigne l'ensemble des nombres premiers. Par compacité, un énoncé θ est conséquence de $T \cup \{p.1 \neq 0\}_{p\in\mathbb{P}}$ si, et seulement si, il est conséquence d'un fragment fini de $T \cup \{p.1 \neq 0\}_{p\in\mathbb{P}}$, i.e d'un sous-ensemble de $T_k = T \cup \{p.1 \neq 0\}_{p\in\mathbb{P},p<k}$ où k est un entier.
Tout corps algébriquement clos de caractéristique $\geq k$ est un modèle de T_k, par conséquent un tel corps doit satisfaire θ.
2. Considérons un énoncé θ satisfait par tout corps algébriquement clos de caractéristique $\geq k$, et un corps K algébriquement clos de caractéristique nulle. Comme la théorie des corps algébriquement clos de caractéristique nulle est complète, la théorie de K est égale à $T \cup \{p.1 \neq 0\}_{p\in\mathbb{P}}$, et tout fragment fini Σ de $Th(K)$ est donc contenu dans $T \cup \{p.1 \neq 0\}_{p\in\mathbb{P},p<N}$ pour un certain N. Si l'on pose $M = \max(N,k)$ alors tout corps algébriquement clos de caractéristique $\geq M$ est un modèle de Σ, par conséquent $\Sigma \cup \{\theta\}$ est consistant. Si jamais θ était faux dans K alors on aurait $Th(K) \vdash \neg\theta$; par compacité il existerait un fragment fini Σ de T tel que $\Sigma \vdash \neg\theta$, et on vient de voir que ce n'est pas le cas. Par conséquent, θ est satisfait dans K.
3. Fixons un sous-ensemble fini I de $\mathbb{N}^m$, et notons chaque $i \in I$ sous la forme $i = (i_1,\dots,i_m)$. Pour nous simplifier l'écriture ci-dessous, notons $\phi_I\left((a_i^j)_{i\in I, j\in\{1,\dots,m\}}, y_1,\dots,y_m\right)$ le terme
$$\left(\sum_{i\in I} a_i^1 y_1^{i_1}\dots y_m^{i_m}, \dots, \sum_{i\in I} a_i^m y_1^{i_1}\dots y_m^{i_m}\right) .$$
Maintenant, considérons l'énoncé θ_I suivant :
$$\forall_{i\in I, j\leq m} a_i^j \left(\forall y_1\dots y_m \forall z_1\dots z_m \ \phi_I((a_i^j),y_1,\dots,y_m) = \phi_I((a_i^j),z_1,\dots,z_m)) \to \bigwedge_{i\in I}(y_i = z_i)\right) \to$$
$$\Big(\forall r_1\dots r_m \,\exists s_1\dots s_m \ \phi_I((a_i^j),s_1,\dots,s_m) = (r_1,\dots,r_m)\Big) .$$
L'énoncé θ_I, en langage courant, dit « pour toute application polynômiale P de A^m dans A^m telle que les degrés des monômes apparaissant dans P appartiennent tous à I, P est injective si, et seulement si, P est surjective ». Par conséquent, la propriété $\mathcal{P}_m$ est exprimée par la famille $\{\theta_I\}_{I \text{ fini}\subseteq N^m}$.
4. Si A est un anneau fini, alors une application de A dans A est injective ssi elle est surjective, par conséquent A a la propriété $\mathcal{P}_m$.
5. Fixons $m > 0$, et considérons une application polynômiale $F = (F_1,\dots,F_m)\colon \tilde{\mathbb{F}}_p^m \to \tilde{\mathbb{F}}_p^m$. Rappelons que l'application $\Phi\colon x \mapsto x^p$ est un morphisme de corps de $\tilde{\mathbb{F}}_p$ dans lui-même. Par définition, $x \in \mathbb{F}_{p^n}$ est

équivalent à $\Phi^n(x) = x$. Pour n suffisamment grand, les coefficients de F appartiennent tout à $\mathbb{F}_{p^n}$; on a alors pour tout $x_1, \ldots, x_m \in \mathbb{F}_{p^n}$ et pour tout i

$$\Phi^n(F_i(x_1, \ldots, x_m)) = F_i(\Phi^n(x_1), \ldots, \Phi^n(x_m)) = F_i(x_1, \ldots, x_m) \ .$$

Par conséquent, F envoie chaque $\mathbb{F}_{p^n}^m$ dans lui-même. De plus, puisque tous les coefficients de F appartiennent à $\mathbb{F}_{p^n}$, la restriction de F à $\mathbb{F}_{p^n}^m$ est une application polynômiale.
Supposons maintenant F injective. Alors la restriction de F à $\mathbb{F}_{p^n}^m$ est injective et donc surjective, pour n suffisamment grand (puisque $\mathbb{F}_{p^n}$ est fini et a donc la propriété $\mathcal{P}_m$). Comme $\tilde{\mathbb{F}}_p^m = \bigcup_{n>0} \mathbb{F}_{p^n}$, on en déduit que F est surjective, par conséquent $\tilde{\mathbb{F}}_p^m$ a la propriété $\mathcal{P}_m$.

6. Rappelons que la théorie des corps algébriquement clos de caractéristique p est complète pour tout $p > 0$. Par conséquent, le fait que $\tilde{\mathbb{F}}_p$ satisfasse $\mathcal{P}_m$ entraîne que $\mathcal{P}_m$ est vérifiée par tout corps algébriquement clos de caractéristique p. Finalement, le résultat de la question 2 nous permet de conclure.