Infos:

- Wünsche für die letzte Stunde?
  - z. B.:
    - Prüfung zusammen durchlösen
    - Mini-Prüfung für euch vorbereiten
    - Zusammenfassung der Theorie in Logik
    - Aufgaben zu Logik
    - etwas lustiges/entspanntes

Feedback:

- gut gelöst :)
- Bonus, Generator bestimmen: $F = \mathbb{Z}_3[x]_{/x^2+x+2 = m(x)}$

  $2x+2$ ist ein Generator von F^*

  $|F^*| = |F\setminus\{0\}| = 9-1 = 8 \Rightarrow$ mögl. Ordnungen: 1, 2, 4, 8

	$2x+2$
2	$(2x+2)^2 = 4x^2+8x+4 = x^2+2x+1 \overset{-m(x)}{=} x-1 = x+2 \neq 1$
4	$(2x+2)^4 = ((2x+2)^2)^2 = (x+2)^2 = x^2+4x+4 = x^2+x+1 \overset{-m(x)}{=} -1 = 2 \neq 1$

$\Rightarrow$ $ord(2x+2) = 8$ und $2x+2$ ist ein Generator

Let F be a finite field. Show that there exists a non-constant polyomial $p(x) \in F[x]$ with no roots.

Idee: Wie der Beweis, dass es ∞ viele Primzahlen gibt.

Nehme an nur endlich viele PZ $p_1, p_2, \dots, p_k$

Sei $m = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1 \Rightarrow R_{p_i}(m) = 1 \Rightarrow p_i \nmid m \quad \forall i$

Aber Widerspruch, da $m \neq p_i \ \forall i$ und m muss ein Primfaktor haben.

Sei $F = \{a_1, a_2, \dots, a_m\}$.

Wir wollen $p(x) \in F[x]$ s.d. $p(a) \neq 0 \quad \forall a \in F$.

$\Rightarrow$ wir nehmen uns alle Nullstellen a_i und "+1"

$p(x) = (x-a_0)\cdot(x-a_1)\cdot \dots \cdot (x-a_m) + 1$

$\Rightarrow p(a) = 0 + 1 \neq 0 \quad \forall a \in F$

$\Rightarrow$ p hat keine Nullstelle $\square$

Proof systems:

$A \vee B \equiv \neg A \to B$

(a) Prove or disprove: If Π complete, then Π_1 complete or Π_2 complete.

Nehme an Π_3 complete und $\underbrace{\Pi_1 \text{ nicht complete}}_{(*)}$

Sei $s_2 \in S_2$ s.d. $\tau_2(s_2) = 1$.

$\Rightarrow \tau(s_1, s_2) = 1 \quad \forall s_1 \in S_1$

Da Π complete gibt es $p_1, p_2 \in P_1 \times P_2$

s.d. $\mathcal{Q}((s_1, s_2), (p_1, p_2)) = 1$

$\Leftrightarrow \underline{\mathcal{Q}_1(s_1, p_1) = 1}$ oder $\underline{\mathcal{Q}_2(s_2, p_2) = 1}$

das wollen wir!

Wie können wir ausschliessen?

"Es gibt Aussagen, die wir nicht beweisen können"

(*) $\Rightarrow$ es gibt $s_1 \in S_1$ s.d. $\tau_1(s_1) = 1$ und $\underbrace{\mathcal{Q}(s_1, p_1) = 0 \quad \forall p_1 \in P_1}$.

jeder Beweis schlägt fehl

$\Rightarrow$ wähle s_1 wie oben.

$\Rightarrow \mathcal{Q}((s_1, s_2), (p_1, p_2)) = 1$ und $\mathcal{Q}_1(s_1, p_1) = 0$

$\Rightarrow \mathcal{Q}_2(s_2, p_2) = 1 \quad \square$

z.Z. Π_2 complete

$\to$ finde Beweis $p_2 \in P$

s.d. $\mathcal{Q}_2(s_2, p_2) = 1$

(b) Prove or disprove: If Π_1 sound or Π_2 sound, then Π sound.

Nehme an o.E.d.A. Π_1 sound.

Sei $(s_1, s_2) \in S_1 \times S_2$ s.d. $\mathcal{Q}((s_1, s_2), (p_1, p_2)) = 1$

mit $(p_1, p_2) \in P_1 \times P_2$.

$\Rightarrow \underset{(1)}{\mathcal{Q}(s_1, p_1) = 1}$ oder $\underset{(2)}{\mathcal{Q}(s_2, p_2) = 1}$.

Fall (1): $\Rightarrow \tau_1(s_1) = 1$ (da Π_1 sound)

$\Rightarrow \tau(s_1, s_2) = 1$

Fall (2): keine Info da wir nichts über Π_2 wissen!

$\Rightarrow$ wir können $\tau(s_1, s_2) = 0$ nicht ausschliessen.

Vlt. Gegenbsp.?

Wir brauchen: $\mathcal{Q}(s_1, p_1) = 0$

$\mathcal{Q}(s_2, p_2) = 1$

$\tau(s_1, s_2) = 0 \Leftrightarrow \tau_1(s_1) = 0$ und $\tau_2(s_2) = 0$

z.Z. Π sound

$\downarrow$

z.Z. $\tau(s_1, s_2) = 1$

$\Leftrightarrow \tau_1(s_1) = 1$ oder $\tau_2(s_2) = 1$

Gegenbsp. möglichst einfach wählen!

$\to$ wähle $S_1 = S_2 = P_1 = P_2 = \{0\}$.

$\tau_1(0) = 0$, $\mathcal{V}_1(0,0) = 0$ (→ Π_1 complete)

$\tau_2(0) = 0$, $\mathcal{V}_2(0,0) = 1$ (Π_2 unsound)

$\Rightarrow$ $\tau(0) = 0$, $\mathcal{V}((0,0),(0,0)) = 1$

$\Rightarrow$ Π unsound $\lightning$

Logical Calculi:

- Wichtig: nichts von Lemma 2.7. anwenden!

Die nötige Theorie wird sehr gut in Abschnitt 6.4.2 vom Skript erklärt :)

$$\emptyset \vdash_{R_1} F \to F$$
$$\{F\} \vdash_{R_2} F \vee F$$
$$\{\neg F \vee \neg F\} \vdash_{R_3} F \to (\neg F \vee \neg F)$$
$$\{F \to (G \vee H), G \to H\} \vdash_{R_4} F \to H$$

Formally derive $A \to \neg A$ from $\{\neg A\}$.

Strategie: von hinten anfangen

(1) letzter Schritt muss R_4 sein, der Rest passt nicht.

$$\{\underbrace{A}_{F} \to (G \vee \underbrace{\neg A}_{H}), G \to \underbrace{\neg A}_{H}\} \vdash_{R_4} \underbrace{A}_{F} \to \underbrace{\neg A}_{H}$$

$\Rightarrow$ wir müssen $A \to (G \vee \neg A)$ und $G \to \neg A$ herleiten

a) R_3, R_4 b) R_3, R_4

a) $\{A \to (L \vee (G \vee \neg A)), L \to (G \vee \neg A)\} \vdash_{R_4} \underbrace{A}_{F} \to \underbrace{(G \vee \neg A)}_{H}$ ✗

so etwas können wir nicht bekommen.
Nur R_4 passt, aber dann bekommen wir das Gleiche einfach länger.

b) $\{\underbrace{\neg A}_{\neg F} \vee \underbrace{\neg A}_{\neg F}\} \vdash_{R_3} \underbrace{A}_{F} \to (\underbrace{\neg A}_{\neg F} \vee \underbrace{\neg A}_{\neg F})$

$G = \neg A$

$\{\neg A\} \vdash_{R_2} \neg A \vee \neg A$

schon gegeben!

$\emptyset \vdash_{R_1} \underbrace{\neg A}_{F} \to \underbrace{\neg A}_{F}$

$\Rightarrow$

$\emptyset \vdash_{R_1} \neg A \to \neg A$ (1)

$\{\neg A\} \vdash_{R_2} \neg A \vee \neg A$ (2)

$\{(2)\} \vdash_{R_3} A \to (\neg A \vee \neg A)$ (3)

$\{(3), (1)\} \vdash_{R_4} A \to \neg A$

so muss am Ende eure Abgabe aussehen