Proof Example: The Irrationality of $\sqrt{2}$

During the lecture a student asked for an example of natural style proof in which one uses the inference rule:

$$\frac{\Phi \vdash \Psi, \varphi}{\Phi, \neg\varphi \vdash \Psi}\ (\neg \vdash).$$

Proofs in natural style have only one goal, thus this rule may be used when the set Ψ is empty, that is, when we are trying to find a contradiction:

$$\frac{\Phi \vdash \varphi}{\Phi, \neg\varphi \vdash \mathbb{F}}\ (\neg \vdash).$$

Intuitively, this can be expressed as: "Since we are trying to find a contradiction, and $\neg\varphi$ is assumed, then we try to prove φ".

The proof below uses this rule.

Theorem: $\sqrt{2}$ is not a rational number.

Proof: By contradiction: we assume that there exists a rational number r such that $\sqrt{2} = r$, and we try to derive a contradiction.

By the definition of rational numbers, there exist n and m, such that $r = n/m$ and n, m are coprime (that means that there does not exist a number different from 1 which divides both n and m).

(Comment: intuitively, this definition of rational numbers takes into account their unique representation x/y in which the fraction is already simplified by the greatest common divisor – GCD – of the nominator and the denominator. In more exact terms, if one would define the rational numbers as a number which can be expressed as x/y, then one can prove a lemmata stating that each rational number can be expressed as x'/y', where x', y' are coprime, because one can take $x' = x/\mathrm{GCD}(x, y)$ and similarly for y'.)

Therefore, we now have the assumption:

not (there exists $d\neg = 1$ such that d divides n and m).

Now we apply the inference rule mentioned above:

We prove:

there exists $d\neg = 1$ such that d divides n and m.

We take as witness for d the number 2 (which is different from 1) and we prove: 2 divides n and m.

By definition of $\sqrt{x}$ (that is: the positive number y such that $y^2 = x$), we obtain $n^2/m^2 = 2$ and from this $n^2 = 2\ m^2$.

Thus 2 divides n^2, from here 2 divides n (because 2 is prime), therefore there exists a k such that $n = 2\ k$.

We replace this into the previous equality and obtain $4\ k^2 = 2\ m^2$, thus $2\ k^2 = m^2$, hence 2 divides m^2 and finally 2 divides m.

Remark 1. This theorem was first proved by the ancient mathematician Hippasus around 500 BC in the same manner. A consequence of this theorem is the existence of irrational numbers (that is, numbers which can not be expressed as fractions). At the respective time this was a revolutionary discovery. Hippasus was a member of the mathematical school of Pythagoras, which was probably the most advanced "mathematical society" of the time, and which developed many interesting results about numbers and geometry (in particular the famous theorem about the square triangle). They believed that all numbers which express lengths of segments must "exist", and they also believed that all numbers can be expressed as fractions. However, the lenght of the hypothenusis (in German: *Hypothenuse*) of the square triangle with kathetes (in German: *Kathete*) of length 1 is equal to $\sqrt{2}$, thus the latter must "exist", although it cannot be expressed as a fraction.

Pythagoras did not agree to this new theorem because it contradicted his basic convictions about numbers, however he could not find a mistake in the proof of Hippasus, and this created a conflict with him which finally escalated in sentencing him to death. (The school of Pythagoras had a strict code of conduct which included the penalty of death by drowning.)

You may find more details at `http://encyclopedia.thefreedictionary.com/Square+root+of+2`.

Remark 2. In order to keep the proof simple I omitted the details about the *type* of the numbers (positive, different from zero, etc.). They can be easily filled in (left as an exercise for the reader).

Remark 3. Another useful exercise is to identify the formal inference steps (sequent rules) which are used – most of them are the same or very similar to the ones discussed in the lecture.