# 1 Three important announcements

## 1.1 Change in office hours

From now, my office hours on Wednesday are going to be: 1:20 to 2:50 pm. The Monday office hours remained unchanged, 1:00 to 2:30 pm.

## 1.2 Change in due date for Homework No. 2

Homework no. 2 should be handed in on Monday February 6, rather than on Wednesday February 1.

## 1.3 Trouble with Homework No. 1

More than half of the students had Homework No. 1 marked "unacceptable" and will get it back unread. The reason is that the students violated the rules clearly specified in the notes, page 6. **Please do not make this mistake again!**

# 2 Homework assignment no. 3, due on Wednesday February 8

1. Book, Exercises 1.4. (pages 37-38-39): Problems 6(a)(b)(e), 7(g)(i)(j)(k), 11(b).

2. Book, Exercises 1.5. (pages 44-45-46): Problems 3(f)(g)(h), 6(a)(d), 9, 10, 12(a)(c)(d).

3. Do the parsing problems stated on Page 36 of the notes. That is, parse the three boxed sentences of page 35.

# 3 The rules for formal proofs

A ***formal proof*** is a list of ***steps***, each one of which consists of a ***statement*** (i.e., a closed sentence) accompanied with a ***justification***. The justification of a step consists of a reason showing why the statement in that step follows

according to the rules), given the previous steps. The last step of a proof is called the ***conclusion***.

To ***prove*** a statement $S$ using certain ***input statements*** means ***to produce a proof whose conclusion is*** $S$, in which each step is either an input statement or follows by the ***rules of inference***.

So, to be able to write a proof, one needs to know which are the input statements and which are the rules of inference.

## 3.1 Which statements are valid input statetements?

The following are input statements that can be brought into a proof at any time.

(V.a) ***axioms*** (also known as "postulates");

(V.b) ***definitions***;

(V.c) the ***hypotheses***.

(V.d) In addition, it is always permitted to start a proof within a proof by introducing any sentence you want as an assumption (for example, "Assume pigs can fly"), or by declaring a ***new*** letter to have a particular value, which may be arbitrary. (For example, one step can read: "let $a = \sqrt{3}$", or "let $a$ be arbitrary") or by introducing a new object characterized by a property and giving it a name ("pick $a$ such that $a^2 = 3$", or "let $a = 5$"). However, whatever is proved after this is done is only valid in the "proof within a proof", and one can only get out of it by applying one of the rules that tell us how to get out from a proof within a proof and go back to the main proof. (The rules that allow us to do this are: Rules 2, 8, 12, and 13.)

***Remark.*** The issue of proofs within proofs For example, if you assume that "pigs can fly", as you are certainly permitted to do, then you can prove things under this assumption. For example, you may be able to prove that "pigs have wings." However, you cannot just claim that you have proved that pigs have wings. ***You have only proved that pigs have wings under the assumption that pigs can fly.*** That is, you proved that pigs have wings in an imaginary world in which pigs can fly. Does that enable us to say something about the real world? Yes, it does, but what we can say is very little. Rule $\Longrightarrow_{in}$ will enable to conclude, for the "real world", that "if

pigs can fly then pigs have wings." You still cannot conclude that pigs have wings, since you do not know that pigs can fly. (If you knew that, you could use Rule $\Longrightarrow_{out}$ to infer that pigs have wings.)

## 3.2 The fourteen basic rules of inference.

Here are the basic rules of inference. You will see that there are exactly ***fourteen*** of them. We could get away with fewer rules but these fourteen rules are very easy to remember, so I very much prefer to have them this way.

**RULE 1.** (***The tautology proof rule***.) You are allowed to bring in any statement which is an instance of a tautology.

**RULE 2.** (The ***proof by contradiction*** rule.) If, assuming $\sim P$, you get to $C$, and $C$ is an instance of a contradiction, then you can go to $P$.

$$\frac{\begin{array}{l}\text{Assume } \sim P \\ \quad \vdots \\ C \qquad [contradiction]\end{array}}{P}$$

**RULE 3.** (Rule $\vee_{use}$, a.k.a. ***proof by cases***.) If you have $P \vee Q$ and $P \Rightarrow R$ and $Q \Rightarrow R$ then you can go to $R$:

$$\frac{\begin{array}{l}P \vee Q \\ P \Rightarrow R \\ Q \Rightarrow R\end{array}}{R}$$

**RULE 4.** (Rule $\vee_{get}$.) (a) If you have $P$ then you can go to $P \vee Q$; (b) if you have $Q$ then you can go to $P \vee Q$:

$$\frac{P}{P \vee Q} \qquad \text{and} \qquad \frac{Q}{P \vee Q}$$

**RULE 5.** (Rule $\wedge_{use}$.) (a) If you have $P \wedge Q$ then you can go to $P$; (b) if you have $P \wedge Q$ then you can go to $Q$:

$$\frac{P \wedge Q}{P} \qquad \text{and} \qquad \frac{P \wedge Q}{Q}$$

**RULE 6.** (Rule $\wedge_{get}$.) If you have $P$ and $Q$ then you can go to $P \wedge Q$.

$$\frac{\begin{array}{l} P \\ Q \end{array}}{P \wedge Q}$$

**RULE 7.** (Rule $\Rightarrow_{use}$, also called ***Modus Ponens***.) If you have $P$ and $P \Rightarrow Q$ then you can go to $Q$:

$$\frac{\begin{array}{l} P \Rightarrow Q \\ P \end{array}}{Q}$$

**RULE 8.** (Rule $\Rightarrow_{get}$.) If you have started a proof within a proof by assuming $P$, and have proved $Q$, then you can get out of the proof within a proof and go back to the main proof with $P \Longrightarrow Q$:

$$\frac{\begin{array}{l} \text{Assume } P \\ \quad \vdots \\ Q \end{array}}{P \Rightarrow Q}$$

**RULE 9.** (Rule $\Leftrightarrow_{use}$.) If you have $P \Leftrightarrow Q$ then (a) you can go to $P \Rightarrow Q$; (b) you can go to $Q \Rightarrow P$.

$$\frac{P \Leftrightarrow Q}{P \Rightarrow Q} \qquad \text{and} \qquad \frac{P \Leftrightarrow Q}{Q \Rightarrow P.}$$

**RULE 10.** (Rule $\Leftrightarrow_{get}$.) If you have $P \Rightarrow Q$ and $Q \Rightarrow P$ then you can go to $P \Leftrightarrow Q$:

$$\frac{\begin{array}{l} P \Rightarrow Q \\ Q \Rightarrow P \end{array}}{P \Leftrightarrow Q:}$$

*In the following four rules,*

- *$x$ is a variable,*
- *$P$ is a sentence which contains no quantifier involving the variable $x$,*
- *$a$ is a symbol such as a letter or numeral,*
- *$P(x \to a)$ is what you get from $P$ by substituting $a$ for $x$ in **all** the occurrences of $x$ in $P$. (For example, $P$ could be something like $x^2 + 2x \geq -1$, and $a$ could be $3$, in which case $P(x \to a)$ is $3^2 + 2 \cdot 3 \geq -1$.)*

**RULE 11.** (Rule $\forall_{use}$, a.k.a. the ***specialization rule***. If $a$ is a constant whose value has been declared before, and you have $(\forall x)P$, then you can go to $P(x \to a)$. (Example: if you have $(\forall x)(x \in \mathbb{R} \Rightarrow x^2 + 2x \geq -1)$, and you have said before "let $a = 3$" or "let $a$ be arbitrary", then you can go to $a \in \mathbb{R} \Rightarrow a^2 + 2a \geq -1$).)

**RULE 12.** (Rule $\forall_{get}$.) ***Suppose the letter $a$ has not appeared before***. Then you can start a proof within a proof by saying "Let $a$ be arbitrary." If in this proof within a proof you get to $P(x \to a)$, then you can go to $(\forall x)P$ in your main proof.

REMARK: Naturally, instead of "$a$" you could use "$b$," or "$z$," or "$\alpha$," or "$\beta$," or "$\aleph$," or "$\diamond$," or any symbol you want. What is important is that what you do should apply to a ***completely arbitrary*** object in our universe of discourse. Otherwise, you will not be proving that $P$ is true for ***all*** $x$. For example, it would not be O.K. to prove that $(\forall x)(x \in \mathbb{R} \Rightarrow (\exists y)y^2 = x)$ (i.e., that every real number has a real square root) by saying "Let $a$ be arbitrary. Take $a = 9$. Then $(\exists y)y^2 = a$ is true, so $a \in \mathbb{R} \Rightarrow (\exists y)y^2 = a$ is true, so $(\forall x)(x \in \mathbb{R} \Rightarrow (\exists y)y^2 = x)$." What is wrong here? What is wrong is that if $a$ is arbitrary we have no right to assume that $a = 9$. For all we know, $a$ could be 8, or 7, or $-22$, or any other real number. Our CAT (creator of arbitrary things) will immediately prove us wrong, by picking $x$ to be another

**RULE 13.** (Rule $\exists_{use}$.) ***Suppose that the letter $a$ has NOT appeared before. Suppose you have proved*** $(\exists x)P$. Then

you can start a proof within a proof by introducing a new object, calling it $a$, and stipulating that $P(x \to a)$. This effectively declares $a$ to be a constant, locally, within the "proof within a proof." If you ever get to something that does *not* contain $a$, then you can use it outside your proof within a proof, in the main proof.

REMARK: **It is important that the new object be given a name that has not been used before.** For example, suppose $P$ stands for "$x$ killed Polonius," and our universe of discourse is the set of all people. Suppose you are told that $(\exists x)P$, i.e. that somebody killed Polonius. Then you can introduce a name for this individual. You can call him/her $a$ or, if you prefer, "the killer," in which case you would be able to say that $P(x \to a)$, i.e., that $a$ killed Polonius. But you cannot say "let's call this person Hamlet," or "let's call him Laertes," because Hamlet and Laertes are names of characters that have already appeared in the play. If you call the killer "Hamlet" or "Laertes" then you would be *prejudging*, and declaring that $P(x \to \text{Hamlet})$, i.e. that Hamlet killed Polonius, or that $P(x \to \text{Laertes})$, i.e. that Laertes killed Polonius. One of these happens to be true, and the other one is false, but in either case you cannot just conclude that it is true by merely choosing a name for the killer.)

**RULE 14.** (Rule $\exists_{get}$, a.k.a. ***the witness rule***.) From $P(x \to a)$ you can go to $(\exists x)P$.

REMARK: Here is an example. Suppose we are working in $\mathbb{Z}$, and you want to prove that $(\exists x)x^2 + 3 \cdot x = 10$. You would first show that $2^2 + 3 \cdot 2 = 10$. Now, if $P$ is the formula "$x^2 + 3 \cdot x = 10$", then $P(x \to 2)$ is the formula "$2^2 + 3 \cdot 2 = 10$". So we have proved $P(x \to 2)$, and Rule $\exists_{get}$ allows us to go to $(\exists x)x^2 + 3 \cdot x = 10$.

In addition to our 14 logical rules, that have to do with the seven logical connectives, there is a rule that has to do with the equal sign.

**RULE SEE:** (The ***substitution of equals for equals*** rule) If $t$, $s$ are terms. $P$ is a statement, and $Q$ is a statement obtained from $P$ by substituting $t$ for $s$ in some or all the occurrences of $s$ in $P$, then (i) from $t = s$ and $P$ you can go to $Q$, and (ii) from $s = t$ and $P$ you can go to $Q$.