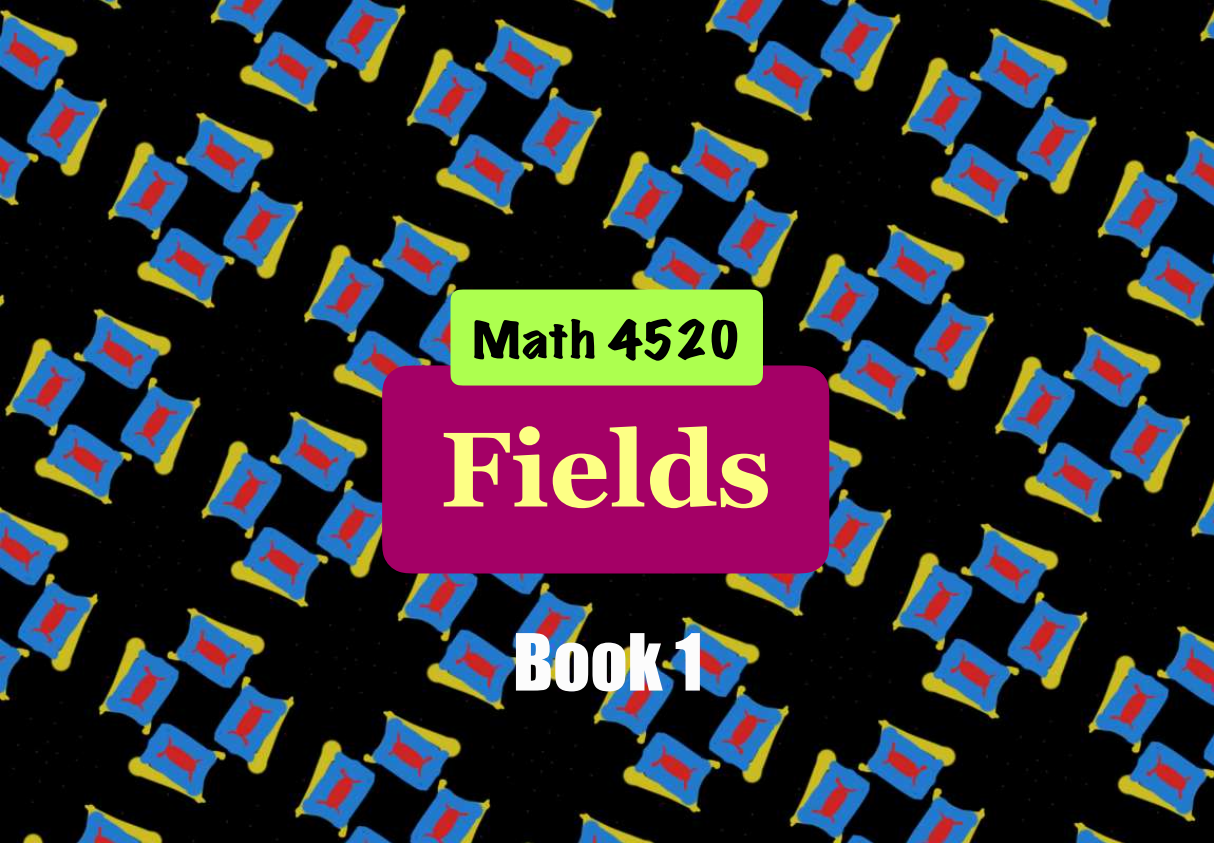




Math 4520

Fields

Book 1

A field is a number system with $+$, $-$, $\times$, $\div$, 0 , 1 in which we can divide by every nonzero element.

$\mathbb{R} = \{\text{real numbers}\}$ is a field

$\mathbb{C} = \{\text{complex numbers}\}$ " " "

$\mathbb{Q} = \{\text{rational numbers}\}$ " " "

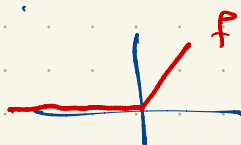
$\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}$, $i = \sqrt{-1}$

$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$

$\mathbb{Z} = \{\text{integers}\} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$ is not a field. $\mathbb{Z}$ is a commutative ring with 1 (having no zero divisors).

Other examples of fields?

$$f(x) = \begin{cases} x, & \text{if } x \geq 0 \\ 0, & \text{if } x < 0 \end{cases}$$



$$g(x) = \begin{cases} 0, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$



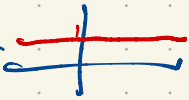
$$f(x) + g(x) = |x|$$

$$f(x) - g(x) = x$$

$$f(x)g(x) = 0$$

$$f \neq 0$$

$f(x)$ and $g(x)$ are nonzero functions whose product is 0 (these are called zero divisors in ring theory).

The continuous functions $\mathbb{R} \rightarrow \mathbb{R}$ form a commutative ring with identity  but not a field.

$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ is a field of order 5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$$3 + 4 = 2$$

$$3 - 4 = 4$$

$$3 \times 1 = 2$$

$$\frac{3}{4} = 2$$

$\mathbb{R}, \mathbb{C}, \mathbb{Q}$ are infinite fields; $\mathbb{F}_5$ is a finite field.
In $\mathbb{Z}$, $8 \equiv 3 \pmod{5}$. (8 is congruent to 3 mod 5)
In $\mathbb{F}_5$, $8 = 3$.

$$\frac{3}{4} = 2 \iff 3 = 2 \times 4$$

$$2 \times 4 = 8 = 3$$

Fields

Let F be a set containing distinct elements called 0 and 1 (thus $0 \neq 1$). Suppose addition, subtraction, multiplication and division are defined for all elements of F (except division by 0 is not defined).

Thus $a + b, a - b, ab, \frac{a}{d} \in F$ whenever $a, b, d \in F$ and $d \neq 0$.

Define $-a = 0 - a$.

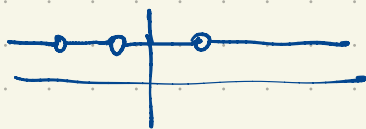
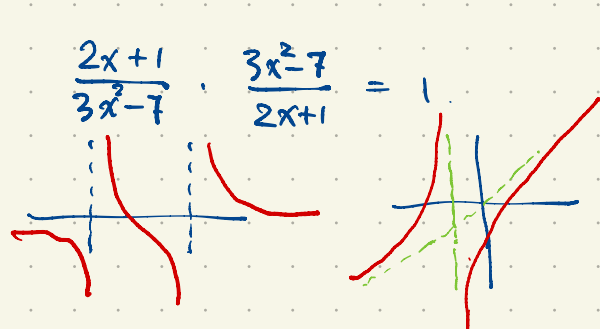
If the following properties are satisfied by *all* elements $a, b, c, d \in F$ with $d \neq 0$, then F is a **field**.

$a + b = b + a$	$a + (b + c) = (a + b) + c$	$ab = ba$
$a + 0 = a$	$a(bc) = (ab)c$	$1a = a$
$a + (-a) = 0$	$a(b + c) = ab + ac$	$\frac{a}{d} d = a$
$a + (-b) = a - b$		

The ring of polynomials in x with real coefficients is

$\mathbb{R}[x]$ is a commutative ring with identity having no zero divisors (if $f(x), g(x)$ are nonzero polynomials then $f(x)g(x)$ is a nonzero polynomial)

$\mathbb{R}(x) = \{ \text{rational functions in } x \text{ with real coefficients} \}$, a field. $\frac{1}{f(x)} = f(x)^{-1}$



$$\mathbb{R}(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x], g(x) \neq 0 \right\}$$

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

$\mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$ is a field.

$$\alpha = 3 + 7\sqrt{2}, \beta = 5 - \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\alpha + \beta = (3 + 7\sqrt{2}) + (5 - \sqrt{2}) = 8 + 6\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\alpha - \beta = (3 + 7\sqrt{2}) - (5 - \sqrt{2}) = -2 + 8\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\alpha\beta = (3 + 7\sqrt{2})(5 - \sqrt{2}) = 15 - 3\sqrt{2} + 35\sqrt{2} - 14 = 1 + 32\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\frac{\alpha}{\beta} = \frac{3 + 7\sqrt{2}}{5 - \sqrt{2}} \cdot \frac{5 + \sqrt{2}}{5 + \sqrt{2}} = \frac{15 + 35\sqrt{2} + 35\sqrt{2} + 14}{25 - 2} = \frac{29 + 70\sqrt{2}}{23} = \frac{29}{23} + \frac{70}{23}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

$$\mathbb{Q}[i] = \{ a + bi : a, b \in \mathbb{Q} \}, i = \sqrt{-1}$$

This is a field.

$$\alpha = 1 + \frac{1}{3}i, \beta = \frac{3}{2} - i \Rightarrow \alpha + \beta = \frac{5}{2} - \frac{2}{3}i$$

$$\alpha - \beta = -\frac{1}{2} + \frac{4}{3}i$$

$$\alpha\beta = \frac{3}{2} - i + \frac{1}{2}i + \frac{1}{3} = \frac{11}{6} - \frac{1}{2}i \in \mathbb{Q}[i]$$

$$\frac{\alpha}{\beta} = \frac{1 + \frac{1}{3}i}{\frac{3}{2} - i} \cdot \frac{6}{6} = \frac{6 + 2i}{9 - 6i} \cdot \frac{9 + 6i}{9 + 6i} = \frac{54 + 36i + 18i - 12}{81 + 36} = \frac{42 + 54i}{117} = \frac{14}{39} + \frac{18}{39}i \in \mathbb{Q}[i]$$

Example $R = \{ \text{real } 2 \times 2 \text{ matrices} \} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$ noncommutative ring with identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ having zero divisors

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

The subset $F = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b \in \mathbb{R} \right\} \subset R$ is a subring which is actually a field

$$\det \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = a^2 + b^2 \neq 0 \text{ whenever } \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

$$F = \{ \underbrace{aI + bJ} : a, b \in \mathbb{R} \}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \text{ basis for } F.$$

$$a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

$$J^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$$

$$(aI + bJ)(cI + dJ) = acI + adJ + bcJ + bdJ^2 = (ac - bd)I + (ad + bc)J \in F$$

$$(cI + dJ)(aI + bJ) = (ca - db)I + (cb + da)J$$

All field axioms hold in F , so F is a field.

Rename element $aI + bJ \in F$ as $aI + bi = a + bi \in \mathbb{C}$
 $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \quad a, b \in \mathbb{R}$

$$\text{In } \mathbb{C}: (a + bi)(c + di) = ac + adi + bci - bd = (ac - bd) + (ad + bc)i$$

Our example F is essentially the same as $\mathbb{C}$. More precisely, they are isomorphic: we have a bijection $f: \mathbb{C} \rightarrow F$, $f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ for all $a, b \in \mathbb{R}$ such that

$$f(zw) = f(z)f(w), \quad f(z + w) = f(z) + f(w) \quad \text{for all } z, w \in \mathbb{C}.$$

$\mathbb{Q}[i]$ is isomorphic to the ring $E = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} : a, b, c, d \in \mathbb{Q} \right\}$

$$f: \mathbb{Q}[i] \rightarrow E, \quad f(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

$\alpha = 1 + \frac{1}{3}i$ $\{1, i\}$ basis for $\mathbb{Q}[i]$ over $\mathbb{Q}$

$$\beta = \frac{3}{2} - i$$

$$f(\beta) = \begin{bmatrix} \frac{3}{2} & -1 \\ 1 & \frac{3}{2} \end{bmatrix}$$

$$f(\beta)^{-1} = \begin{bmatrix} \frac{3}{2} & -1 \\ 1 & \frac{3}{2} \end{bmatrix}^{-1} = \frac{1}{\frac{9}{4} + 1} \begin{bmatrix} \frac{3}{2} & 1 \\ -1 & \frac{3}{2} \end{bmatrix} = \frac{4}{13} \begin{bmatrix} \frac{3}{2} & 1 \\ -1 & \frac{3}{2} \end{bmatrix}$$

$$f\left(\frac{\alpha}{\beta}\right) = f(\alpha) f(\beta)^{-1} = \frac{4}{13} \begin{bmatrix} 1 & \frac{1}{3} \\ -\frac{1}{3} & 1 \end{bmatrix} \begin{bmatrix} \frac{3}{2} & 1 \\ -1 & \frac{3}{2} \end{bmatrix} = \frac{4}{13} \begin{bmatrix} \frac{7}{6} & \frac{3}{2} \\ -\frac{3}{2} & \frac{7}{6} \end{bmatrix} = \frac{4}{13} \cdot \frac{1}{6} \begin{bmatrix} 7 & 9 \\ -9 & 7 \end{bmatrix} = \frac{2}{39} \begin{bmatrix} 7 & 9 \\ -9 & 7 \end{bmatrix} = \frac{1}{39} \begin{bmatrix} 14 & 18 \\ -18 & 14 \end{bmatrix}$$

$$\frac{3}{2} - \frac{1}{3} = \frac{9-2}{6} = \frac{7}{6}$$

$$f\left(\frac{14}{39} + \frac{18}{39}i\right) = \frac{1}{39} \begin{bmatrix} 14 & 18 \\ -18 & 14 \end{bmatrix} \quad \checkmark$$

$\mathbb{Q}[\sqrt{2}] \cong K = \left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}$ basis for K : $I, J = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$, $J^2 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2I$

$\det \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = a^2 - 2b^2 \neq 0$ if $a, b \in \mathbb{Q}$ are not both zero.

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}^{-1} = \frac{1}{a^2 - 2b^2} \begin{bmatrix} a & -b \\ -2b & a \end{bmatrix}$$

Note: $\left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ is a commutative ring with identity having zero divisors

$$\begin{bmatrix} \sqrt{2} & 1 \\ 2 & \sqrt{2} \end{bmatrix} \begin{bmatrix} -\sqrt{2} & 1 \\ 2 & -\sqrt{2} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = aI + bJ, \quad J = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}, \quad J^2 = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2I$$

$\alpha = \sqrt[3]{2} = 2^{1/3}$ $1, \alpha, \alpha^2$ is a basis: every element of $\mathbb{Q}[\alpha]$ is uniquely expressible as a linear combination $a \cdot 1 + b \cdot \alpha + c \cdot \alpha^2$ $a, b, c \in \mathbb{Q}$

$\mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 : a, b, c \in \mathbb{Q}\}$ (field)

Compare $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ (field) $a, b, c \in \mathbb{Q}$

$$\alpha^3 = 2$$

$$\begin{aligned}\alpha^3 &= 2 \\ \alpha^4 &= 2\alpha \\ \alpha^5 &= 2\alpha^2 \\ \alpha^6 &= 4\end{aligned}$$

$\mathbb{Q}[\alpha]$ is a 3-dimensional vector space over the scalars $a, b, c \in \mathbb{Q}$

If $E \supseteq F$ is a field extension (F is a subfield of E)

$$\begin{aligned}u &= 2 + \alpha + \alpha^2 \\ v &= 1 - \alpha + \alpha^2\end{aligned}$$

$$u + v = 3 + 2\alpha^2$$

$$u - v = 1 + 2\alpha$$

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

$$\frac{u}{v} = \frac{2 + \alpha + \alpha^2}{1 - \alpha + \alpha^2} = \underbrace{a + b\alpha + c\alpha^2}_{\text{rational numbers}} \Rightarrow 2 + \alpha + \alpha^2 = (1 - \alpha + \alpha^2)(a + b\alpha + c\alpha^2)$$

$$\begin{aligned}&= a + (b - a)\alpha + (a - b + c)\alpha^2 + (b - c)\alpha^3 + c\alpha^4 \\&= a + (b - a)\alpha + (a - b + c)\alpha^2 + 2(b - c) + 2c\alpha \\&= (a + 2b - 2c) + (-a + b + 2c)\alpha + (a - b + c)\alpha^2\end{aligned}$$

$$a + 2b - 2c = 2$$

$$-a + b + 2c = 1$$

$$a - b + c = 1$$

$$\begin{aligned}\left[\begin{array}{ccc|c}1 & 2 & -2 & 2 \\ -1 & 1 & 2 & 1 \\ 1 & -1 & 1 & 1\end{array}\right] &\sim \left[\begin{array}{ccc|c}1 & 2 & -2 & 2 \\ 0 & 3 & 0 & 3 \\ 1 & -1 & 1 & 1\end{array}\right] \xrightarrow{R_3 - R_1} \left[\begin{array}{ccc|c}1 & 2 & -2 & 2 \\ 0 & 1 & 0 & 1 \\ 1 & -1 & 1 & 1\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 2 & -2 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & -3 & 3 & -1\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -3 & 3 & -1\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 3 & 2\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 0 & -2 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2/3\end{array}\right] \sim \left[\begin{array}{ccc|c}1 & 0 & 0 & 4/3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2/3\end{array}\right] \xrightarrow{\begin{matrix} \leftarrow a \\ \leftarrow b \\ \leftarrow c \end{matrix}}\end{aligned}$$

$$\frac{u}{v} = \frac{4}{3} + \alpha + \frac{2}{3}\alpha^2 \quad \checkmark$$

$$3.65152175(2)$$

Check: $\alpha \approx 1.25992104989$

$u \approx 4.84732210186$

$v \approx 1.32748000207$

$\frac{u}{v} \approx 3.6515217512$

A good way to check!

$$\mathbb{Q}[\alpha]_{\alpha=2^{1/3}} \cong \{aI + bA + cA^2 : a, b, c \in \mathbb{Q}\} = \left\{ \begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix} : a, b, c \in \mathbb{Q} \right\} = \mathbb{Q}[A]$$

$$A = \begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$A^2 = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix} = 2I$$

$$A^4 = 2A$$

An isomorphism $f: \mathbb{Q}[\alpha] \rightarrow \mathbb{Q}[A]$

is given by $f(a + b\alpha + c\alpha^2) = aI + bA + cA^2$

$$\text{eg, } f(u) = f(2 + \alpha + \alpha^2) = 2I + A + A^2 = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{bmatrix}$$

$$f(v) = f(1 - \alpha + \alpha^2) = I - A + A^2 = \begin{bmatrix} 1 & 2 & -2 \\ 1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$$

$$f(uv) = f(u)f(v) = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & -2 \\ -1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 2 \\ 1 & 2 & 4 \\ 2 & 1 & 2 \end{bmatrix} = 2 + A + 2A^2$$

$$f\left(\frac{u}{v}\right) = f(u)f(v)^{-1} = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & -2 \\ -1 & 1 & 2 \\ 1 & -1 & 1 \end{bmatrix}^{-1}$$

$\mathbb{C} \supset \mathbb{R}$ is a field extension

$\mathbb{C} = \mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$ has basis $\{1, i\}$ over $\mathbb{R}$

$\mathbb{R} \supset \mathbb{Q}$ $1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{10}, \dots$

$\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$

Consider the prime field $\mathbb{F}_{101} = \{0, 1, 2, \dots, 100\}$ with $\alpha = 89$, $\beta = 23$. (Addition, multiplication, etc. mod 101)

$$\alpha + \beta = 112 = 11$$

$$\alpha - \beta = 66$$

$$\alpha\beta = 2047 = 27$$

$$\frac{\beta}{\alpha} = 23 \cdot 42 = 966 = 57$$

$$23 \cdot 42 \times \alpha = \beta \quad ?$$

$$42 \cdot \alpha = 1 \quad ?$$

101 is prime

$$\frac{\beta}{\alpha} = \beta \cdot \frac{1}{\alpha} = 23 \cdot 42 = 966 = 57$$

How do we compute inverses in $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$, p prime?
Review: basic properties of $\mathbb{Z}$ (handout on website)

$$\gcd(89, 101) = 1$$

89 has (positive) divisors $(1, 89)$
101 has (positive) divisors $(1, 101)$

the only common number is 1
(common divisor of 89 and 101)

$$\begin{array}{cc} 3 \cdot 5 & 3 \cdot 7 \\ \downarrow & \downarrow \\ \gcd(15, 21) & = 3 \end{array}$$

Divisors of 15: $-15, -5, -3, -1, 1, 3, 5, 15$

Divisors of 21: $-21, -7, -3, -1, 1, 3, 7, 21$

Common divisors of 15 and 21: $-3, -1, 1, 3$

greatest common divisor of 15 and 21: 3.

If $b = ra$ ($a, b, r \in \mathbb{Z}$) then we say

- a divides b
- a is a divisor of b
- b is a multiple of a
- a is a factor of b
- $a \mid b$

vertical bar

$$3 \mid 15 \quad 7 \nmid 15 \quad 7 \text{ does not divide } 15$$

$$3 < 5 \quad 8 \nmid 5$$

$$0 \mid 0$$

$$0 = -17 \cdot 0$$

Divisors of 1: $-1, 1$

Divisors of 0: $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$

$3 \mid 0$ because $0 = 0 \cdot 3$

Fact: Given $a, b \in \mathbb{Z}$, not both zero, $\gcd(a, b) = r \cdot a + s \cdot b$ for some $r, s \in \mathbb{Z}$.
 We can "easily" compute $\gcd(a, b)$, r, s , using the extended Euclidean algorithm.

eg. $\gcd(89, 101) = \square = \boxed{42} \cdot 89 + \boxed{-37} \cdot 101$.

$$101 = 1 \cdot 89 + 12$$

$$89 = 7 \cdot 12 + 5$$

$$12 = 2 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\leftarrow \gcd(101, 89) = 1$$

$$1 = 5 - 2 \cdot 2$$

$$= 5 - 2 \cdot (12 - 2 \cdot 5)$$

$$= 5 \cdot 5 - 2 \cdot 12$$

$$= 5 \cdot (89 - 7 \cdot 12) - 2 \cdot 12$$

$$= 5 \cdot 89 - 37 \cdot 12$$

$$= 5 \cdot 89 - 37 \cdot (101 - 89)$$

$$= \boxed{42} \cdot 89 - \boxed{37} \cdot 101$$

check: $3738 - 3737 = 1$

$$42 \cdot 89 \equiv 1 \pmod{101} \quad \text{in } \mathbb{Z}$$

$$42 \cdot 89 = 1 \quad \text{in } \mathbb{F}_{101}$$

$$\begin{aligned} 21 &= 1 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + \boxed{3} \leftarrow \gcd(21, 15) = 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

$$3 = \boxed{42} \cdot 21 + \boxed{3} \cdot 15 \quad ?$$

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 \\ &= 15 - 2 \cdot (21 - 15) \\ &= 3 \cdot 15 - 2 \cdot 21 \end{aligned}$$

Check: $45 - 42 = 3$.

It is faster to keep track of the coefficients only:

101	89	
1	0	101
0	1	89
1	-1	12
-7	8	5
15	-17	2
-37	42	$\boxed{1}$
*	*	0

$$\begin{aligned} 3x + 5y &= 13 \\ 7x - 11y &= 29 \end{aligned}$$

x	y	
3	5	13
7	-11	29

The last non-zero remainder is the gcd

$$\leftarrow \gcd(101, 89) = 1 = -37 \cdot 101 + 42 \cdot 89$$

Euclid's Algorithm (for finding the gcd of two numbers) relies on repeated application of the Division Algorithm.

Theorem: Let $n, d \in \mathbb{Z}$ with $d > 0$. Then $n = q \cdot d + r$ for some $q, r \in \mathbb{Z}$ which are unique.

$$\left. \begin{aligned} n &= q \cdot d + r \\ 0 &\leq r < d \end{aligned} \right\}$$

$\mathbb{R}[x]$ = ring of all polynomials in x with real coefficients

$\mathbb{R}[x]^* = \{\text{units of } \mathbb{R}[x]\} = \{\text{nonzero constant polynomials}\}$

A ^{nonzero} element $f \in \mathbb{R}[x]$ (or any commutative ring with identity) is reducible if $f = gh$ for some $g, h \in \mathbb{R}[x]$, where neither g nor h is a unit.

$$x^2 + 1 = gh \quad ?$$

$$x^2 + 1 = (x^2 + 1) \cdot 1$$

$$x^2 + 1 = (5x^2 + 5) \cdot \left(\frac{1}{5}\right) \quad \text{unit}$$

$$x^2 + 1 = gh \Rightarrow g \text{ or } h \text{ is a unit. Why?}$$

$(x^2 + 1 \text{ is irreducible})$

If $f(x) \in \mathbb{R}[x]$ then the degree of $f(x)$ is the largest n such that the coefficient of x^n in $f(x)$ is nonzero: (denoted $\deg f(x)$)

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \quad a_n \neq 0 \quad (a_0, a_1, \dots, a_n \in \mathbb{R})$$

$$\deg(x^2 + 1) = 2$$

$$\deg(g(x)h(x)) = \deg g(x) + \deg h(x)$$

$$\begin{aligned} \deg(x) &= 1 \\ \deg(5) &= 0 \\ \deg(0) & \end{aligned}$$

$$0 \cdot (x^2 + 1) = 0$$

$$\deg(0) + \deg(x^2 + 1) = \deg 0 \quad \text{This is a problem.}$$

One approach says: $\deg f(x)$ is only defined for nonzero polynomials.

The other approach: $\deg 0 = -\infty$

If $x^2 + 1 = g(x)h(x)$, $g(x), h(x) \in \mathbb{R}[x]$ then the factors $g(x), h(x)$ have degrees 0, 2 or 1, 1 or 2, 0.

But degree 0 polynomials are nonzero constants (i.e. units).

Otherwise $\deg g(x) = \deg h(x) = 1$ i.e. $g(x) = ax + b$, $h(x) = cx + d$, $a, b, c, d \in \mathbb{R}$, $a \neq 0$, $c \neq 0$.

Both $\mathbb{Z}$ and $\mathbb{R}[x]$ are commutative rings with identity, having no zero divisors. Neither is a field.
Units = {invertible elements} = $\{\pm 1\}$ or {nonzero real constants} respectively.

Both rings have the Division Algorithm:

In $\mathbb{Z}$: For all $n, d \in \mathbb{Z}$ with $d > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $n = \underset{\substack{\uparrow \\ \text{divisor}}}{q}d + \underset{\substack{\uparrow \\ \text{remainder}}}{r}$, $0 \leq r < d$.

In $\mathbb{R}[x]$: For all $f(x), d(x) \in \mathbb{R}[x]$ with $d(x) \neq 0$, there exist unique $q(x), r(x) \in \mathbb{R}[x]$ such that

$$f(x) = q(x)d(x) + r(x), \quad \deg r(x) < \deg d(x).$$

Euclid's Algorithm works in both $\mathbb{Z}, \mathbb{R}[x]$. (It's just more ugly in $\mathbb{R}[x]$.)

$2x+1 = 2(x+\frac{1}{2})$
irreducible

In $\mathbb{Z}$, $\gcd(a, b) = ra + sb$ for some $r, s \in \mathbb{Z}$. Here $a, b \in \mathbb{Z}$, not both zero.

In $\mathbb{R}[x]$, $\gcd(f(x), g(x))$ is the largest monic polynomial divisor of both $f(x), g(x)$.
 $\uparrow$ the leading term has coefficient 1.

$$\gcd(\underset{\substack{\uparrow \\ (3x+1)x}}{3x^2+x}, \underset{\substack{\uparrow \\ 4 \cdot x}}{4x}) = x.$$

$$\gcd(\underset{\substack{\uparrow \\ (x+\frac{1}{3}) \cdot 3}}{3x+1}, \underset{\substack{\uparrow \\ (x+\frac{1}{3}) \cdot 9x}}{9x^2+3x}) = x + \frac{1}{3}$$

We want to require $\gcd(f(x), g(x))$ to be the monic polynomial of largest degree dividing both $f(x)$ and $g(x)$.

$$\gcd(f(x), g(x)) = r(x)f(x) + s(x)g(x) \quad \text{for some } r(x), s(x) \in \mathbb{R}[x].$$

If F is any field then $F[x] = \{\text{polynomials in } x \text{ with coefficients in } F\}$ works the same way.

Euclidean rings: eg. $\mathbb{Z}, \mathbb{R}[x], F[x], \dots$ (integral domain which has the Division Algorithm).

Let $f(x) \in F[x]$ where F is a field. ($f(x)$ is a polynomial in x with coefficients in F).

A root of $f(x)$ is a value a such that $f(a) = 0$. (Often $a \in F$ or $a \in$ some larger field.)

eg. $x^2 + 1$ has roots $\pm i$ in $\mathbb{C}$

If $f(x) \in F[x]$ has a root $a \in F$ then $x-a$ divides $f(x)$, i.e. $f(x) = (x-a)q(x)$ for some $q(x) \in F[x]$.

Roots of $f(x) \longleftrightarrow$ factors of $f(x)$ of degree 1 (i.e. linear factors)

polynomials of degree 0 are constant
 1 linear
 2 quadratic
 3 cubic
 4 quartic

In one direction: if $x-a \mid f(x)$ ($x-a$ divides $f(x)$) then $f(a) = (a-a)q(a) = 0$
 so a is a root in F .

Conversely, if $a \in F$ is a root of $f(x)$, we get a linear factor $x-a$ because using the Division Algorithm,

$$f(x) = q(x)(x-a) + r(x), \quad q(x), r(x) \in F[x], \quad \deg r(x) < 1 \quad \text{so } \deg r(x) \leq 0$$

$\deg(x-a) = 1$ i.e. $r(x) = r \in F$ (a constant)

$$f(x) = q(x)(x-a) + \overset{\substack{\uparrow \\ \text{constant}}}{r} \quad 0 = f(a) = \underset{0}{q(a)(a-a)} + r \Rightarrow r = 0. \Rightarrow f(x) = q(x)(x-a).$$

$\Rightarrow x-a \mid f(x)$.

Factor $f(x) = x^3 - x^2 + 2x - 2 = (x-1)(x^2 + 2)$ factored into irreducible factors in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$

$f(1) = 1 - 1 + 2 - 2 = 0$

$f(x) = (x-1)(x+i\sqrt{2})(x-i\sqrt{2})$ in $\mathbb{C}[x]$
 Linear factors

If $f(x)$ has degree 1, 2 or 3 then every factorization of $f(x)$ has a linear factor.

If $\deg f(x) = 4$ then it is possible that $f(x)$ might factor into irreducible ^{quadratic} factors with no roots in F .

Eg. in $\mathbb{R}[x]$, $x^4 + 1$ has no real roots. Is it irreducible in $\mathbb{R}[x]$?

$$x^4 + 1 = (x^2 + ax + c)(x^2 - ax + c) \quad \text{Finish on/before Monday.}$$

$$c = \pm 1, \quad 2c - a^2 = 0 \quad (\text{coefficient of } x^2), \quad a^2 = 2, \quad a = \pm\sqrt{2} \\ c = 1$$

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \quad (\text{irreducible factors } x^2 \pm \sqrt{2}x + 1) \quad \text{discriminant } (\sqrt{2})^2 - 4 \cdot 1 \cdot 1 = -2$$

What are the irreducible polynomials in $\mathbb{R}[x]$?

$$x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}) \quad \text{reducible in } \mathbb{R}[x]$$

The irreducible polynomials in $\mathbb{R}[x]$ are

$$\text{discriminant } 0^2 - 4(1)(-2) = 8 > 0$$

- all polynomials of degree 1, i.e. $ax + b$, $a, b \in \mathbb{R}$, $a \neq 0$
- all polynomials of the form $ax^2 + bx + c$, $a, b, c \in \mathbb{R}$, $a \neq 0$, $\underbrace{b^2 - 4ac}_{\text{discriminant}} < 0$

$x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ but reducible in $\mathbb{R}[x]$

$$x^2 - 2x + 1 = (x - 1)^2 \quad \text{reducible} \\ (-2)^2 - 4 \cdot 1 \cdot 1 = 0$$

Polynomials in $\mathbb{R}[x]$ of degree 3 are reducible since using Calculus I or using a little algebra (roots of polynomials in $\mathbb{R}[x]$ come in pairs under complex conjugation).

Polynomials in $\mathbb{R}[x]$ of degree 4 are always reducible by the fact that $\mathbb{C}$ is algebraically closed:

Every polynomial in $\mathbb{C}[x]$ of degree ≥ 1 has a root in $\mathbb{C}$. (Fundamental Theorem of Algebra).

Irreducible polynomials in $\mathbb{C}[x]$ are the polynomials of degree 1.

In $\mathbb{Q}[x]$ there are irreducible polynomials of every degree $n \geq 1$, eg. $x^n - 2$ is irreducible for every $n \geq 1$.

Eg. $x^4 - 2 \in \mathbb{Q}[x]$ is irreducible.

If $x^4 - 2 = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Q}[x]$ but neither $g(x)$ nor $h(x)$ is a unit. Get contradiction on Wednesday...

Let's try $m(x) = x^3 + 2x + 2 \in \mathbb{Z}[x]$. Show: this is irreducible in $\mathbb{Z}[x]$.
Proof by contradiction: Any factorization of $m(x)$ in $\mathbb{Z}[x]$ with non-constant factors has the form

$$x^3 + 2x + 2 = (x + a)(x^2 + bx + c), \quad ac = 2. \Rightarrow (a, c) = (\pm 1, \pm 2) \text{ or } (\pm 2, \pm 1)$$

$$\text{or } (-x)(-x^2) \quad (\text{we can ignore this case since it simplifies to } (x \dots)(x^2 \dots))$$

Since $m(1) = 5$, $m(-1) = -1$, $m(2) = 14$, $m(-2) = -10$ are all nonzero, this is a contradiction.

General fact: If $m(x) \in \mathbb{Z}[x]$ is monic irreducible in $\mathbb{Z}[x]$, then $m(x)$ is also irreducible in $\mathbb{Q}[x]$.
This is an elementary (but slightly tricky) theorem in ring theory. We will use this fact freely.
So: $m(x) = x^3 + 2x + 2$ is irreducible in $\mathbb{Q}[x]$.

Eg. Show $m(x) = x^4 + 2x + 2 \in \mathbb{Q}[x]$ is irreducible. It suffices to prove irreducibility in $\mathbb{Z}[x]$.

Prove this by contradiction. If $m(x)$ factors nontrivially in $\mathbb{Z}[x]$, then either

Case (i) $x^4 + 2x + 2 = (x + a)(x^3 + bx^2 + cx + d)$, $a, b, c, d \in \mathbb{Z}$, or

Case (ii) $x^4 + 2x + 2 = (x^2 + ax + b)(x^2 + cx + d)$, $a, b, c, d \in \mathbb{Z}$.

Case (i) leads to an easy contradiction: $ad = 2 \Rightarrow a \in \{\pm 1, \pm 2\}$ and $m(-a) = 0$.

Here $m(1) = 5$, $m(-1) = 1$, $m(2) = 22$, $m(-2) = 14$ are nonzero, a contradiction.

In Case (ii), $a + c = 0$ so $x^4 + 2x + 2 = (x^2 + ax + b)(x^2 - ax + d)$,

$$bd = 2 \Rightarrow (b, d) = (1, 2), (2, 1), (-1, -2) \text{ or } (-2, -1)$$

$$\begin{aligned} b + d - a^2 &= 0 \\ ad - ab &= 2 \\ a(d - b) &= 2 \\ bd &= 2 \end{aligned}$$

If $b = 1$ and $d = 2$ then $a = 2$ and

$$b + d - a^2 = 1 + 2 - 2^2 = -1, \text{ a contradiction.}$$

If $b = 2$ and $d = 1$ then $a = -2$ and $b + d - a^2 = 2 + 1 - (-2)^2 = -1$, again a contradiction.

These cases cannot hold since $b + d = a^2 \geq 0$.

A very standard construction of a field extension $E \supseteq F$, starting from a known field F , is to start with $m(x) \in F[x]$ irreducible of degree n . Declare θ to be a root of $m(x)$ and $E = F[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1} : a_0, \dots, a_{n-1} \in F\}$. Then E is a field. It is an extension of degree n with basis $1, \theta, \theta^2, \dots, \theta^{n-1}$.

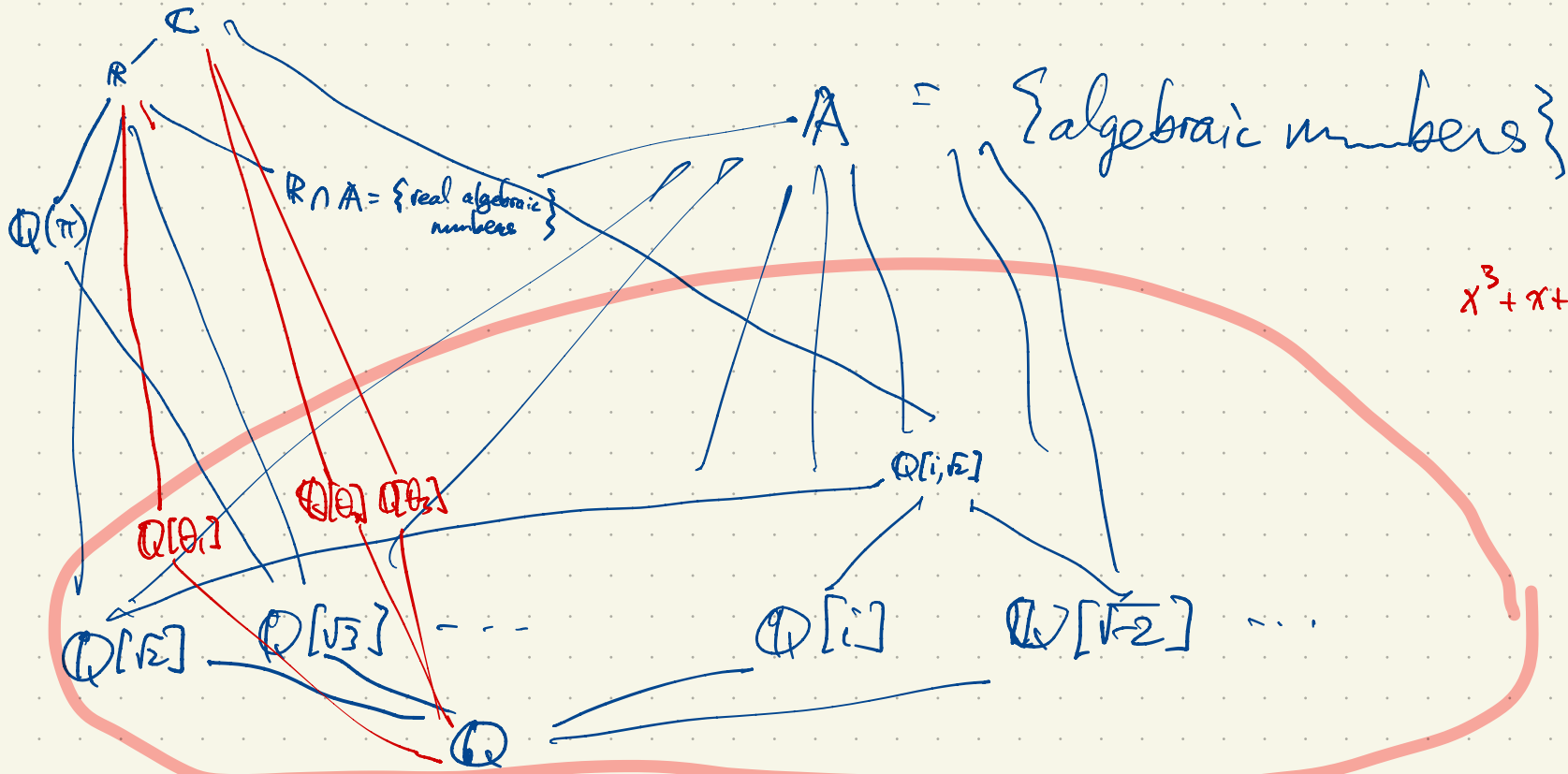
If $m(x) = g(x)h(x)$, $g(x), h(x) \in F[x]$ of degree $< n$, then $m(\theta) = 0 = \underbrace{g(\theta)h(\theta)}_{\text{nonzero elements of } E}$

Every finite degree $E \geq \mathbb{R}$ field extension is either $E = \mathbb{R}$ or $E = \mathbb{C}$.
(dimension as a vector space)

there are extensions $E \supset \mathbb{R}$ of infinite degree eg. $\mathbb{R}(x) = \{\text{rational functions with real coefficients}\}$.

The only finite extension of $\mathbb{C}$ is $\mathbb{C}$. $\mathbb{C}(x) \supset \mathbb{C}$ is an infinite extension (degree/dimension is infinite).

There are finite extension fields $E \supset \mathbb{Q}$ of every degree. These examples are called (algebraic) number fields.



$$x^3 + x + 3 = (x - \theta_1)(x - \theta_2)(x - \theta_3)$$

$\theta = \theta_1$
 $\theta_3 = \overline{\theta_2}$

An element $x \in \mathbb{C}$ is algebraic if it is a root of some nonzero poly. $f(x) \in \mathbb{Q}[x]$.

If x is not algebraic, then x is transcendental. eg. $\pi, e, \dots$

Most real and complex numbers are transcendental because $|\mathbb{Q}| = |\mathbb{A}| =$ countably infinite but $|\mathbb{R}| = |\mathbb{C}|$ is uncountable.

Cardinality proves the existence of transcendental numbers.

How can we prove a number is transcendental?

$\sqrt{2}$ is irrational but algebraic, not transcendental.

Prove that $\sqrt{2}$ is irrational: Suppose $\sqrt{2} = \frac{a}{b}$ as a reduced fraction, a, b positive integers, $\gcd(a, b) = 1$.

Then $2 = \frac{a^2}{b^2}$ so $a^2 = 2b^2$ is even, so a is even: $a = 2c$, $c \in \mathbb{Z}$. so $4c^2 = 2b^2$ i.e. $2c^2 = b^2$ is even.

so $b = 2d$, $d \in \mathbb{Z}$. Then $\gcd(a, b) \geq 2$, a contradiction.

This proof that $\sqrt{2} \notin \mathbb{Q}$ is due to Euclid.

~~Proof that e is irrational:~~ Suppose $e = \frac{a}{b}$, a, b positive integers, $\gcd(a, b) = 1$. Then

$$a = be = b \left(1 + 1 + \frac{1}{2} + \frac{1}{6} + \dots \right) = b \sum_{k=0}^{\infty} \frac{1}{k!} = b \left(1 + 1 + \frac{1}{2} + \dots + \frac{1}{b!} + \frac{1}{(b+1)!} + \frac{1}{(b+2)!} + \dots \right)$$

$$0! = 1$$

$$1! = 1$$

$$2! = 1 \times 2 = 2$$

$$3! = 1 \times 2 \times 3 = 6$$

$$4! = 1 \times 2 \times 3 \times 4 = 24$$

etc.

$$(b-1)! a = b \left((b-1)! + (b-1)! + \frac{(b-1)!}{2!} + \frac{(b-1)!}{3!} + \dots + \frac{(b-1)!}{(b-1)!} + \frac{(b-1)!}{b!} + \frac{(b-1)!}{(b+1)!} + \dots \right)$$

integers

$$\text{integers} = \text{integers} + 1 + \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \dots$$

integer between 0 and 1, a contradiction.

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots; \quad \text{for } |x| < 1.$$

$$\begin{aligned} \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+2)(b+3)} + \dots &< \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \frac{1}{(b+1)(b+1)(b+1)} + \dots \\ &= \frac{1}{b+1} \left(1 + \frac{1}{b+1} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + \dots \right) \\ &= \frac{1}{b+1} \cdot \frac{1}{1 - \frac{1}{b+1}} = \frac{1}{b+1-1} = \frac{1}{b} \end{aligned}$$

In HW1, θ is a root of $m(x) = x^3 + x + 3$ i.e. $\theta^3 + \theta + 3 = 0 \Rightarrow \theta^3 = -3 - \theta$

$$F = \mathbb{Q}[\theta] = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{Q}\}$$

$$(\theta+1)^{-1} = \frac{1}{\theta+1} = a + b\theta + c\theta^2$$

$$1 = (a + b\theta + c\theta^2)(1 + \theta)$$

$$= a + (a+b)\theta + (b+c)\theta^2 + c\theta^3$$

$$= a + (a+b)\theta + (b+c)\theta^2 + c(-3-\theta)$$

$$= \underbrace{(a-3c)}_1 + \underbrace{(a+b-c)}_0 \theta + \underbrace{(b+c)}_0 \theta^2$$

$$\begin{array}{l} a - 3c = 1 \\ a + b - c = 0 \\ b + c = 0 \end{array} \quad \left[\begin{array}{ccc|c} 1 & 0 & -3 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \end{array} \right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -3 & 1 \\ 0 & 1 & 2 & -1 \\ 0 & 1 & 1 & 0 \end{array} \right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -3 & 1 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & -1 & 1 \end{array} \right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -3 & 1 \\ 0 & 1 & 2 & -1 \\ 0 & 0 & 1 & -1 \end{array} \right] \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1 \end{array} \right]$$

$$\Rightarrow a = -2, b = 1, c = -1 \Rightarrow (\theta+1)^{-1} = -2 + \theta - \theta^2$$

$$\text{Check } (\theta+1)(-2+\theta-\theta^2) = -2-\theta-\theta^3 = -2-\theta-(-3-\theta) = 1 \quad \checkmark$$

Similar to #4: Let's find a ^{monic} cubic polynomial in $\mathbb{Q}[x]$ of degree ≤ 3 having α as a root.

i.e. $g(x) = x^3 + ax^2 + bx + c$, $a, b, c \in \mathbb{Q}$ such that $g(\alpha) = 0$ where $\alpha = 1 + \theta + \theta^2$.

(The answer is unique.)

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

$$\alpha^2 = (1 + \theta + \theta^2)^2 = 1 + \theta^2 + \theta^4 + 2\theta + 2\theta^2 + 2\theta^3 = 1 + \theta^2 + (-3\theta - \theta^2) + 2\theta + 2\theta^2 + 2(-3-\theta) = -5 - 3\theta + 2\theta^2$$

$$\begin{aligned} \alpha^3 &= \alpha^2 \cdot \alpha = (1 + \theta + \theta^2)(-5 - 3\theta + 2\theta^2) = -5 - 8\theta - 6\theta^2 - \theta^3 + 2\theta^4 \\ &= -5 - 8\theta - 6\theta^2 - (-3-\theta) + 2(-3\theta - \theta^2) \\ &= -2 - 13\theta - 12\theta^2 \end{aligned}$$

$$\text{We need } g(\alpha) = 0 = \alpha^3 + a\alpha^2 + b\alpha + c \Rightarrow a\alpha^2 + b\alpha + c = -\alpha^3$$

$$\Rightarrow a(-5 - 3\theta + 2\theta^2) + b(1 + \theta + \theta^2) + c = -(-2 - 13\theta - 12\theta^2)$$

$$\Rightarrow \underbrace{(-5a + b + c)}_{-2} + \underbrace{(-3a + b)}_{-13} \theta + \underbrace{(2a + b)}_{-12} \theta^2 = -2 - 13\theta - 12\theta^2$$

The smallest subfield of $\mathbb{R}$ containing π is $\mathbb{Q}(\pi)$.

Any subfield $E \subseteq \mathbb{C}$ contains $\mathbb{Q}$.

Assuming a subfield $E \subseteq \mathbb{C}$ contains π then it must contain $1, \pi, \pi^2, \pi^3, \pi^4, \dots$ so E contains every expression of the form

$$a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \dots + a_n\pi^n, \quad n \geq 0, \quad a_0, a_1, \dots, a_n \in \mathbb{Q}.$$

ie. $E \supseteq \mathbb{Q}[\pi] = \{ \text{all polynomials in } \pi \text{ with rational coefficients} \}.$

↑ subring of $\mathbb{C}$ but not a field.

$\frac{1}{\pi} \notin \mathbb{Q}[\pi]$. Proof by contradiction: If $\frac{1}{\pi} = a_0 + a_1\pi + a_2\pi^2 + \dots + a_n\pi^n$ with $n \geq 0, a_0, \dots, a_n \in \mathbb{Q}$

then $1 = a_0\pi + a_1\pi^2 + \dots + a_n\pi^{n+1}$

$$0 = -1 + a_0\pi + a_1\pi^2 + \dots + a_n\pi^{n+1}$$

π is then a root of a nonzero polynomial $-1 + a_0x + a_1x^2 + \dots + a_nx^{n+1} \in \mathbb{Q}[x]$.

$$\mathbb{Q}(\pi) = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in \mathbb{Q}[\pi], \beta \neq 0 \right\} = \left\{ \frac{a_0 + a_1\pi + a_2\pi^2 + \dots + a_m\pi^m}{b_0 + b_1\pi + b_2\pi^2 + \dots + b_n\pi^n} : a_0, \dots, a_m; b_0, \dots, b_n \in \mathbb{Q}; m, n \geq 0; b_0, \dots, b_n \text{ not all zero} \right\}.$$

$\mathbb{Q}(x) = \{ \text{rational functions in } x \text{ with rational coefficients} \}$
coefficients in $\mathbb{Q}$.

$\mathbb{Q}[x] = \{ \text{polynomials in } x \text{ with rational coefficients} \}$

Ring $\mathbb{Z} \rightarrow \mathbb{Q}$
Field

$$\mathbb{Q}[x] \rightarrow \mathbb{Q}(x)$$

$$\mathbb{Q}[\pi] \rightarrow \mathbb{Q}(\pi).$$

$$\mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$$

$$\mathbb{Q}[e] \rightarrow \mathbb{Q}(e)$$

$$\mathbb{Q}(e) \cong \mathbb{Q}(x) \cong \mathbb{Q}(\pi) \quad \text{but not equal}$$

The function $\phi: \mathbb{Q}(x) \rightarrow \mathbb{Q}(\pi)$

$$\phi(f(x)) = f(\pi) \quad \text{evaluate at } \pi$$

$$\phi(f(x) + g(x)) = f(\pi) + g(\pi) = \phi(f(x)) + \phi(g(x))$$

$$\phi(f(x)g(x)) = f(\pi)g(\pi) = \phi(f(x))\phi(g(x))$$

ϕ is bijective

so ϕ is an isomorphism.

This works because e and π are transcendental.

We know that e and π are irrational.

What about $e+\pi$ or $e\pi$?

We guess that both $e+\pi$ and $e\pi$ are irrational but we don't know.

However we do know that $e+\pi$ and $e\pi$ can't both be rational.

Proof by contradiction: Suppose $e+\pi, e\pi \in \mathbb{Q}$. Then

$(x-e)(x-\pi) = x^2 - (e+\pi)x + e\pi \in \mathbb{Q}[x]$ which has roots e and π so e and π are algebraic.

This contradicts the fact that e and π are transcendental.

Moreover, this reasoning shows that $e+\pi$ and $e\pi$ can't both be algebraic: at least one of them is not only irrational but transcendental.

If α, β are irrational then can $\alpha+\beta$ be rational? Yes.

Can $\alpha\beta$ be rational? (eg. $\sqrt{2} + (3-\sqrt{2}) = 3$) Yes.

eg. $\sqrt{2} \cdot \frac{3}{\sqrt{2}} = 3$

Can α^p be rational? Try $\sqrt{2}^{\sqrt{2}}$.

Case (I). $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$. In this case we're done.

Case (II). $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$. Then $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

Either way we see the answer is true. (This is an example of a non-constructive proof.)

Actually it is known that $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ but this is not easy to prove.

The smallest fields have order 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, ...

(prime powers)

Order 2: $\{0, 1\} \cong \mathbb{F}_2$

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Order 3: $\{0, 1, \alpha\} \cong \mathbb{F}_3$

+	0	1	α
0	0	1	α
1	1	α	0
α	α	0	1

x	0	1	α
0	0	0	0
1	0	1	α
α	0	α	1

$\alpha = 2 = \underline{1+1}$

Order 4: $\{0, 1, \alpha, \beta\} \cong \mathbb{F}_4$

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

x	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

If $1+\beta=0$
we get a contradiction

$1+\alpha = \alpha(\beta+1) = \alpha\alpha = \beta$

$\alpha+\alpha = \alpha(1+1) = \alpha 0 = 0$

$\mathbb{F}_2 \subset \mathbb{F}_4$ (subfield)

$\mathbb{F}_4 \not\cong \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

Polynomials over $\mathbb{F}_2$:

There are 2^n polynomials of degree n over $\mathbb{F}_2$:

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, \quad a_0, \dots, a_{n-1} \in \mathbb{F}_2.$$

(necessarily monic).