Math 220 Fall 2021, Lecture 10: Deduction rules

0.1. Deduction rules

We now speak the language of mathematical propositions; let us now see how/when we can obtain ("deduce") one proposition from another (or from several others). In other words, let us see what kind of logical steps can be used in proofs.

0.1.1. Modus ponens

Modus ponens: Let P and Q be two propositions. Assume that you have proved P, and you have proved $P \implies Q$ (i.e., that P implies Q). Then, you can deduce Q.

Example 0.1.1. We know that 3 is a positive integer. If 3 is a positive integer, then $3 \geq 1$. Thus, $3 \geq 1$.
(Here, P is "3 is a positive integer", and Q is "$3 \geq 1$".)

0.1.2. Modus tollens

Modus tollens: Let P and Q be two propositions. Assume that you have proved NOT Q, and you have proved $P \implies Q$ (i.e., that P implies Q). Then, you can deduce NOT P.

Example 0.1.2. We know that 7 is not even. If 7 was a multiple of 4, then 7 would be even. Thus, 7 is not a multiple of 4.
(Here, P is "7 is a multiple of 4", and Q is "7 is even".)

Note that we have used conjunctive mood ("If 7 was", "7 would be"). Strictly speaking, this is not necessary; we could just as well have said "If 7 is a multiple of 4, then 7 is even".

0.1.3. AND-introduction

AND-introduction: Let P and Q be two propositions. Assume that you have proved P, and you have proved Q. Then, you can deduce P AND Q.

0.1.4. AND-elimination

AND-elimination: Let P and Q be two propositions. Assume that you have proved P AND Q. Then, you can deduce P, and you can deduce Q.

0.1.5. OR-introduction

OR-introduction from the left: Let P and Q be two propositions. Assume that you have proved P. Then, you can deduce P OR Q.

OR-introduction from the right: Let P and Q be two propositions. Assume that you have proved Q. Then, you can deduce P OR Q.

0.1.6. ∀-introduction

∀-introduction: Let S be a set. Let $P(x)$ be a predicate that depends on a variable x that is supposed to belong to S. Assume that you have proved $P(x)$ under the assumption that x is an arbitrary element of S. Then, you can deduce that $\forall x \in S : P(x)$.

Example 0.1.3. Let us prove that

$$(a+b)^2 = a^2 + 2ab + b^2 \qquad \text{for all } a, b \in \mathbb{R}.$$

In other words, let us prove that

$$\forall a, b \in \mathbb{R} : (a+b)^2 = a^2 + 2ab + b^2.$$

The proof goes as follows:
Let $a, b \in \mathbb{R}$ be arbitrary. Then,

$$\begin{aligned}
(a+b)^2 &= (a+b)(a+b) \\
&= (a+b)a + (a+b)b \qquad \text{(by distributivity)} \\
&= aa + ba + ab + bb \qquad \text{(by distributivity again)} \\
&= \underbrace{aa}_{=a^2} + \underbrace{ab + ab}_{=2ab} + \underbrace{bb}_{=b^2} \qquad \text{(since } ba = ab\text{)} \\
&= a^2 + 2ab + b^2.
\end{aligned}$$

So we have proved that $(a+b)^2 = a^2 + 2ab + b^2$ under the assumption that a and b are arbitrary elements of $\mathbb{R}$. Thus, by ∀-introduction, we can deduce that

$$\forall a, b \in \mathbb{R} : (a+b)^2 = a^2 + 2ab + b^2.$$

So ∀-introduction is the rule that is behind our "Let $a, b \in \mathbb{R}$ be arbitrary" reasoning. It is essentially the only way to prove a statement that begins with "∀".

0.1.7. ∀-elimination

∀-elimination: Let $P(x)$ be a predicate that depends on a variable x. Let S be a set. Assume that we have proved that $\forall x \in S : P(x)$. Assume that s is an element of S. Then, we can deduce that $P(s)$.

Example 0.1.4. We have just shown that

$$\forall a, b \in \mathbb{R} : (a+b)^2 = a^2 + 2ab + b^2.$$

Furthermore, we know that $5 \in \mathbb{R}$ and $9 \in \mathbb{R}$. Thus, we can deduce that

$$(5+9)^2 = 5^2 + 2 \cdot 5 \cdot 9 + 9^2.$$

Formally speaking, we are applying the $\forall$-elimination rule to $x = (a, b)$ and $s = (5, 9)$.

0.1.8. $\exists$-introduction

$\exists$-introduction: Let S be a set. Let $P(x)$ be a predicate that depends on a variable x that is supposed to belong to S. Assume that you have defined/constructed/found some $s \in S$ and proved that $P(s)$ holds. Then, you can deduce that $\exists x \in S : P(x)$.

Example 0.1.5. We claim that there exists a positive integer that is even and divisible by 3.

Indeed, 6 is such a positive integer. Thus, we conclude (by $\exists$-introduction) that there exists a positive integer that is even and divisible by 3.

Formally, we are applying the $\exists$-introduction rule to $S = \{\text{positive integers}\}$ and

$$P(x) = \text{“}x \text{ is even and divisible by 3”}$$

and $s = 6$.

0.1.9. $\exists$-elimination

$\exists$-elimination: Let S be a set. Let $P(x)$ be a predicate that depends on a variable x that is supposed to belong to S. Assume that you have proved that $\exists x \in S : P(x)$. Then, you can introduce a $x \in S$ that satisfies $P(x)$.

Example 0.1.6. We claim that every integer n that is divisible by 4 must be even.

In other words, we claim that

$$\forall n \in \mathbb{Z} : (4 \mid n) \Longrightarrow (2 \mid n).$$

To prove it, we let n be an arbitrary element of $\mathbb{Z}$. Assume that $4 \mid n$. That is, there exists some integer k such that $n = 4 \cdot k$ (this is just the definition of divisibility). Consider this k. (Here, we applied the $\exists$-elimination rule!) Now, we compute

$$n = \underbrace{4}_{=2\cdot 2} \cdot k = 2 \cdot 2 \cdot k.$$

Thus, there exists some integer m such that $n = 2 \cdot m$ (namely, $m = 2 \cdot k$). (Here, we applied the $\exists$-introduction rule.) In other words, $2 \mid n$. This completes our proof.

0.1.10. $\Longrightarrow$-introduction

$\Longrightarrow$-introduction: Let P and Q be two propositions. Assume that you have proved Q under the assumption of P. Then, you can deduce $P \Longrightarrow Q$ (without the assumption of P).

Example 0.1.7. In the previous example, we proved that $2 \mid n$ under the assumption of $4 \mid n$. Thus, by the $\Longrightarrow$-introduction rule, we have proved $(4 \mid n) \Longrightarrow (2 \mid n)$.

0.1.11. $\Longrightarrow$-elimination

$\Longrightarrow$-elimination: Let P and Q be two propositions. Assume that you have proved $P \Longrightarrow Q$, and you have also proved P. Then, you can deduce Q.

This is what we previously called "modus ponens".

0.1.12. $\Longleftrightarrow$-introduction

$\Longleftrightarrow$-introduction: Let P and Q be two propositions. Assume that you have proved Q under the assumption of P, and you have also proved P under the assumption of Q. Then, you can deduce $P \Longleftrightarrow Q$.

Example 0.1.8. Let n be an integer. We claim that n is even if and only if $n+1$ is odd. In other words, we claim that

$$(n \text{ is even}) \Longleftrightarrow (n+1 \text{ is odd}).$$

To prove this, we have to prove
(1) that $n+1$ is odd under the assumption that n is even, and
(2) that n is even under the assumption that $n+1$ is odd.
(We will do this later, as we seriously do number theory.)

Thus, a proof of an equivalence $P \Longleftrightarrow Q$ is a two-part process: The first part is proving Q under the assumption of P (this is called the "forward direction", or the "$\Longrightarrow$ direction"); the second part is proving P under the assumption of Q (this is called the "backward direction", or the "$\Longleftarrow$ direction").

0.1.13. $\Longleftrightarrow$-elimination

$\Longleftrightarrow$-elimination: Let P and Q be two propositions. Assume that you have proved $P \Longleftrightarrow Q$. Then, if you have proved P, you can deduce Q, and vice versa.

0.1.14. $\Longleftrightarrow$-symmetry

$\Longleftrightarrow$-symmetry: Let P and Q be two propositions. Assume that you have proved $P \Longleftrightarrow Q$. Then, you can deduce that $Q \Longleftrightarrow P$.

0.1.15. $\Longleftrightarrow$-transitivity

$\Longleftrightarrow$-transitivity: Let P, Q and R be three propositions. Assume that you have proved $P \Longleftrightarrow Q$ and $Q \Longleftrightarrow R$. Then, you can deduce that $P \Longleftrightarrow R$.

0.1.16. False-elimination

False-elimination ("ex falso quod libet", which means "from a false statement, anything follows"): Let P and Q be two propositions. Assume that you have proved P and you have also proved NOT P. (This is called a **contradiction**.) Then, you can deduce Q.

Example 0.1.9. If you can prove $2 > 3$ and NOT $(2 > 3)$, then $0 = 1$.

This rule looks strange, because it lets you deduce any (completely unrelated) statement from a contradiction. But the point is, it is impossible to unconditionally prove a contradiction (i.e., unconditionally prove P and NOT P at the same time). (Strictly speaking, it is probably impossible. The impossibility itself cannot be proved, but if someone would be able to prove P and NOT P at the same time, then mathematics would "collapse", as any statement would be automatically true and false.) However, it will often happen that you will deduce contradictions under assumptions. What this means is that the assumptions are never satisfied.

0.1.17. Proof by contradiction I

Proof by contradiction I: Let P be a proposition. Assume that you have proved a contradiction under the assumption of P. Then, you can deduce that NOT P.

Example 0.1.10. We claim that $\sqrt{2}$ is irrational.

In other words, we claim that

$$\text{NOT } \left(\sqrt{2} \in \mathbb{Q}\right).$$

The way to prove this is by assuming $\sqrt{2} \in \mathbb{Q}$, and deriving a contradiction.

How do we do this? Assume $\sqrt{2} \in \mathbb{Q}$. However, every element of $\mathbb{Q}$ (i.e., every rational number) can be written as a **reduced fraction** – i.e., as a fraction $\frac{p}{q}$ where p and q are two integers such that $q \neq 0$ and such that $\gcd(p,q) = 1$ (that is, p and q have no common divisors > 1 that could be cancelled). In other words,

$$\forall x \in \mathbb{Q} : \left(\exists p, q \in \mathbb{Z} : q \neq 0 \text{ AND } x = \frac{p}{q} \text{ AND } \gcd(p,q) = 1\right).$$

By $\forall$-elimination, we can apply this to $x = \sqrt{2}$, so we obtain

$$\exists p, q \in \mathbb{Z} : q \neq 0 \text{ AND } \sqrt{2} = \frac{p}{q} \text{ AND } \gcd(p,q) = 1$$

(because of our assumption that $\sqrt{2} \in \mathbb{Q}$). By $\exists$-elimination, we can pick such integers p, q. Now, $\sqrt{2} = \frac{p}{q}$ entails $\sqrt{2} \cdot q = p$. By squaring, we obtain $2q^2 = p^2$.

Now, if p was odd, then p^2 must be odd, which contradicts $2q^2 = p^2$. So p is not odd. (This was itself a proof by contradiction!) Thus, p is even (since any integer is odd or even). So $p = 2k$ for some integer k; consider this k. (Again, this was $\exists$-elimination.) Thus,

$$\begin{aligned} 2q^2 = p^2 &= (2k)^2 \qquad (\text{since } p = 2k) \\ &= 4k^2. \end{aligned}$$

Cancelling 2, we transform this into $q^2 = 2k^2$. However, if q was odd, then q^2 would be odd as well, which would contradict $q^2 = 2k^2$. (Another proof by contradiction!) So q is even. Now we have shown that p and q are both even (this is a use of AND-introduction). This contradicts $\gcd(p, q) = 1$. Thus, we have obtained a contradiction from our assumption $\sqrt{2} \in \mathbb{Q}$. Hence, we have proved NOT $\left(\sqrt{2} \in \mathbb{Q}\right)$.