Proof Examples

① Indirect Proof:

Show that x^2 is even $\Rightarrow$ x is even.

We show the statement indirectly by showing that x is odd $\Rightarrow$ x^2 is odd:

x is odd
$\Rightarrow x = 2k+1$ for some k (x odd)
$\Rightarrow x^2 = (2k+1)^2$
$\Rightarrow x^2 = 4k^2 + 4k + 1$ (qr. formula)
$\Rightarrow x^2 = 2(2k^2+2k) + 1$
$\Rightarrow x^2 = 2d + 1$ (for $d = 2k^2+2k$)
$\Rightarrow x^2$ is odd (def. odd)

This shows the statement indirectly.

[Note that we used a very common idea here: Use the definition of odd to work on a "lower" level and then use the definition at the end to get back to a "higer" level.]

② Proof by contradiction:

Show that $\sqrt{2}$ is irrational.

We show the statement by contradiction.

Assume that $\sqrt{2}$ was rational. Then there would exist $x, y \in \mathbb{Z}$ such that

$\sqrt{2} = \frac{x}{y}$ and the fraction $\frac{x}{y}$ is fully simplified!

So $\sqrt{2} = \frac{x}{y}$ which means $2 = \frac{x^2}{y^2}$.

$\Rightarrow 2y^2 = x^2$

$\Rightarrow x^2$ is even

$\Rightarrow x$ is even (as showed in 1)

So now x is even.

$\Rightarrow x = 2k$ for some k

$\Rightarrow x^2 = 4k^2$

$\Rightarrow 2y^2 = 4k^2$ (eq. from above)

$\Rightarrow y^2 = 2k^2$

$\Rightarrow y^2$ is even

$\Rightarrow y$ is even (as in 1)

But now x and y are even.
This is a contradiction, since we assumed that $\frac{x}{y}$ is a fully simplified, but if both are even we could further simplify the fraction!

Therefore the statement must be true.

[You can find the same proof using more formal notation in the script.]

3 Proof by Case Distinction:
Show that $(A \to B) \vee (B \to A)$ is a tautology.

To show that $(A \to B) \vee (B \to A)$ is a tautology we need to show that the formula yields true for all truth assignments of A and B.

We show that by case distinction. It is clear that in any truth assignment either $A = 0$ or $A = 1$.

Case 1 for $A=0$:

If a is false then $A \to B$ will always evaluate to true. Per definition of $\vee$, this means the entire formula evaluates to true since one side yields true.

Recall the truth table for $A \to B$:

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

Case 2 for $A=1$:

If A is true then $B \to A$ will always evaluate to true. Per definition of $\vee$, the entire formula will evaluate to true.

Since in both cases the statement is true, we showed that the statement is true in general.

[Yes, there are easier ways to show this probably :)]

④ Proof by Induction:
Show that de Morgans Rule holds for arbitrarily large formulas. I.e. show that for any $n \geq 2$:

$$\neg(X_1 \vee X_2 \vee \dots \vee X_n) \equiv \neg X_1 \wedge \neg X_2 \wedge \dots \wedge \neg X_n$$

We show the statement by Induction:

BASE CASE for $n=2$:

$\neg(X_1 \vee X_2) \equiv \neg X_1 \wedge \neg X_2$ per Lemma 2.1

INDUCTION HYPOTHESIS: We assume that for some k it holds that $\neg(X_1 \vee X_2 \vee \dots \vee X_k) \equiv \neg X_1 \wedge \neg X_2 \wedge \dots \wedge \neg X_k$.

INDUCTION STEP: Assume the statement holds for some $k \geq 2$. We now show that it then also holds for $k+1$:

$$\begin{aligned}
&\neg(X_1 \vee X_2 \vee \ldots \vee X_k \vee X_{k+1}) \\
&\equiv \neg((X_1 \vee X_2 \vee \ldots \vee X_k) \vee X_{k+1}) && \text{(associativity)} \\
&\equiv \neg(X_1 \vee X_2 \vee \ldots \vee X_k) \wedge \neg X_{k+1} && \text{(de Morgans Rule)} \\
&\equiv (\neg X_1 \wedge \neg X_2 \wedge \ldots \wedge \neg X_k) \wedge \neg X_{k+1} && \text{(Induction Hypothesis)} \\
&\equiv \neg X_1 \wedge \neg X_2 \wedge \ldots \wedge \neg X_k \wedge \neg X_{k+1}
\end{aligned}$$

here we used our assumption for k!

This shows the statement by Induction.

[Note that this proof is not very formal. You need to watch out when you do sth. like $A \wedge B \wedge \ldots \wedge X$ and we also left out brackets because we assume associativity as understood.]

(5) Proof by Pigeonhole Principle:

Show that if we select 400 random people at least two of them share a birthday.

One year has 365 days. We have 400 people. Per pigeonhole principle there exists a day where two people share their birthday.

[Exercise: Make this more formal as in the script.]

(6) Disprove by exhibiting a counterexample:

Disprove $\neg \exists x (x \in \mathbb{N} \wedge prim(x) \wedge \exists z (z \in \mathbb{N} \wedge x = 2z + 3z + 1))$

try to read this in words!

Counterexample:

11 is in $\mathbb{N}$, is prime and for $z = 2$: $2 \cdot 2 + 3 \cdot 2 + 1 = 11$

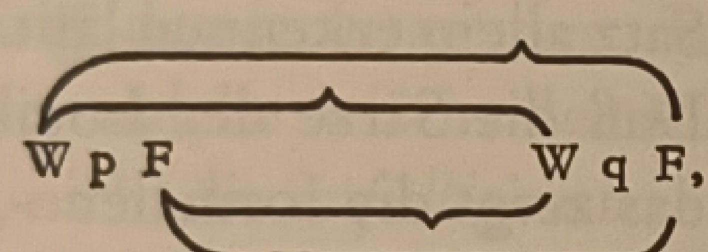
BONUS Proof by picture:

DO NOT DO THIS IN THE EXAM!

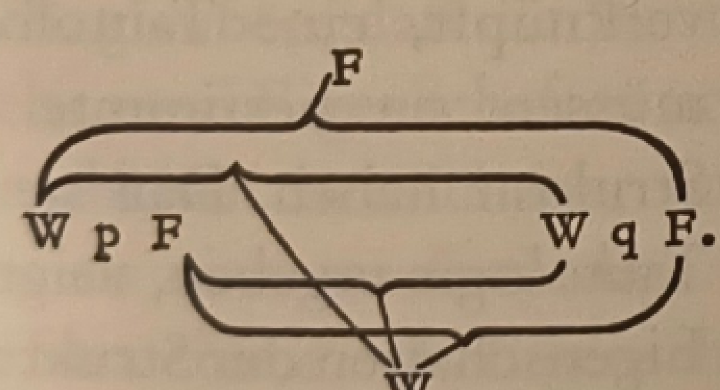
Try to prove that your favourite formula is a tautology by using Wittgensteins prove-by-picture method.

6.1202 Es ist klar, daß man zu demselben Zweck statt der Tautologien auch die Kontradiktionen verwenden könnte.

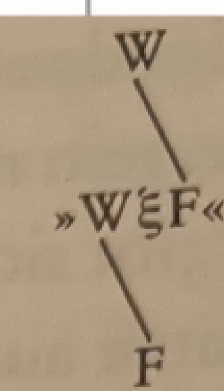
6.1203 Um eine Tautologie als solche zu erkennen, kann man sich, in den Fällen, in welchen in der Tautologie keine Allgemeinheitsbezeichnung vorkommt, folgender anschaulichen Methode bedienen: Ich schreibe statt »p«, »q«, »r« etc. »WpF«, »WqF«, »WrF« etc. Die Wahrheitskombinationen drücke ich durch Klammern aus, z. B.:



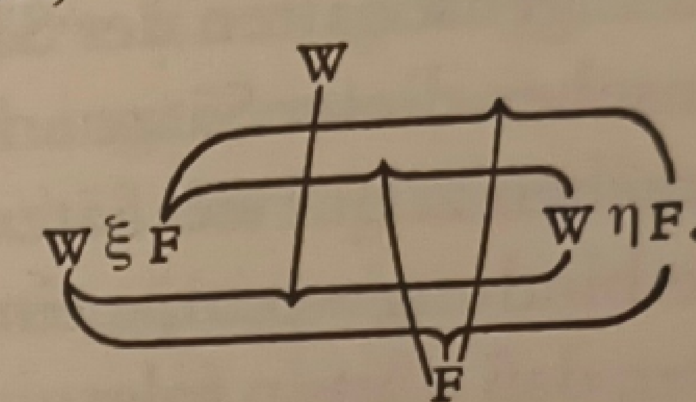
und die Zuordnung der Wahr- oder Falschheit des ganzen Satzes und der Wahrheitskombinationen der Wahrheitsargumente durch Striche auf folgende Weise:



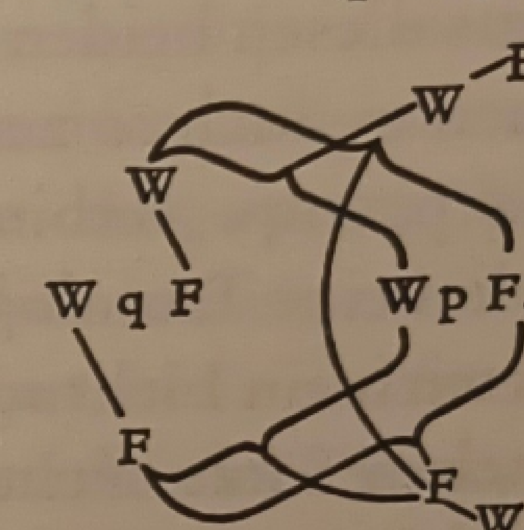
Dies Zeichen würde also z. B. den Satz $p \supset q$ darstellen. Nun will ich z. B. den Satz $\sim(p.\sim p)$ (Gesetz des Widerspruchs) daraufhin untersuchen, ob er eine Tautologie ist. Die Form »$\sim\xi$« wird in unserer Notation



geschrieben; die Form »$\xi.\eta$« so:



Daher lautet der Satz $\sim(p.\sim q)$ so:



Setzen wir hier statt »q« »p« ein und untersuchen die Verbindung der äußersten W und F mit den innersten, so ergibt sich, daß die Wahrheit des ganzen Satzes *allen* Wahrheitskombinationen seines Argumentes, seine Falschheit keiner der Wahrheitskombinationen zugeordnet ist.

6.121 Die Sätze der Logik demonstrieren die logischen Eigenschaften der Sätze, indem sie sie zu nichtssagenden Sätzen verbinden.

Diese Methode könnte man auch eine Nullmethode nennen. Im logischen Satz werden Sätze miteinander ins Gleichgewicht gebracht und der Zustand des Gleichge-

*Tractatus logico-philosophicus - edition suhrkamp p. 93f

This is not exam relevant and you do not need to understand it, but it is a cool alternative to truth tables.