Math 114L, Spring 2021, Solutions to HW #5

---

x2.8. Prove that for every structure $\mathbf{A}$, the identity $\sigma(x) = x$ on A is an automorphism—the *trivial* one. Prove also that the structure $\mathbf{N}$ of arithmetic has no other automorphisms—it is *rigid*.

Solution. To prove that $\mathrm{id} : \mathbb{N} \to \mathbb{N}$ is an isomorphism we just need to verify that it satisfies the conditions in Section 3B, and, of course, these are all trivial

To prove that $\mathbf{N} = (\mathbb{N}, 0, S, +, \cdot)$ is rigid, we need to verify that if $\sigma : \mathbb{N} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathbb{N}$ is an isomorphism, then

$$\text{for every } n, \sigma(n) = n,$$

and we do this by induction.

Basis, $\sigma(0) = 0$. This is true because 0 is a "distinguished element" (named by the constant 0), and so it is preserved by every isomorphism.

Induction Step. Assume $\sigma(n) = n$ and compute:

$$\sigma(S(n) = S(\sigma(n)) \quad (\text{ because } \sigma \text{ preserves } S)$$
$$= S(n) \quad (\text{by the induction hypothesis}).$$

x2.14. Prove that if a binary relation $P(x, y)$ is elementary in a structure $\mathbf{A}$, then so is the *converse relation*

$$\breve{P}(x, y) \iff P(y, x).$$

Solution. If $P^2_1(x, y) = x, P^2_2(x, y) = y$ are the two projections, then

$$\breve{P}(x, y) \iff P(y, x) \iff P(P^2_2(x, y), P^2_1(x, y)),$$

and so $\breve{P}(x, y)$ is elementary in $\mathbf{A}$ by (2) and (3) of Theorem 3J.1.

x2.15. Prove that if $f(\vec{x}), g(\vec{x})$ are elementary functions in a structure $\mathbf{A}$, then so is the relation

$$P(\vec{x}) \iff f(\vec{x}) = g(\vec{x}).$$

Solution. The equality relation

$$\mathrm{Eq}(u, v) \iff u = v$$

is elementary by (1) of Theorem 3J.1, and hence so is

$$P(\vec{x}) \iff \mathrm{Eq}(f(\vec{x}), g(\vec{x})) \iff f(\vec{x}) = g(\vec{x})$$

by (3) of the same theorem.

x2.17. Determine whether the (usual) ordering relation on real numbers is elementary on the field $\mathbf{R} = (\mathbb{R}, 0, 1, +, \cdot)$, and if your answer is positive, find a formula which defines them. (You need to know something about the real numbers to do this.)

Solution. The ordering on $\mathbb{R}$ is elementary in **R**, because non-negative real numbers have square roots and this characterizes them. So

$$x \geq 0 \iff (\exists y)[x = y^2], \quad x \leq y \iff (y - x) \geq 0.$$

x2.22. Prove that the following functions and relations on $\mathbb{N}$ are arithmetical.

1. $p(i) = p_i =$ the i'th prime number, so that $p_0 = 2, p_1 = 3, p_2 = 5,$ etc.
2. $f_n(x_0, \dots, x_n) = p_0^{x_0+1} \cdot p_1^{x_1+1} \cdots p_n^{x_n+1}$. (This is a different function of $n+1$ arguments for each n.)
3. $R(u) \iff$ there exists some n and some $x_1, \dots, x_n$ such that $u = f_n(x_1, \dots, x_n)$.

Solution. 1. The function

$$h(u, i) = \text{ the least prime number which is greater than } u$$

(which disregards its second argument) is arithmetical, because its graph is arithmetical,

$$h(u, i) = w \iff u < w \wedge \text{Prime}(w) \wedge (\forall y)[(u < y \wedge \text{Prime}(y)) \rightarrow w \leq y];$$

and $p(i) = p_i$ is defined by the primitive recursion

$$p(0) = 2, \quad p(i+1) = h(p(i), i)$$

as in (4-1), and so it is arithmetical by Theorem 4A.1.

2. Here we are asked to prove that every one of the functions

$$f_0(x_0) = 2^{x_0+1},\ f_1(x_0, x_1) = 2^{x_0+1} \cdot 3^{x_1+1}, \dots$$

is arithmetical. and perhaps the simplest way is to do this by induction on n.

At the basis, let $2(x) = 2$, which is clearly arithmetical, and compute:

$$f_0(x_0) = 2^{x_0+1} = \exp(2(x), S(x)),$$

so that f_0 is arithmetical by (3) of Theorem 3J.1 and the fact that $\exp(u, v)$ is arithmetical.

At the induction step, the definition gives

$$f_{n+1}(x_0, \dots, x_n, x_{n+1}) = f_n(x_1, \dots, x_n) \cdot p_{n+1}^{x_{n+1}+1}.$$

Letting $\vec{x} = (x_0, \dots, x_n)$ to simplify notation, set

$$f_n'(\vec{x}, x_{n+1}) = f_n(P_1^{n+2}(\vec{x}, x_{n+1}), \dots, P_{n+1}^{n+2}(\vec{x}, x_{n+1})) = f_n(\vec{x});$$

the function

$$g(\vec{x}, x_{n+1}) = p_{n+1}^{x_{n+1}+1}$$

is arithmetical. by similar arguments (and recalling that p_{n+1} is just a number, like $2 = p_0$ in the basis); and finally

$$f_{n+1}(x_0, \dots, x_n, x_{n+1}) = f'_n(\vec{x}, x_{n+1}) \cdot g(\vec{x}, x_{n+1}),$$

so f_{n+1} is arithmetical by Theorem 3J.1 again, as the product of two arithmetical functions.

3. The observation here is that the numbers

$$p_0^{x_0+1} \cdot p_1^{x_1+1} \cdots p_n^{x_n+1}$$

are (easily) characterized by the fact that *if some prime p divides them, then every smaller prime $q < p$ also divides them*; but this is an arithmetical condition:

$$R(u) \iff u \geq 2 \wedge (\forall p)(\forall q)[(\text{Prime}(p) \wedge \text{Prime}(q) \wedge p \mid u \wedge q < p) \Longrightarrow q \mid u],$$

where $x \mid y$ is the divisibility relation.

x2.25. Prove that the ring of integers $\mathbf{Z}$ admits coding of tuples (Example 4B.2).

Solution. By Lagrange's Theorem (which is needed here), every natural number is the sum of four squares—and, obviously, every $x \in \mathbb{Z}$ which is the sum of four (or any number of) squares is a natural number; so we can set

$$x \in \mathbb{N}' \iff \exists x_1 \exists x_2 \exists x_3 \exists x_4 [x = x_1^2 + x_2^2 +_3^2 + x_4^2].$$

This is an elementary subset of $\mathbf{Z}$. We also let $0' = 0$, and we take $S'.+', \cdot'$ to be the restrictions to $\mathbb{N}'$ of the successor function addition and multiplication on $\mathbb{Z}$, so that $(\mathbb{N}', 0'S',, +', \cdot')$ is obviously isomorphic with $\mathbf{N}$. Moreover, these functions are elementary in $\mathbf{Z}$ (which simply means that their graphs are elementary relations in $\mathbf{Z}$), e.g.,

$$x +' y = z \iff x, y, z \in \mathbb{N}' \wedge x + y = z;$$

thus $(\mathbb{N}', 0'S',, +', \cdot')$ is a copy of $\mathbf{N}$ in $\mathbf{Z}$.

To code tuples in $\mathbf{Z}$ we use the fact that every integer is either a natural number or the negation of a natural number, and so we can code an n-tuple $(w_0, \dots, w_{n-1})$ by a natural number code of the sequence

$$(w_0, \text{sign}(w_0), \dots, w_{n-1}, \text{sign}(w_{n-1}))$$

of natural numbers, where

$$\text{sign}(w) = \begin{cases} 0, & \text{if } w \geq 0, \\ 1, & \text{otherwise.} \end{cases}$$

Let me know of errors or better solutions.

Using the β-function to code tuples of natural numbers, we set

$$\gamma(a,b,i) = \begin{cases} 0, & \text{if } a \notin \mathbb{N}' \vee b \notin \mathbb{N}' \vee i \notin \mathbb{N}', \\ \beta(a,b,2i), & \text{otherwise, if } \beta(a,b,2i+1) = 0, \\ -\beta(a,b,2i), & \text{otherwise,} \end{cases}$$

and verify easily that this function is $\mathbf{Z}$-elementary and that it codes tuples in $\mathbf{Z}$.

x2.23. The Ackermann function is defined by the following *double recursion*:

$$\begin{aligned} A(0,x) &= x+1 \\ A(n+1,0) &= A(n,1) \\ A(n+1,x+1) &= A(n,A(n+1,x)) \end{aligned}$$

1. Compute $A(1,2)$.
2. Compute $A(2,1)$.
3. Prove that the Ackermann function is arithmetical.

Solution.

1. We can compute $A(1,2)$ by applying the given equations as needed,

$$\begin{aligned} A(1,2) = A(0,A(1,1)) = A(1,1)+1 = A(0,A(1,0))+1 \\ = A(1,0)+2 = A(0,1)+2 = 2+2 = 4. \end{aligned}$$

This is messy, not systematic, and does not help much in the next part of the problem. It is better to prove the general formula

$$(*) \qquad A(1,x) = x+2,$$

which is almost immediate by induction on x: at the basis,

$$A(1,0) = A(0,1) = 1+1 = 2,$$

and at the induction step,

$$A(1,x+1) = A(0,A(1,x)) = A(1,x)+1 = (x+2)+1 = x+3.$$

Now $(*)$ gives $A(1,2) = 4$ immediately.

2. Applying (just once) the third of the given equations and $(*)$:

$$A(2,1) = A(1,A(2,0)) = A(2,0)+2 = A(1,1)+2 = 1+2+2 = 5.$$

It is also not difficult to prove by induction the general formula

$$A(2,x) = 2x+3.$$

3. This is quite difficult, in fact, and requires an analysis of the definition of $A(n,x)$; the idea is that all the values of it can be computed by applying the given equations, which we must make precise in a useful way. We give the proof in some detail.

A sequence of triples

$$\alpha = \Big((n_0, x_0, w_0), (n_1, x_1, w_1), \ldots , (n_k, x_k, w_k)\Big)$$

is an *Ackermann derivation* if one of the following conditions holds for each $i \leq k$:

(1) $n_i = 0$ and $w_i = x_i + 1$.
(2) $n_i > 0, x_i = 0$, and there is some $j < i$ such that $n_j = n_i - 1$, $x_j = 1$, and $w_i = w_j$.
(3) $n_i > 0, x_i > 0$, and there exist numbers $j, l < i$ such that

$$n_j = n_i,\ x_j = x_i,\ n_l = n_i - 1,\ x_l = w_j,\ w = w_l.$$

Intuitively, an Ackermann derivation is a "proof' that $A(n_i, x_i) = w_i$ for each triple in the derivation, and we establish this in two, simple lemmas:

Lemma 1. If α is an Ackermann derivation as above, then for each $i \leq k$, $A(n_i, x_i) = w_i$.

Proof of this is by induction on $i \leq k$, for the given Ackermann derivation.

Lemma 2. If $A(n, x) = w$, then there exists an Ackermann derivation as above such that $n_k = n, x_k = x$ and $w_k = w$.

Proof is by induction on n and within this (in the induction step) induction on x. (One uses the trivial fact that the concatenation of two Ackermann derivations is also an Ackermann derivation.)

It follows that

$$A(n, x) = w \iff \text{there exists an Ackermann derivation such that } n_k = n, x_k = x, w_k = w,$$

and from this we can get an arithmetical definition of the graph of $A(n, x)$ using the tuple-coding supplied by the β-function.

`Let me know of errors or better solutions.`