If we try to create a bigger ring where $x^2+x+1=0$ has a root,

$$\mathbb{F}_2[x]/\underbrace{(x^2+x+1)}_{I} \cong (\mathbb{F}_2)^2$$

$f(x)$

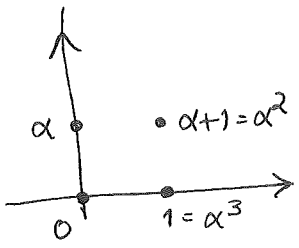
$\cong$ as $\mathbb{F}_2$-vector spaces

$\Downarrow$

$\alpha := x+I$ is a root of x^2+x+1

i.e. $\alpha^2+\alpha+1=0$

or $\alpha^2=\alpha+1$



$\alpha^3 = \alpha\cdot\alpha^2 = \alpha(\alpha+1) = \alpha^2+\alpha = \alpha+1+\alpha = 1$

Can calculate in $\mathbb{F}_4$ multiple ways, e.g.

$\alpha^4 = (\alpha^2)^2 = (\alpha+1)^2 = \alpha^2+2\alpha+1 = \alpha^2+1 = \alpha+1+1 = \alpha$

$\alpha^3\cdot\alpha = 1\cdot\alpha = \alpha$

$x^2+\alpha+1 \;\big)\; \alpha^4 \;\big)\; \alpha^2+\alpha$

$\alpha^4+\alpha^3+\alpha^2$

$\alpha^3+\alpha^2$

$\alpha^3+\alpha^2+\alpha$

α

Interestingly, $\mathbb{F}_2[x]/(x^2+x+1)$ is a field (since $\{1,\alpha,\alpha+1\}$ all have inverses: $\alpha^{-1}=\alpha+1$, $1^{-1}=1$)

and we'll see why this had to be later.

28/1/2019

④ What happens if we try to make $3\in\mathbb{Z}$ invertible by adjoining a root to $3x-1=0$?

i.e. create $\mathbb{Z}[x]/(3x-1)$ as a new ring

↑ not monic, so the structure is trickier!

To understand it, we can try to map

$$\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Q}$$

extending $\mathbb{Z}\to\mathbb{Q}$

and $x \longmapsto \frac{1}{3}$

hopefully show $\ker\varphi = (3x-1)$, and identify $\operatorname{im}\varphi \subset \mathbb{Q}$.

Certainly $\ker\varphi \supseteq (3x-1)$

but also if $f(x)\in\ker\varphi$, write $f(x) = (3x-1)\,g(x) = (x-\frac{1}{3})\,\tilde{g}(x)$ with $g(x)\in\mathbb{Q}[x]$

(since $f(\frac{1}{3})=0$)

$f(x) = a_0+a_1x+\dots+a_nx^n$, $a_i\in\mathbb{Z}$

$g(x) = b_0+b_1x+\dots+b_{n-1}x^{n-1}$, $b_i\in\mathbb{Q}$

and then

$$a_0+a_1x+\dots+a_nx^n = \underbrace{-b_0}_{a_0} + \underbrace{(3b_0-b_1)}_{a_1}x + \underbrace{(3b_1-b_2)}_{a_2}x^2 + \dots + (3b_{n-1}-b_n)x^{n-1} + 3b_{n-1}x^n$$

$\Rightarrow b_0\in\mathbb{Z}$ $\Rightarrow b_1 = 3b_0-a_1 \in\mathbb{Z}$ $\Rightarrow b_2 = 3b_1-a_2\in\mathbb{Z}$ etc.

(24)

Hence $\ker\varphi = (3x-1) \subset \mathbb{Z}[x]$

so $\mathbb{Z}[x]/(3x-1) \cong \operatorname{im}\varphi \subset \mathbb{Q}$

contains $\frac{1}{3}, \frac{2}{3}, \frac{-1}{3}, \frac{-2}{3}, \frac{5}{3}, \ldots$

also $\frac{1}{9}, \frac{2}{9}, \frac{-17}{9}, \ldots$

$\frac{1}{27}, \frac{417}{27}, \frac{-4}{27}, \ldots$

Not hard to see $\operatorname{im}\varphi = \left\{ \frac{a}{3^d} : a \in \mathbb{Z}, d \in \{0,1,2,\ldots\} \right\}$ subring $\subset \mathbb{Q}$.

$\cong \mathbb{Z}[x]/(3x-1)$

$\frac{a_1}{3^{d_1}} + \frac{a_2}{3^{d_2}} = \frac{b}{3^{\max(d_1,d_2)}}$

$\frac{a_1}{3^{d_1}} \cdot \frac{a_2}{3^{d_2}} = \frac{a_1 a_2}{3^{d_1+d_2}}$

---

(5) What if we try to make $\bar{3} \in \mathbb{Z}/15\mathbb{Z}$ invertible,

i.e. create $\mathbb{Z}/15\mathbb{Z}[x] / \underbrace{(\bar{3}x-\bar{1})}_{I}$

so $\alpha = x + \underbrace{(3x-1)}_{I}$ has $\alpha = \bar{3}^{-1}$ i.e. $\alpha \cdot 3 = 1$

But then since $\bar{3}\cdot\bar{5} = 0$

$\underbrace{\alpha\cdot\bar{3}}_{1}\cdot\bar{5} = \alpha\cdot 0 = 0$

$\bar{5} = 0$ in this ring!

(Check: $I \ni (-\bar{5})\cdot(\bar{3}x-\bar{1}) = (-\bar{15})x + \bar{5} = \bar{5}$)

Also since $\bar{3}\alpha = \bar{1}$ in this ring,

$\underbrace{\bar{2}\cdot\bar{3}}_{\bar{6}=\bar{1}}\alpha = \bar{2}\cdot\bar{1} = \bar{2}$

$\alpha = \bar{2}$ in this ring, so $\mathbb{Z}/15\mathbb{Z}[x]/(\bar{3}x-\bar{1}) \in \{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$

Starting to guess ... $\mathbb{Z}/15\mathbb{Z}[x]/(\bar{3}x-\bar{1}) \cong \mathbb{Z}/5\mathbb{Z}$ as rings

by sending

$\mathbb{Z}/15\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{Z}/5\mathbb{Z}$ which surjects,

extending $\mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$

$\bar{a}$ mod 15 $\mapsto$ $\bar{a}$ mod 5

$x \mapsto \bar{2}$

so $\operatorname{im}\varphi = \mathbb{Z}/5\mathbb{Z}$

and it's a bijection since $|\mathbb{Z}/15\mathbb{Z}[x]/(\bar{3}x-\bar{1})| \leq 5$.

§11.7 Fields of fractions

We're used to how $\mathbb{Q}$ was created from $\mathbb{Z}$

as $\mathbb{Q} \overset{\text{DEF'N}}{:=} \left\{ \frac{a}{b} : a,b \in \mathbb{Z}, b \neq 0 \right\}$

with $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

(and $\frac{a}{b} = \frac{am}{bm}$ for $m \neq 0$)

But we're also used to working with rational functions

this way, e.g. $\frac{x}{y-5} + \frac{3x-1}{y^3} = \frac{xy^3 + (y-5)(3x-1)}{y^3(y-5)} = \frac{f(x,y)}{g(x,y)}$ with $f,g \in \mathbb{R}[x,y]$

In fact, we'll even want to do this for fractions made from $\mathbb{F}[x_1, x_2, \ldots x_n]$

where $\mathbb{F}$ is any field, e.g. $\mathbb{F} = \mathbb{F}_p$.

Does it make sense? Yes, for domains.

DEF'N-PROP: (THM 11.7.2) Given a domain R, its fraction field or field of fractions is the set $\mathbb{F} = \mathrm{Frac}(R) := \{$ equivalence classes of symbols $\frac{a}{b}$ with $a,b \in R$, $b \neq 0$ for the equivalence relation $\frac{a}{b} \approx \frac{a'}{b'}$ if $ab' = a'b$ in $R \}$

with $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$

$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$

Q: Why is $bd \neq 0$?

$0 := \frac{0}{1}$, $1 = \frac{1}{1}$

and in fact there is an injective ring homom. $R \longrightarrow \mathbb{F}$.

$a \longmapsto \frac{a}{1}$

(COROLLARY: {domains R} = {subrings of fields $\mathbb{F}$})

proof: This is hiding many assertions!

$\approx$ is an equiv. relation: $\frac{a}{b} \approx \frac{a}{b}$ since $ab = ab$

$\frac{a}{b} \approx \frac{a'}{b'} \Rightarrow \frac{a'}{b'} \approx \frac{a}{b}$ since both mean $ab' = a'b$

$\frac{a}{b} \approx \frac{a'}{b'}$, $\frac{a'}{b'} \approx \frac{a''}{b''} \Rightarrow ab' = a'b$

$a'b'' = a''b'$

so $ab' \cdot a'b'' = a'b \cdot a''b'$

{ cancel $a'b'$ in domain R

$ab'' = a''b$

i.e. $\frac{a}{b} = \frac{a''}{b''}$ ✓

$+$ is well-defined: if $\frac{a}{b} \approx \frac{a'}{b'}$ then $\frac{a}{b} + \frac{c}{d} \stackrel{?}{=} \frac{a'}{b'} + \frac{c}{d}$

$\frac{ad+bc}{bd}$ $\qquad$ $\frac{a'd+b'c}{b'd}$

since $ab' = a'b$ gives what ... ... one needs here:

$ab'd^2 + bb'cd = a'bd^2 + bb'cd$

and $\times$ is well-defined: $\frac{ac}{bd} \stackrel{?}{=} \frac{a'c}{b'd}$ needs $ab'cd = a'bcd$

$+$ and $\times$ are associative, commutative (easy to check)

$\mathbb{F}^+ = (\mathbb{F}, +)$ is an abelian group (easy to check)

$\times$ distributes over $+$ (easy to check)

The fact that $R \xrightarrow{\varphi} \mathbb{F}$, $a \longmapsto \frac{a}{1}$ is a ring homom., and injective (easy to check) ∎

NOTATION/EXAMPLE: For $\mathbb{F}$ a field, $\mathbb{F}(x)$, $\mathbb{F}(x,y)$, $\mathbb{F}(x_1, \dots, x_n)$ are the rational function fields with coefficients in $\mathbb{F}$ in one, two, many variables

e.g. $\mathbb{F}_2(x,y) = \left\{ \frac{f(x,y)}{g(x,y)} : f, g \in \mathbb{F}_2[x,y] \text{ polynomials}, g \neq 0 \right\}$