

## THINGS TO KNOW FOR THE IN CLASS EXAM

The in-class part of the exam will ask you to provide a combination of definitions and proofs of theorems. The theorems that you should know will come mostly from the first section of the class on cardinality. The harder definitions will come mostly from the second part of the class on first order logic.

To remind you of something which is probably obvious: The list of definitions and theorems are short enough that you can just memorize them by rote. You could do worse things (like not learn them at all), but over the long term you'll learn them better if you understand them, rather than memorize them. This is probably especially true of the definitions. Everything we do in class will build upon the definitions that we've already introduced, and if you haven't internalized the old definitions, following lectures will grow progressively harder as the semester goes on..

### 1. DEFINITIONS

You should know the definitions of injection, surjection, bijection, what it means to say  $|A| \leq |B|$ , and what it means for a set to be countable. You should know how to define a formula in propositional logic, and how to define terms and formulas in first order logic. Given a language  $L$ , you should be able to say what an  $L$ -structure is, and what it means for an  $L$ -structure to satisfy a formula in first order logic. Note that this will involve knowing what an interpretation is. You should be able to say what it means to say  $\phi \models \psi$ .

**injection:**  $f : A \rightarrow B$  is an *injection* iff for all  $a_1, a_2 \in A$ ,  $f(a_1) = f(a_2)$  implies  $a_1 = a_2$

**surjection:**  $f : A \rightarrow B$  is a *surjection* iff for all  $b \in B$  there is some  $a \in A$  such that  $f(a) = b$ .

**bijection:**  $f : A \rightarrow B$  is a *bijection* iff it is a surjection and an injection.

$|A| \leq |B|$ :  $|A| \leq |B|$  iff there is an injection  $f : A \rightarrow B$

**countable:** A set  $A$  is *countable* iff  $|A| \leq |\mathbb{N}|$ , that is, iff there is an injection from  $A$  to  $\mathbb{N}$

**formulas in propositional logic:** We define formulas in propositional logic inductively, using propositional letters  $\{p, q, r, \dots\}$ , logical connectives  $\wedge, \vee, \rightarrow, \leftrightarrow, \neg$ , and parentheses:

- (1): A propositional letter is a formula
- (2): If  $\varphi_1$  and  $\varphi_2$  are formulas, then so is
  - (a):  $(\varphi_1 \rightarrow \varphi_2)$
  - (b):  $(\varphi_1 \wedge \varphi_2)$
  - (c):  $(\varphi_1 \vee \varphi_2)$
  - (d):  $(\varphi_1 \leftrightarrow \varphi_2)$
  - (e):  $\neg\varphi$

**For the remaining definitions in this section, we first fix a particular language,  $L$ .** That is, we work with a fixed set of relations  $\{R_i\}$ , functions  $\{f_j\}$ , and constant symbols  $\{c_k\}$ .

**Terms in first order logic:**

- (i): Each constant is a term.
- (ii): Each variable is a term
- (iii): If  $f$  is a  $n$ -ary function, and  $t_1, \dots, t_n$  are terms, then  $f(t_1, \dots, t_n)$  is a term.

**formulas in first order logic:**

- (i): If  $t_1$  and  $t_2$  are terms, then  $t_1 = t_2$  is a formula.
- (ii): If  $R$  is an  $n$ -ary relation, and  $t_1, \dots, t_n$  are terms, then  $R(t_1, \dots, t_n)$  is a relation.
- (iii): If  $\varphi$  and  $\psi$  are formulas, then so is  $\varphi \wedge \psi$ .
- (iv): likewise for  $\vee, \rightarrow, \leftrightarrow$ .
- (v): If  $\varphi$  is a formula, then so is  $\neg\varphi$ .
- (vi): If  $\varphi$  is a formula, then so is  $\exists x\varphi$
- (vii): If  $\varphi$  is a formula, then so is  $\forall x\varphi$

**an  $L$ - structure.** An  $L$ -structure,  $\mathfrak{M}$ , is a tuple  $(M, \{R_i\}, \{f_j\}, \{c_k\})$  where  $M$  is a set (called the *universe* of the structure) and each  $R_i$  is a relation on  $M^n$  (where  $n$  is the arity of  $R_i$ ),  $\{f_i\}$  is a collection of functions defined on tuples from  $M$ , and  $\{c_k\}$  is a collection of elements of  $M$ . These correspond to the relations, functions, and constants in the language,  $L$ .

Note that a *model in the language  $L$*  is the same thing as an  $L$ -structure.

**interpretation.** An *interpretation*,  $I$ , is a pair  $(\mathfrak{M}, \beta)$  such that  $\mathfrak{M}$  is a model, and  $\beta$  is a map from the set of variables to  $M$ , the universe of  $\mathfrak{M}$ . Intuitively, an interpretation is a decision about what element of  $M$  each of the variables is going to stand for.

Also we will make the definition that  $I \frac{m}{x}$  is the interpretation obtained by changing  $\beta$  so that  $\beta(x) := m$  and leaving everything else the same.

$I \models \varphi$ . Throughout this definition we will assume that  $I = (\mathfrak{M}, \beta)$ .

First one should note that it easy to extend  $\beta$  from a map defined on all of the variables, to a map defined on all of the terms. We do this inductively as follows: if  $x$  is a variable, we let  $I(x) = \beta(x)$ . If  $c$  is a constant, then  $I(c)$  is the constant  $c$  as an element of  $M$  (rather than as a symbol in the language). And finally, if  $t = f(t_1, \dots, t_n)$ , then  $I(t) := f(I(t_1), \dots, I(t_n))$ .

Now we can define inductively  $I \models \varphi$ .

- (i).  $\varphi$  is  $t_1 = t_2$ : In this case  $I \models \varphi$  iff  $I(t_1) = I(t_2)$ .
- (ii).  $\varphi$  is  $R(t_1, \dots, t_n)$ : In this case  $I \models \varphi$  iff the relation  $R$  holds in  $\mathfrak{M}$  of  $(I(t_1), \dots, I(t_n))$ .
- (iii).  $\varphi$  is  $\neg\psi$ : In this case  $I \models \varphi$  iff it is not the case that  $I \models \psi$ .
- (iv).  $\varphi$  is  $\psi_1 \wedge \psi_2$ : In this case  $I \models \varphi$  iff  $I \models \psi_1$  and  $I \models \psi_2$ .
- (v).  $\varphi$  is  $\exists x\psi$ : In this case  $I \models \varphi$  iff there is some  $m$ , such that  $I \frac{m}{x} \models \psi$
- (vi).  $\varphi$  is  $\forall x\psi$ : In this case  $I \models \varphi$  iff for all  $m$  in  $M$ ,  $I \frac{m}{x} \models \psi$ .

$M \models \varphi$ : We say that an  $L$  structure  $\mathfrak{M} \models \varphi$  iff whenever  $I$  is an interpretation of the form  $(\mathfrak{M}, \beta)$ , that  $I \models \varphi$ .

$\psi \models \varphi$ : We say that  $\psi \models \varphi$  iff whenever  $\mathfrak{M} \models \psi$  then  $\mathfrak{M} \models \varphi$ .

## 2. THEOREMS

You should know how to prove that  $\mathbb{N}^k$  is countable, and how to prove that the real numbers are uncountable. You should know how to prove that the power set of a set is bigger than the set itself.

The theorem about the power set is in the handout.

**Theorem 2.1.**  $\mathbb{N}^k$  is countable.

*Proof.* In class we did this by induction. One can also do it as follows. Let  $p_1, \dots, p_k$  be  $k$  distinct primes. Define  $f : \mathbb{N}^k \rightarrow \mathbb{N}$  by  $f : (n_1, \dots, n_k) \mapsto p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$ . Since prime decomposition is unique, this map is injective.  $\square$

**Theorem 2.2.**  $\mathbb{R}$  is uncountable.

*Proof.* One may do this by diagonalization, as in class. Here I give a different proof. We have shown that the power set of the natural numbers. Thus, giving an injection from the power set of  $\mathbb{N}$  to  $\mathbb{R}$  will suffice to show that  $\mathbb{R}$  is uncountable.

Note that one may assign a subset of  $\mathbb{N}$  a sequence of one's and zero's in the following fashion: let the  $n$ th digit in the string be a one if  $n$  is in the subset and a zero otherwise. For example the set of even numbers is assigned the sequence  $(0, 1, 0, 1, 0, 1, \dots)$  and the set  $\{3, 1, 4\}$  is assigned the sequence  $(1, 0, 1, 1, 0, 0, 0, \dots)$ .

Note that this defines an injection from the power set of  $\mathbb{N}$  to the set of infinite sequences of one's and zero's. For take  $S_1$  and  $S_2$  different subsets of  $\mathbb{N}$ . Since they are different there must be some  $n$  in one and not in the other. But then the two sequences will differ in the  $n$ th place. In fact it defines a bijection, but we only need that it's an injection.

Now simply map the sequence of one's and zero's to the real numbers by putting a decimal point in front of the sequence. The same argument as above shows that this is an injection.  $\square$

## 3. ADDITIONAL DEFINITIONS

You don't need to know these for the in-class part of the exam, but they will come up on the take home section, so I thought I'd add them here.

**definable:** Fix a model  $\mathfrak{M}$  in language  $L$ . We say that a subset  $D \subseteq M^n$  (where  $M$  is the universe of  $\mathfrak{M}$ ) is *definable* iff there is a formula  $\varphi(x_1, \dots, x_n)$  in the language  $L$ , such that for every interpretation  $I = (\mathfrak{M}, \beta)$ , one has  $I \frac{d_1, \dots, d_n}{x_1, \dots, x_n} \models \varphi$  precisely when  $(d_1, \dots, d_n)$  is in  $D$ .

**Example 3.1.** Let  $\mathfrak{M} := (\mathbb{N}, +)$ , and let  $D$  be the set of numbers divisible by 5. Then  $D$  is definable by the formula  $\varphi(x) := \exists y(y + y + y + y + y = x)$ .

We say that an  $n$ -ary relation  $R$ , (as a subset of  $M^n$ ) is definable by  $\varphi(x_1, \dots, x_n)$  iff the subset of elements satisfying the relation is a definable subset. That is, for every interpretation  $I = (\mathfrak{M}, \beta)$ , one has that  $R(a_1, \dots, a_n)$  holds precisely when  $I \frac{a_1, \dots, a_n}{x_1, \dots, x_n} \models \varphi$ .

**Example 3.2.** *The unary relation  $R(x)$  on the natural numbers that holds of  $n$  iff  $n$  is divisible by five is definable in  $(\mathbb{N}, +)$  by  $\exists y(y + y + y + y + y = x)$ . Intuitively, this means that if you add  $R(x)$  to your language, forming the model  $(\mathbb{N}, +, R)$ , you won't say anything in the new language you couldn't say before: it's just an abbreviation for  $\exists y(y + y + y + y + y = x)$ .*

**isomorphism:** Let  $\mathfrak{M}$  and  $\mathfrak{N}$  both be  $L$ -structures. An *isomorphism*,  $g$ , between  $\mathfrak{M}$  and  $\mathfrak{N}$  is a bijection between  $M$  and  $N$ , the universes of the two models, such that  $g$  preserves relations, functions, and constants in the following three ways:

- (1). Say  $R$  is a relation in  $L$ . Then  $R(m_1, \dots, m_n)$  holds in  $\mathfrak{M}$  iff  $R(g(m_1), \dots, g(m_n))$  is true in  $\mathfrak{N}$ ,
- (2). if  $f$  is a function in  $L$ , then  $g(f(m)) = f(g(m))$ , and
- (3). if  $c$  is a constant in  $L$ , then  $g(c) = c$ .

**automorphism:** An automorphism of  $\mathfrak{M}$  is an isomorphism from  $\mathfrak{M}$  to itself.