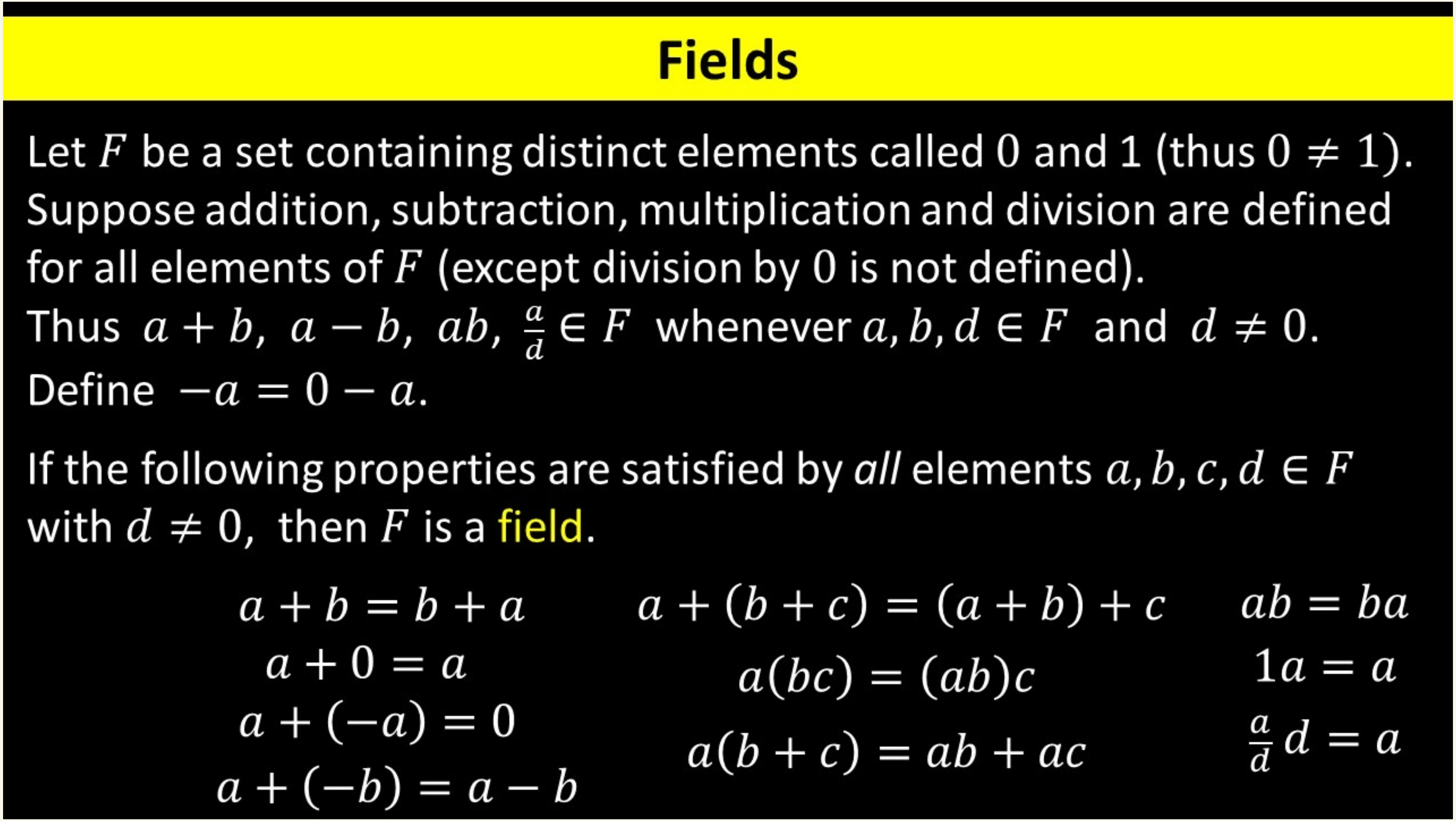
Fields

Book I



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.

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

$\mathbb{Q}^{2\times 2} = \{2\times 2$ matrices over $\mathbb{Q}\} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Q} \right\}$ is not a field.

$0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ identity

$A + 0 = A$, $AI = A = IA$

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ has no inverse. $A\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = I$ has no solution for A.

Moreover, $AB \neq BA$ in general.

$\mathbb{Q}^{2\times 2}$ is a (non-commutative) ring with identity.

It has a subring $D = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a,d \in \mathbb{Q} \right\}$ is a commutative subring with identity.

But D is not a field since it has non-invertible elements.

D has zero divisors: $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. A field can never have zero divisors.

(If d is a zero divisor then $cd = 0$ where $c,d \neq 0$ so $0\cdot\frac{1}{d} = \frac{0}{d} = \frac{cd}{d} = (\frac{c}{d})d = c \neq 0$, contradiction)

For a commutative ring R with identity, being able to divide is stronger than having no zero divisors.

An example of a commutative ring with identity having no zero divisors but not a field (division fails in general) is $\mathbb{Z}$

Eg. $F = \left\{ \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} : a,b \in \mathbb{Q} \right\} \subset \mathbb{Q}^{2\times 2}$ is a subring, containing $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

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

If $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ then $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}^{-1} = \frac{1}{a^2-2b^2}\begin{bmatrix} a & -b \\ -2b & a \end{bmatrix}$ (Note: $a^2-2b^2 \neq 0$ since $\sqrt{2} \notin \mathbb{Q}$).

Why is F a commutative subring? Elements of F have the form

$\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = aI + bS$ where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $S = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix}$ so $F = \{aI + bS : a,b \in \mathbb{Q}\}$ is the span of $\{I, S\}$ in $\mathbb{Q}^{2\times 2}$ (F is a 2-dimensional subspace of $\mathbb{Q}^{2\times 2}$, a 4-dimensional vector space).

$(aI+bS)(cI+dS) = acI + (ad+bc)S + bdS^2 = (cI+dS)(aI+bS)$, $S^2 = \begin{bmatrix}0&1\\2&0\end{bmatrix}\begin{bmatrix}0&1\\2&0\end{bmatrix} = 2I$

$= (ac+2bd)I + (ad+bc)S$

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

$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$

$(a+b\sqrt{2})(c+d\sqrt{2}) = ac + (ad+bc)\sqrt{2} + 2bd = (ac+2bd) + (ad+bc)\sqrt{2}$

Note: $F \cong K$ (they are isomorphic)

An explicit isomorphism $\phi : K \to F$ is given by $\phi(a+b\sqrt{2}) = \begin{bmatrix}a&b\\2b&a\end{bmatrix} = aI+bS$.

ϕ is bijective

$\phi(x+y) = \phi(x)+\phi(y)$

$\phi(xy) = \phi(x)\phi(y)$

Similarly $\left\{\begin{bmatrix}a&b\\-b&a\end{bmatrix} : a,b\in\mathbb{R}\right\} \subset \mathbb{R}^{2\times2}$ is a subring isomorphic to $\mathbb{C}$.

An isomorphism $\mathbb{C} \to \left\{\begin{bmatrix}a&b\\-b&a\end{bmatrix} : a,b\in\mathbb{R}\right\}$ is $a+bi \longmapsto \begin{bmatrix}a&b\\-b&a\end{bmatrix}$ $(a,b\in\mathbb{R})$.

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

$\alpha = 5+3\sqrt{2}$, $\beta = 7-\sqrt{2}$

$\alpha+\beta = 12+2\sqrt{2}$

$\alpha-\beta = -2+4\sqrt{2}$

$\alpha\beta = (5+3\sqrt{2})(7-\sqrt{2}) = 35-5\sqrt{2}+21\sqrt{2}-6 = 29+16\sqrt{2}$

$$\frac{\alpha}{\beta} = \frac{5+3\sqrt{2}}{7-\sqrt{2}} = \frac{5+3\sqrt{2}}{7-\sqrt{2}}\cdot\frac{7+\sqrt{2}}{7+\sqrt{2}} = \frac{35+5\sqrt{2}+21\sqrt{2}+6}{47} = \frac{41+26\sqrt{2}}{47} = \frac{41}{47}+\frac{26}{47}\sqrt{2}$$

Alternatively, $\frac{\alpha}{\beta} = \alpha\beta^{-1}$

in matrix representation: $\underbrace{\begin{bmatrix}5&3\\6&5\end{bmatrix}}_{\alpha}\cdot\frac{1}{47}\begin{bmatrix}7&1\\2&7\end{bmatrix} = \frac{1}{47}\begin{bmatrix}41&26\\52&41\end{bmatrix}$

$\beta \longmapsto \begin{bmatrix}7&-1\\-2&7\end{bmatrix}$

$\beta^{-1} \longmapsto \frac{1}{47}\begin{bmatrix}7&1\\2&7\end{bmatrix}$

Similar: $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[\theta]$, $\theta = \sqrt[3]{2}$.

$\{a+b\theta : a,b\in\mathbb{Q}\}$ is not a field, not even a ring, since it's not closed under multiplication.

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

$\theta^3 = 2$

$\theta^4 = 2\theta$

$\theta^5 = 2\theta^2$

$\theta^6 = 4$

$\alpha = 5+3\theta$

$\beta = 7-\theta$

$\alpha+\beta = 12+2\theta$

$\alpha-\beta = -2+4\theta$

$$\alpha\beta = (5+3\theta)(7-\theta) = 35-5\theta+21\theta-3\theta^2$$
$$= 35+16\theta-3\theta^2$$

$$\frac{\alpha}{\beta} = \frac{5+3\theta}{7-\theta} = \boxed{a} + \boxed{b}\theta + \boxed{c}\theta^2 = \frac{251}{341} + \frac{182}{341}\theta + \frac{26}{341}\theta^2 = \frac{1}{341}(251+182\theta+26\theta^2)$$

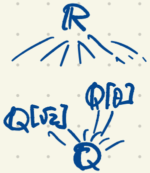
rational coefficients
$a, b, c \in \mathbb{Q}$

$\theta^3 = 2$

$\theta^3 - 2 =$

$\theta = \sqrt[3]{2}$

θ is a root of $x^3 - 2 = (x-\theta)(x^2+\theta x+\theta^2)$



$$5+3\theta = (a+b\theta+c\theta^2)(7-\theta)$$
$$= 7a + (7b-a)\theta + (7c-b)\theta^2 - 2c$$
$$= (7a-2c) + (7b-a)\theta + (7c-b)\theta^2$$

Hopefully

$$\begin{aligned} 7a \quad\;\; -2c &= 5 \\ -a + 7b \qquad &= 3 \\ -b + 7c &= 0 \end{aligned}$$

$$\left[\begin{array}{ccc|c} 7 & 0 & -2 & 5 \\ -1 & 7 & 0 & 3 \\ 0 & -1 & 7 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 0 & 49 & -2 & 26 \\ -1 & 7 & 0 & 3 \\ 0 & -1 & 7 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & -7 & 0 & -3 \\ 0 & 49 & -2 & 26 \\ 0 & 1 & -7 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & -7 & 0 & -3 \\ 0 & 1 & -7 & 0 \\ 0 & 49 & -2 & 26 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -49 & -3 \\ 0 & 1 & -7 & 0 \\ 0 & 0 & 341 & 26 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & -49 & -3 \\ 0 & 1 & -7 & 0 \\ 0 & 0 & 1 & \frac{26}{341} \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & \frac{251}{341} \\ 0 & 1 & c & \frac{182}{341} \\ 0 & 0 & 1 & \frac{26}{341} \end{array}\right]$$

$$\begin{array}{r} 26 \\ 7 \\ \hline 182 \end{array} \qquad \begin{array}{r} 49 \\ 26 \\ \hline 294 \\ 98 \\ \hline 1274 \end{array} \qquad \begin{array}{r} 341 \\ 3 \\ \hline 1023 \end{array}$$

$$-3 + 49 \cdot \frac{26}{341}$$
$$= -3 + \frac{1274}{341}$$
$$= \frac{-1023 + 1274}{341} = \frac{251}{341}$$

Check: $\frac{1}{341}(251+182\theta+26\theta^2)(7-\theta) = \frac{1}{341}(1757 + 1023\theta + 0\theta^2 - 52)$

$$= \frac{1}{341}(1705 + 1023\theta)$$
$$= 5 + 3\theta \quad ✓$$

$\mathbb{Q}[\theta]$ is a cubic field extension of $\mathbb{Q}$: it is a 3-dimensional vector space over $\mathbb{Q}$, with basis $1, \theta, \theta^2$.

Alternatively, use 3x3 matrices to represent elements of $\mathbb{Q}[\theta]$.

Take $T = \begin{bmatrix}0&0&2\\1&0&0\\0&1&0\end{bmatrix}$ to represent θ. $\quad T^3 = \begin{bmatrix}2&0&0\\0&2&0\\0&0&2\end{bmatrix} = 2I$

$$E = \{aI+bT+cT^2 : a,b,c\in\mathbb{Q}\} = \underbrace{\left\{\begin{bmatrix}a&2c&2b\\b&a&2c\\c&b&a\end{bmatrix} : a,b,c\in\mathbb{Q}\right\}}_{\text{This subring is a field.}} \subset \underbrace{\mathbb{Q}^{3\times3}}_{\text{noncommutative ring with identity having zero divisors}}$$

$\mathbb{Q}[\theta] \cong E$ via the isomorphism

$$\begin{array}{ccc}\mathbb{Q}[\theta] & & E\\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$}\\ a+b\theta+c\theta^2 & \mapsto & aI+bT+cT^2\end{array}$$

Are there any fields "between" $\mathbb{Q}$ and $\mathbb{Q}[\sqrt{2}]$, or between $\mathbb{Q}$ and $\mathbb{Q}[\theta]$?

Are there any fields "between" $\mathbb{R}$ and $\mathbb{C}$?

Suppose $\mathbb{R} \subset F \subset \mathbb{C}$ is a tower of fields (F is a subfield of $\mathbb{C}$ and $\mathbb{R}$ is a subfield of F).

'$\subset$' always means strict containment in this course.

$\subseteq$ vs $\subset$

$\leq$ vs $<$

Since $F \supset \mathbb{R}$, there exists $\alpha\in F$, $\alpha\notin\mathbb{R}$. Then $\alpha, 1$ are linearly independent over $\mathbb{R}$, i.e. $\alpha \neq a\cdot 1$ for any $a\in\mathbb{R}$. However $\mathbb{C}$ is 2-dimensional over $\mathbb{R}$ with basis $1, i$ (every complex number is uniquely expressible as $z = a\cdot 1 + b\cdot i$ with $a,b\in\mathbb{R}$). So $1, \alpha$ is a basis for F. So $F = \mathbb{C}$.

Is there any field extension $\mathbb{C} \subset F$ with F 2-dimensional over $\mathbb{C}$?

No, but there do exist fields $F \supset \mathbb{C}$ which are infinite-dimensional extensions.

Consider the ring $\mathbb{C}[x] = \{$ polynomials in x with complex coefficients $\}$

$$= \{ a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \ : \ a_i \in \mathbb{C}, \ n \geq 0 \}$$

This is a ring but not quite a field eg.

$$\frac{5 + 7x + ix^2}{3 - (4+i)x + 43x^2} \notin \mathbb{C}[x]$$

$\mathbb{C}(x)$ = field of fractions of $\mathbb{C}[x]$

= field of rational functions in x with complex coefficients

Just like constructing $\mathbb{Q}$ from $\mathbb{Z}$.

Another example of this: We'll construct a countably infinite subfield of $\mathbb{R}$ containing π.

This contains the subring $\mathbb{Q}[\pi] = \{ a_0 + a_1\pi + a_2\pi^2 + \dots + a_n\pi^n \ : \ n \geq 0, \ a_i \in \mathbb{Q} \}$

$\pi \in \mathbb{Q}[\pi]$ has no (multiplicative) inverse in $\mathbb{Q}[\pi]$ since if

$$1 = \pi (a_0 + a_1\pi + a_2\pi^2 + \dots + a_n\pi^n) \quad a_i \in \mathbb{Q}, \ n \geq 0,$$

a contradiction since π is transcendental. (π would be a root of a nonzero polynomial $a_n x^{n+1} + a_{n-1} x^n + \dots + a_2 x^3 + a_1 x^2 + a_0 x - 1$)

(Lindemann 1800's)

$\mathbb{Q}(\pi) = \{ \frac{a}{b} : a, b \in \mathbb{Q}[\pi], \ b \neq 0 \}$ is the field of quotients of the ring $\mathbb{Q}[\pi]$

$\mathbb{Q}(\sqrt{2}) = \{ \frac{a}{b} : a, b \in \mathbb{Q}[\sqrt{2}], \ b \neq 0 \} = \mathbb{Q}[\sqrt{2}]$ is already a field. $\sqrt{2}$ is algebraic: it is a root of a nonzero poly. $x^2 - 2 \in \mathbb{Q}[x]$

Every $\alpha \in \mathbb{C}$ is either algebraic or transcendental, never both.

$$\underbrace{\mathbb{Q}}_{\text{countable}} \subset \underbrace{\mathbb{R}}_{\text{uncountable}} \subset \underbrace{\mathbb{C}}_{\text{uncountable}}$$

$$\underbrace{\mathbb{Q} \subset \mathbb{A}}_{\text{countable}} \subset \underbrace{\mathbb{C}}_{\text{uncountable.}}$$

$\mathbb{A} = \{\text{algebraic numbers}\}.$

$$\begin{tikzcd} & \mathbb{A} \arrow[dr, phantom, "\subset"] & \\ \mathbb{Q} \subset \mathbb{A}\cap\mathbb{R} \arrow[ur, phantom, "\subset"] \arrow[dr, phantom, "\subset"] & & \mathbb{C} \\ & \mathbb{R} \arrow[ur, phantom, "\subset"] & \end{tikzcd}$$

$\mathbb{Q} = \{a_1, a_2, a_3, a_4, \dots\}$

$$\begin{array}{cccc} a_1+a_1x & a_1+a_2x & a_1+a_3x & \dots \\ a_2+a_1x & a_2+a_2x & a_2+a_3x & \dots \\ a_3+a_1x & a_3+a_2x & a_3+a_3x & \dots \\ \vdots & \vdots & \vdots & \end{array}$$

$\mathbb{Q}[\pi]$ is a countably infinite ring

so $\mathbb{Q}(\pi)$ is a countably infinite field.

Elements of $\mathbb{Q}(\pi) \subset \mathbb{R}$ look like

$$\frac{53.8\pi^3 - 17\pi + \frac{53}{7}}{42\pi^2 + 119\pi + \frac{103}{698}}$$

Compare: $\mathbb{Q}(e) \subset \mathbb{R}$, another countable subfield of $\mathbb{R}$.

Actually $\mathbb{Q}(e) \cong \mathbb{Q}(\pi) \cong \mathbb{Q}(x)$. An isomorphism is $f(e) \longmapsto f(\pi)$ where $f(x) \in \mathbb{Q}(x)$.
(x being an indeterminate ie. an $\left\{\begin{matrix}\text{abstract}\\ \text{general}\\ \text{generic}\end{matrix}\right.$ symbol)

$\mathbb{Q}(x) \longrightarrow \mathbb{Q}(\pi)$ evaluation

$\mathbb{Q}(x) \longrightarrow \mathbb{Q}(e)$

$\mathbb{Q}(x) \longrightarrow \mathbb{Q}(\sqrt{2})$ doesn't quite work eg. the image of $\frac{x^3+7x^2-3}{x^2-2} \in \mathbb{Q}(x)$ is undefined; you can't evaluate this at $\sqrt{2}$.

But the evaluation maps at $\pi, e, \sqrt{2}, \dots$

$$\left.\begin{array}{l} \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\pi] \\ \mathbb{Q}[x] \longrightarrow \mathbb{Q}[e] \\ \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\sqrt{2}] \\ \quad\vdots \end{array}\right\}$$ all well-defined ring homomorphisms.

If $\phi: R \to S$ where R, S are rings, we say ϕ is a ring homomorphism if

$$\left.\begin{array}{l}\phi(a+b) = \phi(a) + \phi(b) \\ \phi(ab) = \phi(a)\phi(b)\end{array}\right\} \text{ for all } a,b \in R$$

We don't necessarily require $\phi(1) = 1$; and in general the rings R, S may not have identity. If R, S are rings with identity ($1_R \in R$, $1_S \in S$) we might consider only homomorphisms of rings with identity i.e. $\phi(1_R) = \phi(1_S)$.

* Suppose F, K are fields. If $\phi: F \to K$ is a ring homomorphism then either

(i) $\phi(F) = \{0\}$ i.e. $\phi(a) = 0$ for all $a \in F$, or (trivial)

(ii) ϕ is one-to-one i.e. $\phi(F) \subseteq K$ is a subfield isomorphic to F.

Any homomorphism $\mathbb{Q}(x) \to \mathbb{R}$ is either trivial or it has the form $\mathbb{Q}(x) \to \mathbb{Q}(a)$, $f(x) \mapsto f(a)$ is an evaluation at some transcendental number $a \in \mathbb{R}$.

We have ring homomorphisms $\mathbb{Q}[x] \longrightarrow \mathbb{C}^{n\times n}$ ($n\times n$ complex matrices) where we evaluate at a matrix $A \in \mathbb{C}^{n\times n}$, i.e. $f(x) \mapsto f(A)$

$$\frac{47}{3}x^2 + \frac{18}{11}x - \frac{41}{7} \mapsto \frac{47}{3}A^2 + \frac{18}{11}A - \frac{41}{7}I$$

(*) In a field F, every ideal is either $\{0\}$ or F.

An automorphism of a field F is an isomorphism $\phi: F \to F$. Eg

(i) Automorphisms of $\mathbb{Q}[\sqrt{2}]$? We want $\phi: \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ bijective with

$$\phi(a+b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b).$$

- The identity $\phi(x) = x$ for all $x \in \mathbb{Q}[\sqrt{2}]$
- Conjugation $\phi(a+b\sqrt{2}) = a - b\sqrt{2}$ for all $a,b \in \mathbb{Q}$. (This is algebraic conjugation, not complex conjugation).

These are the only automorphisms of $\mathbb{Q}[\sqrt{2}]$.

If $\phi : F \to F$ is any automorphism of a field F then

$\phi(0) = \phi(0+0) = \phi(0) + \phi(0) \Rightarrow \phi(0) = 0$

$\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1)$ where $\phi(1) \neq \underset{\phi(0)}{0}$ since ϕ is one-to-one. Multiply both sides by $\phi(1)^{-1}$ to get $\phi(1) = 1$.

$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1+1 = 2$

$\phi(3) = \phi(2+1) = \phi(2) + \phi(1) = 2+1 = 3$

So $3 + (-3) = 0$

$\underset{3}{\phi(3)} + \underset{-3}{\underbrace{\phi(-3)}} = \phi(0) = 0$

If $m, n \in \mathbb{Z}$ with $n \neq 0$,

$\phi(n \cdot \frac{m}{n}) = \phi(m) = m$

$\underset{n}{\phi(n)} \phi(\frac{m}{n}) \Rightarrow \phi(\frac{m}{n}) = \frac{m}{n}$. So $\phi(x) = x$ for all $x \in \mathbb{Q}$.

$\phi(\sqrt{2})^2 = \phi(\sqrt{2}^2) = \phi(2) = 2 \Rightarrow \phi(\sqrt{2}) = \pm\sqrt{2}$.

If $\phi(\sqrt{2}) = \sqrt{2}$ then $\phi(a+b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b\sqrt{2}$ for all $a, b \in \mathbb{Q}$

If $\phi(\sqrt{2}) = -\sqrt{2}$ then $\phi(a+b\sqrt{2}) = \phi(a) + \phi(b)\phi(\sqrt{2}) = a + b(-\sqrt{2}) = a - b\sqrt{2}$.

If F is any field then $\text{Aut}\, F = \{\text{all automorphisms of } F\}$ is a group under composition. Its identity is ι where $\iota : F \to F$, $\iota(x) = x$ for all $x \in F$ (the identity map).

$\text{Aut}\, \mathbb{Q} = \{\iota\}$ is trivial.

$\text{Aut}\, \mathbb{R} = \{\iota\}$ is trivial but why?

$\mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$ has two automorphisms.

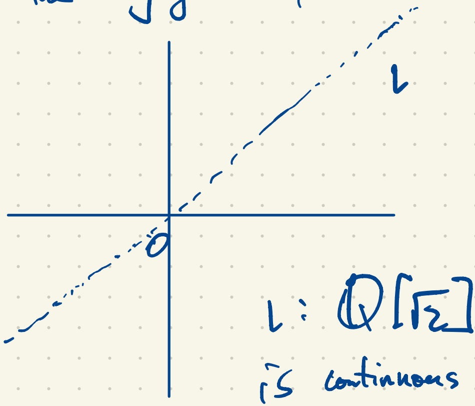
$\text{Aut}\, \mathbb{Q}[\sqrt{2}]$ is a group of order 2.

$\text{Aut}\, \mathbb{C}$ contains ι and τ = complex conjugation, $\tau(a+bi) = a - bi$ for all $a, b \in \mathbb{R}$.

But $\text{Aut}\, \mathbb{C}$ is uncountable. $\mathbb{C}$ has uncountably many automorphisms.

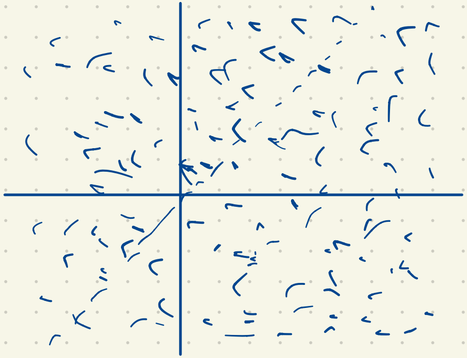
The only continuous automorphisms of $\mathbb{C}$ are ι, τ.

The conjugation $\phi \in \operatorname{Aut} \mathbb{Q}[\sqrt{2}]$ defined by $\phi(a+b\sqrt{2}) = a-b\sqrt{2}$ $(a,b \in \mathbb{Q})$ is badly discontinuous



$\iota : \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{2}]$

is continuous



graph of ϕ

ϕ is badly discontinuous.

$\mathbb{R}(x)$ = { rational functions of x with real coefficients } is a field.

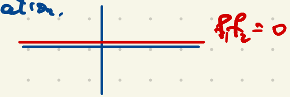
Can we replace "rational functions" with "functions" or "continuous functions" $\mathbb{R} \to \mathbb{R}$?

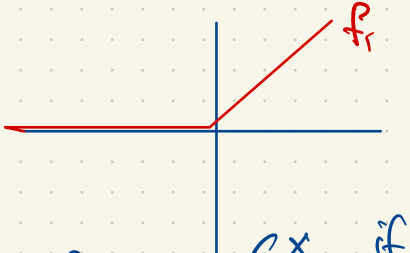
{ functions $\mathbb{R} \to \mathbb{R}$ }

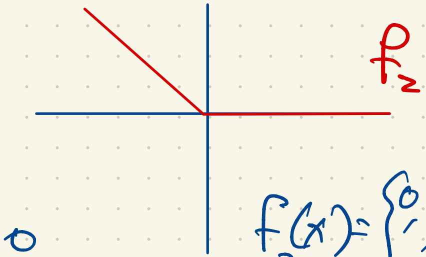
{ continuous functions $\mathbb{R} \to \mathbb{R}$ }

are rings with zero divisors so they are not fields.

Commutative rings with identity under pointwise multiplication.







$$f_1(x) = \begin{cases} x, & \text{if } x \geq 0 \\ 0, & \text{if } x \leq 0 \end{cases}$$

$$f_2(x) = \begin{cases} 0 & \text{if } x \geq 0 \\ -x, & \text{if } x \leq 0 \end{cases}$$

$f_1 f_2 = 0$ but f_1, f_2 are nonzero functions.

How do we check that $f(x) \in \mathbb{Q}[x]$ is irreducible (i.e. in $\mathbb{Q}[x]$)?

eg. $f(x) = x^4 + x^2 + x + 1$

If $f(x) = \underbrace{(x^2+ax+b)}_{\text{degree 2 in } \mathbb{Z}[x]}\underbrace{(x^2+cx+d)}_{\text{degree 2 in } \mathbb{Z}[x]}$ then $bd=1$ implies $b=d=\pm 1$. If $b=d=1$ then $f(x) = (x^2+ax+1)(x^2-ax+1)$ has no x term, a contradiction.

$a,b,c,d \in \mathbb{Z}$

If $b=d=-1$ then $f(x) = (x^2+ax-1)(x^2-ax-1)$ has no x term, again a contradiction.

If $f(x) = (x+a)(x^3+bx^2+cx+d)$ where $a,b,c,d \in \mathbb{Z}$ then $ad=1$ so $a=d=\pm 1$, but $\left.\begin{array}{l} f(1)=4 \\ f(-1)=2 \end{array}\right\}$ so ± 1 are not roots of $f(x)$.

So $f(x)$ is irreducible in $\mathbb{Z}[x]$; so $f(x)$ is irreducible also in $\mathbb{Q}[x]$.

Why do we care about automorphisms of fields?

Historically the study of fields originated in questions about finding roots of polynomials.

The roots of ax^2+bx+c $(a \neq 0)$ are $\dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$.

Similarly the roots of ax^3+bx^2+cx+d $(a\neq 0)$ are given explicitly using formulas of a,b,c,d using $+, -, \times, \div$ and extracting square roots and cube roots.

Similarly for polynomials of degree 4. But for degree ≥ 5, no such formula exists. The reason is found in group theory. Galois theory gives the connection between fields and groups. Given a polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Q}[x]$ then $f(x) = (x-r_1)(x-r_2)\cdots(x-r_n)$ where $r_1, \ldots, r_n \in \mathbb{C}$. The roots lie in $F = \mathbb{Q}(r_1, \ldots, r_n) \subset \mathbb{C}$. Let $G = \operatorname{Aut} F$. G permutes $r_1, \ldots, r_n$ (in particular G is a subgroup of $\underset{\text{order } n!}{S_n}$).

If F is a field then $F[a]$ = ring of all polynomials in "a" with all coefficients in F.

$\quad$ = the smallest ring containing F and a

$F(a)$ = the field of all rational functions in "a" with coefficients in F

$\quad$ = the smallest field extension of F containing a.

You can do all this for more than one element a e.g.

$F[a_1, \cdots, a_k]$ = the ring of all polynomials in $a_1, \cdots, a_k$ with coefficients in F

$\quad$ = the smallest ring containing F and $a_1, \cdots, a_k$

$\quad$ = the ring generated by $F, a_1, \cdots, a_k$

$F(a_1, \cdots, a_k)$ = the field extension of F generated by $a_1, \cdots, a_k$ together with F.

eg. $\mathbb{Q}[\sqrt{2}] = \{ a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + a_3\sqrt{2}^3 + \cdots + a_m\sqrt{2}^m : m \geq 0,\ a_i \in \mathbb{Q} \} = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ since $\sqrt{2}$ is algebraic.

$E = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ ... is this a field? $\mathbb{Q}[\sqrt{2}, \sqrt{5}] = \{ a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10} : a, b, c, d \in \mathbb{Q} \}$

eg. $\alpha = \sqrt{2} + \sqrt{5} \in \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ is a root of a polynomial $f(x) \in \mathbb{Q}[x]$, in fact $f(x) \in \mathbb{Z}[x]$.

In fact $\alpha \notin \mathbb{Q}$ (why?)

$$\alpha = \sqrt{2} + \sqrt{5}$$
$$\alpha^2 = 7 + 2\sqrt{10}$$
$$\alpha^2 - 7 = 2\sqrt{10}$$
$$\alpha^4 - 14\alpha^2 + 49 = 40$$
$$\alpha^4 - 14\alpha^2 + 9 = 0$$

Candidate: $x^4 - 14x^2 + 9$

You can check that this poly. is irred. in $\mathbb{Q}[x]$ (using steps we used on Friday Sept 13).

$f(x) = x^4 - 14x^2 + 9$ is the <u>minimal polynomial</u> of α over $\mathbb{Q}$ in the sense that a polynomial $g(x) \in \mathbb{Q}[x]$ has α as a root iff $f(x) \mid g(x)$ ie. $g(x) = u(x)f(x)$, $u(x) \in \mathbb{Q}[x]$.

<u>Proof</u>: If $g(x) = u(x)f(x)$ for some $u(x) \in \mathbb{Q}[x]$ then $g(\alpha) = u(\alpha)\underset{0}{\cancel{f(\alpha)}} = 0$ i.e. $g(x)$ is a poly. with coeffs in $\mathbb{Q}$ having α as a root. Conversely, suppose $g(x) \in \mathbb{Q}[x]$ having α as a root. Then $g(x) = q(x)f(x) + r(x)$ with $q(x), r(x) \in \mathbb{Q}[x]$, deg $r(x) < 4$.

Now $\underset{0}{\cancel{g(\alpha)}} = q(\alpha)\underset{0}{\cancel{f(\alpha)}} + r(\alpha) = 0 \implies r(\alpha) = 0$.

If $r(x) \neq 0$ then take

$d(x) = \gcd(f(x), r(x)) = a(x)f(x) + b(x)r(x)$ by Euclid's Algorithm

$d(\alpha) = a(\alpha)\cancel{f(\alpha)} + b(\alpha)\cancel{r(\alpha)} = 0.$

Contradiction since $f(x)$ is irreducible in $\mathbb{Q}[x]$.

If $\alpha \in \mathbb{C}$ is algebraic (α is a root of coefficients in $\mathbb{Q}$) then there is a unique minimal polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ of smallest degree which is monic i.e. its leading coeff. is 1.

The minimal poly. of $\sqrt{2}+\sqrt{5}$ is $x^4-14x^2+9 = (x^4-14x^2+49)-40 = (x^2-7)^2-40 = (x^2-7+2\sqrt{10})(x^2-7-2\sqrt{10})$

$= (x-(-\sqrt{2}+\sqrt{5}))(x-(\sqrt{2}-\sqrt{5}))(x-(\sqrt{2}+\sqrt{5}))(x-(-\sqrt{2}-\sqrt{5}))$

$= (x+\sqrt{2}-\sqrt{5})(x-\sqrt{2}+\sqrt{5})(x-\sqrt{2}-\sqrt{5})(x+\sqrt{2}+\sqrt{5})$

The roots $\sqrt{2}+\sqrt{5}$, $-\sqrt{2}-\sqrt{5}$, $-\sqrt{2}+\sqrt{5}$, $\sqrt{2}-\sqrt{5}$

$\sqrt{7-2\sqrt{10}} = -\sqrt{2}+\sqrt{5}$ since $(-\sqrt{2}+\sqrt{5})^2 = 7-2\sqrt{10}$

$(\sqrt{2}-\sqrt{5})^2 = 7-2\sqrt{10}$

$\sqrt{7+2\sqrt{10}} = \sqrt{2}+\sqrt{5}$ since $(\sqrt{2}+\sqrt{5})^2 = 7+2\sqrt{10}$

$(-\sqrt{2}-\sqrt{5})^2 = 7+2\sqrt{10}$

$\sqrt{2} \notin \mathbb{Q}$ by Euclid's argument

If $\sqrt{2} = \frac{m}{n}$, $m,n \in \mathbb{Z}$ in lowest terms i.e. $\gcd(m,n)=1$ then $m^2 = 2n^2$ is even so $m = 2r$, $r \in \mathbb{Z}$, $4r^2 = 2n^2$, $n^2 = 2r^2$ is even so n is even, a contradiction.

The same argument shows $\sqrt{5}, \sqrt{10} \notin \mathbb{Q}$.

$\pm\sqrt{2}\pm\sqrt{5} \notin \mathbb{Q}$, since their squares are $7 \pm 2\sqrt{10} \notin \mathbb{Q}$.

This gives another explanation why x^4-14x^2+9 is irreducible in $\mathbb{Q}[x]$.

$E = \mathbb{Q}[\sqrt{2},\sqrt{5}] = \mathbb{Q}[\alpha]$, $\alpha = \sqrt{2}+\sqrt{5}$

$\parallel$

$\{a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10} : a,b,c,d \in \mathbb{Q}\}$

$= \{a+b\alpha+c\alpha^2+d\alpha^3 : a,b,c,d \in \mathbb{Q}\}$

This equality is explained as follows: $E = \mathbb{Q}[\sqrt{2},\sqrt{5}] = \{a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10} : a,b,c,d \in \mathbb{Q}\}$ is a 4-dimensional vector space over $\mathbb{Q}$ with basis $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$.

$E \supseteq \mathbb{Q}[\alpha]$, $\alpha^4-14\alpha^2+9=0$ so $\alpha^4 = 14\alpha^2-9$

$\alpha^5 = 14\alpha^3-9\alpha$

$\alpha^6 = 14\alpha^4-9\alpha^2 = 14(14\alpha^2-9)-9\alpha^2 = 187\alpha^2-126$

$\parallel$

$\{a+b\alpha+c\alpha^2+d\alpha^3 : a,b,c,d \in \mathbb{Q}\}$

There is no nonzero $(a,b,c,d) \in \mathbb{Q}^4$ with $a+b\alpha+c\alpha^2+d\alpha^3 = 0$

So $1, \alpha, \alpha^2, \alpha^3$ are linearly independent over $\mathbb{Q}$.

An important class of examples of fields is: (algebraic) number fields are finite-dimensional extensions $E \supseteq \mathbb{Q}$ eg.

$$\mathbb{Q},\quad \mathbb{Q}[\sqrt{2}],\quad \mathbb{Q}[\sqrt{5}],\quad \mathbb{Q}[i],\quad \mathbb{Q}[\sqrt{-13}],\quad \underset{\alpha=\sqrt{2}+\sqrt{5}}{\mathbb{Q}[\alpha]=\mathbb{Q}[\sqrt{2},\sqrt{5}]},\quad \text{etc.}$$

Not $\mathbb{R}, \mathbb{C}$ which are infinite-dimensional over $\mathbb{Q}$.

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \dots$ are linearly independent over $\mathbb{Q}$.