امکانات: خط‌کش بدون درجه و یک پرگار

(ruler and compass)

بخش جبری اثبات گنگ بودن عدد π و اعداد گویا

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$

$2x = 3$

$\mathbb{Z} \subseteq \mathbb{Q}$ $\quad x = \frac{3}{2}$

$x^2 = 2$

$x^2 - 2 = 0$

$\frac{-b \pm \sqrt{\Delta}}{2a}$

$\mathbb{Q} \subseteq \mathbb{R}$

$x^2 = 2$

① آیا π ریشه‌ی یک معادله‌ی چندجمله‌ای با ضرایب در $\mathbb{Q}$ است؟

② آیا فرمول مشخصی برای حل یک معادله‌ی چندجمله‌ای بر حسب ضرایب آن وجود دارد؟ (آبل - روفینی)

$x^2 + 1 = 0$

$R \subseteq \square$

فرض کنید i یک نماد باشد که $i^2 + 1 = 0$

imaginary

و $\mathbb{R}(i)$ را در نظر بگیرید.

$= \{a + bi \mid a, b \in \mathbb{R}\}$

قضیه (قضیه اساسی جبر)

در $\underbrace{\mathbb{R}(i)}_{}$ $= \mathbb{C}$ همه‌ی ریشه‌های همه‌ی معادلات چندجمله‌ای وجود دارند.

نظریه گالوا میان دو بخش با اهمیت جبر ارتباط برقرار می‌کند.

میدان‌ها $\Longleftrightarrow$ گروه‌ها

$\sigma : F \to F$

$f(x) = 0 \to f(x)$

$\{x_1, \dots, x_n\}$ $\{$

منابع:

- Fields and Galois theory / John M. Howie
- Algebra (Serge Lang)
- Emil Artin (Galois theory)

تعاریف اولیه

تعریف

میدان $(F, +, \cdot, 0, 1)$

منظور از یک مجموعه جابه‌جایی یکدار F است به همراه دو عمل $+ : F \to F$, $(x,y) \mapsto x+y$ و $\cdot : F^2 \to F$, $(x,y) \mapsto x\cdot y$

و دو عنصر متمایز $0, 1$ که ویژگی‌های زیر را دارد. (1)

R_1 $a+(b+c) = (a+b)+c$

R_2 $a+b = b+a$

R_3 $a+0 = a$

R_4 $\forall a \; \exists b \;\; a+b = 0$

$(\mathbb{Z}, +, \cdot, 0, 1)$

R_5 $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

R_6 $a\cdot(b+c) = a\cdot b + a\cdot c$

R_7 $a\cdot b = b\cdot a$

R_8 $1 \neq 0$, $a\cdot 1 = a$

تعریف

(حوزه صحیح) (integral domain)

یک حلقه جابه‌جایی یکدار است که ویژگی زیر را نیز دارا است:

R_9

$$\forall a \neq 0 \;\; \forall b, c \qquad a\cdot b = a\cdot c \Rightarrow b = c$$

تعریف

اگر حلقه‌ی جابه‌جایی و یکدار ما ویژگی زیر را هم داشته باشد به آن یک میدان می‌گوییم

$R_{10} \quad \forall a\neq 0\ \exists b \quad ab=1$

$(\mathbb{Z},+,\cdot;0,1)$

2

مثال $R_{10} \Rightarrow R_9$

اثبات فرض کنید ویژگی R_{10} برقرار باشد.

و فرض کنید $a\cdot b=a\cdot c$.

بنابر ویژگی R_{10} یک عنصر z وجود دارد به طوری که

$z\cdot a=1$

طرفین عبارت بالا در z ضرب کنید

$z\cdot(ab)=z\cdot(ac)$

$(z\cdot a)\cdot b=(z\cdot a)\cdot c \Rightarrow b=c$

مثال $R_9 \not\Rightarrow R_{10}$

$(\mathbb{Z},+,\cdot;0,1)$ ویژگی R_9 را داراست ولی ویژگی R_{10} را دارا نیست.

$a\cdot b=a\cdot c$

مثال

ویژگی R_9 را می‌توان با ویژگی زیر جایگزین کرد

$R_{11} \quad \forall a,b \quad a\cdot b=0 \Rightarrow a=0$ یا $b=0$

(اگر هم $a\neq 0$ و هم $b\neq 0$ آن‌گاه $ab\neq 0$)

اثبات $R_{11} \overset{?}{\Rightarrow} R_9$ فرض کنید فضای مورد نظر ما ویژگی R_{11} را دارا باشد

هم‌چنین فرض کنید $a\cdot b=a\cdot c$ سؤال آیا در این صورت $b=c$؟

$a\neq 0$

$a\cdot b=a\cdot c \Rightarrow$

$ab-ac=0 \Rightarrow$

$a(b-c)=0 \xRightarrow{R_{11}}$

$b-c=0 \Rightarrow b=c$

سوال آیا $R_9 \overset{?}{\Rightarrow} R_{11}$

$R_9: \forall \underset{a\neq 0}{a,b,c} \quad ab=ac \Rightarrow b=c$

$R_{11}: \forall a,b \quad ab=0 \Rightarrow a=0$ یا $b=0$

فرض کنید R_9 برقرار است، و فرض کنید

$ab=0$

و فرض کنید $a\neq 0$.

در این صورت

$a\cdot b = a\cdot 0$

بنابراین بنا بر ویژگی R_9 داریم

$b=0$

مثال

نشان دهید که هر حوزه‌ی صحیح متناهی

یک میدان است.

$\forall \underset{\neq 0}{a} \; \exists b \; ab=1$

اثبات $F=\{0,1,a_1,\dots,a_n\}$

عنصر $\underset{\neq 0}{a_1}$ را در نظر بگیریم. فرض کنید که a_1

دارای وارون ضربی نباشد

$\forall b \quad a_1 b\neq 1$

در این صورت عناصر $\underset{\neq}{b_1, b_2}$ به گونه‌ای پیدا

می‌شوند که

$a_1b_1 = a_1b_2$

در این صورت $b_1=b_2$

$a_1, a_2, \dots, a_5$

$1\neq a_1a_2$

$1\neq a_1a_3$

$1\neq a_1a_4$

$1\neq a_1a_5$

$1\neq a_1a_1$

توجه

یک حلقه در صورتی حوزه‌ی صحیح است که

زیرحلقه‌ی یک میدان باشد

$(D,+,\cdot,0,1) \subseteq (F,+,\cdot,0,1)$

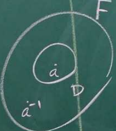
میدان

$(\mathbb{Z},+,\cdot,0,1)\subseteq(\mathbb{Q},+,\cdot,0,1)$

① هر حلقه‌ای که زیرحلقهٔ یک میدان باشد حوزهٔ صحیح است.

② هر حوزهٔ صحیح زیرحلقهٔ یک میدان است.

اثبات 1: فرض کنید $\underbrace{(D,+,\cdot,0,1)}_{\text{حلقه}} \subseteq (\underset{\text{میدان}}{F},+,\cdot,0,1)$



فرض کنید $\underset{\neq 0}{a}, b, c \in D$ ، $ab = ac$.

$a, b, c \in D \subseteq F$

$a, b, c \in F$

در F، $ab = ac$

a در F وارون دارد. (a وارون، z)

در F اتفاق زیر می‌افتد:

$ab = ac \Rightarrow$

$\underline{za}b = \underline{za}c \Rightarrow b = c$

در F عنصر b, c با هم مساوی هستند.

بنابراین در D این دو عنصر با هم برابرند.