1 Duas demonstrações comentadas

A VR e a VS vão vir com uma folha extra com dicas, e essas dicas vão incluir as duas demonstrações abaixo, mas sem os comentários em português.

1.1 Uma demonstração que usa as duas regras do '∃'

1) Suponha $a \in \mathbb{Z}$
2) Suponha $\mathsf{impar}(a)$
3) Então $\mathsf{impar}(a)$
4) Então $\exists b \in \mathbb{Z}.2b+1=a$ (Por 3, def)
5) Suponha $b \in \mathbb{Z}, 2b+1=a$
6) Então $\begin{aligned} a^2 &= (2b+1)^2 \\ &= 4b^2+4b+1 \\ &= 2(b^2+2b)+1 \end{aligned}$
7) Então $2b^2+2b \in \mathbb{Z} \land 2(b^2+2b)+1=a^2$
8) Então $\exists c \in \mathbb{Z}.2c+1=a^2$ $(c := 2b^2+2b)$ $(\exists F)$
9) Então $\mathsf{impar}(a^2)$
10) Então $\mathsf{impar}(a^2)$ (Usa 4, fecha 5) $(\exists D)$
11) Então $\mathsf{impar}(a) \to \mathsf{impar}(a^2)$ (fecha 2)
12) Então $\forall a \in \mathbb{Z}.\mathsf{impar}(a) \to \mathsf{impar}(a^2)$ (fecha 1) $(\forall D)$

A linha 3 corresponde a esta proposição,
3) $a \in \mathbb{Z}, \mathsf{impar}(a) \vdash \mathsf{impar}(a)$
que é bem fácil de provar em LK (tente!).

Na linha 4 nós usamos a justificativa "completa": o "def" quer dizer "por definição", que no caso é pela definição de impar, que é: Para $x \in \mathbb{Z}$, $\mathsf{impar}(x) := \exists a \in \mathbb{Z}.2a+1=x$ (veja os quadros de 15/agosto), mas muitas vezes vamos omitir a justificativa, ou parte dela. E lembre que vimos, nas aulas em que lemos as páginas 14 e 15 do livro da Judith Gersting, que podemos mudar os nomes de variáveis ligadas: $(\exists a \in \mathbb{Z}.2a+1=x) = (\exists b \in \mathbb{Z}.2b+1=x)$.

A linha 5 adiciona "$b \in \mathbb{Z}, 2b+1=a$" ao contexto pra gente poder mencionar a variável b nas linhas seguintes. Isto foi discutido nos quadros de 22/agosto a 4/setembro, principalmente na parte sobre "O erro mais comum".

A linha 6 é uma "prova álgebrica" (veja a p.27 do Scheinerman).

A passagem da linha 7 para a linha 8 (vamos escrever isto como "$7 \to 8$" daqui por diante) usa a regra fácil para o '∃', que no Scheinerman aparece como "Esquema de prova 7: afirmações existenciais", na p.65.

A passagem $9 \to 10$ usa a linha 4, que corresponde à proposição:
$a \in \mathbb{Z}, \mathsf{impar}(a) \vdash \exists b \in \mathbb{Z}.2b+1=a$,
para deletar as hipóteses $b \in \mathbb{Z}, 2b+1=a$ do contexto da linha 9; a linha 9 é:
$a \in \mathbb{Z}, \mathsf{impar}(a), b \in \mathbb{Z}, 2b+1=a \vdash \mathsf{impar}(a^2)$,
e a linha 10 é:
$a \in \mathbb{Z}, \mathsf{impar}(a) \vdash \mathsf{impar}(a^2)$.
A passagem $9 \to 10$ usa a "regra difícil para o '∃' ", que pode ser escrita assim em LK:

$$\frac{\Gamma \vdash \exists y \in B.P \quad \Gamma, y \in B, P \vdash Q}{\Gamma \vdash Q}\ (\exists D)$$

mas ela só é aplicável se a variável y não está livre na proposição Q.

A passagem $10 \to 11$ fica assim em LK (caso particular e versão geral):

$$\frac{a \in \mathbb{Z}, \mathsf{impar}(a) \vdash \mathsf{impar}(a^2)}{a \in \mathbb{Z} \vdash \mathsf{impar}(a) \to \mathsf{impar}(a^2)} \qquad \frac{\Gamma, P \vdash Q}{\Gamma \vdash P \to Q}$$

A passagem $11 \to 12$ fica assim (caso particular e versão geral):

$$\frac{a \in \mathbb{Z} \vdash \mathsf{impar}(a) \to \mathsf{impar}(a^2)}{\vdash \forall a \in \mathbb{Z}.\mathsf{impar}(a) \to \mathsf{impar}(a^2)}\,(\forall D) \qquad \frac{\Gamma, y \in B \vdash P}{\Gamma \vdash \forall y \in B.P}\,(\forall D)$$

1.2 Uma demonstração com lemas e indução

1) Lema: $\forall a \in \mathbb{Z}.\mathsf{par}(a) \to \mathsf{impar}(a+1)$
2) Lema: $\forall a \in \mathbb{Z}.\mathsf{impar}(a) \to \mathsf{par}(a+1)$
3) Suponha $n \in \mathbb{N}$
4) Então $n \in \mathbb{Z}$
5) Então $\mathsf{par}(n) \to \mathsf{impar}(n+1)$ (Por 1, com $a := n$) $(\forall F)$
6) Então $\mathsf{impar}(n) \to \mathsf{par}(n+1)$ (Por 2, com $a := n$) $(\forall F)$
7) Então $\mathsf{par}(n) \vee \mathsf{impar}(n) \to \mathsf{par}(n+1) \vee \mathsf{impar}(n+1)$ (Por 5 e 6)
8) Então $\forall n \in \mathbb{N}.\mathsf{par}(n) \vee \mathsf{impar}(n) \to \mathsf{par}(n+1) \vee \mathsf{impar}(n+1)$ (Fecha 4) $(\forall D)$
9) Lema: $\mathsf{par}(0)$
10) Então $\mathsf{par}(0) \vee \mathsf{impar}(0)$
11) Então $\forall n \in \mathbb{N}.\mathsf{par}(n) \vee \mathsf{impar}(n)$ (Por 10 e 8) (Ind)

O capítulo 1 do Scheinerman menciona "lemas" na p.15, mas nós não usamos lemas de forma muito explícita nos quadros do curso. As linhas "Lema:" da demonstração podem ser entendidas ou como linhas "Então" cuja justificativa, se fosse escrita explicitamente, seria "isto é uma cópia de uma proposição que já provamos na página tal", ou como uma linha "Suponha" mencionando uma proposição que vamos provar depois.

A linha 5 usa a regra fácil do '$\forall$', que é assim em LK:

$$\frac{\Gamma \vdash \forall y \in B.P \quad \Gamma \vdash t \in B}{\Gamma \vdash P[y := t]}\,(\forall F)$$

Repare que

$$(\forall F) \begin{bmatrix} \Gamma := \\ y := a \\ B := \mathbb{Z} \\ P := \mathsf{par}(a) \to \mathsf{impar}(a+1) \\ t := n \end{bmatrix}$$

dá exatamente a passagem de 1 e 4 para 5.

A passagem de 5 e 6 para 7 usa a idéia de que "todas as regras admissíveis são válidas" que discutimos na última aula do curso, em que pouquíssima gente veio (12/dezembro). Nós vimos em sala como verificar que uma certa regra era admissivel usando uma tabela com uma linha para cada caso, e dá pra fazer o mesmo pra esta regra aqui (mas a tabela ficaria grande):

$$\frac{\Gamma \vdash A \to B \quad \Gamma \vdash C \to D}{\Gamma \vdash A \vee C \to D \vee B}\,(Ad1)$$

Repare que

$$(Ad1) \begin{bmatrix} \Gamma := n \in \mathbb{N} \\ A := \mathsf{par}(n) \\ B := \mathsf{impar}(n+1) \\ C := \mathsf{impar}(n) \\ D := \mathsf{par}(n+1) \end{bmatrix}$$

dá exatamente a passagem de 5 e 6 para 7.

A passagem de 9 para 10 usa uma regra admissível bem fácil (qual? Exercício!), e a passagem de 10 e 8 para 11 usa indução — mas não as induções que provam equivalências de séries de números, que eu avisei que cairiam na P2! Lembre de fazer os exercícios 21.2 e 21.3 da p.193 do Scheinerman para treinar o tipo de indução que vai cair na P2!

Regras estruturais:
weakening, permutation, contraction

$$\frac{\Delta \vdash \Gamma}{\Delta, A \vdash \Gamma}\ (WL-) \qquad \frac{\Delta \vdash \Gamma}{\Delta \vdash \Gamma, A}\ (WR-)$$

$$\frac{\Delta, \Gamma \vdash \Sigma}{\Delta, A, \Gamma \vdash \Sigma}\ (WL) \qquad \frac{\Delta \vdash \Gamma, \Sigma}{\Delta \vdash \Gamma, A, \Sigma}\ (WR)$$

$$\frac{\Delta, A, B, \Gamma \vdash \Sigma}{\Delta, B, A, \Gamma \vdash \Sigma}\ (PL) \qquad \frac{\Delta \vdash \Gamma, A, B, \Sigma}{\Delta \vdash \Gamma, B, A, \Sigma}\ (PR)$$

$$\frac{\Delta, A, A \vdash \Gamma}{\Delta, A \vdash \Gamma}\ (CL-) \qquad \frac{\Delta \vdash \Gamma, A, A}{\Delta \vdash \Gamma, A}\ (CR-)$$

$$\frac{\Delta, A, A, \Gamma \vdash \Sigma}{\Delta, A, \Gamma \vdash \Sigma}\ (CL) \qquad \frac{\Delta \vdash \Gamma, A, A, \Sigma}{\Delta \vdash \Gamma, A, \Sigma}\ (CR)$$

Identidade e cut:

$$\frac{}{A \vdash A}\ (I)$$

$$\frac{\Gamma \vdash \Delta, A \quad A, \Sigma \vdash \Pi}{\Gamma, \Sigma \vdash \Delta, \Pi}\ (Cut)$$

Regras lógicas pro $\land$:

$$\frac{\Gamma \vdash \Delta, A \land B}{\Gamma \vdash \Delta, A}\ (R\land_1)$$

$$\frac{\Gamma \vdash \Delta, A \land B}{\Gamma \vdash \Delta, B}\ (R\land_2)$$

$$\frac{\Gamma, A \land B \vdash \Delta}{\Gamma, A, B \vdash \Delta}\ (L\land)$$

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma \vdash B, \Pi}{\Gamma, \Sigma \vdash A \land B, \Delta, \Pi}\ (R\land)$$

Regras lógicas pro $\lor$:

$$\frac{\Gamma, A \lor B \vdash \Delta}{\Gamma, A \vdash \Delta}\ (L\lor_1)$$

$$\frac{\Gamma, A \lor B \vdash \Delta}{\Gamma, B \vdash \Delta}\ (L\lor_2)$$

$$\frac{\Gamma \vdash A \lor B, \Delta}{\Gamma \vdash A, B, \Delta}\ (R\lor)$$

$$\frac{\Gamma, A \vdash \Delta \quad \Sigma, B \vdash \Pi}{\Gamma, \Sigma, A \lor B \vdash \Delta, \Pi}\ (L\lor)$$

Regras lógicas pro $\to$:

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma, B \vdash \Pi}{\Gamma, \Sigma, A \to B \vdash \Delta, \Pi}\ (\to L)$$

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma \vdash B, \Pi}{\Gamma \vdash A \to B, \Delta}\ (\to R)$$

Regras lógicas pro $\neg$:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ (\neg L)$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ (\neg R)$$

Regras lógicas para o $\forall$:

$$\frac{\Gamma \vdash P, \Delta}{\Gamma \vdash \forall y.P, \Delta}\ (\forall R)^*$$

$$\frac{\Gamma, P[y := t] \vdash \Delta}{\Gamma, \forall y.P \vdash \Delta}\ (\forall L)$$

Regras lógicas para o $\exists$:

$$\frac{\Gamma \vdash P[y := t], \Delta}{\Gamma \vdash \exists y.P, \Delta}\ (\exists R)$$

$$\frac{\Gamma, P \vdash \Delta}{\Gamma, \exists y.P \vdash \Delta}\ (\exists L)^*$$

Nas regras $(\forall R)^*$ e $(\exists L)^*$ o '$*$' quer dizer que o y não pode aparecer como variável livre em Γ ou Δ.