Teoria de Modelos e Aplicações

Caio Lopes, Henrique Lecco

ICMC - USP

28 de julho de 2020

Revisão

Revisão

Definição

Uma teoria é $\forall_2$ se suas fórmulas podem ser escritas na forma "para todos $x_1, x_2, ..., x_n$ existem $y_1, y_2, ..., y_m$ tais que..."

Revisão

Definição

Uma teoria é $\forall_2$ se suas fórmulas podem ser escritas na forma "para todos $x_1, x_2, \ldots, x_n$ existem $y_1, y_2, \ldots, y_m$ tais que..."

Definição

Uma teoria é κ-categórica se todo modelo de cardinalidade κ é isomorfo.

Revisão

Definição

Uma teoria T é *modelo-completa* se, dados $\mathcal{A}, \mathcal{B}$ modelos de T, então $\mathcal{A} \subset \mathcal{B} \Rightarrow \mathcal{A} \prec \mathcal{B}$.

Revisão

Definição

Uma teoria T é *modelo-completa* se, dados $\mathcal{A}, \mathcal{B}$ modelos de T, então $\mathcal{A} \subset \mathcal{B} \Rightarrow \mathcal{A} \prec \mathcal{B}$.

Teorema (Teste de Lindström)

Seja λ um cardinal não enumerável. Se T é uma L-teoria $\forall_2$ e λ-categórica, então ela é modelo-completa.

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos.

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos. Por exemplo:

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos. Por exemplo:

- Comutatividade da soma: $\forall a \forall b(a + b = b + a)$;

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos. Por exemplo:

- Comutatividade da soma: $\forall a \forall b(a + b = b + a)$;
- Elemento neutro do produto: $\forall a(a.1 = a)$;

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos. Por exemplo:

- Comutatividade da soma: $\forall a \forall b(a + b = b + a)$;
- Elemento neutro do produto: $\forall a(a.1 = a)$;
- Existência de inverso do produto: $\forall a \exists b(a.b = 1)$.

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos. Por exemplo:

- Comutatividade da soma: $\forall a \forall b(a + b = b + a)$;
- Elemento neutro do produto: $\forall a(a.1 = a)$;
- Existência de inverso do produto: $\forall a \exists b(a.b = 1)$.

Afirmação:

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos. Por exemplo:

- Comutatividade da soma: $\forall a \forall b (a + b = b + a)$;
- Elemento neutro do produto: $\forall a (a.1 = a)$;
- Existência de inverso do produto: $\forall a \exists b (a.b = 1)$.

Afirmação: A teoria de corpos é $\forall_2$.

Teoria de Corpos

Considere $L_{ring} = \{0, 1, +, .\}$ Note que com essa linguagem podemos escrever todos os axiomas da teoria de corpos. Por exemplo:

- Comutatividade da soma: $\forall a \forall b (a + b = b + a)$;
- Elemento neutro do produto: $\forall a (a.1 = a)$;
- Existência de inverso do produto: $\forall a \exists b (a.b = 1)$.

Afirmação: A teoria de corpos é $\forall_2$.

Denotamos a teoria de corpos de T_{corpo}.

Corpos algebricamente fechados

Definição

Um corpo K é algebricamente fechado (AC) se dado $p(x) \in K[x]$ com $deg(p) \geq 1$, existe $a \in K$ tal que $p(a) = 0$.

Corpos algebricamente fechados

Definição

Um corpo K é algebricamente fechado (AC) se dado $p(x) \in K[x]$ com $deg(p) \geq 1$, existe $a \in K$ tal que $p(a) = 0$.

Como transformar isso em uma fórmula?

Corpos algebricamente fechados

Definição

Um corpo K é algebricamente fechado (AC) se dado $p(x) \in K[x]$ com $deg(p) \geq 1$, existe $a \in K$ tal que $p(a) = 0$.

Como transformar isso em uma fórmula? Não dá!

Corpos algebricamente fechados

Definição

Um corpo K é algebricamente fechado (AC) se dado $p(x) \in K[x]$ com $deg(p) \geq 1$, existe $a \in K$ tal que $p(a) = 0$.

Como transformar isso em uma fórmula? Não dá! O que podemos fazer é uma fórmula para cada grau, da seguinte forma:

Corpos algebricamente fechados

$$\forall a_0 \forall a_1 \exists x (a_0 + a_1 x = 0)$$

Corpos algebricamente fechados

$$\forall a_0 \forall a_1 \exists x (a_0 + a_1 x = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \exists x (a_0 + a_1 x + a_2 x^2 = 0)$$

Corpos algebricamente fechados

$$\forall a_0 \forall a_1 \exists x (a_0 + a_1 x = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \exists x (a_0 + a_1 x + a_2 x^2 = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \forall a_3 \exists x (a_0 + a_1 x + a_2 x^2 + a_3 x^3 = 0)$$

Corpos algebricamente fechados

$$\forall a_0 \forall a_1 \exists x (a_0 + a_1 x = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \exists x (a_0 + a_1 x + a_2 x^2 = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \forall a_3 \exists x (a_0 + a_1 x + a_2 x^2 + a_3 x^3 = 0)$$

...e assim por diante.

Corpos algebricamente fechados

$$\forall a_0 \forall a_1 \exists x (a_0 + a_1 x = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \exists x (a_0 + a_1 x + a_2 x^2 = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \forall a_3 \exists x (a_0 + a_1 x + a_2 x^2 + a_3 x^3 = 0)$$

...e assim por diante.

Definimos AC como a coleção de fórmulas que expressam um corpo ser algebricamente fechado:

Corpos algebricamente fechados

$$\forall a_0 \forall a_1 \exists x (a_0 + a_1 x = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \exists x (a_0 + a_1 x + a_2 x^2 = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \forall a_3 \exists x (a_0 + a_1 x + a_2 x^2 + a_3 x^3 = 0)$$

...e assim por diante.

Definimos AC como a coleção de fórmulas que expressam um corpo ser algebricamente fechado:

$$AC = \{\forall a_0 \forall a_1 ... \forall a_n \exists x (a_0 + a_1 x + ... + a_n x^n = 0) : n \in \mathbb{N}\}$$

Corpos algebricamente fechados

$$\forall a_0 \forall a_1 \exists x (a_0 + a_1 x = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \exists x (a_0 + a_1 x + a_2 x^2 = 0)$$

$$\forall a_0 \forall a_1 \forall a_2 \forall a_3 \exists x (a_0 + a_1 x + a_2 x^2 + a_3 x^3 = 0)$$

...e assim por diante.

Definimos AC como a coleção de fórmulas que expressam um corpo ser algebricamente fechado:

$$AC = \{\forall a_0 \forall a_1 ... \forall a_n \exists x (a_0 + a_1 x + ... + a_n x^n = 0) : n \in \mathbb{N}\}$$

Observe que AC também é $\forall_2$.

Corpos algebricamente fechados

Definição

Chamamos de ACF a teoria de corpos algebricamente fechados, que nada mais é que a união de AC e T_{corpo}.

Corpos algebricamente fechados

Definição

Chamamos de ACF a teoria de corpos algebricamente fechados, que nada mais é que a união de AC e T_{corpo}.

Como ambas AC e T_{corpo} são $\forall_2$, então ACF também é $\forall_2$

Corpos algebricamente fechados

Nosso objetivo é obter que ACF é modelo-completo.

Corpos algebricamente fechados

Nosso objetivo é obter que ACF é modelo-completo. Faremos isso utilizando o teste de Lindström, mas não diretamente.

Corpos algebricamente fechados

Nosso objetivo é obter que ACF é modelo-completo. Faremos isso utilizando o teste de Lindström, mas não diretamente.

É possível falarmos sobre a característica de um corpo utilizando fórmulas de primeira ordem.

Corpos algebricamente fechados

Nosso objetivo é obter que ACF é modelo-completo. Faremos isso utilizando o teste de Lindström, mas não diretamente.

É possível falarmos sobre a característica de um corpo utilizando fórmulas de primeira ordem.

Note que não existe uma única fórmula de primeira ordem que formalize o conceito de característica!

Corpos algebricamente fechados

Nosso objetivo é obter que ACF é modelo-completo. Faremos isso utilizando o teste de Lindström, mas não diretamente.

É possível falarmos sobre a característica de um corpo utilizando fórmulas de primeira ordem.

Note que não existe uma única fórmula de primeira ordem que formalize o conceito de característica! O que faremos é definir uma fórmula para cada p:

Característica de um corpo

Definição

A característica de um corpo é p se $1 + 1 + ... + 1 = 0$ (p-vezes). Caso isso nunca ocorra, a característica é 0.

Característica de um corpo

Definição

A característica de um corpo é p se $1 + 1 + ... + 1 = 0$ (p-vezes). Caso isso nunca ocorra, a característica é 0.

Portanto a teoria de corpos algebricamente fechados de característica p é dada por $T_{corpo} \cup AC \cup \{p.1 = 0\}$ e a denotamos por ACF_p.

Característica de um corpo

Definição

A característica de um corpo é p se $1 + 1 + ... + 1 = 0$ (p-vezes). Caso isso nunca ocorra, a característica é 0.

Portanto a teoria de corpos algebricamente fechados de característica p é dada por $T_{corpo} \cup AC \cup \{p.1 = 0\}$ e a denotamos por ACF_p.

No caso de característica 0, ela é dada por $T_{corpo} \cup AC \cup \{p.1 \neq 0 : \text{p}primo\}$ e a denotamos por ACF_0.

Grau de transcendência

Definição

Seja L/K uma extensão de corpos.

Grau de transcendência

Definição

Seja L/K uma extensão de corpos. Dizemos que $S \subset L$ é algebricamente independente de K se

Grau de transcendência

Definição

Seja L/K uma extensão de corpos. Dizemos que $S \subset L$ é algebricamente independente de K se para todo $p(x) \in K[X]$,

Grau de transcendência

Definição

Seja L/K uma extensão de corpos. Dizemos que $S \subset L$ é algebricamente independente de K se para todo $p(x) \in K[X]$, $p(x)$ não tem raiz em S.

Grau de transcendência

Definição

Seja L/K uma extensão de corpos. Dizemos que $S \subset L$ é algebricamente independente de K se para todo $p(x) \in K[X]$, $p(x)$ não tem raiz em S.
O grau de transcendência de uma extensão de corpos L/K é o maior cardinal de um subconjunto algebricamente independente de L sobre K.

Grau de transcendência

Definição

Seja L/K uma extensão de corpos. Dizemos que $S \subset L$ é algebricamente independente de K se para todo $p(x) \in K[X]$, $p(x)$ não tem raiz em S.

O grau de transcendência de uma extensão de corpos L/K é o maior cardinal de um subconjunto algebricamente independente de L sobre K.

Grau de transcendência

Definição

Seja L/K uma extensão de corpos. Dizemos que $S \subset L$ é algebricamente independente de K se para todo $p(x) \in K[X]$, $p(x)$ não tem raiz em S.
O grau de transcendência de uma extensão de corpos L/K é o maior cardinal de um subconjunto algebricamente independente de L sobre K.

Em certo sentido, isso mede o quão "espaçosa" é essa extensão.

Definição

O grau de uma extensão de corpos L/K é a dimensão do espaço vetorial L sobre o corpo K.

Dois resultados algébricos

Lemma (Lema 1)

Dois corpos algebricamente fechados de mesma característica e mesmo grau de transcendência sobre o seu subcorpo $\mathbb{F}_p$ (ou $\mathbb{Q}$) são isomorfos.

Dois resultados algébricos

Lemma (Lema 1)

Dois corpos algebricamente fechados de mesma característica e mesmo grau de transcendência sobre o seu subcorpo $\mathbb{F}_p$ *(ou* $\mathbb{Q}$*) são isomorfos.*

https://math.stackexchange.com/questions/3623568

Dois resultados algébricos

Lemma (Lema 1)

Dois corpos algebricamente fechados de mesma característica e mesmo grau de transcendência sobre o seu subcorpo $\mathbb{F}_p$ (ou $\mathbb{Q}$) são isomorfos.

https://math.stackexchange.com/questions/3623568

Lemma (Lema 2)

Seja κ um cardinal não enumerável. Toda extensão de grau κ tem grau de transcendência κ.

Dois resultados algébricos

Lemma (Lema 1)

Dois corpos algebricamente fechados de mesma característica e mesmo grau de transcendência sobre o seu subcorpo $\mathbb{F}_p$ (ou $\mathbb{Q}$) são isomorfos.

https://math.stackexchange.com/questions/3623568

Lemma (Lema 2)

Seja κ um cardinal não enumerável. Toda extensão de grau κ tem grau de transcendência κ.

Ideia da prova:

Dois resultados algébricos

Lemma (Lema 1)

Dois corpos algebricamente fechados de mesma característica e mesmo grau de transcendência sobre o seu subcorpo $\mathbb{F}_p$ (ou $\mathbb{Q}$) são isomorfos.

https://math.stackexchange.com/questions/3623568

Lemma (Lema 2)

Seja κ um cardinal não enumerável. Toda extensão de grau κ tem grau de transcendência κ.

Ideia da prova: existem no máximo enumeráveis polinômios com coeficientes em $\mathbb{F}_p$ ou $\mathbb{Q}$.

Dois resultados algébricos

Lemma (Lema 1)

Dois corpos algebricamente fechados de mesma característica e mesmo grau de transcendência sobre o seu subcorpo $\mathbb{F}_p$ (ou $\mathbb{Q}$) são isomorfos.

https://math.stackexchange.com/questions/3623568

Lemma (Lema 2)

Seja κ um cardinal não enumerável. Toda extensão de grau κ tem grau de transcendência κ.

Ideia da prova: existem no máximo enumeráveis polinômios com coeficientes em $\mathbb{F}_p$ ou $\mathbb{Q}$. Além disso, o grau ser κ nos permite construir um conjunto de cardinalidade κ que não vai se anular em nenhum dos polinômios.

ACF

Já vimos que ACF é $\forall_2$,

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são.

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável.

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável. Logo, estamos nas condições de utilizar o teste de Lindström, obtendo que ACF_p e ACF_0 são modelo completo.

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável. Logo, estamos nas condições de utilizar o teste de Lindström, obtendo que ACF_p e ACF_0 são modelo completo.

Theorem

ACF é modelo-completo

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável. Logo, estamos nas condições de utilizar o teste de Lindström, obtendo que ACF_p e ACF_0 são modelo completo.

Theorem

ACF é modelo-completo

Prova: Sejam $\mathcal{A}, \mathcal{B}$ modelos de ACF tais que $\mathcal{A} \subset \mathcal{B}$.

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável. Logo, estamos nas condições de utilizar o teste de Lindström, obtendo que ACF_p e ACF_0 são modelo completo.

Theorem

ACF é modelo-completo

Prova: Sejam $\mathcal{A}, \mathcal{B}$ modelos de ACF tais que $\mathcal{A} \subset \mathcal{B}$. Note que, nesse caso, ambos precisam ter a mesma característica.

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável. Logo, estamos nas condições de utilizar o teste de Lindström, obtendo que ACF_p e ACF_0 são modelo completo.

Theorem

ACF é modelo-completo

Prova: Sejam $\mathcal{A}, \mathcal{B}$ modelos de ACF tais que $\mathcal{A} \subset \mathcal{B}$. Note que, nesse caso, ambos precisam ter a mesma característica. Portanto ambos são modelos para algum ACF_p ou para ACF_0.

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável. Logo, estamos nas condições de utilizar o teste de Lindström, obtendo que ACF_p e ACF_0 são modelo completo.

Theorem

ACF é modelo-completo

Prova: Sejam $\mathcal{A}, \mathcal{B}$ modelos de ACF tais que $\mathcal{A} \subset \mathcal{B}$. Note que, nesse caso, ambos precisam ter a mesma característica. Portanto ambos são modelos para algum ACF_p ou para ACF_0. Mas, como vimos anteriormente, essas teorias são modelo-completo.

ACF

Já vimos que ACF é $\forall_2$, portanto ACF_p e ACF_0 também são. Pelo Lema 2, essas teorias são $\kappa-$categóricas se κ for não enumerável. Logo, estamos nas condições de utilizar o teste de Lindström, obtendo que ACF_p e ACF_0 são modelo completo.

Theorem

ACF é modelo-completo

Prova: Sejam $\mathcal{A}, \mathcal{B}$ modelos de ACF tais que $\mathcal{A} \subset \mathcal{B}$. Note que, nesse caso, ambos precisam ter a mesma característica. Portanto ambos são modelos para algum ACF_p ou para ACF_0. Mas, como vimos anteriormente, essas teorias são modelo-completo. Portanto $\mathcal{A} \prec \mathcal{B}$.

Nullstellensatz

Theorem

Seja K um corpo algebricamente fechado.

Nullstellensatz

Theorem

Seja K um corpo algebricamente fechado. Seja I um ideal próprio de $K[x_1, ..., x_n]$.

Nullstellensatz

Theorem

Seja K um corpo algebricamente fechado. Seja I um ideal próprio de $K[x_1, ..., x_n]$. Então existem $a_1, ..., a_n \in K$ tais que $f(a_1, ..., a_n) = 0$ para todo $f(x_1, ..., x_n) \in I$.

Nullstellensatz

Esse teorema foi provado por David Hilbert em 1900.

Nullstellensatz

Esse teorema foi provado por David Hilbert em 1900.

É ele que nos permite transitar entre Geometria e Álgebra, uma vez que faz a conexão direta entre propriedades algébricas de $K[x_1, ..., x_n]$ e propriedades geométricas de variedades algébricas cujo anel de coordenadas é K.

Inicialmente, Hilbert queria mostrar quais polinômios $p(x, y) \in \mathbb{C}[x, y]$ se anulam no círculo $x^2 + y^2 = 1$.

Inicialmente, Hilbert queria mostrar quais polinômios $p(x, y) \in \mathbb{C}[x, y]$ se anulam no círculo $x^2 + y^2 = 1$. Obviamente o polinômio $p(x, y) = x^2 + y^2 - 1$ satisfaz, mas quais mais?

Inicialmente, Hilbert queria mostrar quais polinômios $p(x,y) \in \mathbb{C}[x,y]$ se anulam no círculo $x^2 + y^2 = 1$. Obviamente o polinômio $p(x,y) = x^2 + y^2 - 1$ satisfaz, mas quais mais?

Hilbert descobriu que apenas os polinômios da forma $p(x,y) = q(x,y)(x^2 + y^2 - 1)$, onde $q(x,y)$ é um polinômio qualquer de $\mathbb{C}[x,y]$, zeram no círculo.

Inicialmente, Hilbert queria mostrar quais polinômios $p(x, y) \in \mathbb{C}[x, y]$ se anulam no círculo $x^2 + y^2 = 1$. Obviamente o polinômio $p(x, y) = x^2 + y^2 - 1$ satisfaz, mas quais mais?

Hilbert descobriu que apenas os polinômios da forma $p(x, y) = q(x, y)(x^2 + y^2 - 1)$, onde $q(x, y)$ é um polinômio qualquer de $\mathbb{C}[x, y]$, zeram no círculo. O Nullstellensatz é a generalização desse resultado.

Nullstellensatz - demonstração

Theorem

Seja F um corpo algebricamente fechado.

Nullstellensatz - demonstração

Theorem

Seja F um corpo algebricamente fechado. Seja I um ideal próprio de $F[x_1, ..., x_n]$.

Nullstellensatz - demonstração

Theorem

Seja F um corpo algebricamente fechado. Seja I um ideal próprio de $F[x_1, ..., x_n]$. Então existem $a_1, ..., a_n$ tais que $f(a_1, ..., a_n) = 0$ para todo $f(x_1, ..., x_n) \in I$.

Nullstellensatz - demonstração

Theorem

Seja F um corpo algebricamente fechado. Seja I um ideal próprio de $F[x_1, ..., x_n]$. Então existem $a_1, ..., a_n$ tais que $f(a_1, ..., a_n) = 0$ para todo $f(x_1, ..., x_n) \in I$.

Prova: Primeiro, lembre-se que um anel é dito Noetheriano se seus ideais são finitamente gerados.

Nullstellensatz - demonstração

Theorem

Seja F um corpo algebricamente fechado. Seja I um ideal próprio de $F[x_1, ..., x_n]$. Então existem $a_1, ..., a_n$ tais que $f(a_1, ..., a_n) = 0$ para todo $f(x_1, ..., x_n) \in I$.

Prova: Primeiro, lembre-se que um anel é dito Noetheriano se seus ideais são finitamente gerados. Agora note que $F[x_1, ..., x_n]$ é Noetheriano, pois:

Nullstellensatz - demonstração

Theorem

Seja F um corpo algebricamente fechado. Seja I um ideal próprio de $F[x_1, ..., x_n]$. Então existem $a_1, ..., a_n$ tais que $f(a_1, ..., a_n) = 0$ para todo $f(x_1, ..., x_n) \in I$.

Prova: Primeiro, lembre-se que um anel é dito Noetheriano se seus ideais são finitamente gerados. Agora note que $F[x_1, ..., x_n]$ é Noetheriano, pois:

1. Todo corpo é Noetheriano, pois todo ideal é gerado pela unidade do produto.

Nullstellensatz - demonstração

Theorem

Seja F um corpo algebricamente fechado. Seja I um ideal próprio de $F[x_1, ..., x_n]$. Então existem $a_1, ..., a_n$ tais que $f(a_1, ..., a_n) = 0$ para todo $f(x_1, ..., x_n) \in I$.

Prova: Primeiro, lembre-se que um anel é dito Noetheriano se seus ideais são finitamente gerados. Agora note que $F[x_1, ..., x_n]$ é Noetheriano, pois:

1. Todo corpo é Noetheriano, pois todo ideal é gerado pela unidade do produto.
2. Se A é Noetheriano, então $A[x_1, ..., x_n]$ também é (Teorema da base de Hilbert)

Nullstellensatz - demonstração

Sejam $f_1, ..., f_k$ os geradores de I.

Nullstellensatz - demonstração

Sejam $f_1, ..., f_k$ os geradores de I. Seja J um ideal maximal que contém I (lema de Zorn).

Nullstellensatz - demonstração

Sejam $f_1, \ldots, f_k$ os geradores de I. Seja J um ideal maximal que contém I (lema de Zorn). Defina

$$K = \frac{F[x_1, \ldots, x_n]}{J}$$

Nullstellensatz - demonstração

Sejam $f_1, ..., f_k$ os geradores de I. Seja J um ideal maximal que contém I (lema de Zorn). Defina

$$K = \frac{F[x_1, ..., x_n]}{J}$$

Como J é maximal, segue que K é um corpo.

Nullstellensatz - demonstração

Sejam $f_1, ..., f_k$ os geradores de I. Seja J um ideal maximal que contém I (lema de Zorn). Defina

$$K = \frac{F[x_1, ..., x_n]}{J}$$

Como J é maximal, segue que K é um corpo. Além disso, temos que $F \subset K$.

Nullstellensatz - demonstração

Sejam $f_1, ..., f_k$ os geradores de I. Seja J um ideal maximal que contém I (lema de Zorn). Defina

$$K = \frac{F[x_1, ..., x_n]}{J}$$

Como J é maximal, segue que K é um corpo. Além disso, temos que $F \subset K$.

Seja L o fecho algébrico de K.

Nullstellensatz - demonstração

Sejam $f_1, ..., f_k$ os geradores de I. Seja J um ideal maximal que contém I (lema de Zorn). Defina

$$K = \frac{F[x_1, ..., x_n]}{J}$$

Como J é maximal, segue que K é um corpo. Além disso, temos que $F \subset K$.

Seja L o fecho algébrico de K.Temos, então, que

$$F \subset K \subset L,$$

Nullstellensatz - demonstração

Sejam $f_1, ..., f_k$ os geradores de I. Seja J um ideal maximal que contém I (lema de Zorn). Defina

$$K = \frac{F[x_1, ..., x_n]}{J}$$

Como J é maximal, segue que K é um corpo. Além disso, temos que $F \subset K$.

Seja L o fecho algébrico de K.Temos, então, que

$$F \subset K \subset L,$$

onde $F \models ACF$ e $L \models ACF$.

Nullstellensatz - demonstração

Como $F \subset K$, temos que os polinômios $f_1, ..., f_k$ estão bem definidos em $K[x_1, ..., x_n]$.

Nullstellensatz - demonstração

Como $F \subset K$, temos que os polinômios $f_1, ..., f_k$ estão bem definidos em $K[x_1, ..., x_n]$.

Temos que $\overline{a} = (x_1 + J, ..., x_n + J)$ é um elemento de $K^n \subset L^n$.

Nullstellensatz - demonstração

Como $F \subset K$, temos que os polinômios $f_1, ..., f_k$ estão bem definidos em $K[x_1, ..., x_n]$.

Temos que $\overline{a} = (x_1 + J, ..., x_n + J)$ é um elemento de $K^n \subset L^n$. Note que $f_1(\overline{a}) = ... = f_k(\overline{a}) = \overline{0}$.

Nullstellensatz - demonstração

Como $F \subset K$, temos que os polinômios $f_1, ..., f_k$ estão bem definidos em $K[x_1, ..., x_n]$.

Temos que $\overline{a} = (x_1 + J, ..., x_n + J)$ é um elemento de $K^n \subset L^n$. Note que $f_1(\overline{a}) = ... = f_k(\overline{a}) = \overline{0}$.

Sejam $b_1, ..., b_m$ os coeficientes em F que definem $f_1, ..., f_k$.

Nullstellensatz - demonstração

Como $F \subset K$, temos que os polinômios $f_1, ..., f_k$ estão bem definidos em $K[x_1, ..., x_n]$.

Temos que $\overline{a} = (x_1 + J, ..., x_n + J)$ é um elemento de $K^n \subset L^n$. Note que $f_1(\overline{a}) = ... = f_k(\overline{a}) = \overline{0}$.

Sejam $b_1, ..., b_m$ os coeficientes em F que definem $f_1, ..., f_k$. Temos que:

$$L \models \varphi(b_1, ..., b_m) := \exists \overline{a}((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0)$$

Nullstellensatz - demonstração

Como ACF é modelo-completo e $F \subset L$, segue que

Nullstellensatz - demonstração

Como ACF é modelo-completo e $F \subset L$, segue que

$$F \models \varphi(b_1, ..., b_m) := \exists \overline{a}((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0).$$

Nullstellensatz - demonstração

Como ACF é modelo-completo e $F \subset L$, segue que

$$F \models \varphi(b_1, ..., b_m) := \exists \overline{a}((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0).$$

Portanto existe $\overline{a} \in F^n$ tal que $f_1(\overline{a}) = ... = f_k(\overline{a}) = 0$.

Nullstellensatz - demonstração

Como ACF é modelo-completo e $F \subset L$, segue que

$$F \models \varphi(b_1, ..., b_m) := \exists \overline{a}((f_1(\overline{a}) = 0) \wedge ... \wedge (f_k(\overline{a}) = 0).$$

Portanto existe $\overline{a} \in F^n$ tal que $f_1(\overline{a}) = ... = f_k(\overline{a}) = 0$. Como $f_1, ..., f_k$ geram I, então $f(\overline{a}) = 0$ para todo $f \in I$

Acabou

Até a próxima aula!