MATH 570: MATHEMATICAL LOGIC

HOMEWORK 7

Due date: Oct 13 (Tue)

1. Let K be a field and let $\overline{K}$ be an algebraic closure of K. A nonconstant polynomial $f \in K[X_1, ..., X_n]$ is called *irreducible over* K if whenever $f = gh$ for some $g, h \in K[X_1, ..., X_n]$, 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.

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and prove the following:

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

HINT: Your proof should be shorter than the statement of the problem.

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

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

(a) Define a theory T whose models are exactly the τ-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)?

(d) Show that the model $\mathbf{M}_\omega$ 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 $\mathbf{N} \models T$, $\mathbf{N} \hookrightarrow_e \mathbf{M}_\omega$.

HINT: Use the proof of upward Löwenheim–Skolem to build an elementary extension of $\mathbf{N}$ with the additional requirement of having infinitely many infinite equivalence classes. Then, wake up, and realize that there is only one (up to isomorphism) such model.

(e) Is T complete? Prove your answer.

3. [Informal[1]] Give your best shot at answering the following questions using your knowledge/intuition/experience with programming. Below, let τ be a finite signature.

(a) Is there an algorithm/program recognizing the axioms of $\mathbb{FOL}(\tau)$? That is, an algorithm that takes as input a finite $\mathbb{FOL}(\tau)$-word w and outputs `yes` if and only if w is an axiom of $\mathbb{FOL}(\tau)$.

(b) Is there an algorithm/program recognizing PA? (In the same sense as in part (a).)

(c) Let T be a τ-theory that can be recognized by a program. Is there an algorithm/program that recognizes proofs from T? That is, given a finite sequence $(w_i)_{i<n}$ of $\mathbb{FOL}(\tau)$-words, it outputs `yes` if and only if $(w_i)_{i<n}$ is a proof from T.

[1] You don't have to write this up, but still have to think through and discuss in the problem sessions.

(d) For a τ-theory T, let $\mathsf{Provable}(s)$ denote the unary relation on the $\mathbb{FOL}(\tau)$-words defined as follows: for an $\mathbb{FOL}(\tau)$-word w

$$\mathsf{Provable}(w) \iff w \text{ is a } \tau\text{-sentence and } T \vdash w.$$

In other words, $\mathsf{Provable}(w)$ holds if and only if there exists a proof $(w_i)_{i<n}$ of w from T. Assuming that T can be recognized by a program, do you think it is always possible to write a program implementing this unary relation? If yes, what would it be (roughly)? If no, what is a potential issue?