Homework8

Qi'ao Chen
21210160025

November 19, 2021

Exercise 1. Let M be a substructure of N. Let $\bar{a} \in M^n$ be a tuple and $\varphi(x_1, \dots, x_n)$ be a quantifier-free formula. Show that $M \vDash \varphi(\bar{a}) \Leftrightarrow N \vDash \varphi(\bar{a})$

Proof. M is a substructure of N, then the inclusion map $i : M \to N$ is an embedding.

First we prove that for any term $t(\bar{x})$, $t^M(\bar{a}) = t^N(\bar{a})$ by induction on the complexity of term t.

If t is a constant c, then $c^N = i(c^M) = c^M$.

If t is a variable v_i, then $t^M(\bar{a}) = a_i = t^N(\bar{a})$.

If t is of the form $f(t_1(\bar{x}), \dots, t_n(\bar{x}))$, then, for all $i = 1, \dots, n$, $t_i^M(\bar{a}) = t_i^N(\bar{a})$ by induction. Because i is an embedding, then $f^M(b_1, \dots, b_n) = i(f^M(b_1, \dots, b_n)) = f^N(i(b_1), \dots, i(b_n)) = f^N(b_1, \dots, b_n)$. Hence $f^M = f^N \mid M^n$

$$\begin{aligned} t^M(\bar{a}) &= f^M(t_1^M(\bar{a}), \dots, t_n^M(\bar{a})) \\ &= f^N(t_1^N(\bar{a}), \dots, t_n^N(\bar{a})) \\ &= t^N(\bar{a}) \end{aligned}$$

Then we prove the exercise by induction on the complexity of $\varphi(\bar{x})$.

If φ is of the form $t_1(\bar{x}) = t_2(\bar{x})$. Then

$$\begin{aligned} M \vDash t_1(\bar{a}) = t_2(\bar{a}) &\Leftrightarrow t_1^M(\bar{a}) = t_2^M(\bar{a}) \\ &\Leftrightarrow t_1^N(\bar{a}) = t_2^N(\bar{a}) \\ &\Leftrightarrow N \vDash t_1(\bar{a}) = t_2(\bar{a}) \end{aligned}$$

If φ is of the form $R(t_1(\bar{x}), \dots, t_m(\bar{x}))$, then

$$\begin{aligned}
M \vDash R(t_1(\bar{a}), \dots, t_m(\bar{a})) &\Leftrightarrow (t_1^M(\bar{a}), \dots, t_m(\bar{a})) \in R^M \\
&\Leftrightarrow (i(t_1^M(\bar{a})), \dots, i(t_m^N(\bar{a}))) \in R^N \\
&\Leftrightarrow (t_1^M(\bar{a}), \dots, t_m^N(\bar{a})) \in R^N \\
&\Leftrightarrow (t_1^N(\bar{a}), \dots, t_n^N(\bar{a})) \in R^N \\
&\Leftrightarrow N \vDash R(t_1(\bar{a}), \dots, t_m(\bar{a}))
\end{aligned}$$

If φ is of the form $\neg\psi$, then

$$M \vDash \varphi(\bar{a}) \Leftrightarrow M \nvDash \psi(\bar{a}) \Leftrightarrow N \nvDash \psi(\bar{a}) \Leftrightarrow N \vDash \varphi(\bar{a})$$

If φ is of the form $\psi_1 \wedge \psi_2$, then

$$\begin{aligned}
M \vDash \varphi(\bar{a}) \Leftrightarrow M \vDash \psi_1(\bar{a}) \text{ and } M \vDash \psi_2(\bar{a}) & \\
& N \vDash \psi_1(\bar{a}) \text{ and } N \vDash \psi_2(\bar{a}) \\
& N \vDash \varphi(\bar{a})
\end{aligned}$$

$\square$

Exercise 2. Let M be an ω-saturated elementary extensions of $(\mathbb{R}, +, \cdot, -, 0, 1, \leq)$. Suppose that $a \in M$. Show that there is $b \in M$ s.t. $b > a^n$ for all positive integers n.

Proof. Let $\varphi_n(x, y)$ be

$$\neg y = x \wedge \underbrace{x \cdot x \cdot \cdots \cdot x}_{n \text{ times}} \leq y$$

Let $\Sigma(x) = \{\varphi_n(a, x) \mid n \in \mathbb{N}_+\}$. For any finite $\Sigma_0(x) \subseteq \Sigma(x)$, it's equivalent to $\varphi_N(a, x)$ for some sufficient large N. But since $\mathbb{R} \vDash \forall x \exists y \varphi_n(x, y)$ and M is an elementary extension of $\mathbb{R}$, $M \vDash \forall x \exists y \varphi_n(x, y)$ and hence there is a $b_a \in M$ such that $M \vDash \varphi_N(a, b)$.

Hence $\Sigma(x)$ is finitely satisfiable and there is $p \in S_n(a)$ with $p \supseteq \Sigma$. Then M being ω-saturated implies that $p(x)$ is realised by $b \in M$ and therefore $M \vDash \Sigma(b)$. So for any positive n, $b > a^n$. $\square$

Exercise 3. Let K be a field and $x, y \in K$ be elements. Show that $xy = 0 \Leftrightarrow (x = 0 \vee y = 0)$

Proof. $\Rightarrow$. If both x and y are nonzero. Then as $xy = 0$, $1 = y^{-1}x^{-1}xy = 0$, which violates the axiom of field.

$\Leftarrow$. For any $a \in K$,

$$0 = 0 \cdot a + (-0 \cdot a) = (0 + 0) \cdot a + (-0 \cdot a) = 0 \cdot a + 0 \cdot a + (-0 \cdot a) = 0 \cdot a$$

and similarly $a \cdot 0 = 0$. □

Exercise 4. Let a, b be positive integers. Let g be the greatest common divisor of a and b. Show that $g = ax + by$ for some $x, y \in \mathbb{Z}$.

Proof. Let $I = \{ax + by : x, y \in \mathbb{Z}\}$. For any $ax + by, ax' + by' \in I$, $ax + by + ax' + by' = a(x + x') + b(y + y') \in I$. $(ax + by)(ax' + by') = a(axx' + bxy' + aby) + by' \in I$. $0 = a \cdot 0 + b \cdot 0 \in I$. Hence I is an ideal.

Then $I = n\mathbb{Z}$ for some $n \geq 0$ by Theorem 15. Then $n = ax_n + by_n$ for some $x_n, y_n \in \mathbb{Z}$ which implies $g \mid n$. But as $a, b \in n\mathbb{Z}$, we have $n \mid a$ and $n \mid b$, and so $n \leq g$. Thus $n = g$ and $I = g\mathbb{Z}$. Therefore $g = ax + by$ for some $x, y \in \mathbb{Z}$ □

Exercise 5. If $x, y, n \in \mathbb{Z}$ and $n > 0$, then $x \equiv y \mod n$ means $x - y \in n\mathbb{Z}$. Show that $\equiv$ is an equivalence relation

Proof. $x - x = 0 \in n\mathbb{Z}$, therefore $x \equiv x$.

If $x \equiv y$, then $x - y \in n\mathbb{Z}$ and hence $y - x = (-1)(x - y) \in n\mathbb{Z}$.

If $x \equiv y$ and $y \equiv z$, then $x - y, y - z \in n\mathbb{Z}$. There is $a, b \in \mathbb{Z}$ such that $x - y = na$ and $y - z = nb$. Since $x - z = (x - y) + (y - z) = n(a + b) \in n\mathbb{Z}$, $x \equiv z$ □

Exercise 6. Suppose that $x \equiv x' \mod n$ and $y \equiv y' \mod n$. Show that $xy \equiv x'y' \mod n$

Proof. There is $a, b \in \mathbb{Z}$ such that $x - x' = an$ and $y - y' = bn$. We have $x' = x - an$, $y' = y - bn$ and $x'y' = xy + n(abn - bx - ay)$. Hence $x'y' - xy \in n\mathbb{Z}$ □

Exercise 7. Suppose that p is a prime and $x \not\equiv 0 \mod p$. Show that there is y s.t. $xy \equiv 1 \mod p$

Proof. Since $x \not\equiv 0 \mod p$, $p \nmid x$ and so x and p is coprime and there is $m, n \in \mathbb{Z}$ such that $mx + pn = 1$. Thus $mx - 1 \in p\mathbb{Z}$ and so $mx \equiv 1 \mod p$ □