EXAM 1: TAKEHOME – SOLUTIONS

Problem 1

Define a number, x, to be *algebraic* iff there is some polynomial $x^n + q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + \ldots + q_0 = 0$ with each $q_i \in \mathbb{Q}$. For example, $\sqrt{2}$ is a algebraic number, as is any rational number, but π is not. Show that there are countably many algebraic numbers. (Feel free to use without proof the fact that any polynomial in one variable has a finite number of solutions.)

Proof. First let us count the polynomials over $\mathbb{Q}$ of degree n. As in the statement of the problem above, we only need to consider *monic* polynomials, that is polynomials with leading coefficient equal to one. However, whether you do this, or count all polynomials makes no difference to the answer.

Define a map, f, from the set of monic polynomials of degree n to $\mathbb{Q}^n$ as follows: Let $p(x)$ be the monic polynomial $x^n + q_{n-1}x^{n-1} + q_{n-2}x^{n-2} + \ldots + q_0 = 0$. $f : p(x) \mapsto (q_{n-1}, \ldots, q_0)$. Clearly this map is injective. $\mathbb{Q}$ is countable, and thus $\mathbb{Q}^n$ is countable. Thus the set of all monic polynomials of degree n is countable.

The set of all monic polynomials over $\mathbb{Q}$ is the union over $n \in \mathbb{N}$ of the sets of monic polynomials over $\mathbb{Q}$ of degree n, and a countable union of countable sets is countable.

The set of all solutions to monic polynomials is $\bigcup\{\text{solutions to } p_i\}$, where the union is taken over all monic polynomials with coeffiecients in $\mathbb{Q}$, and a countable union of finite sets is countable. □

Problem 2

(a). Let $p\mathfrak{n}q$ stand for "neither p nor q". That is, $p\mathfrak{n}q$ is true when, and only when, both p and q are false. Show that every formula in propositional logic is equivalent to one only using $\mathfrak{n}$.

Proof. I'll just note that $\neg p$ is equivalent to $p\mathfrak{n}p$, and $p \wedge q$ is equivalent to $(p\mathfrak{n}p)\mathfrak{n}(q\mathfrak{n}q)$ and leave you to confirm this with truth tables. □

(b). Suppose that p stands for "There are tickets." and q stands for "I will go to the game." Use your newfound skill with $\mathfrak{n}$ to say (i) $\neg q$, and (ii) $p \to q$ in English using only "neither ... nor" as a logical connective.

"I will not go to the game" becomes "I will neither go to the game, nor will I go to the game."

"If there are tickets I will go to the game" becomes the rather more unwieldy: $((p\mathfrak{n}p)\mathfrak{n}q)\mathfrak{n}((p\mathfrak{n}p)\mathfrak{n}q)$, which in English would be something like, "Neither (1) it is neither the case that there are neither tickets nor are there tickets nor is it the case that I will go to the game, nor (2) it is neither the case that there are neither tickets nor are there tickets, nor is it the case that I will go to the game."

Problem 3

Consider the following structure: $(\mathbb{R}, +, \cdot, <, f)$ where $+, \cdot, <$ are as normal, and f is a unary function. Express the following in first order logic (in the language of $+, \cdot, <, f$):

(a). Every positive number has a square root. Life is simpler if you first show that 0 is definable. Note that 0 is definable by the formula $\varphi(x) := \forall y, y + x = y$. Now we can use 0 as though it were in the language, and write:

$$\forall x \exists y((0 < x) \rightarrow (y \cdot y = x))$$

(b). If f is strictly monotone then f is injective.

$$(\forall x, y\,((x < y) \rightarrow (f\,(x) < f\,(y))) \vee \forall x, y((x < y) \rightarrow (f(y) > f(x)))) \rightarrow$$

$$(\forall z, w((f(z) = f(w)) \rightarrow (z = w)))$$

(c). f is continuous.

Here we first show that the function, $||$, is definable. This is a unary function, and a unary function is by definition a subset of $\mathbb{R}^2$. Let $\varphi(x, y)$ be the following formula: $y \cdot y = x \cdot x \wedge \neg(y < 0)$. Then it is easy to see that the pairs (r_1, r_2) that make φ true are precisely those of the form $(r_1, |r_1|)$. Two comments: (1) there are, of course, many other formulas that also define the absolute value function, and (2) I am being informal. Technically, I should say "Then it is easy to see that given any interpretation, $I = (\mathbb{R}, \beta)$, the only pairs r_1, r_2 such that $I\frac{r_1, r_2}{x, y} \models \varphi \ldots$

Now to say f is continuous: $\forall \epsilon, x, y, \exists, \delta((0 < \epsilon \wedge |x - y| < \delta) \rightarrow (|f(x) - f(y)| < \epsilon))$

Problem 4

(a). Find a finite collection of sentences in some language such that there is a finite model of size 1 through size n but no larger models.

Let φ_n be $\neg \exists x_0, \ldots, x_n \bigwedge_{0 \leq i < j \leq n} (x_i \neq x_j)$. In other words: "there does not exist $n+1$ distinct elements. Clearly this is true in any model of size n or smaller, and false in any larger model.

(b). Find a finite collection of sentences in some language such that there is a finite model of any even size, but no finite model of any odd size.

There are many ways to do this. For those who know some group theory, one can give the group axioms, and add the statement that there is an element of order two. Then one applies the theorem that the order of any element divides the order of the group.

Another way to do this – one that requires no prior knowledge – uses the language with a single unary function, f. Let φ_1 say $\forall x \exists y(x \neq y \wedge f(x) = f(y))$ and let φ_2 say $\forall x, y, z(f(x) = f(y) \wedge f(y) = f(z)) \rightarrow (z = y \vee z = x)$. In other words, φ_1 and φ_2 say f is precisely 2 to 1. Now assume $\mathfrak{M}$ satisfies φ_1 and φ_2. Then for each $x \in \mathfrak{M}$ there is a unique y that gets mapped to the same thing under f. Thus, $\mathfrak{M}$ has even size (if it is finite).

(c). Find a finite collection of sentences in some language such that there is a finite model of size n^2 for any n but no finite models of size m for m not a square.

Here the easiest thing to do is picture an $n \times n$ square and add enough to the language that one can force any model to look like this. I'll attempt in giving the solution to give an indication of how one might go about thinking of the problem. Thus the proof will be longer than is absolutely necessary.

A first attempt at forcing our models to look like squares might look like this: let $L := \{\pi_1, \pi_2, 0\}$, where both π_1 and π_2 are unary functions and 0 is a constant. We will think of π_1, π_2 as the projection functions onto the x-axis and y-axis respectively and we will think of 0 as the origin (although, of course, in a model they could be anything). We will try to come up with enough formulas φ_i so that they are in fact forced to behave as such in any model.

Let φ_1 be $\forall x \pi_1(\pi_2(x) = \pi_2(\pi_1(x) = 0$. That is, if you project first in one direction, then the other, you'll always end up at zero.

Let φ_2 be the following statement: $\forall x, y(\exists z_1, z_2 \pi_1(z_1) = x \wedge \pi_2(z_2) = y) \rightarrow (\exists w(\pi_1(w) = x \wedge \pi_2(w) = y) \wedge \forall w_2(\pi_1(w_2) = x \wedge \pi_2(w_2) = y) \rightarrow (w_1 = w_2)$ That is, take a point x in the image of π (which we are thinking of as the x-axis), and a point y in the image of π_2 (which we are thinking of as the y-axis). Then there is a point w such that $\pi_1(w) = x$ and $\pi_2(w) = y$. Furthermore, there is only one such point. (We think of w as (x, y).)

Now we consider whether these axioms force the model to have a square number of elements. If our model is finite then clearly the image of π_1 and the image of pi_2 must both be finite. Let's say one is size m and the other is size n. Then φ_2 says that there is a bijection between pairs in the images of π_1 and π_2 and the whole model. Thus the model must have size mn.

But can one prove that $m = n$ from the two axioms listed so far? After thinking for a while, one concludes that one cannot prove this, as one can easily come up with a model of size, say, 6, that satisfies both φ_1 and φ_2.

Now one thinks about what further axioms one can add to insure that $m = n$. After a while, one gives up (at least if "one" is me).

Instead we consider what we can add to the language to make our life easier. There is at least one clear possibliltity. We add a binary relation R to L and we add φ_3: $\forall x, y(R(x, y) \rightarrow (\exists z \pi_1(z) = x \wedge \exists w \pi(w) = y)$. That is, R is relation that holds between the image of π_1 and the image of π_2. Finally we add φ_4, which I will just state in English: For all x in the image of π_1 there is precisely one y in the image of π_2 such that $R(x, y)$, and vice versa. Now with these two additional axioms, we see that m must equal n, and we are done.

(d). Find a finite collection of sentences in some language such that there is a finite model of size p for each prime p, but no other finite models.

OK, this was hard, and you shouldn't feel bad if you didn't get it.

We work in the language with $+, \cdot, <, 0, 1, c$

Let φ_{field} be the conjunction of the field axioms i.e. addition makes the model a commutative group with identity 0, and multiplication makes the nonzero elements a commutative group with identity 1, and multiplication distributes over addition. Let φ_{order} be the conjunction of the axioms for a linear order. Add the axioms that 0 is the least element and that c is the greatest element. Finally, add the axioms that say if x is less than c, then $x + 1$ is the least element greater than x, and that if x equals c, then $x + 1 = 0$.

Now note that for each prime, p, the integers mod p with $[1] < [2] < \cdots < [p]$ form a model of the above axioms. Now we want to show that there are no other models. First we note that each element is of the form $1+\cdots+1$ for some number of 1's (since the model is finite, repeatedly adding one eventurally gets to the greatest element and we have insisted that there are no elements that lie in between x and $x+1$).

Now we should really pause and prove (by induction and the distributive law) that multiplication works like we expect (for instance that $(1+1+1)\cdot(1+1+1+1)$ equals 1 added to itself 12 times). But since this is standard proof from algebra, we skip it.

Now we note 1 added to itself a number of times equal to the size of the model is 0. If this number is not prime, and instead equals mn, the 1 added to itself m times multiplied by 1 added to itself n times will equal zero. But then these numbers will not have multiplicative inverses and the model will not be a field.

Problem 5

Fix a language L. Fix a model $\mathfrak{M}$ in the language L. Suppose that a relation R is definable in $\mathfrak{M}$, say by $\varphi(x_1, \ldots, x_n)$. Now suppose that one expands the language to $L' := L \cup R$. Let $\mathfrak{M}'$ be identical to $\mathfrak{M}$ except that it includes the new relation R. Show that for every formula σ in L' there is a formula θ using only the symbols from L such that $\mathfrak{M}' \models \sigma \leftrightarrow \theta$.

Proof. This is a straightforward proof by induction on the rank of formula.

First of all the formulas of rank 1:

(i). ψ is of the form $t_1 = t_2$.
Then ψ is already in L.

(ii). ψ is of the form $S(t_1, \ldots, t_n)$ when S is a relation in the language L.
Then ψ is already in L

(iii). ψ is of the form $S(t_1, \ldots, t_n)$ where S is a relation not in L.
Then ψ must be $R(x_1, \ldots, x_n)$, since R is the only thing in L' which is not in L. By hypothesis, $\mathfrak{M} \models R(x_1, \ldots, x_n) \leftrightarrow \varphi(x_1, \ldots, x_n)$, and φ is a formula in L. Thus φ is the θ we are looking for.

Now assume that we have proven the claim for rank $< n$.

(iv). ψ is of the form $\neg\sigma$.
Then $\mathfrak{M} \models \sigma \leftrightarrow \theta_1$ by induction. Thus $\models \neg\sigma \leftrightarrow \neg\theta_1$, and clearly $\neg\theta$ consists only of symbols from L, since θ (by induction) only uses L.

(v) and (vi). ψ is of the form $\sigma_1 \wedge \sigma_2$ or $\exists x \sigma$.
Both of these cases are the same as case (iv).

□

Problem 6

(a). Consider $\mathfrak{M} := ([0,1], <)$. Show that 0 and 1 are definable in $\mathfrak{M}$, that is, show that the set containing only 0 is definable, and that the set containing only 1 is definable.

Proof. 0 is definable by $\forall x(y < x \vee x = y)$, and 1 is definable by $\forall x(x < y \vee x = y)$ □

(b). Show that any automorphism of a model maps any definable set to itself.

It is a good idea to back to the definitions to see precisely what we have to prove. Fix a model $\mathfrak{M}$. We say that a subset, S, of M^n is definable by $\varphi(x_1, \dots, x_n)$ iff for every interpretation $I = (\mathfrak{M}, \beta)$, one has that $(a_1, \dots, a_n) \in S$ holds precisely when $I\frac{a_1,\dots,a_n}{x_1,\dots,x_n} \models \varphi$.

Thus we have to show that for an automorphism, f, and any interpretation I, we have that $I\frac{a_1,\dots,a_n}{x_1,\dots,x_n} \models \varphi$ iff $I\frac{f(a_1),\dots,f(a_n)}{x_1,\dots,x_n} \models \varphi$.

Now that we have stated clearly what we need to show, we attempt a proof. We will proceed, as usual, by induction, first on terms and then on formulas.

(i). φ is of the form $t_1 = t_2$.

When one tries to prove this, one quickly realizes that it is harder than it first seems. One has to describe the relationship between $I\frac{a}{x}(t)$ and $I\frac{f(a)}{x}(t)$. After playing around with a couple examples one comes up with the following claim: (and yes, when I realized that this claim was necessary, I felt guilty and decided to grade 6(b) rather leniently)

Lemma 0.1. *If the variables of t are contained in $x_1, \dots, x_n$, then $I\frac{f(a_1),\dots,f(a_n)}{x_1,\dots,x_n}(t) = f(I\frac{a_1,\dots,a_n}{x_1,\dots,x_n}(t))$*

Proof. To make things easier to read, I will write $I\frac{a_1,\dots,a_n}{x_1,\dots,x_n}$ as $I\frac{\vec{a}}{\vec{x}}$ and $I\frac{f(a_1),\dots,f(a_n)}{x_1,\dots,x_n}$ as $I\frac{f(\vec{a})}{f(\vec{x})}$

By induction on the rank of t. Suppose that t is c, a constant. Then any interpretation just maps the symbol "c" to the element c in M, and $f(c) = c$. Thus $f(I\frac{\vec{a}}{\vec{x}}(c)) = c = I\frac{f(\vec{a})}{\vec{x}}(c)$.

Now suppose t is x_i for $1 \leq i \leq n$. Now $I\frac{\vec{a}}{\vec{x}}(x_i) = a_i$ and $I\frac{f(\vec{a})}{\vec{x}}(x_i) = f(a_i)$. Thus we have $f(I\frac{\vec{a}}{\vec{x}}(x_i)) = f(a_i) = I\frac{f(\vec{a})}{\vec{x}}(x_i)$, as desired.

Now suppose that the claim is true for terms of rank $< n$, and t have rank n. Then $t = g(t_1, \dots, t_n)$ where $t_1, \dots, t_n$ have rank less than n and g is some function in L. Then for any interpretation $I(g(t_1, \dots, t_n)) = g(I(t_1), \dots, I(t_n))$. What does this mean in our case? Prepare yourself for a barrage of symbols:

$$f(I\frac{\vec{a}}{\vec{x}}(g(t_1, \dots, t_n)) = f(g(I\frac{\vec{a}}{\vec{x}}(t_1), \dots, g(I\frac{\vec{a}}{\vec{x}}(t_n)))$$

But remember that, by definition of automorphism, $f(g(s_1, \dots, s_n) = g(f(s_1), \dots, f(s_n))$ for any terms s_i. Thus the above is equal to

$$g(f(I\frac{\vec{a}}{\vec{x}}(t_1)), \dots, f(I\frac{\vec{a}}{\vec{x}}(t_n)))$$

Now we apply the inductive hypothesis to the above and get that it is equal to

$$g(I\frac{f(\vec{a})}{\vec{x}}(t_1), \dots, I\frac{f(\vec{a})}{\vec{x}}(t_n))$$

which, by definition is

$$I\frac{f(\vec{a})}{\vec{x}}g((t_1), \dots, (t_n))$$

which was what we were trying to prove. □

Now back to the case where φ is $t_1 = t_2$. We have to show that $I\frac{\vec{a}}{\vec{x}} \models \varphi$ iff $I\frac{f(\vec{a})}{\vec{x}} \models \varphi$. By definition, $I\frac{\vec{a}}{\vec{x}} \models \varphi$ iff $I\frac{\vec{a}}{\vec{x}}(t_1) = I\frac{f(\vec{a})}{\vec{x}}(t_2)$ which occurs iff $f(I\frac{\vec{a}}{\vec{x}}(t_1)) = f(I\frac{\vec{a}}{\vec{x}}(t_2))$ since f is a bijection. But by the lemma, $f(I\frac{\vec{a}}{\vec{x}}(t)) = I\frac{f(\vec{a})}{\vec{x}}(t)$. Thus $I\frac{f(\vec{a})}{\vec{x}}(t_1) = I\frac{f(\vec{a})}{\vec{x}}(t_2)$ which is what it means for $I\frac{f(\vec{a})}{\vec{x}}$ to satisfy φ.

$I\frac{f(\vec{a})}{\vec{x}}$

(ii). φ is of the form $R(t_1, \ldots, t_n)$.

We must show that $I\frac{\vec{a}}{\vec{x}} \models \varphi$ iff $I\frac{f(\vec{a})}{\vec{x}} \models \varphi$. By definition, $I\frac{\vec{a}}{\vec{x}} \models \varphi$ iff $R(I\frac{\vec{a}}{\vec{x}}(t_1), \ldots, I\frac{\vec{a}}{\vec{x}}(t_n))$ holds in $\mathfrak{M}$. By the definition of automorphism, $R(I\frac{\vec{a}}{\vec{x}}(t_1), \ldots, I\frac{\vec{a}}{\vec{x}}(t_n))$ holds iff $R(f(I\frac{\vec{a}}{\vec{x}}(t_1)), \ldots, f(I\frac{\vec{a}}{\vec{x}}(t_n)))$. By the lemma, this is just the same as $R(I\frac{f(\vec{a})}{\vec{x}}(t_1), \ldots, I\frac{f(\vec{a})}{\vec{x}}(t_n))$ holding in $\mathfrak{M}$, which in turn is the definition of $I\frac{f(\vec{a})}{\vec{x}} \models \varphi$

(iii). φ is of the form $\neg\psi$

$I\frac{\vec{a}}{\vec{x}} \models \neg\psi$ iff it is not the case that $I\frac{\vec{a}}{\vec{x}} \models \psi$ iff (by induction) it is not the case that $I\frac{f(\vec{a})}{\vec{x}} \models \psi$.

(iv). φ is of the form $\psi_1 \wedge \psi_2$

This works just like the previous case.

(v). φ is of the form $\exists y \psi(y, x_1, \ldots, x_n$

Again, just like case (iii).

(c). Show that 0 and 1 are the only definable elements in $\mathfrak{M}$

For this one just needs to play around with some maps from M to M until one finds a useful automorphism. For instance, let f be defined as $f : x \mapsto x^2$. It is easy to check that this maps $[0, 1]$ to $[0, 1]$ and preserves order, and hence is an automorphism. But it is also clear that only 0 and 1 are fixed by f. Thus by (b), 0 and 1 are the only definable elements.