Math 570: Mathematical Logic HOMEWORK 7 **Due: Nov 2–3**

1. Let K be a field and let $\overline{K}$ be an algebraic closure of K. A nonconstant polynomial $f \in K[X_1, \dots, X_n]$ is called *irreducible over* K if whenever $f = g \cdot h$ for some $g, h \in K[X_1, \dots, X_n]$, either $\deg(g) = 0$ or $\deg(h) = 0$. Furthermore, f is called *absolutely irreducible* if it is irreducible over $\overline{K}$.

For example, the polynomial $X^2 + 1 \in \mathbb{R}[X]$ is irreducible over $\mathbb{R}$, but it is not absolutely irreducible since $X^2 + 1 = (X + i)(X - i)$ in $\mathbb{C}[X]$. On the other hand, $XY - 1 \in \mathbb{Q}[X, Y]$ is absolutely irreducible.

Denoting $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, prove the following:

Theorem (Noether-Ostrowski Irreducibility Theorem). *For $f \in \mathbb{Z}[X_1, \dots, X_n]$ and prime p, let f_p denote the polynomial in $\mathbb{F}_p[X_1, \dots, X_n]$ obtained by applying the canonical map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ to the coefficients of f (i.e. modding out the coefficients by p). For all $f \in \mathbb{Z}[X_1, \dots, X_n]$, f is absolutely irreducible (as an element of $\mathbb{Q}[X_1, \dots, X_n]$) if and only if for sufficiently large primes p, f_p is absolutely irreducible (as an element of $\mathbb{F}_p[X_1, \dots, X_n]$).*

HINT: Coming up with a proof should be easier than understanding the statement of the problem.

REMARK: The original algebraic proof of this theorem is quite involved!

2. Let $\sigma := (E)$, where E is a binary relation symbol.

(a) Define a theory T whose models are exactly the σ-structures in which E is an equivalence relation with exactly one equivalence class of size n, for each natural number $n \geq 1$.

(b) How many countable models does T have (up to isomorphism)?

(c) How many models of cardinality $\aleph_1$ does T have (up to isomorphism)?

CAUTION: This question is easy but tricky. Look at your solution with a critical eye.

(d) Show that the model $\boldsymbol{M}_\omega$ of T that is countable and has infinitely many infinite equivalence classes is *elementarily universal* among countable models, i.e. for every other countable model $\boldsymbol{N} \models T$, $\boldsymbol{N} \hookrightarrow_e \boldsymbol{M}_\omega$.

HINT: Use the proof of upward Löwenheim–Skolem to build a countable elementary extension of $\boldsymbol{N}$ with the additional requirement of having infinitely-many infinite equivalence classes. Then wake up and realize that what you have built is $\boldsymbol{M}_\omega$.

(e) Is T complete? Prove your answer.

3. Review the sketch of Gödel's proof of the Incompleteness theorem and be ready to present it on the board.

4. Prove that Tarski's theorem that $\mathrm{Th}(\boldsymbol{N})$ is not arithmetical (Theorem 5.5 in the current version of the notes) is equivalent to the Fixed Point lemma for $\boldsymbol{N}$ (Lemma 5.4). Don't just say "well, both are true and hence equivalent"; instead, using one as a black box, deduce the other, and vice versa.

5. Review the quine we wrote in class. Explain why it is indeed a quine and what makes this possible.

6. Primitive recursion. Let $g : \mathbb{N}^k \to \mathbb{N}$ and $h : \mathbb{N}^k \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. We say that $f : \mathbb{N}^k \times \mathbb{N} \to \mathbb{N}$ is defined by *primitive recursion* from g, h if for all $\vec{a} \in \mathbb{N}^k$ and $n \in \mathbb{N}$,

$$f(\vec{a}, 0) = g(\vec{a})$$
$$f(\vec{a}, n+1) = h(\vec{a}, n, f(\vec{a}, n))$$

(a) Show that $n \mapsto 2^n$ is defined by primitive recursion from the constant 1 function and doubling function. Give a couple more examples.

(b) **Dedekind's analysis of recursion.** Assuming that f is defined by primitive recursion from g, h as above, complete the statement below (replace the dots with a statement) and prove it: for each $\vec{a} \in \mathbb{N}^k, n \in \mathbb{N}$, and $m \in \mathbb{N}$,

$$\begin{aligned} f(\vec{a}, n) = m \text{ if and only if there is } \vec{b} \in \mathbb{N}^{<\mathbb{N}} \text{ such that } |\vec{b}| = n+1& \\ \text{and } \vec{b}(0) = g(\vec{a})& \\ \text{and for each } i < n+1, \ldots& \\ \text{and } \vec{b}(n) = m.& \end{aligned}$$

We refer to this $\vec{b}$ as the *certificate* verifying that indeed $f(\vec{a}, n) = m$. For example, $(1, 2, 4, 8, 16, 32)$ is the certificate for $2^5 = 32$.

(c) Suppose that there is an arithmetical function (i.e. definable in $(\mathbb{N}, 0, S, +, \cdot)$) $\beta : \mathbb{N}^2 \to \mathbb{N}$ such that for each $\vec{b} \in \mathbb{N}^{<\mathbb{N}}$ there is a "code" $w \in \mathbb{N}$ such that for each $i < |\vec{b}|$, $\beta(w, i) = \vec{b}(i)$ (such a function indeed exists and is called *Gödel's coding function*). Prove that if f is defined by primitive recursion from arithmetical functions g, h, then f is again arithmetical.