Fields: Commutative ring s.t. non-zero elements are invertible.

$\iff$ Commutative Ring whose only ideals are 0 and R.

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{F}_{p^n}$,

$= \mathrm{Frac}\,\mathbb{Z}$. $\qquad \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$\mathbb{C}(t)$ = "field of rational functions in one variable over $\mathbb{C}$"

$= \mathrm{Frac}\,\mathbb{C}[t]$

$\dfrac{f(t)}{g(t)}$ for $f(t), g(t)$ polynomials.

$F(t_1, t_2, t_3, \ldots, t_n) = \mathrm{Frac}\, F[t_1, \ldots, t_n]$

$\uparrow$ some field

$F(t_1, t_2, \ldots) = \mathrm{Frac}\, F[t_1, t_2, \ldots]$ countably many variables.

Weird: $\overline{\mathbb{Q}(t_i \mid i \in S)} \cong \mathbb{C}$. alg. closure.

$S = \mathcal{P}(\mathbb{N})$.

$\mathbb{C}[x,y]/y^2-(x^3+1) \leftarrow$ Integral domain

$\uparrow$ irreducible.

$\mathrm{Frac}\, \mathbb{C}[x,y]/y^2-x^3+1$ is a field.

$\cong$ (Weierstrass theory of elliptic functions).

Field of meromorphic functions on

$\mathbb{C}/\langle 1, e^{2\pi i/3}\rangle$

If R is a commutative ring and $\mathfrak{p} \subseteq R$ is a prime ideal

then $\mathrm{Frac}(R/\mathfrak{p})$ is a field.

If $\mathfrak{p}$ is maximal then $R/\mathfrak{p}$ is already a field.

$\mathbb{Q}_p \rightsquigarrow$ Complete $\mathbb{Q}$ for the p-adic topology

defined by p-adic absolute value

way of measuring distance by divisibility by a prime number p.

$\mathbb{R}$ sort completed $\mathbb{Q}$ for the topology defined by $|\ |$ euclidean absolute value.

Observation: If K is a field then there is a unique map

$$\phi : \mathbb{Z} \to K.$$

$$1 \mapsto 1$$

$$2 \mapsto 1+1$$

$$3 \mapsto 1+1+1, \ \ldots$$

This map has a kernel. ✓ Prime ideals of $\mathbb{Z}$

$(0) \quad (p) \quad p$ prime number.

$\mathrm{Im}\,\phi \cong \mathbb{Z}/\ker\phi$ is an integral domain.
$\cap$ (subring of a field).
K.

So $\ker\phi$ is a prime ideal.
$\mathbb{Z}$ is a PID so we know what prime ideals are.

Either $\ker\phi = 0$

$$\begin{array}{c} \mathbb{Z} \hookrightarrow K \\ \vdots \\ \mathbb{Q} \hookrightarrow K \end{array}$$

by defn / univ property of localization

$\ker\phi = (p)$

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow K.$$
$$\| $$
$$\mathbb{F}_p$$

Defn/Theorem: The characteristic of a field K is the smallest positive # n such that

$$\underbrace{1+1+1 \cdots +1}_{n \text{ times}} = 0$$

or 0 if there is no such n.

$\iff$

K has char $p \iff \mathbb{F}_p \hookrightarrow K$

K has char $0 \iff \mathbb{Q} \hookrightarrow K$.

Remark If R is any ring and F is a field then any map $F \to R$ of rings is injective ($\ker$ is an ideal $\neq F \Rightarrow = (0)$).

Remark/Exercise: If K has characteristic p then for any $\alpha \in K$

$$\underbrace{\alpha + \alpha + \dots + \alpha}_{p \text{ times}} = 0.$$

$$\overset{/\!/}{p(\alpha)} = \underbrace{(1+1+\dots+1)}_{p \text{ times}}\alpha.$$

$$= 0\alpha = 0.$$

If $K \subseteq L$ are both fields we say K is a subfield of L or L/K is an extension (of fields).

Degree of a field extension L/K

$[L:K]$ = dim of L as a K-vector space.

e.g. $[\mathbb{C}:\mathbb{R}] = 2$

$\mathbb{C}$ has basis $1, i$ as an $\mathbb{R}$-vector space.

This can be infinite, but for us we'll just write $n \in \mathbb{N}$ if it's finite or ∞ if it's not.

$L/K \rightsquigarrow$ how to build L from K?

Idea: Just "add in" one element at a time.

Suppose $\alpha \in L$, I want to look at

$K(\alpha)$ ← defined to be the smallest subfield of L containing both K and α.

(The intersection of all such)

$K \subseteq K(\alpha) \subseteq L.$

The trick of everything: $K(\alpha)$ admits a simple abstract description.

↓

as an extension of K, not as a subfield of L.

Observation: There is a unique map

$$K[t] \to L$$

sending $t \mapsto \alpha$ and = identity on K.

← universal property of polynomial rings.

Kernel of this map:

$$(0) \quad \text{or} \quad (M_\alpha(t))$$

Monic irreducible polynomial.

Makes sure you don't write down the same ideal twice.

If Ker is 0

$K[t] \hookrightarrow L$ ← Say α is transcendental over K.

$\downarrow$ $\vdots$ extends uniquely.

$K(t) \hookrightarrow L$ $\quad K(t) \xrightarrow{\sim} K(\alpha) \subseteq L$.

$t \mapsto \alpha$

If Ker is $(m_\alpha(t))$ ← minimal polynomial of α over K

$K[t]/(m_\alpha(t)) \hookrightarrow L$ ← maximal ideal so quotient is a field.

Image is $K(\alpha)$.

$K[t]/(m_\alpha(t)) \xrightarrow{\sim} K(\alpha) \subseteq L$.

Example: $\mathbb{R} \subseteq \mathbb{C}$

$i \in \mathbb{C}$.

$\mathbb{R}[t] \longrightarrow \mathbb{R}(i)$

$t \longmapsto i$

kernel is (t^2+1)

$\mathbb{R}[t]/(t^2+1) \xrightarrow{\sim} \mathbb{R}(i) = \mathbb{C}$.

$\mathbb{R}[t]/(t^2+1) \xrightarrow{\sim} \mathbb{C}$

WARNING: There is another isomorphism like this:

$\mathbb{R}[t]/t^2+1 \longrightarrow \mathbb{C}$

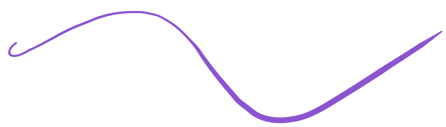
identity on $\mathbb{R}$.

$t \longmapsto$ root of t^2+1.

$t \longmapsto i$ ← just saw

$t \longmapsto -i$ ← another one

[illegible]



$$\begin{tikzcd} K\text{-algebras} \arrow[r, shift left, "\text{Forgetful}"] & \text{Sets} \arrow[l, shift left, "\text{Polynomial ring.}"] \end{tikzcd}$$

$$\mathrm{Hom}_{K\text{-algebras}}(K[t_i \mid i \in I], A)$$

$$= \mathrm{Hom}_{\text{sets.}}(I, A)$$