MATHEMATICS 300 — FALL 1998

Introduction to Mathematical Reasoning

Instructor: H. J. Sussmann

HANDOUT NO. 14. November 23, 1998

THERE IS NO HOMEWORK ASSIGNMENT FOR THE WEEK AFTER THANKSGIVING

NOTE: This handout was written in a hurry, so it probably contains lots of errors and typos. I am rushing it through because I want you to get it before the Thanksgiving vacation. There will be an improved version later, with typos corrected.

The handout contains:

1. Solutions to two homework problems (the 728! problem and the "top player" problem).
2. A discussion of derived rules (shortcuts).

SOLUTIONS TO TWO HOMEWORK PROBLEMS

The 728! problem: Prove that every product of 728 consecutive natural numbers is divisible by 728!.

PROOF: To understand how the proof goes, let us first do a proof for for the case of 5! rather than 728!. My feeling is that once you see what is going on for 5 you will understand the case of 728 too.

Let us try to prove that

(S) *A product of* 5 *consecutive numbers is always divisible by* 5!.

I am going to show you first that

A. *if we knew that that a product of* 4 *consecutive numbers is always divisible by* 4!, *then our desired conclusion (that is, Statement (S)) follows.*

So let us suppose that in some way we already knew that a product of 4 consecutive numbers is always divisible by 4!. Let us pick a number n which is the product of 5 consecutive numbers, and let me try to prove that n is divisible by 5! Our number n is of the form

$$n = k(k+1)(k+2)(k+3)(k+4)\,,$$

so what we really want to do is prove that

B. *For every natural number k, the number $k(k+1)(k+2)(k+3)(k+4)$ is divisible by* 5!.

Let us prove B by induction. If you take $k = 1$, then $k(k+1)(k+2)(k+3)(k+4)$ is just 5!, which of course is divisible by 5! So this case is trivial.

Now let us do the inductive step. Suppose that

(1) $\quad k(k+1)(k+2)(k+3)(k+4)$ is divisible by 5!,

and let us prove that

(2) $\quad (k+1)(k+2)(k+3)(k+4)(k+5)$ is divisible by 5!.

Write

$$\begin{aligned}
&(k+1)(k+2)(k+3)(k+4)(k+5)\\
&\quad = (k+1)(k+2)(k+3)(k+4).k + (k+1)(k+2)(k+3)(k+4).5\\
&\quad = k(k+1)(k+2)(k+3)(k+4) + 5(k+1)(k+2)(k+3)(k+4)\,.
\end{aligned}$$

Now, we are assuming (1), that is, that $k(k+1)(k+2)(k+3)(k+4)$ is divisible by 5! Also, we are assuming that we know that that a product of 4 consecutive numbers is always divisible by 4!. Clearly, $(k+1)(k+2)(k+3)(k+4)$ is such a product, so $(k+1)(k+2)(k+3)(k+4)$ is divisible by 4!, and then $5(k+1)(k+2)(k+3)(k+4)$ is divisible by 5.4!, i.e. by 5!.

So we have shown that

(a) $k(k+1)(k+2)(k+3)(k+4)$ is divisible by 5!,

and

(b) $5(k+1)(k+2)(k+3)(k+4)$ is divisible by 5!.

Adding these up, we get

(c') $k(k+1)(k+2)(k+3)(k+4) + 5(k+1)(k+2)(k+3)(k+4)$ is divisible by 5!,

that is

(c) $(k+1)(k+2)(k+3)(k+4)(k+5)$ is divisible by 5!,

which is exactly (2).

By the PMI, $k(k+1)(k+2)(k+3)(k+4)$ is divisible by 5! for every natural number k. That is, B holds.

Now let us look at what we have done. We have proved that

IF every product of 4 consecutive numbers is divisible by 4!,

THEN every product of 5 consecutive numbers is divisible by 5!.

This, of course, does not yet solve our problem, for *how do we know that a product of* 4 *consecutive numbers is always divisible by* 4!*?*

The answer is, **we don't, yet.** However, it is just a matter of repeating the same argument once more, and you will prove that

IF every product of 3 consecutive numbers is divisible by 3!,

THEN every product of 4 consecutive numbers is always divisible by 4!.

Once again, our problem is not solved, for how do we know that a product of 3 consecutive numbers is always divisible by 3!?

The answer is, **we don't, yet.** However, it is just a matter of repeating the same argument once again, you can prove that:

IF every product of 2 consecutive numbers is divisible by 2!,

THEN every product of 3 consecutive numbers is always divisible by 3!.

Next, it is is even more trivial than what we have done before to show that

IF every "product of 1 consecutive number" (that is, every number) is divisible by 1!

THEN a product of 2 consecutive numbers is always divisible by 2!.

Finally, *a single number is always divisible by* 1!, because $1! = 1$ and every natural number is divisible by 1.

So, let us see what we have proved:

1. Every natural number is divisible by 1!.
2. If every natural number is divisible by 1!, then every product of 2 consecutive numbers is always divisible by 2!.
3. If every product of 2 consecutive numbers is always divisible by 2!, then every product of 3 consecutive numbers is divisible by 3!.
4. If every product of 3 consecutive numbers is divisible by 3!, then every product of 4 consecutive numbers is divisible by 4!.
5. If every product of 4 consecutive numbers is divisible by 4!, then every product of 5 consecutive numbers is divisible by 5!.

Now all you have to do is combine these four statements, and draw the conclusion that

$$\boxed{\text{A product of 5 consecutive numbers is always divisible by 5!}}$$

which is exactly what we wanted.

The beauty of this proof is that you can see right away that there is nothing special about the number 5. You can also prove that

6. If every product of 5 consecutive numbers is divisible by 5!, then every product of 6 consecutive numbers is divisible by 6!.
7. If every product of 6 consecutive numbers is divisible by 6!, then every product of 7 consecutive numbers is divisible by 7!.
8. If every product of 7 consecutive numbers is divisible by 7!, then every product of 8 consecutive numbers is divisible by 8!.
9. If every product of 8 consecutive numbers is divisible by 8!, then every product of 9 consecutive numbers is divisible by 9!.
10. If every product of 9 consecutive numbers is divisible by 9!, then every product of 10 consecutive numbers is divisible by 10!.
11. If every product of 10 consecutive numbers is divisible by 10!, then every product of 11 consecutive numbers is divisible by 11!.
12. If every product of 11 consecutive numbers is divisible by 11!, then every product of 12 consecutive numbers is divisible by 12!.

$$\vdots \quad \vdots \quad \vdots$$

728. If every product of 727 consecutive numbers is divisible by 727!, then every product of 728 consecutive numbers is divisible by 728!.

From this you can now conclude, for example, that

a product of 9 *consecutive numbers is always divisible by* 9!.

and

a product of 728 *consecutive numbers is always divisible by* 728!.

What kind of proof is this, exactly? Well, **it's a method of proof we already know. It's called induction.**

What we are really proving is

(P) *For every natural number* m*, the product of any* m *consecutive natural numbers is divisible by* $m!$.

What I did above was essentially an outline of a proof of this fact by induction. Specifically: : we consider the statement

$p(m)$: the product of any m consecutive natural numbers is divisible by $m!$

and we prove it by induction with respect to m . To do this:

I. we first prove $p(1)$;

II. we then prove that, for every m, $p(m)$ implies $p(m+1)$.

Statement $p(1)$ says that a single number is always divisible by 1, and this is obviously true. So Part I is taken care of.

Now let us do Part II. It's just a matter of doing with a general m what we did before with $m = 4$. (With the computer it's easy: I'll just copy my proof for $m = 4$ verbatim, change "4" to "m", and make a couple of trivial adjustments.)

So let us assume that we already know that every product of m consecutive numbers is divisible by $m!$. Let us pick a number n which is the product of $m+1$ consecutive numbers, and let us try to prove that n is divisible by $(m+1)!$. Our number n is of the form

$$n = k(k+1)(k+2)(k+3)...(k+m)\,,$$

so what we really want to do is prove that

B. *For every natural number* k*, the number* $k(k+1)(k+2)(k+3)...(k+m)$ *is divisible by* $(m+1)!$.

Let us prove B by induction. If you take $k = 1$, then $k(k+1)(k+2)(k+3)...(k+m)$ is just $(m+1)!$, which of course is divisible by $(m+1)!$. So this case is trivial.

Now let us do the inductive step. Suppose that

(*) $k(k+1)(k+2)(k+3)...(k+m)$ is divisible by $(m+1)!$,

and let us prove that

(**) $(k+1)(k+2)(k+3)...(k+m)(k+m+1)$ is divisible by $(m+1)!$.

Write

$$\begin{aligned}&(k+1)(k+2)(k+3)...(k+m)(k+m+1)\\ &\quad = (k+1)(k+2)(k+3)...(k+m).k + (k+1)(k+2)(k+3)...(k+m).(m+1)\\ &\quad = k(k+1)(k+2)(k+3)...(k+m) + (m+1)(k+1)(k+2)(k+3)...(k+m)\,.\end{aligned}$$

Now, we are assuming (*), that is, that $k(k+1)(k+2)(k+3)...(k+m)$ is divisible by $(m+1)!$. Also, we are assuming that we know that that a product of m consecutive numbers is always divisible by $m!$. Clearly, $(k+1)(k+2)(k+3)...(k+m)$ is such a product, so $(k+1)(k+2)(k+3)...(k+m)$ is divisible by $m!$, and then $(m+1)(k+1)(k+2)(k+3)...(k+m)$ is divisible by $(m+1).m!$, i.e. by $(m+1)!$.

So we have shown that

(a) $k(k+1)(k+2)(k+3)...(k+m)$ *is divisible by* $(m+1)!$

and

(b) $(m+1)(k+1)(k+2)(k+3)...(k+m)$ *is divisible by* $(m+1)!$.

Adding these up, we get

- $k(k+1)(k+2)(k+3)...(k+m)+(m+1)(k+1)(k+2)(k+3)...(k+4)$ *is divisible by* $(m+1)!$;

that is

- $(k+1)(k+2)(k+3)...(k+m)(k+m+1)$ *is divisible by* $(m+1)!$,

which is exactly (**).

By the Principle of Mathematical Induction, $k(k+1)(k+2)(k+3)...(k+m)$ is divisible by $(m+1)!$ for every natural number k . That is, B holds. This completes the proof. **QED**

REMARK: One thing that may render this proof mysterious to some of you is that involves a **double induction.** We want to prove that $p(m)$ is true for all m, and we do this by induction. In the proof by induction, at one point we have to prove that $(\forall m)(p(m) \Rightarrow p(m+1))$. So we fix m , assume $p(m)$, and set out to prove $p(m+1)$. Then, to prove $p(m+1)$ for this fixed m (assuming $p(m)$) we observe that $p(m+1)$ is itself a universal statement about natural numbers, since it says that

$$(\forall k)(k(k+1)(k+2)...(k+m) \text{ is divisible by } m!).$$

So we prove this statement by induction. In other words, **we do an induction within another induction.** The basic structure is:

- We want to prove $(\forall m)p(m)$.
- We prove this by induction:

STEP 1: prove $p(1)$ (easy);

STEP 2: prove $(\forall m)(p(m) \Rightarrow p(m+1))$;

To do Step 2:

Let m be arbitrary.

Assume $p(m)$. Try to prove $p(m+1)$.

$p(m+1)$ says "$(\forall k)q(k)$", where $q(k)$ is the statement

"$k(k+1)...(k+m)$ is divisible by $(m+1)!$."

To prove $(\forall k)q(k)$," use induction:

STEP A: Prove $q(1)$ (easy).

STEP B: Prove "$(\forall k)(q(k) \Rightarrow q(k+1))$".

To do Step B:

Let k be arbitrary.

Assume $q(k)$. Try to prove $q(k+1)$.

$\vdots \quad \vdots$

(Here we do our algebraic computation, as above.)

$\vdots \quad \vdots$

$q(k+1)$.

$q(k) \Rightarrow q(k+1)$. [Rule 3]

$(\forall k)(q(k) \Rightarrow q(k+1))$. [Rule 5]

END OF STEP B.

By the PMI, we have proved $p(m+1)$.

$p(m) \Rightarrow p(m+1)$. [Rule 3]

$(\forall m)(p(m) \Rightarrow p(m+1))$. [Rule 5]

END OF STEP 2.

- By the PMI, we have proved $(\forall m)p(m)$.

Now, to do the homework problem, all you have to do is plug in (i.e. specialize to) $m = 728$.

THE "TOP PLAYER" PROBLEM

We want to prove

(A) *Every tournament has a top player.*

We rephrase this as

(B) *For every natural number n, every tournament with n players has a top player.*

Now the statement we want to prove is ready for a proof by induction.

PROOF: Let S be the set of all natural numbers n such that every tournament with n players has a top player.

We want to prove that $S = \mathbb{N}$. By the PMI, it suffices to prove:

1. $1 \in S$,
2. $(\forall n)(n \in S \Rightarrow n+1 \in S)$.

Proof of 1. We have to show that $1 \in S$. That is, we haqve to show that every tournament with one player has a top player. So let T be a tournament with one player. Call this player a. We claim that a is a top player. Let P be the set of players of T. We have to show that

$$(\forall b)((b \in P \wedge b \neq a) \Rightarrow ((a \text{ beats } b) \vee (\exists c)(c \in P \wedge ((a \text{ beats } c) \wedge (c \text{ beats } b))))). \tag{1}$$

Let b be arbitrary. Assume that $b \in P \wedge b \neq a$. Since T has just one player, if $b \in P$ then $b = a$, because $a \in P$. So we have $b = a$ and $b \neq a$. So So we have $b = a \wedge b \neq a$. But this is a contradiction, and from a contradiction everything follows. In particular, a beats b follows. So

$$(a \text{ beats } b) \vee (\exists c)(c \in P \wedge ((a \text{ beats } c) \wedge (c \text{ beats } b))).$$

Therefore

$$(b \in P \wedge b \neq a) \Rightarrow ((a \text{ beats } b) \vee (\exists c)(c \in P \wedge ((a \text{ beats } c) \wedge (c \text{ beats } b)))),$$

by Rule 3. Since b was arbitrary, (1) holds.

Proof of 1. We have to show that $(\forall n)(n \in S \Rightarrow n+1 \in S)$. Let n be arbitrary. Assume $n \in S$. We want to prove that $n+1 \in S$.

We have to prove that if T is any tournament with $n+1$ players then T has a top player. So let T be an arbitrary tournament with $n+1$ players. Let P be the set of players of T, so P has $n+1$ members. Pick a player $a \in P$. Let $\tilde{T}$ be the tournament obtained by removing a from T. Then $\tilde{T}$ is a tournament with n players. Since we are assuming that $n \in S$, it follows that $\tilde{T}$ has a top player. Pick one such player. Call this player t.

We now show that either t or a is a top player of T. We consider three cases:

- CASE 1: t beats a.

- CASE 2: a beats t but t beats someone who beats a.

- CASE 3: a beats t and t does not beat anyone who beats a.

In Cases 1 and 2, t is a top player of T. (Proof: Let b be any player of T other than t. If $b \neq a$, then t beats b or beats someone who beats b, because t is a top player of $\tilde{T}$. If $b = a$, then t beats a—if we are in Case 1—or t beats someone who beats a—if we are in Case 2. So for all $b \in P$ other than t, either t beats b or t beats someone who beats b. So t is a top player for T, as desired.)

Now lets us look at Case 3. We show that in this case a is a top player of T. Let b be any player of T other than a. We want to show that either a beats b or a beats someone who beats b. We consider two possibilities, namely,

- CASE I: $b = t$.

- CASE II: $b \neq t$.

In Case I, we are done, because a beats b, since a beats t and $t = b$.

Now let us look at Case II. We consider two possibilities:

- CASE α: t beats b.

- CASE β: t does not beat b.

In Case α, we have a beats t and t beats b, so a beats someone who beats b, and we are done.

In Case β, b beats t. We consider two possibilities:

- CASE μ: a beats b.

- CASE ν: a does not beat b.

In Case μ we are done. (Remember that we are trying to prove that either a beats b or a beats someone who beats b.) Now let us look at Case ν. Since t is a top player for $\tilde{T}$, either t beats b or t beats someone who beats b. Since we are assuming that we are in Case β, we know that t does not beat b. So t must beat someone who beats b. Pick one such player. Call this player c. So t beats c and c beats b.

Now, remember that we are assuming that t does not beat anyone who beats a. So c cannot beat a, for if it did then t would not beat c. So a beats c. But c beats b. So a beats someone who beats b. **END OF THE PROOF.**

DERIVED RULES (SHORTCUTS)

In a formal proof you are supposed to use the eight basic rules and nothing else. However, if you really had to do this all the time, then your proofs would become too long. This is why one often "skips steps," or "carries out several steps together." In fact, what you do is observe that in many cases there are certain sequences of steps that appear over and over again. So you know in advance that whenever you have such-and-such formulas you can always go to some other formula. We collect this information into a list of **derived rules**.

EXAMPLE: Suppose you want to go from "$(\forall x)(p(x) \Rightarrow q(x))$" and "$p(a)$ to $q(a)$." (For example, you want to deduce the conclusion that "Socrates is mortal" from the premisses "All men are mortal" and "Socrates is a man." In formal language, if "$p(x)$" stands for "x is a man," "$q(x)$" stands for "x is mortal," and "a" stands for "Socrates," then the premisses are precisely "$(\forall x)(p(x) \Rightarrow q(x))$" and "$p(a)$," and what you want to get is "$q(a)$.") Then you could do it as follows:

(1)	$(\forall x)(p(x) \Rightarrow q(x))$.	[Hypothesis]
(2)	$p(a)$.	[Hypothesis]
(3)	$p(a) \Rightarrow q(a)$.	[Rule 4, from (10)]
(4)	$q(a)$.	[Modus Ponens, from (2) and (3)).

However, this situation is going to occur over and over again, and you do not want to repeat the above four steps every time, so you can create a **DERIVED RULE**, or **SHORTCUT:**

> **DERIVED RULE 1.** If you have "$(\forall x)(p(x) \Rightarrow q(x))$" and "$p(a)$" then you can go to "$q(a)$."

JUSTIFICATION: Steps (1), (2), (3), (4) above.

Now that you have Derived Rule 1, every time you need to go from (1) and (2) as above you can skip (3), and go directly to (4), invoking the derived rule.

Here are a few more derived rules. There are lots of them. Hundreds of them. But you do not need to memorize them, because they are all rather trivial and reflect plain common sense, and you can derive them whenever you want to. For example, Derived Rule 10 is the basis of "proofs by contradiction." Another example: Derived Rule 15 says another completely obvious and trivial thing: suppose that B necessarily must be true when A is false, and also when A is true. Then B must be true (because A is either true or false, and in either case A is true.)

> **DERIVED RULE 2.** If you have $A \wedge B$ then you can go to A.

JUSTIFICATION: $(A \wedge B) \Rightarrow A$ is a tautology, so you can bring it in any time you want. If in addition you have $A \wedge B$, then from this and $(A \wedge B) \Rightarrow A$ you get A by Modus Ponens (Rule 2).

> **DERIVED RULE 3.** If you have $A \wedge B$ then you can go to B.

JUSTIFICATION OF DERIVED RULE 3: $(A \wedge B) \Rightarrow B$ is a tautology, so you can bring it in any time you want. If in addition you have $A \wedge B$, then from this and $(A \wedge B) \Rightarrow B$ you get B by Modus Ponens (Rule 2). $\diamondsuit$

> **DERIVED RULE 4.** If you have A and B then you can go to $A \wedge B$.

JUSTIFICATION OF DERIVED RULE 4: $A \Rightarrow (B \Rightarrow (A \wedge B))$ is a tautology, so you can bring it in any time you want. If in addition you have A and B, then from A and $A \Rightarrow (B \Rightarrow (A \wedge B))$ you get $B \Rightarrow (A \wedge B)$ by Modus Ponens (Rule 2), and then from B and $B \Rightarrow (A \wedge B)$ you get $A \wedge B$. $\diamondsuit$

> **DERIVED RULE 5.** If you have A then you can go to $A \vee B$.

JUSTIFICATION OF DERIVED RULE 5: $A \Rightarrow (A \vee B)$ is a tautology, so you can bring it in any time you want. If in addition you have A, then from A and $A \Rightarrow (A \vee B)$ you get $A \vee B$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 6. If you have B then you can go to $A \vee B$.

JUSTIFICATION OF DERIVED RULE 6: $B \Rightarrow (A \vee B)$ is a tautology, so you can bring it in any time you want. If in addition you have B, then from B and $B \Rightarrow (A \vee B)$ you get $A \vee B$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 7. If you have $A \Rightarrow B$ and $B \Rightarrow A$, then you can go to $A \Leftrightarrow B$.

JUSTIFICATION OF DERIVED RULE 7: $(A \Rightarrow B) \Rightarrow ((B \Rightarrow A) \Rightarrow (A \Leftrightarrow B))$ is a tautology, so you can bring it in any time you want. If in addition you have $A \Rightarrow B$, then from $A \Rightarrow B$ and $(A \Rightarrow B) \Rightarrow ((B \Rightarrow A) \Rightarrow (A \Leftrightarrow B))$ you get $(B \Rightarrow A) \Rightarrow (A \Leftrightarrow A)$ by Modus Ponens (Rule 2). If you also have $B \Rightarrow A$, then from $B \Rightarrow A$ and $(B \Rightarrow A) \Rightarrow (A \Leftrightarrow B)$ you get $A \Leftrightarrow B$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 8. If you have $A \Leftrightarrow B$ then you can go to $A \Rightarrow B$.

JUSTIFICATION OF DERIVED RULE 8: $(A \Leftrightarrow B) \Rightarrow (A \Rightarrow B)$ is a tautology, so you can bring it in any time you want. If in addition you have $A \Leftrightarrow B$, then from $A \Leftrightarrow B$ and $(A \Leftrightarrow B) \Rightarrow (A \Rightarrow B)$ you get $A \Rightarrow B$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 9. If you have $A \Leftrightarrow B$ then you can go to $B \Rightarrow A$.

JUSTIFICATION OF DERIVED RULE 9: $(A \Leftrightarrow B) \Rightarrow (B \Rightarrow A)$ is a tautology, so you can bring it in any time you want. If in addition you have $A \Leftrightarrow B$, then from $A \Leftrightarrow B$ and $(A \Leftrightarrow B) \Rightarrow (B \Rightarrow A)$ you get $B \Rightarrow A$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 10. If assuming $\sim A$ you get a contradiction, then you can go to A.

JUSTIFICATION OF DERIVED RULE 10: Suppose that assuming $\sim A$ you get C, which is a contradiction. Then you can go to $(\sim A) \Rightarrow C$ by Rule 3. Now, if C is a contradiction, then $(\sim A \Rightarrow C) \Rightarrow A$ is a tautology (why?), so you can bring it in. Since you have $\sim A \Rightarrow C$, then from $(\sim q) \Rightarrow C$ and $(\sim A \Rightarrow C) \Rightarrow A$ you get A by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 11. From $\sim A$ and $A \vee B$ you can go to B.

JUSTIFICATION OF DERIVED RULE 11: $(\sim A) \Rightarrow ((A \vee B) \Rightarrow B)$ is a tautology, so you can bring it in any time you want. If in addition you have $\sim A$, then you get $(A \vee B) \Rightarrow B$ by Modus Ponens (Rule 2). If you also have $A \vee B$, then you get B by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 12. From $\sim B$ and $A \vee B$ you can go to A.

JUSTIFICATION OF DERIVED RULE 12: $(\sim B) \Rightarrow ((A \vee B) \Rightarrow A)$ is a tautology, so you can bring it in any time you want. If in addition you have $\sim B$, then you get $(A \vee B) \Rightarrow A$ by Modus Ponens (Rule 2). If you also have $A \vee B$, then you get A by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 13. From $A \vee B$ you can go to $B \vee A$.

JUSTIFICATION OF DERIVED RULE 13: $(A \vee B) \Rightarrow (B \vee A)$ is a tautology, so you can bring it in any time you want. If in addition you have $A \vee B$, then you get $B \vee A$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 14. From $(A \vee B) \vee C$ you can go to $A \vee (B \vee C)$.

JUSTIFICATION OF DERIVED RULE 14: $((A \vee B) \vee C) \Rightarrow (A \vee (B \vee C))$ is a tautology, so you can bring it in any time you want. If in addition you have $(A \vee B) \vee C$, then you can go to $A \vee (B \vee C)$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 15. From $A \vee (B \vee C)$ you can go to $(A \vee B) \vee C$.

JUSTIFICATION OF DERIVED RULE 15: $(A \vee (B \vee C)) \Rightarrow ((A \vee B) \vee C)$ is a tautology, so you can bring it in any time you want. If in addition you have $A \vee (B \vee C)$, then you can go to $(A \vee B) \vee C)$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 16. From $A \wedge B$ you can go to $B \wedge A$.

JUSTIFICATION OF DERIVED RULE 16: $(A \wedge B) \Rightarrow (B \wedge A)$ is a tautology, so you can bring it in any time you want. If in addition you have $A \wedge B$, then you get $B \wedge A$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 17. From $(A \vee B) \vee C$ you can go to $A \vee (B \vee C)$.

JUSTIFICATION OF DERIVED RULE 17: $((A \wedge B) \wedge C) \Rightarrow (A \wedge (B \wedge C))$ is a tautology, so you can bring it in any time you want. If in addition you have $(A \wedge B) \wedge C$, then you can go to $A \wedge (B \wedge C)$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 18. From $A \wedge (B \wedge C)$ you can go to $(A \wedge B) \wedge C$.

JUSTIFICATION OF DERIVED RULE 18: $(A \wedge (B \wedge C)) \Rightarrow ((A \wedge B) \wedge C)$ is a tautology, so you can bring it in any time you want. If in addition you have $A \wedge (B \wedge C)$, then you can go to $(A \wedge B) \wedge C)$ by Modus Ponens (Rule 2). $\diamondsuit$

DERIVED RULE 19. If assuming A and $\sim B$ you get $\sim A$, then you can go to $A \Rightarrow B$.

JUSTIFICATION OF DERIVED RULE 19: Assume A. Then assuming $\sim B$ you can get $\sim A$, and you can also get A, so you can get $A \wedge (\sim p)$ by Derived Rule 4. But $A \wedge (\sim A)$ is a contradiction. So you can get B by Derived Rule 12, still assuming A. In other words, assuming A we get B. By Rule 3, we get $A \Rightarrow B$. ◊

DERIVED RULE 20. If assuming $\sim A$ you get B, then you can go to $A \vee B$.

JUSTIFICATION OF DERIVED RULE 20: $((\sim A) \Rightarrow B) \Rightarrow (A \vee B)$ is a tautology, so you can bring it in any time you want. If you can prove B assuming $\sim A$, then you get $(\sim A) \Rightarrow B$ by Rule 3. But then from $(\sim A) \Rightarrow B$ and $((\sim A) \Rightarrow B) \Rightarrow (A \vee B)$ you get $A \vee B$ by Modus Ponens (Rule 2). ◊

DERIVED RULE 21. If assuming $\sim A$ you get B, and assuming A you also get B, then you can go to B assuming nothing.

JUSTIFICATION OF DERIVED RULE 21: $((\sim A) \Rightarrow B) \Rightarrow ((A \Rightarrow B) \Rightarrow B)$ is a tautology, so you can bring it in any time you want. If you can prove B assuming $\sim A$, then you get $(\sim A) \Rightarrow B$ by Rule 3. But then from $(\sim A) \Rightarrow B$ and $((\sim A) \Rightarrow B) \Rightarrow ((A \Rightarrow B) \Rightarrow B)$ you get $(A \Rightarrow B) \Rightarrow B$ by Modus Ponens (Rule 2). If you can also prove B assuming A, then you get $A \Rightarrow B$ by Rule 3. But then from $A \Rightarrow B$ and $(A \Rightarrow B) \Rightarrow B$ you get B by Modus Ponens (Rule 2). ◊

DERIVED RULE 22. If assuming A you get B, and assuming B you get A, then you can go to $A \Leftrightarrow B$.

JUSTIFICATION OF DERIVED RULE 22: $(A \Rightarrow B) \Rightarrow ((B \Rightarrow A) \Rightarrow (A \Leftrightarrow B))$ is a tautology, so you can bring it in any time you want. If you can prove B assuming A, then you get $A \Rightarrow B$ by Rule 3. But then from $A \Rightarrow B$ and $(A \Rightarrow B) \Rightarrow ((B \Rightarrow A) \Rightarrow (A \Leftrightarrow B))$ you get $(B \Rightarrow A) \Rightarrow (A \Leftrightarrow B)$ by Modus Ponens (Rule 2). If you can also prove A assuming B, then you get $B \Rightarrow A$ by Rule 3. But then from $B \Rightarrow A$ and $(B \Rightarrow A) \Rightarrow (A \Leftrightarrow B)$ you get $A \Leftrightarrow B$ by Modus Ponens (Rule 2). ◊

DERIVED RULE 23. If x and y are two different variables, $p(x, y)$ is a formula with no quantifiers in x and y, a, b are constants, and $p(a, b)$ denotes the formula obtained from $p(x, y)$ by substituting a for x and b for y, then from $(\forall x)(\forall y)p(x, y)$ you can go to $p(a, b)$.

JUSTIFICATION OF DERIVED RULE 23: In one step you can got from $(\forall x)(\forall y)p(x, y)$ to $(\forall y)p(a, y)$ by Rule 4, and then in one more step, applying Rule 4 again, you go to $p(a, b)$. ◊

DERIVED RULE 24. If x, y, and z are three different variables, $p(x,y,z)$ is a formula with no quantifiers in x, y and z, a, b, c are constants, and $p(a,b,c)$ denotes the formula obtained from $p(x,y,z)$ by substituting a for x, b for y, and c for z, then from $(\forall x)(\forall y)(\forall z)p(x,y,z)$ you can go to $p(a,b,c)$.

JUSTIFICATION OF DERIVED RULE 24: This is similar to the justification of the previous derived rule. In one step you can go from $(\forall x)(\forall y)(\forall z)p(x,y,z)$ to $(\forall y)(\forall z)p(a,y,z)$ by Rule 4. Then in one more step, applying Rule 4 again, you can go to $(\forall z)p(a,b,z)$. Finally, in a third step you can go to $p(a,b,c)$ thanks to Rule 4. $\diamondsuit$

DERIVED RULE 25. If x and y are two different variables and $p(x,y)$ is a formula with no quantifiers in x and y, then from $(\forall x)(\forall y)p(x,y)$ you can go to $(\forall y)(\forall x)p(x,y)$.

JUSTIFICATION OF DERIVED RULE 25: You can prove the formula

$$(\forall x)(\forall y)p(x,y) \Rightarrow (\forall y)(\forall x)p(x,y) \qquad (*)$$

as follows, using letters a and b that do not appear in $p(x,y)$:

(1.&)	Assume $(\forall x)(\forall y)p(x,y)$.	[Preparation to apply Rule 3]
(2.&.&)	Let a be arbitrary.	[Preparation to apply Rule 5]
(3.&.&.&)	Let b be arbitrary.	[Preparation to apply Rule 5]
(4.&.&.&)	$(\forall y)p(b,y)$.	[Rule 4, from (1)]
(5.&.&.&)	$p(b,a)$.	[Rule 4, from (4)]
(6.&.&)	$(\forall x)p(x,a)$.	[Rule 5, from (3) and (5)]
(7.&)	$(\forall y)(\forall x)p(x,y)$.	[Rule 5, from (2) and (6)]
(8)	$(\forall x)(\forall y)p(x,y) \Rightarrow (\forall y)(\forall x)p(x,y)$.	[Rule 3, from (1) and (7).]

Now, having proved (*), if you have $(\forall x)(\forall y)p(x,y)$, then you can get $(\forall y)(\forall x)p(x,y)$ by Modus Ponens. $\diamondsuit$

DERIVED RULE 26. If x and y are two different variables and $p(x,y)$ is a formula with no quantifiers in x and y, then from $(\exists x)(\exists y)p(x,y)$ you can go to $(\exists y)(\exists x)p(x,y)$.

JUSTIFICATION OF DERIVED RULE 26: You can prove the formula

$$(\exists x)(\exists y)p(x,y) \Rightarrow (\exists y)(\exists x)p(x,y) \qquad (**)$$

as follows, using letters a and b that do not appear in $p(x,y)$:

(1.&)	Assume $(\exists x)(\exists y)p(x,y)$.	[Preparation to apply Rule 3]
(2.&.&)	Let a be such that $(\exists y)p(a,y)$.	[From (1), preparation to apply Rule 6]
(3.&.&.&)	Let b be such that $p(a,b)$.	[From (20, preparation to apply Rule 6]
(4.&.&.&)	$(\exists x)p(x,b)$.	[Rule 7, from (3)]
(5.&.&.&)	$(\exists y)(\exists x)p(x,y)$.	[Rule 7, from (4)]
(6.&.&)	$(\exists y)(\exists x)p(x,y)$.	[Rule 6, from (3) and (5)]
(7.&)	$(\exists y)(\exists x)p(x,y)$.	[Rule 6, from (2) and (6)]
(8)	$(\exists x)(\exists y)p(x,y) \Rightarrow (\exists y)(\exists x)p(x,y)$.	[Rule 3, from (1) and (7).]

Now, having proved (**), if you have $(\exists x)(\exists y)p(x,y)$, then you can get $(\exists y)(\exists x)p(x,y)$ by Modus Ponens. $\diamondsuit$

There will be millions of derived rules in the next handout.

HAVE A HAPPY THANKSGIVING.