FMC1, 2022.1
(Turma N12 do Thanos)

Prova 1.1
(points: 24; bonus: $0^\flat$; time: 90')

Nome: Θάνος **Gabarito**

2022-04-18

Regras:

I. Não vires esta página antes do começo da prova.

II. Nenhuma consulta de qualquer forma.

III. Nenhum aparelho ligado (por exemplo: celular, tablet, notebook, *etc.*).[1]

IV. Nenhuma comunicação de qualquer forma e para qualquer motivo.

V. $(\forall x)\,[\,\text{Colar}(x) \implies \neg\text{Passar}(x, \text{FMC1})\,]$.[2]

VI. Use caneta para tuas respostas.

VII. Responda dentro das caixas indicadas.

VIII. Escreva teu nome em *cada* folha de rascunho extra *antes de usá-la.*

IX. Entregue *todas* as folhas de rascunho extra, juntas com tua prova.

X. Nenhuma prova será aceita depois do fim do tempo—mesmo se for atraso de 1 segundo.

GABARITO

Lembram-se:

Dados. Os inteiros $(\mathbb{Z}; 0, 1, +, -, \cdot)$ com tipos:

$$0 : \mathsf{Int} \qquad 1 : \mathsf{Int} \qquad + : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int} \qquad - : \mathsf{Int} \to \mathsf{Int} \qquad \cdot : \mathsf{Int} \times \mathsf{Int} \to \mathsf{Int}.$$

Axiomas (até agora).

`(ZA-Ass)`	$(a+b)+c = a+(b+c)$	$(a\cdot b)\cdot c = a\cdot(b\cdot c)$	`(ZM-Ass)`
`(ZA-IdR)`	$a+0 = a$	$a\cdot 1 = a$	`(ZM-IdR)`
`(ZA-Com)`	$a+b = b+a$	$a\cdot b = b\cdot a$	`(ZM-Com)`
`(ZA-InvR)`	$a+(-a) = 0$		
`(ZB-DistR)`	$(a+b)\cdot c = a\cdot c + b\cdot c$	$a\cdot b = 0 \implies a = 0$ ou $b = 0$	`(ZB-NZD)`

Esclarecimento:

Suas demonstrações/refutações precisam ser na linguagem "low-level" que temos elaborado nas aulas. (Escreva apenas a parte de "código". *Não inclua* os Dados/Alvo no teu texto!)

Boas provas!

[1] Ou seja, *desligue antes* da prova.
[2] Se essa regra não faz sentido, melhor desistir desde já.

(8) **A**

Usando os: $\rightarrow, \times, (,)$, e os Var, Nat, Int, Real, String, Set, Prop, Cmd, Type, Obj, Person atribua a tipagem que tu considera melhor para os seguinte:

Obs.: as linhas representam "buracos" ou "lacunas".

A mãe de _____ tem _____ filhos. : Person $\times$ Nat $\rightarrow$ Prop

_ $+ 3 \leq 12$. : Int $\rightarrow$ Prop

o pai de _____ : Person $\rightarrow$ Person

_ + _ | _. : Int $\times$ Int $\times$ Int $\rightarrow$ Prop

Seja _ inteiro. : Var $\rightarrow$ Cmd

Suponha _____. : Prop $\rightarrow$ Cmd

A palavra _____ tem tamanho _____. : String $\times$ Nat $\rightarrow$ Prop

Seja x _____ tal que _____. : Type $\times$ Prop $\rightarrow$ Cmd

(8) # B

Estamos no mundo dos inteiros $(\mathbb{Z}; 0, 1, +, -, \times)$.

(4) **B1.** Defina (com definição completa, em português matemático) a relação $\mid$ de *divide*, e o predicado Odd(_) de «ser ímpar».

(2) Definição (divide).

> Sejam a, b inteiros. Dizemos que a *divide* b sse existe inteiro k tal que $ak = b$.

(2) Definição (ímpar).

> Seja a inteiro. Dizemos que a *é ímpar* sse existe inteiro k tal que $a = 2k + 1$.

(4) **B2.** $(+)$-cancelamento pela esquerda.
Para quaisquer inteiros a, u, v,

$$a + u = a + v \implies u = v.$$

Demonstração.

> Sejam a, u, v inteiros.
> Suponha $a + u = a + v$ [(1)].
> Calculamos:
>
> $$\begin{aligned}
> u &= 0 + u && \text{(ZA-IdL com } a := u\text{)} \\
> &= ((-a) + a) + u && \text{(ZA-InvL com } a := a\text{)} \\
> &= (-a) + (a + u) && \text{(ZA-Ass com } a, b, c := -a, a, u\text{)} \\
> &= (-a) + (a + v) && \text{((1))} \\
> &= ((-a) + a) + v && \text{(ZA-Ass com } a, b, c := -a, a, v\text{)} \\
> &= 0 + v && \text{(ZA-InvL com } a := a\text{)} \\
> &= v. && \text{(ZA-IdL com } a := v\text{)}
> \end{aligned}$$

(8) # C

Demonstre completamente **até um** dos teoremas seguintes:

(6) **C1.** Demonstre que *para quaisquer a, b inteiros, a equação*

$$a + x = b$$

com incógnito x tem resolução única, ou seja: existe único inteiro x tal que $a + x = b$.
Demonstração.

Sejam a, b inteiros.
Existência.
Basta demonstrar que $a + ((-a) + b) = b$.
Calculamos:

$$\begin{aligned} a + ((-a) + b) &= (a + (-a)) + b && \text{(ZA-Ass)} \\ &= 0 + b && \text{(ZA-InvR)} \\ &= b && \text{(ZA-IdL)} \end{aligned}$$

Unicidade.
Sejam u, v inteiros tais que $a + u = b$ (1) e $a + v = b$ (2).
Vou demonstrar $u = v$.
Calculamos:

$$\begin{aligned} (-a) + b &= (-a) + (a + u) && ((1)) \\ &= ((-a) + a) + u && \text{(ZA-Ass)} \\ &= 0 + u && \text{(ZA-InvL)} \\ &= u && \text{(ZA-IdL)} \end{aligned}$$

Similarmente, usando a (2) em vez da (1) temos $(-a) + b = v$.
Logo $u = v$.

(8) **C2.** Zero é um $(\cdot)$-anihilador esquerdo.
Para qualquer inteiro x, $0 \cdot x = 0$.
Demonstração.

Seja x inteiro.
Como 0 é uma resolução da $x + ? = x$ [pelo ZA-IdR com $a := x$] basta demonstrar que $0 \cdot x$ também é [pela **C1**-Unicidade com $u, v := 0, 0 \cdot x$].
Calculamos:

$$\begin{aligned} x + 0 \cdot x &= 1 \cdot x + 0 \cdot x && \text{(ZM-IdL)} \\ &= (1 + 0) \cdot x && \text{(ZB-DistrR)} \\ &= 1 \cdot x && \text{(ZA-IdR)} \\ &= x. && \text{(ZM-IdL)} \end{aligned}$$

Só isso mesmo.

Lemma (ZA-InvL). $(\forall a)\,[\,(-a)+a=0\,]$.
Seja a inteiro.
Calculamos:

$$\begin{aligned}(-a)+a &= a+(-a) && \text{(ZA-Com com } a,b := -a,a)\\ &= 0. && \text{(ZA-IdR com } a := a)\end{aligned}$$

Lemma (ZA-IdL). $(\forall a)\,[\,0+a=a\,]$.
Seja a inteiro.
Temos $0+a=a+0=a$ pelas ZA-Com e ZA-IdR respectivamente.
Lemma (ZM-IdL). $(\forall a)\,[\,1\cdot a=a\,]$.
Similar, usando as ZM-Com e ZM-IdR.