


Eine Woche, ein Beispiel

6.4. basics of fields

This document is aimed for people who have enough mathematical maturity, but miss the chance and time to study Galois theory. For a (relative) complete study of Galois theory which takes time, please see [GTM167].

1. classical motivation
2. common confusion
3. field extension
4. examples of algebraic closed field

1. classical motivation

	ruler-and-compass construction 尺规作图	solving higher degree equations 求根公式
possible	 17-gon	$\cos \frac{2\pi}{5}$ $\frac{1}{4}$ $\cos \frac{2\pi}{17}$ $\frac{1}{17}$
impossible	Squaring the circle Doubling the cube Angle trisection	π 化圆为方 $\sqrt[3]{2}$ 倍立方 $x: 4x^3 - 3x - a = 0$ 三等分角

Ex. Denote

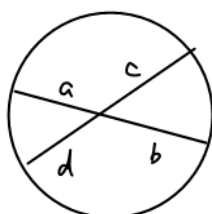
$$F_R := \{z \in \mathbb{C} \mid z \text{ can be drawn by ruler-and-compass, given } 0, 1\}$$

$$= \{\text{algebraic constructible complex numbers}\}$$

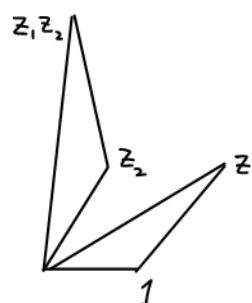
$$F_{\# \text{根}} := \{z \in \mathbb{C} \mid z \text{ can be expressed by } +, -, \times, \div, \text{ radicals}\}$$

Verify that $F_R, F_{\# \text{根}}$ are fields.

Hint. Verify that $\mathbb{Q} \subseteq F_R$ to get some intuition.



$$ab = cd$$



Ex. Given $1, a \in \mathbb{R}^+$, try to draw \sqrt{a} by ruler-and-compass.

Argue that why we can draw \square and 17-gons.

Hint. $\cos \frac{2\pi}{5} = \frac{\sqrt{5}}{4} - 1$

$$\cos \frac{2\pi}{17} = \frac{1}{16}(-1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}})$$

Slogan: consider element \rightsquigarrow set
 object \rightsquigarrow moduli spaces
 if x can be realized $\rightsquigarrow \{x \mid x \text{ can be realized}\}$

2. common confusion

	Abstract field	Subfield of \bar{K} or \mathbb{C}
name of category	Field	Subfield K
Ob	$\{F : \text{field}\}$	$\{(F, \iota) \mid \iota : F \hookrightarrow \bar{K}\}$
Mor	$\text{Mor}_{\text{Field}}(F, E) = \{\alpha : F \hookrightarrow E\}$ usually: finitely many elements	$\text{Mor}_{\text{Subfield}}(F, E) = \left\{ \alpha : F \hookrightarrow E \atop \text{s.t. } \begin{array}{c} \nearrow \\ \bar{K} \\ \searrow \end{array} \right\}$ at most 1 element
Examples	$\mathbb{Q}[x]/(x^2+1)$ $\mathbb{Q}[x]/(x^3-2)$ $\mathbb{Q}(x)$	$\mathbb{Q}(i)$ $\mathbb{Q}(\sqrt[3]{2})$ $\mathbb{Q}(\pi)$

Common questions: (Which category are we considering for these questions?)

- # extensions of K of deg 3
- Automorphism gp of the field.

Abstract fields are not as hard as you may think!

- Ex 1). Write down the definition of $\mathbb{Q}[x]/(x^2+1)$, $\mathbb{Q}(x)$, as well as $\mathbb{Q}(i)$, $\mathbb{Q}(\pi)$
 2). Find a \mathbb{Q} -basis of $\mathbb{Q}[x]/(x^2+1)$, $\mathbb{Q}(x)$. Compute the dim.

Constructing new field by adding roots

$$\begin{array}{r}
 132 \overline{) 13562} \\
 \underline{102} \\
 3362 \\
 \underline{306} \\
 302 \\
 \underline{202} \\
 100
 \end{array}$$

$$13562 \div 102 = 132 \dots 100$$

$$13562 = 102 \times 132 + 100$$

$$\begin{array}{r}
 x^2-2 \overline{) x^4+3x^3+5x^2+6x+2} \\
 \underline{x^4} -2x^2 \\
 3x^3+7x^2+6x+2 \\
 \underline{3x^3} -6x \\
 7x^2+12x+2 \\
 \underline{7x^2} -14 \\
 12x+16
 \end{array}$$

$$(x^4+3x^3+5x^2+6x+2) \div (x^2-2) = (x^2+3x+7) \dots (12x+16)$$

$$x^4+3x^3+5x^2+6x+2 = (x^2-2)(x^2+3x+7) + (12x+16)$$

Ex. factorize $x^3+4x^2-7x-10$ in $\mathbb{Q}[x]$ or $\mathbb{F}_3[x]$.

Ex. Let $F = \mathbb{F}_7[x]/(x^3-3)$.

1) Compute $(x^2+1) \cdot (x-1)$, $\frac{1}{x}$,

2) Show that x^3-3 is irr in $\mathbb{F}_7[x]$, i.e.

$$x^3-3 = f(x)g(x) \Rightarrow \deg f=0 \text{ or } \deg g=0$$

$f, g \in \mathbb{F}_7[x]$

3) Show that $(x^3-3, x^2+x+1) = (1)$ in $\mathbb{F}_7[x]$, by Euclidean division.

In fact, $\mathbb{F}_7[x]$ is ED \Rightarrow PID

4) Compute $(x^2+x+1)^{-1}$ in F .

5) Factorize T^3-3 in $F[T]$.

Rmk. In fact, $K[T]/(f(T))$ is a field $\Leftrightarrow f(T) \in K[T]$ is irreducible

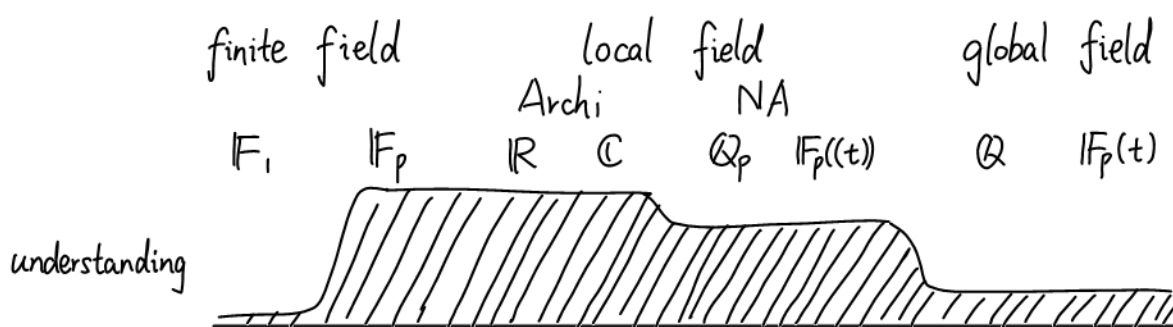
Ex. Let $F = \mathbb{Q}[x]/(x^3-2)$.

1) Compute $\text{Mor}_{\text{field}}(F, \mathbb{C})$. Are all embeddings real?

2) Discussion: What is the difference between $\mathbb{Q}[x]/(x^3-2)$ with $\mathbb{Q}(\sqrt[3]{2})$?

3. field extension

Main examples of fields



Definitions

Def: E/F field extension: $(E, F, \iota: F \hookrightarrow E)$

Def: Base field: $\begin{cases} \mathbb{Q} & \text{char } F = 0 \\ \mathbb{F}_p & \text{char } F = p \end{cases}$

Def. (Algebraic extension)

E/F is alg, if $\forall a \in E$ is alg/ F , i.e., the following equivalent conditions are true.

1) $\forall a \in E, \exists f \in F[x], f \neq 0, f(a) = 0.$

2) $\forall a \in E, [F(a):F] < +\infty.$

3) $E = \bigcup_{\substack{F' \subseteq E \\ F'/F \text{ finite}}} F'$

4) $\forall a \in E, \exists \text{ f.d. } F\text{-v.s. } V \subseteq E \text{ s.t. } aV \subseteq V.$

For $a \in E$, $\text{Min}(a, F) := \text{minimal monic polynomial of } a \text{ in } F.$

E.g. $\overline{\mathbb{Q}}/\mathbb{Q}, \mathbb{Q}(\pi)/\mathbb{Q}, \mathbb{C}/\mathbb{Q}$

We mainly consider alg extension, e.p. fin field extension.

Assume: E/F alg

Slogan:

Galois = normal + separable

Def. (Normal extension)

E/F normal, if $\forall a \in E$, $\underbrace{\text{Min}(a, F) \subseteq F[x] \subseteq E[x]}_{a \in E \text{ is normal}} \text{ splits.}$

E.g. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

Def. (Separable extension)

E/F sep, if $\forall a \in E$, $\underbrace{\text{Min}(a, F) \text{ has no repeated roots in } \bar{F}[x]}_{a \in E \text{ is sep}}.$

E.g. $\mathbb{F}_p(T^{\frac{1}{p}})/\mathbb{F}_p(T)$, where $\mathbb{F}_p(T^{\frac{1}{p}}) := \mathbb{F}_p(T)[x]/(x^p - T)$

Rmk. When $\text{char } F = 0$ or $\#F < +\infty$, E/F is always separable.

Def. (Galois extension)

E/F Galois, if E/F is normal and sep. We denote

$$\begin{aligned} \text{Gal}(E/F) &= \text{Aut}_{F\text{-alg}}(E) \\ &= \{ \sigma : E \rightarrow E \mid \sigma|_F = \text{Id}_F \} \end{aligned}$$

Rmk. When E/F finite,

$$E/F \text{ Galois} \Leftrightarrow [E:F] = \# \text{Aut}_{F\text{-alg}}(E)$$

E.g. & Exercise. Compute $\# \text{Aut}_{F\text{-alg}}(E)$ for $E/F = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{F}_p(T^{\frac{1}{p}})/\mathbb{F}_p(T)$.

<https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisconrexamples.pdf>

Ex. Read it, and compute

$$\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}), \quad \text{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$$

$$\text{Gal}(F/\mathbb{Q}) \quad F: \text{the splitting field of } x^4 - x^2 - 1.$$

I would instead begin with relative easier case:

$$\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \quad \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \quad \text{Gal}(\mathbb{Q}[T]/(T^2-2)^2-2/\mathbb{Q})$$

$\text{Gal}(\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q})$

After that, do 4.2.3 : $\mathbb{Q}(\sqrt[4]{2}(1+i))/\mathbb{Q}$

$$4.1.16: \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$$

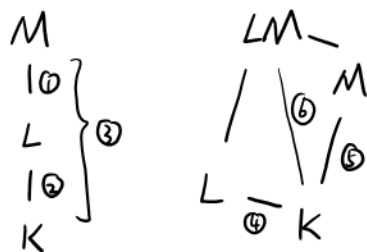
$$4.1.4: \mathbb{Q}(\sqrt{2}, \sqrt{3}, u)/\mathbb{Q}$$

$$4.1.7. F(\alpha)/F$$

$$u^2 = (9-5\sqrt{3})(2-\sqrt{2})$$

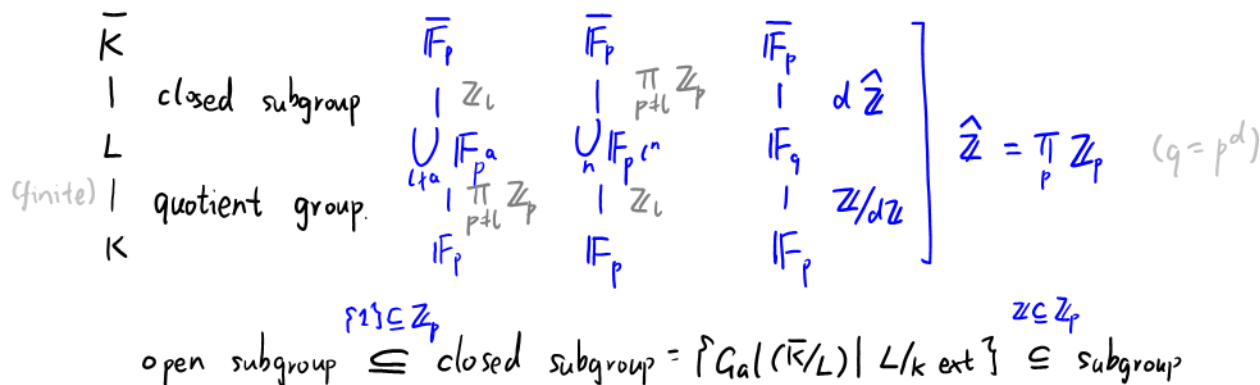
$$\begin{aligned} \text{char } F = p, a \in F, x^p - x - a \in F[x] \text{ irr.} \\ x^p - x - a = 0 \end{aligned}$$

in [近世代数三百题].



$\xrightarrow{\text{normal:}}$ $\textcircled{3} \Rightarrow \textcircled{1}$ $\textcircled{3} \not\Rightarrow \textcircled{2}$ $\textcircled{1} + \textcircled{2} \not\Rightarrow \textcircled{3}$ $\textcircled{6} \not\Rightarrow \textcircled{4}$ $\textcircled{4} + \textcircled{5} \Rightarrow \textcircled{6}$
 $\xrightarrow{\text{separable:}}$ $\textcircled{1} + \textcircled{2} = \textcircled{3}$ $\textcircled{4} + \textcircled{5} = \textcircled{6}$
 $\xrightarrow{\text{Galois:}}$ $\textcircled{3} \Rightarrow \textcircled{1}$ $\textcircled{3} \not\Rightarrow \textcircled{2}$ $\textcircled{1} + \textcircled{2} \not\Rightarrow \textcircled{3}$ $\textcircled{6} \not\Rightarrow \textcircled{4}$ $\textcircled{4} + \textcircled{5} \Rightarrow \textcircled{6}$
 $\xrightarrow{\text{purely inseparable}}$ $\textcircled{1} + \textcircled{2} = \textcircled{3}$ $\textcircled{4} + \textcircled{5} = \textcircled{6}$
 \uparrow only 1 root for minimal poly

[GTM 167, Thm 4.13] char $F = p$. then
 F perfect $\Leftrightarrow F^p = F$

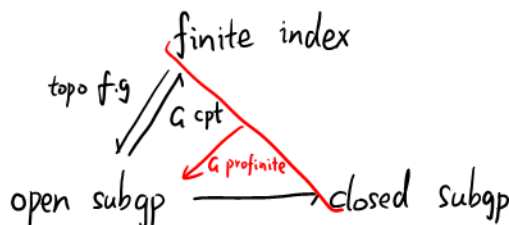


Lem. A subgroup of a profinite group is open iff it's closed and has finite index.

Ref: <https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf>

Q: Do we have any finite index gp of $\text{Gal}(\bar{K}/K)$ which is not open?

In general,



https://groupprops.subwiki.org/wiki/Closed_subgroup_of_finite_index_implies_open

In a topological group, any closed subgroup of finite index must be an open subgroup.

https://groupprops.subwiki.org/wiki/Open_subgroup_implies_closed

Any open subgroup of a topological group is closed.

<https://math.stackexchange.com/questions/4350043/open-subgroup-and-finite-index-subgroup-of-topological-group>

<https://math.stackexchange.com/questions/1092974/finite-index-subgroup-g-of-mathbbz-p-is-open>

<https://math.stackexchange.com/questions/3734250/are-normal-subgroups-of-finite-index-in-an-absolute-galois-groups-open>

Some wonderful exercises for Galois correspondence:

Let E/F be Galois field ext of deg n , $m|n$. prove: \exists subfield ext of deg m .
(Sylow thm & $Z(G) \neq \{1\}$ for a p -gp & classification of f.g. abelian gp)

Cor. For p prime, F field, one can define ${}^p\overline{F} := \bigcup_{[E:F]=p^k} E$, and

$$\overline{F} = \prod_{p \text{ prime}} {}^p\overline{F}$$

Sadly this is totally wrong. Notice that a Sylow p -subgroup may be not normal.

<https://math.stackexchange.com/questions/2125547/finite-field-extension-with-no-non-trivial-subextension>

<https://math.stackexchange.com/questions/1068327/is-bar-mathbb-q-bar-mathbb-q-cap-mathbb-r-2>

Are there any other subfield of $\overline{\mathbb{Q}}$ with finite index (except $\overline{\mathbb{Q}}$ & $\overline{\mathbb{Q}} \cap \mathbb{R}$)?

4. examples of algebraic closed field

$$\textcircled{1} \quad \overline{\mathbb{Q}} \stackrel{\pi}{\subset} \mathbb{C} \stackrel{t}{\subset} \bigcup_n \mathbb{C}((t^{\frac{1}{n}})) = \overline{\mathbb{C}((t))} \stackrel{\mathbb{C}[[t]]}{\text{Puiseux series}}$$

$$\bigcap_{n=0}^{+\infty} \mathbb{Q}_p \stackrel{\mathbb{Z}_p}{\subset} \mathbb{C}_p$$

$\mathbb{Q}_p \cdot \overline{\mathbb{Q}}$

$$\textcircled{2} \text{ char } K = p: \quad \overline{\mathbb{F}_q} = \overline{\mathbb{F}_p} \quad (\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \widehat{\mathbb{Z}})$$

Task. $\textcircled{1}$ Prove they are alg closed. $(\mathbb{C}, \bigcup_n \mathbb{C}((t^{\frac{1}{n}})), \mathbb{C}_p)$
 $\textcircled{2}$ Find an element in each "C".

$\mathbb{Q}_p \cap \overline{\mathbb{Q}}: \text{https://math.stackexchange.com/questions/1280053/explicit-description-of-bbb-q-p-cap-bar-bbb-q}$
 $\mathbb{C}_p \setminus \overline{\mathbb{Q}_p}: \text{https://math.stackexchange.com/questions/123925/is-the-algebraic-closure-of-a-p-adic-field-complete}$
 $\text{https://math.stackexchange.com/questions/2430665/algebraic-closure-of-q-p-is-composite-of-bar-mathbbq-and-mathbbq-p}$
 $\text{https://math.stackexchange.com/questions/2153580/transcendental-numbers-in-mathbbq-p}$