Chapter I

Post's Theorem and other Tools

A note on notation and a few "reminders": The silly symbol "☡"[†] goes at least as far back as the writings of Bourbaki.[‡]

It has been made widely accessible to authors—who like to typeset their writings themselves—through the typesetting system of Donald Knuth (known as "TEX").

I use these "road signs" as follows: A passage enclosed between two single "☡" symbols is purported to be *very noteworthy*, so please heed!

On the other hand, a passage enclosed between two *double* signs ("☡☡") comes with two meanings:

The bad news is that it is rather difficult, or esoteric, or both. The good news is that you do not *need* to understand (or even read) its contents in order to understand the sequel. It is only there in the interest of the "demanding" reader.

☡ Let us recall the notion of Γ-*theorem*. In the definition that follows we use a crucial term about ***sets***: "smallest". This term implies a *comparison*. The comparison is via the *subset relation* "$\subseteq$". Recall that for sets S and S', "$S \subseteq S'$" is short for "every member of S is also a member of S'".[§]

If we have a lot of sets $S, S', S'', S''', \ldots$, we will say that S is *smallest* among them iff it satisfies $S \subseteq X$ where X is *any* among the $S, S', S'', S''', \ldots$.

With these explanations out of the way we define a Γ-*theorem* as a member of the *smallest* ***set*** of formulas which satisfies the three conditions below:

Th1. This ***set*** contains all the formulas of Γ and all the formulas of Λ.[¶]

[†] This symbol is a stylized version of the "(dangerous) winding road" road sign.

[‡] "Nicolas Bourbaki" is the pen-name of a team of top mathematicians who are responsible for the monumental work "Éléments de Mathématique", that starts with Logic and Set Theory as the foundation, and then proceeds to extensively cover fields such as Algebra, Topology, Analysis.

[§] Thus, in particular, it is always the case that $S \subseteq S$, for any set S.

[¶] Recall that Λ denotes all the specific instances of the Axiom Schemata of Chapter 3—the so-called *logical axioms*.

Th2. If *both* A and $A \equiv B$ are in the ***set***, then so is B. We say that this *step* was *an application of Equanimity* ("Eqn1", as we call it in class, in contradistinction with "Eqn2").

Th3. If $A \equiv B$ is in the ***set***, then so is $C[p := A] \equiv C[p := B]$ *for any choice of formula C and variable p.*

We say that this *step* was *an application of Leibniz.*

We write $\Gamma \vdash A$ to indicate that A is in the set of Γ-theorems. We often say "Γ proves A" or "A is proved from Γ" (a synonym for "is proved" is "follows"), or "A is a Γ-theorem".

We write $\vdash A$ rather than $\emptyset \vdash A$. In this case we say that A is an *absolute* or *logical* theorem (i.e., one that holds in *all* of Mathematics).

A *related concept* is that of a Γ-*proof*: This is a *finite (ordered) sequence* of formulas,

$$A_1, \ldots, A_n$$

where each A_i $(i = 1, \ldots, n)$ satisfies:

Pr1. A_i is in Γ or in Λ, **or**

Pr2. A_i is the *conclusion* ("denominator") of one of the two rules (Leibniz, or Equanimity), where the *premise(s)* ("numerator(s)") has/have *already appeared to the left of A_i* in the sequence.

Hmmm. So, is the above "proof"—often called a "*Hilbert-style proof*"—*the same as* an "*Equational*" or "*Calculational*" proof? **NO!**

An Equational proof is a "special technique" (just like the techniques we have learned in trigonometry at school are "special") to prove theorems.

What **is** an Equational (also called Calculational) proof? It is a sequence of Γ-theorems of a *very restricted form*, namely, each such theorem is an equivalence $A \equiv B$ *that is supposed to be provable very easily, very directly* (how "easily" is suggested below—p.3—where we discuss annotation and format of Equational proofs). Indeed the sequence itself has *a very special form*:

$$B_1 \equiv B_2, B_2 \equiv B_3, \ldots, B_{n-2} \equiv B_{n-1}, B_{n-1} \equiv B_n \tag{1}$$

That is, one establishes *all* of the (Meta)theorems "$\Gamma \vdash B_i \equiv B_{i+1}$"[†], for $i = 1, \ldots, n-1$, hopefully *giving a good reason for the validity of each.*

At the end of all this, the transitivity (derived) rule yields (as shown in class)

$$\Gamma \vdash B_1 \equiv B_n$$

which is often all we want to establish. However, sometimes we know more: We may know that $\Gamma \vdash B_1$. We can then conclude $\Gamma \vdash B_n$ by "Eqn1". Some other

[†] Wait a minute! A few words ago I said "theorems". How come I now say "metatheorems"?

times we may know, instead, that $\Gamma \vdash B_n$. We can then conclude $\Gamma \vdash B_1$ by "Eqn2".

The usual "protocol" for writing the above Equational proof (1) is to arrange it with the help of the "conjunctional $\equiv$", that we write as "$=$", as follows:

$$\begin{aligned}
& B_1\\
= & \Big\langle \text{Reason for } \Gamma \vdash B_1 \equiv B_2\text{: Usually a proved equivalence, (may be an axiom)}\\
& \quad \text{via a single application of Leibniz, } \textbf{IF} \text{ we work on a } \textit{part} \text{ of } B_1 \text{ or } B_2 \Big\rangle\\
& B_2\\
= & \Big\langle \text{Reason} \ldots \Big\rangle\\
& \vdots\\
= & \Big\langle \text{Reason} \ldots \Big\rangle\\
& B_n
\end{aligned}$$

In summary: An Equational proof is a sequence of independent, very short *(one-step) Hilbert-style proofs, each such step (as described above) proving an equivalence.*

Equational proofs (from Γ*) are meant to be "practical tools". They are most suitable—being usually very user-friendly—towards proving* theorems, *i.e., when "doing" (or applying) Logic. However, Hilbert-style proofs have the edge when it comes to proving* Metatheorems., *i.e., studying Logic as an object of study.*

0.1 Remark. (1) It turns out (see Appendix, if interested—but you don't have to) that $\Gamma \vdash A$ *iff there is a* Γ*-proof where* A *occurs as the last (rightmost) formula.*

(2) Note the omission of the rule *transitivity* in the definitions of Γ-theorem or -proof, above. We have omitted it for theoretical convenience, since it is a *derived* rule, as you will show in Problem Set #3. This does *not* mean that you are not supposed to *use* it! On the contrary! When we are *inside* our Logic and prove theorems we are encouraged to use any/all of the tools we have available to us. However, from the *outside*, in the Metatheory, when we *study* rather than *use* our Logic, it pays to utilize the *simplest possible description* of it.

(3) Here is a simple example that suggests how to test whether you are in the Theory (here, Propositional Calculus) or in the Metatheory: "$p \equiv p$" is an (absolute, or logical) *theorem* because we can prove it *in the Theory*—we have actually done so in class/text.

On the other hand, "$\vdash p \equiv p$" is a short form for the statement "$p \equiv p$ is provable from the logical axioms alone". Propositional Logic cannot make such a "statement". It can only state *formulas*, and "$\vdash p \equiv p$" is *not* a formula. We state "$\vdash p \equiv p$" from the "outside". It also happens to be a true statement. So, it is a Metatheorem!

Since theoremhood is *defined inductively*, we can prove properties of theorems (from any Γ) *by induction on* Γ*-theorems*.

Now, induction, *in general*, is a technique for proving "properties" of *sets of objects* that have been defined (built) in a very special manner (by a so-called inductive definition, like the one we gave for formulas in class, like the one we gave for theorems earlier on in this paper).

Induction has *two* distinguished parts/steps:

Ind1. *Basis.* Here you verify the property (that may be easy, or hard—don't be fooled by the word "verify") for the *simplest* objects.

Ind2. Here you show that "*the property propagates*": That is, if in order to build an object x we have used, in *the very last building-step*, objects that (all) satisfy the property,[†] then so does x.

In practice we split **Ind2** into two sub-steps: In the first sub-step, we assume that the property holds for the *immediate predecessors* of the "complex" object x.

That is, we imagine that we *step exactly one building step back*—from x—to obtain its immediate predecessors. We then assume that the property is true for all such predecessors.

This is the Induction Hypothesis, in short, I.H.

In the second sub-step we proceed to prove that x, too, has the property.

For example, if we want to prove a property $P(x)$ of a natural number by induction on (natural) numbers, **Ind1** asks us to verify $P(0)$, i.e., for $x = 0$, the "simplest object" *in this context*. **Ind2** asks us to prove "if $P(n)$, then $P(n+1)$", since, in this context, the "immediate predecessor" of $n+1$ is n.

Again, in practice, we do this by assuming $P(n)$ for an undisclosed general fixed n (I.H.) and then proving $P(n+1)$.[‡]

We did quite a few examples in class/Problem sets in the context of WFF. To prove a property $P(x)$ for an arbitrary WFF, A, **Ind1** entailed verifying $P(A)$ for the simplest objects in the context: Namely, formulas A of the forms *true*, *false*, or p (a Boolean variable).

For **Ind2** one had to prove $P(A)$ for "complex" formulas A, on the I.H. that *the immediate predecessors of A in the building process of WFF*—that is, the *immediate subformulas* of A[§]—all satisfied $P(x)$.

► What would the technique of induction on (Γ-)theorems entail?

[†] We may well call such objects *immediate predecessors* of x.

[‡] This "splitting" of the implication, $P(n) \Rightarrow P(n+1)$, is typical in mathematical practice. It is legitimate by the Deduction Theorem (4.1 below).

[§] These "complicated A" can be of the forms $\neg D$, $D \equiv E$, $D \vee E$, $D \Rightarrow E$, $D \wedge E$. D is the immediate subformula of the first, D and E of all the other forms.

To prove that $P(x)$ holds for all Γ-theorems, **Ind1** requires that you prove $P(x)$ for the *simplest* objects in the *theorem building process*. That is, for all A in Γ and all A in Λ.

For **Ind2** you prove that $P(x)$ holds for a Γ-theorem A, *provided* it holds for its immediate predecessors (in the theorem building process).

How do we build theorems? The definition says:

(i) If $\Gamma \vdash B$ and $\Gamma \vdash B \equiv A$, then $\Gamma \vdash A$ (Equanimity application). Here B and $B \equiv A$ are immediate predecessors of A.[†]

- Thus, we must *assume* $P(B)$ *and* $P(B \equiv A)$ and prove $P(A)$.

(ii) If $\Gamma \vdash B \equiv C$ and A *is the string* $D[p := B] \equiv D[p := C]$, then $\Gamma \vdash A$ (Leibniz application). Here $B \equiv C$ is an immediate predecessor of A.

- Thus, we must *assume* $P(B \equiv C)$ and prove $P(A)$. ☡

☡☡ While immediate predecessors of an object n in the natural number building process and an object A in the WFF building process are unique, this is *not* the case in the theorem-building process. A theorem (from any Γ) need not have uniquely defined immediate predecessors. For example, I may prove A in at least two ways via Equanimity. It is possible that I have already proved B and $B \equiv A$. But it is also possible that I have also proved C and $C \equiv A$ where C is a formula *different* (as a string) than B. If this is the case, I have two (at least) sets of (immediate) predecessors of A: $\{B, B \equiv A\}$ and $\{C, C \equiv A\}$.

Still, this does not detract from the validity of the principle of induction on theorems as described above and practiced in the rest of this note. After all, step **Ind2** is "general" and never fixes attention to *specific* predecessors. For example, an argument that $P(B)$ and $P(B \equiv A)$ jointly imply the truth of $P(A)$ is (if done correctly!) *general* and *is independent of which exact formula B might be*. Such a properly applied general argument will also yield that "$P(C)$ and $P(C \equiv A)$ jointly imply the truth of $P(A)$"!

For the full justification of why the principle of induction on theorems works see the Appendix. ☡☡

1. On Γ-theorems and proofs

1.1 Lemma. *If $\Gamma \subseteq \Delta$ and $\Gamma \vdash A$, then also $\Delta \vdash A$.*

Proof. This statement is a property of Γ-theorems.[‡] We naturally (!) prove it by induction on such theorems.

Basis. Say, $A \in \Lambda$. But then $\Delta \vdash A$ (definition of Δ theorems!). Say, $A \in \Gamma$. But then $A \in \Delta$ as well, hence $\Delta \vdash A$ (definition of Δ theorems!).

[†] They are "simpler *theorems*" than A, since they are "proved earlier". Thus, "simpler" is a context-dependent concept. While, in this context, $B \equiv A$ is simpler than A, *as a theorem*, in a different context, e.g., as a *formula*, it is more complex!

[‡] In English "every Γ-theorem has the property of being a Δ-theorem".

Assume the claim for "simpler" Γ-theorems, and move to "more complex ones".

Case: $\Gamma \vdash B$ and $\Gamma \vdash B \equiv A$ (i.e., Equanimity was applied to get A from Γ). By I.H., $\Delta \vdash B$ and $\Delta \vdash B \equiv A$, thus, $\Delta \vdash A$ by Equanimity.

Case: $\Gamma \vdash B \equiv C$ and A is the string $D[p := B] \equiv D[p := C]$ (i.e., Leibniz was applied to get A). By I.H., $\Delta \vdash B \equiv C$, hence (Leibniz!) $\Delta \vdash D[p := B] \equiv D[p := C]$, i.e., $\Delta \vdash A$. □

We have not considered *transitivity* in the induction step, since we know it is a derived rule (Problem set #3).

1.2 Remark. In particular, if $\vdash A$, then $\Gamma \vdash A$ for any Γ, since $\emptyset \subseteq \Gamma$.

1.3 Lemma. (Transitivity of "$\vdash$")
If $\Gamma \vdash A_i$, for $i = 1, \ldots, n$, and if $A_1, \ldots, A_n \vdash B$, then $\Gamma \vdash B$.

Proof. We do induction on Δ-theorems, where, for convenience, we have let $\Delta = \{A_1, \ldots, A_n\}$.

Basis. Say, $B \in \Lambda$. Then (definition of Γ-theorems) $\Gamma \vdash B$. Say, $B \in \Delta$. That is, B is an A_i. But we are told (hypothesis of Lemma!) that $\Gamma \vdash A_i$.

Assume the claim for "simpler" Δ-theorems, and move to "more complex ones".

Case: $\Delta \vdash C$ and $\Delta \vdash C \equiv B$ (i.e., Equanimity was applied to get B from Δ). By I.H., $\Gamma \vdash C$ and $\Gamma \vdash C \equiv B$, thus, $\Gamma \vdash B$ by Equanimity.

Case: $\Delta \vdash C \equiv D$ and B is the string $E[p := C] \equiv E[p := D]$ (i.e., Leibniz was applied to get B). By I.H., $\Gamma \vdash C \equiv D$, hence (Leibniz!) $\Gamma \vdash E[p := C] \equiv E[p := D]$, i.e., $\Gamma \vdash B$. □

"Transitivity of $\vdash$" legitimizes proofs that are based on previous theorems (rather than always going all the way back to axioms).

It also legitimizes the immediate, off the shelf, use of *derived rules of inference* in order to derive new theorems from old ("to continue a proof" as it were). Recall that a derived rule of inference is a template (schema) like "$A_1, \ldots, A_n \vdash B$". For example, MP ($A, A \Rightarrow B \vdash B$) is such a "template".

We are told by 1.3 that

"if $A_1, \ldots, A_n$ are Γ-theorems, then so is B, if we know that $A_1, \ldots, A_n \vdash B$".

Hey! Isn't that *exactly* how we apply the *primitive*[†] *rules* (Equanimity and Leibniz) to derive new theorems? Indeed, the above sounds exactly like (part of) the definition of Γ-theorems, namely, that "if A and $A \equiv B$ are Γ-theorems, then so is B, since we know that $A, A \equiv B \vdash B$ (Equanimity)".

[†] Recall that "primitive" means "given up in front".

2. Soundness

We prove here that our Calculus is truthful, or *Sound*, as people say technically. That is, whenever $\vdash A$, then also $\models A$. This will be a special case of 2.2 below. First a Lemma:

2.1 Lemma. *The two rules of inference "preserve truth". That is,*

$$A, A \equiv B \models B \tag{1}$$

and

$$A \equiv B \models C[p := A] \equiv C[p := B] \tag{2}$$

Proof. (1) Let s be a state appropriate for A and B. Suppose it makes the left hand side of "$\models$" $\underline{t}$, that is, $s(A) = \underline{t}$ and $s(A) = s(B)$. But then $s(B) = \underline{t}$.

(2) Let s be a state appropriate for A, B and $C[p := A] \equiv C[p := B]$. Suppose it makes the left hand side of "$\models$" $\underline{t}$, that is, $s(A) = s(B)$. Now $s(C[p := A])$ is determined by the $s(r)$-values of the various variables, r, in C (r distinct from p) and the value of $s(A)$ which is assigned to *the original p in C*. On the other hand, $s(C[p := B])$ is determined by the $s(r)$-values of the r in C (r distinct from p) and the value of $s(B)$, which is assigned to *the original p in C*. Since $s(A) = s(B)$, $s(C[p := A]) = s(C[p := B])$. □

For the demanding reader who didn't buy the argument in (2) above as being "rigorous enough", here is a rigorous one, by induction on WFF's C: Given that $s(A) = s(B)$ and s is appropriate for $C[p := A] \equiv C[p := B]$.

If C is any of *true*, *false* or r (other than p), then $C[p := A] \equiv C[p := B]$ is the same string as $C \equiv C$, hence $s(C \equiv C) = (s(C) = s(C)) = \underline{t}$. If finally C is p, then $C[p := A] \equiv C[p := B]$ is the same string as $A \equiv B$, hence $s(A \equiv B) = (s(A) = s(B)) = \underline{t}$ again.

For the induction step ("**Ind2**" on WFF), let first C be the string $\neg D$. Note that the I.H. applies on D (immediate predecessor of C).

Now, $C[p := A] \equiv C[p := B]$ is the string $\neg(D[p := A]) \equiv \neg(D[p := B])$, and therefore

$$\begin{aligned} s(\neg(D[p := A]) \equiv \neg(D[p := B])) &= [s(\neg(D[p := A])) = s(\neg(D[p := B]))] \\ &= [\overline{s(D[p := A])} = \overline{s(D[p := B])}] \\ &= \underline{t} \quad \text{(by I.H.)} \end{aligned}$$

Let next C be $D \vee E$. The I.H. applies on D and E (immediate predecessors of C).

Now, $C[p := A] \equiv C[p := B]$ is the string

$$D[p := A] \vee E[p := A] \equiv D[p := B] \vee E[p := B]$$

hence

$$\begin{aligned}s(D[p := A] \vee E[p := A]) &= s(D[p := A]) + s(E[p := A])\\ &= s(D[p := B]) + s(E[p := B]) \quad \text{(by I.H.)}\\ &= s(D[p := B] \vee E[p := B])\end{aligned}$$

The cases where C is any of $D \equiv E$, $D \wedge E$ or $D \Rightarrow E$ are entirely similar to the above and are omitted. ☡☡

2.2 (Meta)theorem. (Soundness of Propositional Calculus) *For any* Γ, $\Gamma \vdash A$ *implies* $\Gamma \models A$.

Proof. (Outline) We do induction on Γ-theorems.

Basis. If A is in Γ, then certainly $\Gamma \models A$ (any state that makes all formulas in Γ $\underline{t}$ will do so for A in particular). If A is in Λ then $\models A$ (some of these you have verified in Problem Set No. 2—the rest you may want to do on your own (that's why we said "Outline"—all else is here)). But then $\Gamma \models A$, since again any state s that makes all the formulas in Γ $\underline{t}$ will make $s(A) = \underline{t}$ (*any state whatsoever will make* $s(A) = \underline{t}$).

We now argue (the "**Ind2**") that the property propagates with the rules of inference, i.e., if a theorem's, A, immediate predecessors (in theoremhood) have it, then so does A.

Equanimity. So let $\Gamma \models B$ and $\Gamma \models B \equiv A$—i.e., we just wrote that *we have assumed the claim for immediate predecessors of* A. Let s be a state appropriate for all of Γ, A and B, such that $s(X) = \underline{t}$ for all X in Γ. Thus, $s(B) = \underline{t}$ and $s(B) = s(A)$. Hence, $s(A) = \underline{t}$.

Leibniz. So let $\Gamma \models B \equiv C$ and A be the string $D[p := B] \equiv D[p := C]$—i.e., we have again assumed the claim for an immediate predecessor (of different type this time) of A. Let s be a state appropriate for all of Γ, B, C and $D[p := B] \equiv D[p := C]$ such that $s(X) = \underline{t}$ for all X in Γ. Thus, $s(B) = s(C)$. Hence, $s\big(D[p := B] \equiv D[p := C]\big) = \underline{t}$ by Lemma 2.1. □

3. Post's Theorem

We will employ below the following Lemma.

3.1 Lemma. (Proof by Cases) $A \Rightarrow C, B \Rightarrow C \vdash (A \vee B) \Rightarrow C$.

Proof. Here $\Gamma = \{A \Rightarrow C, B \Rightarrow C\}$.

$$\begin{aligned}
& (A \lor B) \Rightarrow C \\
= & \Big\langle \vdash A \Rightarrow B \equiv \neg A \lor B \Big\rangle \\
& \neg(A \lor B) \lor C \\
= & \Big\langle \text{Leib: } r \lor C + \text{deMorgan} \Big\rangle \\
& (\neg A \land \neg B) \lor C \\
= & \Big\langle \text{distrib. of } \lor \text{ over } \land \Big\rangle \\
& (\neg A \lor C) \land (\neg B \lor C) \\
= & \Big\langle \text{Leib and } \vdash A \Rightarrow B \equiv \neg A \lor B\text{, twice} \Big\rangle \\
& (A \Rightarrow C) \land (B \Rightarrow C) \\
= & \Big\langle \text{Leib: } r \land (B \Rightarrow C)\text{, and } \Gamma \vdash A \Rightarrow C \equiv \mathit{true} \Big\rangle \\
& \mathit{true} \land (B \Rightarrow C) \\
= & \Big\langle \text{by } \vdash \mathit{true} \land X \equiv X \Big\rangle \\
& B \Rightarrow C
\end{aligned}$$

But $\Gamma \vdash B \Rightarrow C$, hence $\Gamma \vdash (A \lor B) \Rightarrow C$. □

3.2 Metatheorem. (Post's Tautology Theorem) *If* $\models A$, *then* $\vdash A$.

Proof. First, we note the following equivalences.

$$\begin{aligned}
\models \mathit{true} \equiv \neg p \lor p, &\text{ also } \vdash \mathit{true} \equiv \neg p \lor p \\
\models \mathit{false} \equiv \neg p \land p, &\text{ also } \vdash \mathit{false} \equiv \neg p \land p \\
\models C \Rightarrow D \equiv \neg C \lor D, &\text{ also } \vdash C \Rightarrow D \equiv \neg C \lor D \\
\models C \land D \equiv \neg(\neg C \lor \neg D), &\text{ also } \vdash C \land D \equiv \neg(\neg C \lor \neg D) \\
\models (C \equiv D) \equiv ((C \Rightarrow D) \land (D \Rightarrow C)), &\text{ also } \vdash (C \equiv D) \equiv ((C \Rightarrow D) \land (D \Rightarrow C))
\end{aligned} \tag{I.1}$$

Thus, if we *transform* A into A' by applying any sequence of the above equivalences to *eliminate* all occurrences of *true* and *false* and all the connectives except $\neg$ and $\lor$, then we have, on the one hand, that $\models A \equiv A'$ and on the other hand that $\vdash A \equiv A'$, both by the Leibniz rule. Indeed, say it took the following steps to go from A to A':

$$A = A_1 = A_2 = \cdots = A_k = A'$$

Each "=" is a *conjunctional* "≡". Each "=-step" is justified by an application of "Leibniz" using as premise one of the equivalences under I.1 above. Of course, "Leibniz" is applicable both in the semantic and syntactic domain.

Thus, by equanimity, it suffices to prove $\vdash A'$.

A better way to say all this is that, "*without loss of generality*, we assume that the only connectives in A are among $\vee$ and $\neg$ and that the constants *true* and *false* do *not* occur".

Moreover, since $\vdash A \vee A \equiv A$, we may assume *without loss of generality* that A is a string $A_1 \vee \cdots \vee A_n$ *with* $n \geq 2$, so that none of the A_i is a formula $C \vee D$.

We are assuming metanotational abbreviations when it comes to bracketing. In particular, our induction below will be for abbreviated formulas!

Let us call an A_i *reducible* iff it has the form $\neg(C \vee D)$ or $\neg(\neg C)$. Otherwise it is *irreducible*. Thus, the only possible irreducible A_i have the form p or $\neg p$ (where p is a variable). We say that p "occurs positively in $\ldots \vee p \vee \ldots$", while it "occurs negatively in $\ldots \vee \neg p \vee \ldots$". In, for example, $p \vee \neg p$ it occurs *both* positively and negatively.

A is irreducible iff all the A_i are.

We define the *reducibility degree*, of A_i—in short, $rd(A_i)$—to be the number of $\neg$ or $\vee$ connectives in it, *not counting a possible leftmost* $\neg$. *The reducibility degree of A is the sum of the reducibility degrees of all its A_i.*

For example, $rd(p) = 0$, $rd(\neg p) = 0$, $rd(\neg(\neg p \vee q)) = 2$, $rd(\neg(\neg p \vee \neg q)) = 3$, $rd(\neg p \vee q)) = 0$.

So let $\models A$, where A is the string $A_1 \vee \cdots \vee A_n$, $n \geq 2$, where none of the A_i is a formula $C \vee D$, and prove (following Shoenfield) by induction on the reducibility degree of A that $\vdash A$.

For the basis, let A be an irreducible tautology ($rd(A) = 0$). It must be that A is a string of the form "$\cdots \vee p \vee \cdots \neg p \vee \cdots$" for some p, otherwise (if no p appears both "positively" and "negatively") we can find a truth-assignment that makes A false ($\underline{f}$)—a contradiction (indeed, assign $\underline{f}$ to p's that occur positively only, and $\underline{t}$ to those that occur negatively only).

Now

$$
\begin{array}{ll}
 & A\\
= & \Big\langle \text{moving } p \text{ and } \neg p \text{ up in front via assoc, symm. (of } \vee)\\
 & \text{and Leib (whenever working on part of the formula)}\Big\rangle\\
 & p \vee \neg p \vee B \qquad \text{(what is ``}B\text{''?)}\\
= & \Big\langle \text{Leib: } r \vee B + \text{excluded middle, plus ``} \equiv \textit{true}\text{'' intro.}\Big\rangle\\
 & \textit{true} \vee B\\
= & \Big\langle \text{by } \vdash \textit{true} \vee B \equiv \textit{true}\Big\rangle\\
 & \textit{true}
\end{array}
$$

Thus $\vdash A$ which settles the *Basis*-case $rd(A) = 0$.

We now argue the case where $rd(A) = n+1$, on the I.H. that whenever, for any formula Q, $rd(Q) \leq n$, then $\models Q$ implies $\vdash Q$.

By commutativity (symmetry) of "$\vee$", let us assume without restricting generality that $rd(A_1) > 0$.

We have two cases:

(1) A_1 is the string $\neg(\neg C)$, hence A has the form $\neg(\neg C) \vee D$. Clearly $\models C \vee D$. Moreover, $rd(C \vee D) < rd(\neg(\neg C) \vee D)$, hence

$$\vdash C \vee D$$

by the I.H. But,

$$\begin{aligned} & C \vee D \\ = & \Big\langle \text{Leib: } r \vee D + \vdash \neg\neg X \equiv X \Big\rangle \\ & \neg(\neg C) \vee D \end{aligned}$$

Hence, $\vdash \neg(\neg C) \vee D$, that is, $\vdash A$ in this case.

One more case to go:

(2) A_1 is the string $\neg(C \vee D)$, hence A has the form $\neg(C \vee D) \vee E$.

$$\text{We want: } \vdash \neg(C \vee D) \vee E \qquad (i)$$

Since $\vdash X \Rightarrow Y \equiv \neg X \vee Y$, it suffices to show that

$$\vdash (C \vee D) \Rightarrow E$$

We are given that $\models (C \vee D) \Rightarrow E$. Clearly then $C \Rightarrow E$ and $D \Rightarrow E$ are *both* tautologies (**do you believe this?**), and hence so are $\neg C \vee E$ and $\neg D \vee E$ of lower (each) reducibility degree than the original.

By I.H., we have $\vdash \neg C \vee E$ and $\vdash \neg D \vee E$, hence $\vdash C \Rightarrow E$ and $\vdash D \Rightarrow E$. By Lemma 3.1, we have $\vdash (C \vee D) \Rightarrow E$, thus, (i) is established. □

Post's theorem is often called the "Completeness Theorem"[†] of Propositional Calculus. It shows that the syntactic manipulation apparatus completely captures the notion of "truth" (tautologyhood) in the propositional case.

3.3 Corollary. *If* $A_1, \ldots, A_n \models B$, *then* $A_1, \ldots, A_n \vdash B$.

Proof. It is an easy semantic exercise to see (indeed we have done so in class) that

$$\models A_1 \Rightarrow \ldots \Rightarrow A_n \Rightarrow B.$$

[†] Which is really a *Meta*theorem, right?

By 3.2,

$$\vdash A_1 \Rightarrow \ldots \Rightarrow A_n \Rightarrow B$$

hence (by Lemma 1.1)

$$A_1, \ldots, A_n \vdash A_1 \Rightarrow \ldots \Rightarrow A_n \Rightarrow B \tag{1}$$

Applying modus ponens n times to (1) we get

$$A_1, \ldots, A_n \vdash B$$

□

The above corollary is very convenient.

It says that any (correct) schema $A_1, \ldots, A_n \models B$ leads to a *derived rule of inference*, $A_1, \ldots, A_n \vdash B$.

In particular, combining with Lemma 1.3, we get

3.4 Corollary. *If* $\Gamma \vdash A_i$*, for* $i = 1, \ldots, n$*, and if* $A_1, \ldots, A_n \models B$*, then* $\Gamma \vdash B$.

Thus—*unless otherwise requested!*—we can, from now on, *rigorously* mix syntactic with semantic justifications of our proof steps.

For example, we have at once $A \wedge B \vdash A$, because (trivially) $A \wedge B \models A$ (compare with our earlier, much longer, proof given in class).

So, $\Gamma \models A$ implies $\Gamma \vdash A$, right?

Well, yes and no. The statement

$$\text{“}\Gamma \models A \text{ implies } \Gamma \vdash A\text{”} \tag{P}$$

is right. However, we must take exception to the word “So”, above, as it may suggest that the metatheorem (P) somehow is a trivial rephrasing or consequence of Corollary 3.3.

(P) is *not* implied by 3.3 *in general*: When Γ is *infinite*, then in order to prove (P), we ***need*** a sophisticated metatheorem known as *the Compactness of Propositional Logic*—which we are not getting into.

In our course we should be content with the *finite* case given in 3.3 above. Just a related remark here: Soundness (2.2) was proved *without* restriction on whether Γ is finite or not (check the proof once more!)

4. Deduction Theorem, Proof by Contradiction

4.1 Metatheorem. (The Deduction Theorem) $\Gamma, A \vdash B$ *iff* $\Gamma \vdash A \Rightarrow B$, *where "*$\Gamma, A$*" means "all the assumptions in* Γ*, plus the assumption* A*"* (in set notation this would be $\Gamma \cup \{A\}$).

Proof. if-part. This is easy (by Modus Ponens, essentially). Indeed, we are given

$$\Gamma \vdash A \Rightarrow B$$

Thus (Lemma 1.1)

$$\Gamma, A \vdash A \Rightarrow B \tag{1}$$

But we know that $\Gamma, A \vdash A$ (Why?), hence (by Lemma 1.3) and MP,

$$\Gamma, A \vdash B$$

only if-part. Here we want to argue that *all* (Γ, A)-theorems B have a property, that

$$\Gamma \vdash A \Rightarrow B \tag{$*$}$$

Naturally, we will do induction on (Γ, A)-theorems B.

Basis. We have the following cases:

Case where B is in Λ. Then (by **Th1**, p.1) $\Gamma \vdash B$. However,

$$B \models A \Rightarrow B \tag{2}$$

Pause. Do you believe (2)?

By Corollary 3.4 we get $\Gamma \vdash A \Rightarrow B$.

Case where B is in Γ. Then $\Gamma \vdash B$. By (2) and Corollary 3.4 we get $\Gamma \vdash A \Rightarrow B$.

Case where B is *the same string as* A. Now $\models A \Rightarrow A$, that is $\models A \Rightarrow B$, hence $\vdash A \Rightarrow B$ by Post's theorem.

This last one leads to $\Gamma \vdash A \Rightarrow B$ by Lemma 1.1.

Equanimity induction step. Say that B is a (Γ, A) theorem because C and $C \equiv B$ are.

The I.H. requires the truth of $(*)$ when we replace B by the "simpler" (earlier) theorems,[†] C and $C \equiv B$.

That is, we have as I.H. (3) and (4) below:

$$\Gamma \vdash A \Rightarrow C \tag{3}$$

[†] Note how I said "theorems", not "formulas", in connection with the qualification "simpler". If needed, review the discussion on induction starting on p.4.

and

$$\Gamma \vdash A \Rightarrow (C \equiv B) \tag{4}$$

But,

$$A \Rightarrow C, A \Rightarrow (C \equiv B) \models A \Rightarrow B \tag{5}$$

Pause. Do you believe (5)?

Now (3), (4) and (5) yield $\Gamma \vdash A \Rightarrow B$ via Corollary 3.4.

Leibniz induction step. Say that B is a (Γ, A)-theorem, because $C \equiv D$ is, and B is *the same string as* $E[p := C] \equiv E[p := D]$.

The I.H. here is that

$$\Gamma \vdash A \Rightarrow (C \equiv D) \tag{6}$$

Now, by Lemma 2.1(2),

$$C \equiv D \models E[p := C] \equiv E[p := D] \tag{7}$$

hence

$$A \Rightarrow (C \equiv D) \models A \Rightarrow \Big(E[p := C] \equiv E[p := D]\Big) \tag{8}$$

Pause. Do you believe that (8) really follows from (7)?

(6) and (8) yield again $\Gamma \vdash A \Rightarrow \Big(E[p := C] \equiv E[p := D]\Big)$ via Corollary 3.4, that is, $\Gamma \vdash A \Rightarrow B$. □

The mathematician, or indeed the mathematics practitioner, uses the Deduction theorem all the time, without stopping to think about it. Metatheorem 4.1 above makes an honest person of such a mathematician or practitioner.

The everyday "style" of applying the Metatheorem goes like this: Say we have all sorts of assumptions (nonlogical axioms) and we want, *under these assumptions*, to "prove" that "if A, then B" (verbose form of "$A \Rightarrow B$"). We start by ***adding*** *A to our assumptions*, often with the words, "*Assume A*". We then proceed and prove *just* B (not $A \Rightarrow B$), and at that point we rest our case.

Thus, we may view an application of the Deduction theorem as a simplification of the proof-task. It allows us to "split" an implication $A \Rightarrow B$ that we want to prove, moving its premise to join our other assumptions. We now have to prove a *simpler formula*, B, with the help of *stronger* assumptions (that is, all we knew so far, plus A). That often makes our task so much easier!

4.2 Definition. A set of formulas Γ is *inconsistent* or *contradictory* iff Γ *proves every A in* WFF. □

The following Lemma justifies the term "contradictory" for a Γ such as described above:

4.3 Lemma. Γ *is inconsistent iff* $\Gamma \vdash \textit{false}$*.*

Proof. only if-part. If Γ is as in 4.2, in particular it proves *false* since the latter is a well formed formula.

if-part. Say, conversely, that we have

$$\Gamma \vdash \textit{false} \tag{9}$$

Let now A be any formula in WFF whatsoever. We have

$$\textit{false} \models A \tag{10}$$

Pause. Do you believe (10)?

By Corollary 3.4, $\Gamma \vdash A$ follows from (9) and (10). □

Why "contradictory"? For example, because we know that $\models \textit{false} \equiv A \wedge \neg A$.

4.4 Metatheorem. (Proof by contradiction) $\Gamma \vdash A$ *iff* $\Gamma \cup \{\neg A\}$ *is inconsistent.*

Proof. if-part. So let (by 4.3)

$$\Gamma, \neg A \vdash \textit{false}$$

Hence

$$\Gamma \vdash \neg A \Rightarrow \textit{false} \tag{1}$$

by the Deduction theorem. However $\neg A \Rightarrow \textit{false} \models A$, hence, by Corollary 3.4 and (1) above, $\Gamma \vdash A$.

only if-part. So let

$$\Gamma \vdash A$$

By 1.1,

$$\Gamma, \neg A \vdash A \tag{2}$$

Moreover, trivially,

$$\Gamma, \neg A \vdash \neg A \tag{3}$$

Since $A, \neg A \models \textit{false}$, (2) and (3) yield $\Gamma \vdash \textit{false}$ via Corollary 3.4, and we are done by 4.3. □

4.4 legitimizes the tool of "proof by contradiction" that goes all the way back to the ancient Greek mathematicians: To prove A assume instead the opposite ($\neg A$). Proceed then to obtain a contradiction. This being accomplished, it is as good as having proved A.

5. *Appendix: Theorems versus Proofs*

☡☡

5.1 Metatheorem. (Induction on Theorems) *Let $P(x)$ be a property of WFF's. Let Γ be given.*

Suppose we know that

I1. *$P(A)$ holds (is true) for all A in Γ and Λ.*

I2. *Whenever $P(B)$ and $P(B \equiv A)$ both hold, then also $P(A)$ is true.*

I3. *Whenever $P(C \equiv D)$ holds, then also $P(E[p := C] \equiv E[p := D])$ holds,* no matter how we pick E and p.

Then $P(A)$ is true for all *Γ-theorems A.*

Proof. Let us call $\mathcal{S}$ *the set of all* formulas X that make $P(x)$ true. In set notation we symbolize what we have just said by

$$\text{Let } \mathcal{S} = \{X \in \text{WFF} : P(X)\} \tag{1}$$

Thus "$P(X)$" is the "entrance condition" for membership in $\mathcal{S}$. A WFF A is in $\mathcal{S}$ iff it satisfies the entrance condition, i.e.,

$$A \in \mathcal{S} \text{ iff } P(A)^{\dagger} \tag{2}$$

We observe the following facts about $\mathcal{S}$:

Fact1. $\Gamma \subseteq \mathcal{S}$ and $\Lambda \subseteq \mathcal{S}$.

Indeed (see p.1 for the meaning of "$\subseteq$") if A is in either Γ or Λ, hypothesis **I1** yields $P(A)$.

(2), above, then yields $A \in \mathcal{S}$.

Fact2. Whenever B and $B \equiv A$ are (both) in $\mathcal{S}$, then so is A.

Indeed our assumption ("Whenever...") yields that $P(B)$ and $P(B \equiv A)$ both hold by (2) above. Then, hypothesis **I2** yields that $P(A)$ is true. By (2), once more, A is in $\mathcal{S}$.

[†] "iff $P(A)$" is short for "iff $P(A)$ is true". This is a common abbreviation in mathematics parlance and is closely related to the "$\equiv$ *true*" elimination principle. Moreover, we admit that we have relied on our convention, that capital Latin letters stand for formulas, in order to simplify the form of (2). In the absence of such a convention (1) would have compelled us to write more explicitly "$A \in \mathcal{S}$ iff $A \in \text{WFF} \wedge P(A)$".

Fact3. Whenever $C \equiv D$ is in $\mathcal{S}$, then so is $E[p := C] \equiv E[p := D]$, *no matter how we pick E and p.*

Indeed our assumption ("Whenever…") yields that $P(C \equiv D)$ holds by (2) above. Then, hypothesis **I3** yields that $P(E[p := C] \equiv E[p := D])$ holds. By (2), once more, $E[p := C] \equiv E[p := D]$ is in $\mathcal{S}$.

Look at the three Facts above (forget about the reason we gave for them—the "Indeed…-part). They say that the set of formulas $\mathcal{S}$ satisfies *exactly the same three conditions* that the set of Γ-theorems does (see p.1).

However, the set of Γ theorems, let us give it the temporary name $\mathcal{T}$ for convenience, is the *smallest* that satisfies **Fact1**–**Fact3**. That is,

$$\mathcal{T} \subseteq \mathcal{S}$$

hence if $A \in \mathcal{T}$ then $A \in \mathcal{S}$.

Using (2) above, this translates into

$$\text{If } \Gamma \vdash A, \text{ then } P(A)$$

□

5.2 Lemma. *If $A_1, \ldots, A_n$ is a Γ-proof, and if $1 \leq k < n$, then $A_1, \ldots, A_k$ is also a Γ-proof.*

Proof. Refer to the definition of Γ-proof on p.2. It says there "where each A_i $(i = 1, \ldots, n)$ satisfies: …"

But both of **Pr1** and **Pr2** continue to be valid if instead of "where each A_i $(i = 1, \ldots, n)$ satisfies: …" we say "where each A_i $(i = 1, \ldots, k)$ satisfies: …", since $k < n$. □

5.3 Lemma. *If $A_1, \ldots, A_m$ and $B_1, \ldots, B_n$ are two Γ-proofs, then so is*

$$A_1, \ldots, A_m, B_1, \ldots, B_n. \tag{1}$$

Proof. As we check the sequence (1) according to the definition of Γ-proof on p.2, it is immediate that every formula A_i will "pass" (since $A_1, \ldots, A_m$ *is* a proof).

How about the B_j's? Well, if a B_j is in Γ or Λ we are fine. If not, **Pr2**—and the fact the $B_1, \ldots, B_n$ is a proof—tell us that B_j is a conclusion of a rule applied to formulas to the left of B_j *in the sequence* $B_1, \ldots, B_n$.

But this is also true *in the sequence* $A_1, \ldots, A_m, B_1, \ldots, B_n$. So each B_j checks fine. □

5.4 Metatheorem. $\Gamma \vdash A$ *iff A is the last (rightmost) formula in a Γ-proof.*

Proof. only-if-part. We prove by induction on Γ-theorems that each such theorem A has the property: "A figures as the rightmost formula in some Γ-proof".

Basis. Let A be in Γ or Λ. But then, the one-formula sequence "A" is a Γ-proof, and A is its rightmost formula.

Equanimity. Let each of B and $B \equiv A$ appear as the rightmost formula of some proof, e.g.,

$$Q_1, Q_2, \ldots, Q_m, B$$

and

$$R_1, R_2, \ldots, R_n, B \equiv A$$

By 5.3, the following sequence is a Γ-proof.

$$Q_1, Q_2, \ldots, Q_m, B, R_1, R_2, \ldots, R_n, B \equiv A$$

But then so is

$$Q_1, Q_2, \ldots, Q_m, B, R_1, R_2, \ldots, R_n, B \equiv A, A$$

by Equanimity and **Pr2**. Hence A is at the right end of a proof once more.

Leibniz. Let $C \equiv D$ appear as the rightmost formula of some proof, e.g.,

$$Q_1, Q_2, \ldots, Q_m, C \equiv D$$

and let A be the string $E[p := C] \equiv E[p := D]$. Then

$$Q_1, Q_2, \ldots, Q_m, C \equiv D, A$$

is also a proof by Leibniz and **Pr2**. Hence A is at the right end of a proof yet once more. Done with "only-if".

if-part. We prove by induction on the number n (length of a proof) that if

$$R_1, R_2, \ldots, R_n$$

is a Γ-proof, then R_n is a Γ-theorem, i.e., $\Gamma \vdash R_n$.

Basis. Case where $n = 1$. Then, since there is nothing to the left of R_n, **Pr1** must apply, thus R_n is in Γ or Λ. Therefore $\Gamma \vdash R_n$ (**Th1** on p.1).

As I.H., we *assume* that for all $k < n$, if

$$R_1, R_2, \ldots, R_k$$

is a Γ-proof, then $\Gamma \vdash R_k$.

As a result of I.H. and Lemma 5.2,

$$\Gamma \vdash R_i, \text{ for all } i = 1, \ldots, n-1 \tag{2}$$

To conclude the induction step, we consider a Γ-proof of length n

$$R_1, R_2, \ldots, R_n \tag{3}$$

and proceed to prove

$$\textbf{To do: } \Gamma \vdash R_n \tag{4}$$

We consider each case **Pr1** and **Pr2** for R_n:

Pr1: If R_n is in Γ or in Λ, then (as it was the case in the "Basis"), $\Gamma \vdash R_n$.

Pr2: *Subcase Equanimity*, where $R_i, R_j \vdash R_n$, $i \leq n-1$, $j \leq n-1$, and R_j is the string "$R_i \equiv R_n$".

By (2), $\Gamma \vdash R_i$ and $\Gamma \vdash R_i \equiv R_n$. By definition of theorems (**Th2**, p.1), (4) follows.

Subcase Leibniz, where $R_i \vdash R_n$, $i \leq n-1$ and R_i is a string "$C \equiv D$" whereas R_n is a string "$E[p := C] \equiv E[p := D]$".

By (2), $\Gamma \vdash R_i$. By definition of theorems (**Th3**, p.1), (4) follows once more. □

☡☡