Algebra III

April 1, 2024

Chapter 0: Review

Definition: Category

A category $\mathcal{C}$ consists of the following data:

1. A class of objects, $\text{Obj}(\mathcal{C})$.
2. For any pair of objects $X, Y \in \text{Obj}(\mathcal{C})$, a set of morphisms $\text{Mor}_{\mathcal{C}}(X, Y)$, $\text{Hom}_{\mathcal{C}}(X, Y)$ or $\mathcal{C}(X, Y)$.
3. For any triple of objects $X, Y, Z \in \text{Obj}(\mathcal{C})$, a map

$$\begin{aligned} \text{Hom}_{\mathcal{C}}(Y, Z) \times \text{Hom}_{\mathcal{C}}(X, Y) &\to \text{Hom}_{\mathcal{C}}(Y, Z) \\ (g, f) &\mapsto g \circ f \end{aligned}$$

called compositions subject to the following axioms:

1. Associativity: $f \circ (g \circ h) = (f \circ g) \circ h$ whenever this makes sense.
2. For every object $X \in \text{Obj}(\mathcal{C})$, there exists a morphism $\text{id}_X \in \text{Hom}_{\mathcal{C}}(X, X)$ such that

$$\text{id}_X \circ f = f \quad \text{and} \quad g \circ \text{id}_X = g, \quad \forall f \in \text{Hom}_{\mathcal{C}}(W, X),\ g \in \text{Hom}_{\mathcal{C}}(X, W)$$

Example 1

Let E be a set (or a class).
Define $\mathcal{C}$ by taking $\text{Obj}(\mathcal{C}) = E$ and $\text{Hom}_{\mathcal{C}}(X, Y) = \begin{cases} \varnothing & \text{if } x \neq y \\ \{\text{id}_X\} & \text{if } x = y \end{cases}$.

Example 2

Let $\mathcal{C}$ = Set the category of all sets with set functions acting as morphisms.
Let $\mathcal{C}$ = Grp the category of all groups with group homomorphisms acting as morphisms.
Abelian Rings: Ab, Rings: Ring, Commutative Rings: CRing, Vector Spaces over F: Vect_F, Topological Spaces: Top, etc.

Example 3

Let G be a group (or more generally a monoid).
Define $\text{Obj}(\mathcal{C}) = \{*\}$, $\text{Hom}_{\mathcal{C}}(*, *) = G$ and

$$\text{Hom}_{\mathcal{C}}(*, *) \times \text{Hom}_{\mathcal{C}}(*, *) \to \text{Hom}_{\mathcal{C}}(*, *)$$

the group operator.

Example 4

Let $(E, \leq)$ be a preordered set (i.e. reflexive and transitive).
Define $\mathcal{C}$ by $\text{Obj}(\mathcal{C}) = E$,

$$\text{Hom}_{\mathcal{C}}(x, y) = \begin{cases} \varnothing & \text{if } x \not\leq y \\ \{f_{xy}\} & \text{if } x \leq y \end{cases}$$

Notation

If $f \in \text{Hom}_{\mathcal{C}}(X, Y)$ we write $X \xrightarrow{f} Y$ in $\mathcal{C}$.

Definition: Isomorphism

A morphism $f : X \to Y$ in $\mathcal{C}$ is an isomorphism if $\exists g : Y \to X$ such that $g \circ f = \text{id}_X$ and $f \circ g = \text{id}_Y$.

Definition: Endomorphism

A morphism on X with $f : X \to X$.

Definition: Automorphism

An automorphism on X is just an isomorphism $f : X \tilde{\to} X$ from X to itself.
Note that $\text{Aut}_{\mathcal{C}}(X) \subseteq \text{End}_{\mathcal{C}}(X) = \text{Hom}_{\mathcal{C}}(X, X)$.

Remark:

The collection of all endomorphisms on X form a monoid.
The collection of all automorphisms on X forms a group called the automorphism group of X.

Example 1

Let $\mathcal{C} = \text{Set}$, $X = \{1, \ldots, n\}$. Then $\text{Aut}_{\text{Set}}(\{1, \ldots, n\}) = \text{Perm}(X) = S_n$.

Example 2

Let $\mathcal{C} = \text{Vect}_F$, $X = F^n$. Then $\text{Aut}_{\text{Vect}_F}(F^n) = \text{GL}_n(F)$.

Definition: Functors

Let $\mathcal{C}$ and $\mathcal{D}$ be categories.
A functor $F : \mathcal{C} \to \mathcal{D}$ from $\mathcal{C}$ to $\mathcal{D}$ consists of the following data

1. For each object $X \in \text{Obj}(\mathcal{C})$, a chosen object $F(X) \in \text{Obj}(\mathcal{D})$.

2. For each pair of objects $X, Y \in \text{Obj}(\mathcal{C})$, a function

$$\begin{aligned} \text{Hom}_{\mathcal{C}}(X, Y) &\to \text{Hom}_{D}(F(X), F(Y)) \\ f &\mapsto F(f) \end{aligned}$$

such that

1. For any two composable morphisms $X \xrightarrow{f} Y \xrightarrow{g} Z$ in $\mathcal{C}$, we have $F(g \circ f) = F(g) \circ F(f)$.

2. For each object $X \in \mathrm{Obj}(\mathcal{C})$, $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.

Example 1

For $\mathcal{D} := \mathcal{C}$, $\mathrm{Id} : \mathcal{C} \to \mathcal{C}$, $X \mapsto X$, $f \mapsto f$.

Example 2: Forgetful Functors

$\mathcal{U} : \mathrm{Grp} \to \mathrm{Set}$ given as $(G, \cdot) \mapsto G$.
$\mathrm{Ring} \to \mathrm{Ab}$ given as $(R, +, \cdot) \mapsto (R, +)$.

Example 3: Tensors

Let R be a commutative ring, $M \in \mathrm{Mod}_R$.
Then $\otimes_R M : \mathrm{Mod}_R \to \mathrm{Mod}_R$ and $\mathrm{Hom}_R(M, -) : \mathrm{Mod}_R \to \mathrm{Mod}_R$.

Definition:

Let X be an object in a category $\mathcal{C}$ and G a group.
An action of G on X is a group homomorphism $G \to \mathrm{Aut}_{\mathcal{C}}(X)$.

Example 1

Let $\mathcal{C} = \mathrm{Set}$.
A G-set is a set $X \in \mathrm{Set}$ equipped wit a group homomorphism

$$G \to \mathrm{Perm}(X) = \mathrm{Aut}_{\mathrm{Set}}(X)$$

Exercise 1

A G-set is the same thing as a functor $G \to \mathrm{Set}$, $* \mapsto X$, $\mathrm{Hom}_{\mathcal{C}}(*, *) \to \mathrm{Hom}_{\mathrm{Set}}(X, X)$ ($G \to \mathrm{Aut}_{\mathrm{Set}}(X)$).

Definition: Adjunctions

Let $\mathcal{C}$ and $\mathcal{D}$ be categories and $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be functors.
We say that F is left adjoint to G (and that G is right adjoint to F, and that we have a pair of adjoint functors) if for each object $X \in \mathrm{Obj}(\mathcal{C})$ and $Y \in \mathrm{Obj}(\mathcal{D})$, we have a bijection

$$\mathrm{Hom}_{\mathcal{D}}(F(X), Y) \tilde{\to} \mathrm{Hom}_{\mathcal{C}}(X, G(Y))$$

which is "natural in X and Y":
For any $f : X \to X'$ in $\mathcal{C}$,

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{D}}(F(X'), Y) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(X', G(Y)) \\ \downarrow{\scriptstyle -\circ F(f)} & & \downarrow{\scriptstyle -\circ f} \\ \mathrm{Hom}_{\mathcal{D}}(F(X), Y) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \end{array}$$

and for every $g : Y \to Y'$ in $\mathcal{D}$

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{D}}(F(X), Y) & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \\ \downarrow{\scriptstyle -\circ F(f)} & & \downarrow{\scriptstyle -\circ f} \\ \mathrm{Hom}_{\mathcal{D}}(F(X), Y') & \xrightarrow{\sim} & \mathrm{Hom}_{\mathcal{C}}(X, G(Y')) \end{array}$$

We write

$$\begin{array}{c} \mathcal{C} \\ F \downarrow \uparrow G \\ \mathcal{D} \end{array}$$

Example 1

For $M \in \mathrm{Mod}_R$ we have

$$\begin{array}{c} \mathrm{Mod}_R \\ -\otimes_R M \downarrow \uparrow \mathrm{Hom}_R(M,-) \\ \mathrm{Mod}_R \end{array}$$

where

$$\mathrm{Hom}_R(M_1 \otimes M_2, N) \cong \mathrm{Hom}_R(M_1, \mathrm{Hom}_R(M, \mathrm{Hom}_R(M_2, N))$$
$$f \mapsto (x \mapsto (y \mapsto f(x \otimes y)))$$

Example 2

Let $R \xrightarrow{\phi} S$ be a ring homomorphism.
We can regard an S-module N as an R-module via

$$r \cdot x := \phi(r)x, \quad \forall r \in R, ; x \in N$$

This defines a functor $\mathrm{Mod}_S \to \mathrm{Mod}_R$ called a "restriction of scalars", which has a left adjoint called "extension of scalars."

$$\begin{array}{c} \mathrm{Mod}_R \\ S\otimes_R - \downarrow \uparrow \\ \mathrm{Mod}_R \end{array}$$

Recall

For commutative ring R, $\rightsquigarrow \mathrm{Mod}_R$.
e.g. $R = F$ a field, $\mathrm{Mod}_R \equiv \mathrm{Vect}_F$; $R = \mathbb{Z}$, $\mathrm{Mod}_R \equiv$ Ab.

Definition: R-Algebra

An R-algebra is an Abelian group $(A, +)$ that has both the structure of

1. an R-module and
2. a ring

which are compatible in that

$$r(ab) = (ra)b = a(rb), \quad \forall r \in R, \; a, b \in A$$

Example 1

The polynomial ring $R[x]$ is an R-algebra.

Example 2

The ring of $n \times n$ matrices $M_n(R)$ is an R-algebra.

Example 3

If $R \xrightarrow{\phi} S$ is a homomorphism of commutative rings, then S is an R-algebra via $r := \phi(r)a$, $\forall\, r \in R$, $a \in S$.

Example 4

$\mathbb{R} \hookrightarrow \mathbb{C}$. So $\mathbb{C}$ is an $\mathbb{R}$-algebra.
$R \hookrightarrow R[x]$.
More generally, $R[x_1, x_2, \ldots, x_n]$ is an R-algebra.

Commutative R-Algebras

An R-algebra is commutative if it is commutative as a ring.
$\mathsf{CAlg}_R \subset \mathsf{Alg}_R$.

Question: Why are polynomials important?

An algebraic perspective: they are the "free commutative algebras."

Recall

For R a commutative ring, we have the notion of a free R-module – one that admits a basis.
Categorically, we have an adjunction.

$$\begin{array}{c}\mathsf{Set}\\ f\big\downarrow\big\uparrow\mathcal{U}\\ \mathsf{Mod}_R\end{array}$$

The left adjoint of the forgetful functor sends a set I to the free R-module with basis I.

$$F(I) = R^{(I)} = \oplus_{i \in I} R$$

The adjunction says that for any set I and R-module M,

$$\begin{array}{c}\mathrm{Hom}_{\mathsf{Mod}_R}(R^{(I)}, M) \tilde{\to} \mathrm{Hom}_{\mathsf{Set}}(I, M)\\ \exists!R\text{-linear map}_{\substack{f:R^{(I)}\to M\\ e_i\mapsto x_i}} \leftarrow\!\shortmid \{x_i\}_{i\in I}\end{array}$$

Similarly, the forgetful functor $\mathcal{U} : \mathsf{CAlg}_R \to \mathsf{Set}$ has a left adjoint

$$\begin{array}{c}\mathsf{Set}\\ f\big\downarrow\big\uparrow\mathcal{U}\\ \mathsf{CAlg}_R\end{array}$$

which sends a set I to the "free commutative R-algebra on I."
Explicitly, $F(I) = R[\{x_i\}_{i\in I}]$ the polynomial algebra with an indeterminate x_i for each $i \in I$.

Example 1

$I = \{*\} \rightsquigarrow F(\{*\}) = R[x]$.
$I = \{1, \ldots, n\} \rightsquigarrow F(\{1, \ldots, n\}) = R[x_1, \ldots, x_n]$.
$I = \mathbb{N} \rightsquigarrow F(\mathbb{N}) = R[x_1, x_2, \ldots]$.

Adjunction

For any set I and commutative R-algebra $A \in \mathsf{CAlg}_R$, we have a bijection

$$\begin{aligned} \mathrm{Hom}_{\mathsf{CAlg}_R}(R[\{x_i\}_{i\in I}, A) &\cong \mathrm{Hom}_{\mathsf{Set}}(I, A) \\ \exists! R\text{-algebra homomorphism}_{\substack{R[\{x_i\}_{i\in I}] \to A \\ x_i \mapsto a_i}} &\mapsto \{a_i\}_{i\in I} \end{aligned}$$

Exmple 1

Let A be a commutative R-algebra.
For any $a \in A$, there exists a unique R-algebra homomorphism $R[x] \to A$ which sends $X \mapsto a$.
Explicitly, $f(x) \mapsto f(a)$.

Corollary

Let $R \xrightarrow{\phi} S$ be a homomorphism of commutative rings.

For any $a \in S$, there is a unique ring $R[x] \xrightarrow{\overline{\phi}} S$ such that $\overline{\phi}|_R = \phi$ and $\overline{\phi}(X) = a$.

Example 1

Let $R \subseteq S$ be a subring.

For each $a \in S$, there is a unique ring homomorphism $R[x] \xrightarrow{\phi} S$ such that $\phi|_R = \mathrm{id}$ and $\phi'(X) = a$.
We call this the "evaluation at a."

$$\begin{aligned} R[x] &\xrightarrow{\mathsf{ev}_a} S \\ f &\mapsto f(a) \end{aligned}$$

Definition: Subalgebra

Let A be a commutative R-algebra, and let $S \subset A$ be a subset.
The subalgebra of A generated by S, denoted $R[S]$, is the intersection of all subalgebras of A which contain S.
Explicitly,

$$R[S] = \{a \in A : \exists n \geq 1,\ s_1, \ldots, s_n \in S,\ f \in R[x_1, \ldots, x_n],\ a = f(s_1, \ldots, s_n)\}$$

Example 1

Let $A = R[x]$. Then $A \underset{(!)}{=} R[x]$. That is, A is generated by $\{x\}$ as an algebra.
Similarly, $R[x_1, \ldots, x_n]$ is generated as an algebra by $\{x_1, \ldots, x_n\}$.

Example 2

If $R[x]/I$ with $I \subset R[x]$ an ideal, and $x := \overline{X} \in A$, then $A = R[x]$. That is, A is generated by $x = \overline{X}$ as an algebra.
More generally, if $I \subset R[x_1, \ldots, x_n]$ an ideal, then $R[x_1, \ldots, x_n]/I$ is generated by $\{\overline{x}_1, \ldots, \overline{x}_n\}$.

Proposition

If $A \in \mathsf{CAlg}_R$ is a finitely generated, commutative R-algebra, then $A \cong R[x,\dots,x_n]/I$ for some $n \geq 1$ and ideal $I \subset R[x_1,\dots,x_n]$.

April 3, 2024

Definition: Symmetric Polynomials

Let R be a commutative ring.
A polynomial $f \in R[x_1,\dots,x_n]$ is symmetric if $f(x_{\sigma(1)},\dots,x_{\sigma(n)} = f(x_1,\dots,x_n)$ for all $\sigma \in S_n$.
In more detail: the smmetric group S_n acts on $R[x_1,\dots,x_n]$ by R-algebra homomorphism.
$\sigma \in S_n \rightsquigarrow R[x_1,\dots,x_n] \to R[x_1,\dots,x_n]$ given by $x_i \mapsto x_{\sigma(i)}$.
The canonical action of S_n on $\{1,\dots,n\}$ is

$$\begin{aligned} S_n \to \quad \mathsf{Set} \quad &\xrightarrow{F} \mathsf{CAlg}_R \\ * \mapsto \{1,\dots,n\} &\mapsto R[x_1,\dots,x_n] \end{aligned}$$

Exercise 1

The symmetric polynomials form a subalgebra of $R[x_1,\dots,x_n]$.

Example 1

Consider the polynomial

$$(*) \quad (t-x_1)(t-x_2)\cdots(t-x_n) \in R[x_1,\dots,x_n][t]$$

Write

$$t^n - s_1 t^{n-1} + s_2 t^{n-2} + \cdots + (-1)^n s_n$$

where $s_1,\dots,s_n \in R[x_1,\dots,x_n]$.

Examples

Let $n = 2$.

$$(t-x_1)(t-x_2) = t^2 - \underbrace{(x_1+x_2)}_{s_1} t + \underbrace{x_1x_2}_{s_2}$$

Let $n = 3$.

$$(t-x_1)(t-x_2)(t-x_3) = t^3 - \underbrace{(x_1+x_2+x_3)}_{s_1} t^2 + \underbrace{(x_1x_2+x_2x_3+x_1x_3)}_{s_2} t - \underbrace{x_1x_2x_3}_{s_3}$$

Exercise 2

Show that the polynomials $s_1,\dots,s_n \in R[x_1,\dots,x_n]$ are symmetric using the fact that $(*)$ is unchanged by permuting the x_is.

Definition: Elementary Symmetric Polynomials

The polynomials $s_1, \ldots, s_n \in R[x_1, \ldots, x_n]$ are the elementary symmetric polynomials in n variables.
Explicitly,

$$\begin{aligned} s_1 &= x_1 + x_2 + \ldots + x_n \\ s_2 &= \sum_{1 \le i \le j \le n} x_i x_j \\ &\vdots \\ s_k &= \sum_{1 \le i_1 \le \ldots \le i_k \le n} x_{i_1} x_{i_2} \cdots x_{i_k} \\ &\vdots \\ s_k &= x_1 x_2 \cdots x_n \end{aligned}$$

Theorem: Fundamental Theorem on Symmetric Polynomials

Every symmetric polynomial $f \in R[x_1, \ldots, x_n]$ can be expressed in a unique way as a polynomial in the elementary symmetric polynomials.
In particular, $R[s_1, \ldots, s_n] \subseteq R[x_1, \ldots, x_n]$ is the subalgebra of symmetric polynomials.

Recall: Group of Units

If R is a ring, then $U(R) = R^\times = \{a \in R : a \text{ is invertible}\}$.
This is the multiplicative group of units in R.

Exercise 3

This determines a functor Ring → Grp.

Definition: Field

A field is a nonzero commutative ring F in which every nonzero element is invertible (i.e. $F^\times = F \setminus \{0\}$).

Remarks:

A field has no nontrivial ideals.
A commutative ring R is a field if and only if (0) is a maximal ideal.
If $I \subset R$ is an ideal in a commutative ring then $R \setminus I$ is a field if and only if I is a maximal ideal.

Definition: Domain

A (integral) domain is a nonzero commutative ring R such that $\forall\, a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$.

Remarks:

A commutative ring R is a domain if and only if (0) is a prime ideal.
If $I \subset R$ is an ideal in a commutative ring, then $R \setminus I$ is a domain if and only if I is a prime ideal.

Example 1

Every field is a domain.

In fact, every subring of a field is a domain.
Conversely, domains can be characterized as the subrings of fields.

Definition: Field of Fractions

Let R be a domain.
Its field of fractions, $\mathrm{Frac}(R)$, is the set of all "formal fractions"

$$\mathrm{Frac}(R) = \left\{ \frac{a}{b} \,:\, a, b \in R,\ b \neq 0 \right\}$$

More precisely, $\mathrm{Frac}(R) = (R \times (R \setminus \{0\}))/\sim$ where

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = a_2 b_1$$

and we define $\frac{a}{b} := [(a, b)]$.
It is a field under addition and multiplication of fractions

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \quad \text{and} \quad \frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

We have an injective ring homomorphism

$$\begin{aligned} R &\hookrightarrow \mathrm{Frac}(R) \\ a &\mapsto \frac{a}{1} \end{aligned}$$

Example 1

$\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$.

Remark:

$\mathbb{Z}$ is a domain.
Its ideals are $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.
Its prime ideals are (0) and $p\mathbb{Z}$ for p prime.

Definition: Root

Let R be a commutative ring and $f \in R[x]$.
A root or zero of f is an element $r \in R$ such that $f(a) = 0$.

$$\begin{aligned} R[x] &\xrightarrow{\mathrm{ev}_a} R \\ f &\longmapsto 0 \end{aligned}$$

The kernel is $(x - a)$.
That is $f(a) = 0$ if and only if $f \in (x - a)$, if and only if $x - a | f$, if and only if $f(x) = (x - a)g(x)$ for some $g \in R[x]$.

Proposition:

Let R be a domain. Then

1. $R[x]$ is a domain.
2. $\deg(fg) = \deg(f) + \deg(g)$.
3. $R[x]^\times = R^\times$ (i.e. $f \in R[x]^\times \iff f(x) = b_0$ with $b_0 \in R^\times$).

Example 1

If $R = F$ a field, $F[x]^\times$ = the nonzero constant polynomials.

Remark:

If R a domain and $a \in R$ a root of $f \in R[x]$, then

$$f(x) = (x-a)^m g(x)$$

with $g(a) \neq 0$. The m is uniquely determined and called the multiplicity of the root.
Roots of multiplicity 1 are called simple roots.

Remark:

If R is a domain, a polynomial $f \in R[x]$ of degree d has at most d roots.
In fact, at most d roots counted with multiplicity.

Definition: Formal Derivative

The formal derivative of a polynomial

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_2 x^2 a_1 x + a_0 \in R[x]$$

is the polynomial $Df = f' \in R[x]$ defined by

$$f'(x) = d a_d x^{d-1} + \cdots + 2a_2 x + a_1$$

Remark: Properties

$$\begin{aligned} (f+g)' &= f' + g' && R[x] \to R[x] \text{ is } R\text{-linear} \\ (af)' &= af' && \text{for } a \in R \\ (fg)' &= fg' + f'g && \text{(Leibniz Formula)} \end{aligned}$$

Proposition:

$a \in R$ is a multiple root of $f \in R[x]$ if and only if $f(a) = 0$ and $f'(a) = 0$.

Proof

$f(x) = (x-a)^m g(x)$, $g(a) \neq 0$.
Therefore, by Lebniz, $f'(x) = m(x-a)^{m-1} g(x) + (x-a)^m g'(x)$.

Recall:

For a field F, the polynomial ring $F[x]$ is a PID.
$\mathbb{Z}$ is also a PID.

Proposition:

Let R be a PID.
Every nonzero prime ideal is maximal.

Proof

Let $0 \neq p$ be a nonzero prime ideal.
Suppose $p \subseteq I$. Then $p = (p)$ and $I = (a)$ for some $a \in R$ and prime element $p \in R$.
Then $(p) \subseteq (a)$ and $p = ab$ for some $b \in R$. So $p|a$ or $p|b$.
If $p|a$, then $p = I$. If, instead, $b = pc$ for some $c \in R$, then

$$p = acp \implies 1 = ac \implies a \in R^\times \implies (a) = R$$

Example 1

If $f \in F[x]$ is an irreducable polynomial then $F[x]/(f)$ is a field.
For example, $R[x]/(x^2+1)$ is a field ($\cong \mathbb{C}$).
Also, $\mathbb{F}_p = \mathbb{Z}/pz$ is a field.

Example 2

On the other hand,

$$(\mathbb{Z}/n)^\times = \{a \in \mathbb{Z}/n : \gcd(a,n) = 1\}$$
$$|(\mathbb{Z}/n)^\times| = |\{0 \leq k \leq n-1 : \gcd(k,n) = 1\}| = \phi(n)$$

Euler's Totient Function.

Remark

Later in the course, we will prove the Fundamental Theorem of Algebra which states that every nonconstant complex polynomial $f \in \mathbb{C}[x]$ has a root.
This implies that if $f \in \mathbb{C}[x]$ is a monic polynomial with complex coefficients then $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ with $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.
Write it as

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_n$$

with coefficients $a_1, \ldots, a_n \in \mathbb{C}$. Then

$$a_1 = -s_1(\alpha_1, \ldots, \alpha_n) = -(\alpha_1 + \cdots + \alpha_n)$$
$$a_k = (-1)^k s_k(\alpha_1, \ldots, \alpha_n)$$
$$a_n = (-1)^n \alpha_1 \cdots \alpha_n$$

Example 1

$$f(x) = x^2 + bx + c = (x - \alpha_1)(x - \alpha_2)$$

where $\alpha_1 = \frac{-b+\sqrt{b^2-4ac}}{2}$ and $\alpha_2 = \frac{-b-\sqrt{b^2-4ac}}{2}$.
So $\alpha_1 + \alpha_2 = -b$ and $\alpha_1\alpha_2 = c$.

Bottom Line

The coefficients of a monic polynomial are very simple expressions of the roots of the polynomial.

Motivating Question

Can we go the other around?
Can we find simple expressions of the roots of a polynomial in terms of the coefficeints.

April 8, 2024

Chapter 1: Field Theory

Definition: Field Homomorphism

If F and K are fields, a field homomorphism $F \xrightarrow{\phi} K$ is just a ring homomorphism.

Remark

The kernel of a field homomorphism $\phi : F \to K$ is an ideal of F.
Hence, it is either (0) or F. Since $\phi(1_F) = 1_K \neq 0$, $\ker(\phi) = (0)$.
Thus every field homomorphism is automatically injective and embeds F as a subfield of K.

Notation

If $F \subseteq K$ is a subfield, we say that K is an extension of F or that K/F is a field extension.

Remark

The ring of integers $\mathbb{Z}$ is the initial object in the category of rings.

That is, given any ring R, there is a unique ring homomorphism $\mathbb{Z} \to R$ given by $n \mapsto n1_R = \begin{cases} \overbrace{1_R + \cdots + 1_R}^{n} & \text{if } n \geq 0 \\ -\underbrace{(1_R + \cdots + 1_R)}_{n} & \text{if } n < 0 \end{cases}$.

The kernel of an ideal of $\mathbb{Z}$. We have three possibilities

1. $\ker = \mathbb{Z} \implies 1_R = 0$ in $R \implies R = 0$.

2. $\ker = (0) \implies \mathbb{Z} \hookrightarrow R$.

3. $\ker = n\mathbb{Z}$ for some $n \geq 2 \implies \mathbb{Z}/n\mathbb{Z} \hookrightarrow R$.

Proposition

Let F be a field and consider the unique ring homomorphism $\mathbb{Z} \xrightarrow{\phi} F$.
Then the kernel of ϕ is either (0) or $p\mathbb{Z}$ for some prime number p.

Proof

Note that $\mathbb{Z}/n\mathbb{Z} \hookrightarrow F$, but all subrings of fields are domains and $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

Corollary

Let F be a field. It contains precisely one of the following as a subfield

1. $\mathbb{Q}$ or

2. $\mathbb{F}_p$ for p prime.

Proof

The proposition implies either $\mathbb{Z} \hookrightarrow F$ or $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$ for p prime.
If $\mathbb{Z} \hookrightarrow F$ then this extends to an embedding $\mathbb{Q} \hookrightarrow F$ by the universal property of the field of fractions.
On the other hand, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ by definition.
Claim: we can't have more than one such field as a subfield of F.
Observe that if F has a subfield isomorphic to $\mathbb{F}_p$, then $p \cdot 1 = 0$ in F.
On the other hand, if $\mathbb{Q} \subseteq F$ then $p \cdot 1 \neq 0$ for all p.
Finally, if $p \neq q$ primes and $\mathbb{F}_p \subseteq F$ and $\mathbb{F}_q \subseteq F$, then $p \cdot 1 = 0$ and $q \cdot 1 = 0$ in F.
By Bezout's, this means that $a, b \in \mathbb{Z} : ap + bq = 1$. So

$$1 = 1 \cdot 1 = (ap + bq) \cdot 1 = (ap)1 + (bq)1 = a(p \cdot 1) + b(q \cdot 1) = 0 + 0 = 0$$

which cannot be true.

Definition: Field Characteristic

We define the characteristic of a field F by $\operatorname{char}(F) = \begin{cases} 0 & \text{if } \mathbb{Q} \subseteq F \\ p & \text{if } \mathbb{F}_p \subseteq F \end{cases}$.

Remark

Note that the kernel of $\mathbb{Z} \to F$ is $\operatorname{char}(F)\mathbb{Z} \subseteq \mathbb{Z}$.
The characteristic of F is the smallest positive integer n such that $n \cdot 1 = 0$ in F or 0 if $n \cdot 1 \neq 0$ in F for all $n \geq 1$.

Remark

If K/F is a field extension, then K and F have the same characteristic.
$n \cdot 1 = 0$ in F if and only if $n \cdot 1 = 0$ in K. Observe that the composition $\mathbb{Z} \to F \hookrightarrow K$ requires matching kernels.

Aside

In math, one sometimes passes between characteristic zero and characteristic p through the integers.

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Q} \\ \downarrow & & \\ \mathbb{F}_p & & \end{array}$$

Examples

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ have characteristic 0.
$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ has characteristic p.
$\mathbb{C}(t) :=$ Frac$(\mathbb{C}[t])$.
$\mathbb{F}_p(t) :=$ Frac$(\mathbb{F}_p[t])$ is an infinite field of characteristic p.

Remark

If R is a domain, then $R[t]$ is a domain and

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

the field of rational functions.
More generally, $R[t_1, \ldots, t_n]$ is a domain and

$$R(t_1, \ldots, t_n) := \text{Frac}(R[t_1, \ldots, t_n])$$

is the field of rational functions in n variables.

Definition: Degree of a Field Extension

Let K/F be a field extension.
We can regard K as a vector space over F (restriction of scalars $F \hookrightarrow K$).
The degree of the field extension K/F is $\dim$ of the F-vector space K.

Notation

$[K : F] := \dim_F(K)$.

Example

$\mathbb{C}/\mathbb{R}$ is a degree 2 extension. An $\mathbb{R}$-basis for $\mathbb{C}$ is $\{1, i\}$.

Remark

K/F has degree 1 if and only if $K = F$.

Terminology

A degree 2 extension K/F is a quadratic extension.
A degree 3 extension K/F is a cubic extension.
Etc.

Definition: Finite Extension

A field extension K/F is said to be a finite extension if $[K:F]$ is finite.

Example

$F(t)/F$, noting $F \subseteq F[t] \subseteq F(t)$, is an infinite etension. Write $[F(t):F] = \infty$.

Proposition

Let $L/K/F$ be field extensions.
Then $[L:F] = [L:K][K:F]$.

Proof (Sketch)

Idea: if $\{a_i\}_{i\in I}$ is a basis for L/K and $\{b_j\}_{j\in J}$ ia s a basis for K/F, then $\{a_i b_j\}_{(i,j)\in I\times J}$ is a basis for L over F.
Note that $|I \times J| = |I||J|$.

Definition: Algebraic and Transcendental Elements

Let K/F be a field extension.
An element $a \in K$ is said to be algebraic over F if it is a root of a nonzero polynomial with coefficients in F.
Otherwise, we say that a is transcendental over F.

Example

Consider $\mathbb{C}/\mathbb{Q}$.
$\sqrt{2} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since $t^2 - 2 \in \mathbb{Q}[t]$.
$i \in C$ is algebraic over $\mathbb{Q}$ since $t^2 + 1 \in \mathbb{Q}[t]$.
$\omega_n = e^{2\pi i/n} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ since $t^n - 1 \in \mathbb{Q}[t]$.

Remark

Whether or not an element is algebraic or transcendental depends a lot on the ground field F.
e.g. every element $a \in K$ is algebraic over K, since it is a root of $t - a \in K[t]$.

Remark

Often the terms “algebraic number” and “transcendental number” mean a complex number which is algebraic or transcendental over $\mathbb{Q}$.

Theorem: (Hermite 1873)

e is a transcendental number.

Theorem: (Lindemann 1882)

π is a transcendental number.

Exercise (Cantor)

There are only countably many algebraic numbers.

Remark

Whether $a \in K$ is algebraic or transcendental over F is described by the evaluation homomorphism

$$\begin{aligned} F[t] &\xrightarrow{\text{ev}_a} K \\ f &\longmapsto f(a) \end{aligned}$$

That is, a is transcendental if and only if $\ker(\text{ev}_a) = (0)$.
Then a is algebraic if and only if $\ker(\text{ev}_a) \neq (0)$.
$F[t]$ is PID, so if $a \in K$ is algebraic over F then $\ker(\text{ev}_a)$ is a nonzero principal ideal of $F[t]$.
A generator of this principal ideal is only determined up to association (that is up to multiplication by a nonzero constant polynomial).
We can pin it down by requiring the generator to be monic.

Definition: Minimal Polynomial

The unique monic polynomial f of lowest degree with coefficients in F such that $f(a) = 0$ is called the minimal polynomial of a over F.

Notation

$m_a(t) \in F[t]$.

Remark

It generates $\ker(\text{ev}_a)$. For any $f \in F[t]$, $f(a) = 0$ if and only if $m_a | f$.

Note

$F[t]/(m_a(t))$ is isomorphic to a subring of K.
So $F[t]/(m_a(t))$ is a domain and $m_a \in F[t]$ is an irreducible polynomial.

Exercise

The minimal polynomial of $a \in K$ over F is the unique, monic, irreducible polynomial $f \in F[t]$ such that $f(a) = 0$.

Example

Take $\sqrt{2} \in \mathbb{C}$, the root of $t^2 - 2 \in \mathbb{Q}[t]$. This is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ since it is irreducible.
$i \in \mathbb{C}$ is a root of $t^2 + 1 \in \mathbb{Q}[t]$ which is also irreducible and hence the minimal polynomial of i over $\mathbb{Q}$.
$a = \frac{1+i}{2} \in \mathbb{C}$ ($\sqrt{i}$) is a root of $t^4 + 1 \in \mathbb{Q}[t]$, irreducible and therefore minimal of a over $\mathbb{Q}$.
Consider $F = \mathbb{Q}[i] = \{\alpha + i\beta : \alpha, \beta \in \mathbb{Q}\}$. Observe that $t^4 + 1 = (t^2 - i)(t^2 + i) \in F[t]$. We can show that the minimal polynomial of a over F is $t^2 - i$.

Definition: Generated Subring

Let K/F be a field extension and let $S \subseteq K$ be a subset.
The subring generated by S over F is defined to be $F[S]$:= the intersection of all subrings of K which contain F and S.
That is, the F-subalgebra generated by S.

Exercise

$F[S] = \{a \in K : a = f(s_1, \ldots, s_n)$ for some $n \geq 0$, $f \in F[x_1, \ldots, x_n]$, $s_1, \ldots, s_n \in S\}$.

Notation

$S = \{a\} \rightsquigarrow F[a]$.
$S = \{a_1, \ldots, a_n\} \rightsquigarrow F[a_1, \ldots, a_n]$.
Note that $F[a] = \text{im}(F[t] \xrightarrow{\text{ev}_a} K)$ and $F[a_1, \ldots, a_n] = \text{im}(F[t_1, \ldots, t_n] \xrightarrow{\text{ev}_a} K)$.

Definition: Generated Subfield

Let K/F be a field extension and let $S \subseteq K$ be a subset.
Then the subfield generated by S over F is defined to be $F(S) :=$ the intersection of all subfields of K which contain F and S.
Observe that $F[S] \subset F(S)$.

Exercise

$F(S) = \left\{ a \in K \,:\, a = \frac{\alpha}{\beta} \text{ for } \alpha, \beta \in F[S] \right\} = \text{Frac}(F[S])$.

Notation

$S = \{a\} \rightsquigarrow F(a)$.
$S = \{a_1, \ldots, a_n\} \rightsquigarrow F(a_1, \ldots, a_n)$.

Definition: Finitely Generated Field Extension

A field extension K/F is finitely generated if $K = F(S)$ for some $S \subset K$ finite.
That is, finitely generated as a field over F not as an algebra over F or a vector space over F.

Example

$F(t)/F$ is a finitely generated field extension but is not finitely generated as an F-algebra (exercise) nor as an F-vector space.

Example

In $F(t)/F$, the indeterminant $t \in F(t)$ is transcendental over f.
The evaluation homomorphism $F[t] \hookrightarrow F(t)$.

April 10, 2024

Last time: K/F, $S \subset K$, $F[S] \subset F(S)$.
Example: $S, T \subset K \rightsquigarrow F(S)(T) = F(S \cup T)$.
$F(a_1, \ldots, a_n) = F(a_1, \ldots, a_{n-1})(a_n)$.

Remark

Let K/F be a field extension.
If $a \in K$ is transcendental over F, then

$$F[t] \xrightarrow[\sim]{\text{ev}_a} F[a]$$

is an isomorphism. Hence,

$$F(a) \simeq \mathrm{Frac}(F[t]) = F(t)$$

the field of rational functions.
Thus, the field extensions $F(a)$ for $a \in K$ transcendental over F are all isomorphic.

Example

$\mathbb{Q}(\pi) \simeq \mathbb{Q}(e)$ are isomorphic fields.

Bottom Line

Transcendental elements behave like indeterminates t.
The prototypical example is $F(t)/F$.

Proposition

Let K/F be a field extension.
If $a \in K$ is algebraic over F, then $F[a] \simeq F[t]/(m_a(t))$ where $m_a(t) \in F[t]$ is the minimal polynomial of a over F.
Moreover, $F[a]$ is a field. Hence $F[a] = F(a)$.
Also, $[F(a) : F] = \deg(m_a(t))$.
An explicit F-basis of $F(a)$ is $\{1, a, a^2, \ldots, a^{d-1}\}$ where $d := \deg(m_a(t))$.

Proof

$$\begin{array}{ccc} F[t] & \xrightarrow{\mathrm{ev}_a} & K \\ \downarrow & & \uparrow \\ F[t]/m_a(t) & \xrightarrow{\sim} & F[a] \end{array}$$

Now $m_a(t)$ is irreducible, so $(m_a(t))$ is a nonzero prime ideal.
$F[t]$ is PID, therefore every nonzero prime ideal is maximal.
Hence $F[t]/(m_a(t))$ is a field.
Also, $\dim_F(F[t]/(f(t))) = \deg(f)$.
A basis $\{\overline{1}, \overline{t}, \overline{t^2}, \ldots, \overline{t^{d-1}}\}$.
Suppose $a_0 T + a_1 \overline{t} + \cdots + a_{d-1}\overline{t^{d-1}} = 0 = a_0 + a_1 + \cdots + a_{d-1}t^{d-1}$.
That is, $g(t) = a_0 + a_1 t + \cdots + a_{d-1}t^{d-1} \in (f(t))$.
So f divides g but $\deg(f) = d > d-1$. Then $g = 0$ in the new polynomial.
That is $a_0 = a_1 = \cdots = a_{d-1} = 0$.
What is the span? $g(t) = b_0 + b_1 + \cdots b_n t^n = b_0 + b_1 t + \cdots + b_{d-1}t^{d-1} + t^d(\cdots)$.
In $F[t]/(f(t))$, $f(t) = 0$, $f(t) = t^d = a_{d-1} + \cdots + a_0$, $t^d = (a_{d-1}t^{d-1} + \cdots + a_0)$ where $g(t)$ is some polynomial of degree less than d.
Finally, note that $F[t]/(m_a(t)) \xrightarrow{\sim} F[a]$ is given by $\overline{f(t)} \mapsto f(a)$.
Then $\overline{1} \mapsto 1$, $\overline{t} \mapsto a, \ldots, \overline{t^{d-1}} \mapsto a^{d-1}$.

Remark

This proposition explains the choice of the term "degree" for $[K : F]$. If $K = F(a)$ is generated by a single, algebraic element $a \in K$, then the $[F(a) : F]$ is the degree of the minimal polynomial of a over F.

Example 1

$\mathbb{Q}(i) = \mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ (since the minimal polynomial $t^2 + 1$ of i over $\mathbb{Q}$ has degree 2).
$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Example 2

$\xi_p := e^{2\pi i/p} \in \mathbb{C}$ for a prime p is a root of unity for

$$x^p - 1 = (x-1)\overbrace{(x^{p-1} + x^{p-2} + \cdots + x + 1)}^{\Phi_p(x)}$$

Since $\xi_p \neq 1$, ξ_p is a root of $\Phi_p(x)$.
Eisenstein's Criterion applied to $\Phi_p(x+1)$ that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$.
Hence $\Phi_p(x)$ is the minimal polynomial of ξ_p over $\mathbb{Q}$.
Thus, $\mathbb{Q}(\xi_p) = \mathbb{Q}[\xi_p] = \{a_0 + a_1\xi_p + a_2\xi_p^2 \cdots + a_{p-2}\xi_p^{p-2} : a_i \in \mathbb{Q}\}$.

Example

Let $p = 3$. $\mathbb{Q}(\xi_3) = \{a_0 + a_1\xi_3 : a_0, a_1 \in \mathbb{Q}\}$.
So $\mathbb{Q}(\xi_3) = \mathbb{Q}(\sqrt{3}i) = \mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} : a, b \in \mathbb{Q}\}$.

Example 3

$\mathbb{R}(i) = \mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}$.
$\mathbb{R}[i] \simeq \mathbb{R}[t]/(t^2 + 1)$.

To Study:

Eisenstein's Criterion
Gauss' Lemma

Remark

Given a field extension K/F, an element $a \in K$ is algebraic over F if and only if $[F(a) : F] < \infty$.
The above proposition gives the $\Longrightarrow$ direction.
On the other hand, if a is transcendental then $F(a) \simeq F(t)$ and $[F(t) : F] = \infty$.

Proposition

Let K/F be a finite extension of degree n.
Every element of K is algebraic over F and has degree dividing n.

Proof

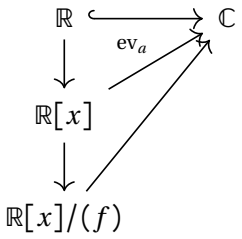
$$[K : F] = [K : F(a)][F(a) : F]$$

Corollary

Every irreducible polynomial $f \in \mathbb{R}[x]$ has degree 1 or 2.

Proof

(Assuming the FTA)
Let $f \in \mathbb{R}[x]$ be irreducible. Then $K : \mathbb{R}[x]/(f)$ is a field.
By the Fundamental Theorem of Algebra, f has a root $a \in \mathbb{C}$.



So $\mathbb{R} \hookrightarrow \mathbb{R}[x]/(f) \hookrightarrow \mathbb{C}$, and

$$2 = [\mathbb{C} : \mathbb{R}] = [\mathbb{C} : \mathbb{R}[x]/(f)][\mathbb{R}[x]/(f) : \mathbb{R}]$$

Therefore $[R[x]/(f) : \mathbb{R}] = \deg(f)$ is either 1 or 2.

Definition: Algebraic Extension

A field extension K/F is said to be an algebraic extension if every element of K is algebraic over F.

Example

We showed above that every finite extension is an algebraic extension.

Theorem:

Let $L/K/F$ be field extensions.
Then L/F is algebraic if and only if L/K is algebraic and K/F is algebraic.

Proof

($\Longrightarrow$) trivial.
($\Longrightarrow$) Let $a \in L$. Then $f(a) = 0$ for some nonzero polynomial $f(t) \in K[t]$. Write

$$f(t) = b_0 + b_1 t + \cdots + b_d t^d$$

with $b_0, \ldots, b_d \in K$.
Each of these b_i is algebraic over F. Hence $E := F(b_0, b_1, \ldots, b_d)$ is a finite extension of F.

$$F(b_0, \ldots, b_d)/F(b_0, \ldots, b_{d-1})/\ldots/F(b_0)/F$$

Note that $f(t) \in E[t]$ and $f(a) = 0$, so $a \in L$ is algebraic over E.
Observe

$$[E(a) : F] = \underbrace{[E(a) : E]}_{\text{finite}}\underbrace{[E : F]}_{\text{finite}}$$

so $E(a)/F$ is finite, hence an algebraic extension.
Therefore $a \in L$ is algebraic over F.

Corollary

Let K/F be a field extension.
The elements of K which are algebraic over F form a subfield of K.

Proof

Let $a, b \in K$ be algebraic over F.
Then $F(a,b)/F$ factors as $F(a,b)/F(a)/F$.
So $F(a,b)/F$ is a finite, hence algebraic, extension.
Therefore $a+b$, $a-b$, ab, a^{-1} (for $a \neq 0$) are algebraic over F.

Example

Apply to $\mathbb{C}/\mathbb{Q}$ to see that the collection of all algebraic numbers forms a subfield of $\mathbb{C}$.
$\overline{\mathbb{Q}}$ is defined as the field of algebraic numbers.
Recall: Theorem (Cantor), $\overline{\mathbb{Q}}$ is countable.
Exercise: $\overline{\mathbb{Q}}/Q$ is an infinite extension.

Adjoining Elements

Let F be a field and $f(x) \in F[x]$ be irreducible.
Then $K := F[x]/(f)$ is a field extension of degree $\deg(f)$.
Note: $K = F(a)$ when $a := \overline{x}$.
Note also that a is a root of $f(x)$.

$$f(a) = f(\overline{x}) = \overline{f(x)} = 0$$

in K.

Example 1

We could define $\mathbb{C} := \mathbb{R}[x]/(x^2+1)$ and define $i := \overline{x}$.

Example 2

Let F be a field.
Suppose $a \in F$ which does not have a square root in F (i.e. $\nexists\, \delta \in F$ such that $\delta^2 = a$).
Then $x^2 - a \in F[x]$ is irreducible.
Then $K := F[x]/(x^2-a)$ is a degree 2 extension.
Setting $\delta := \overline{x} \in K$, $K = F(\delta)$ and $\delta^2 = a \in F$.
In fact, every quadratic extension arises in this way – adjoining a square root.

Example 3

Let F be a field of characteristic $\neq 2$.
Let K/F be a quadratic extension (i.e. $[K:F] = 2$).
Let $\delta \in K$ be an element such that $\delta \notin F$, then $K = F(\delta)$ $(K/F(\delta)/F)$.
So the minimal polynomial of δ over F is a quadratic polynomial.

$$m_\delta(t) = t^2 + bt + c \in F[t]$$

Consider $\Delta := b^2 - 4c \in F$.

Claim: Δ does not have a square root in F. Otherwise

$$m_\delta(t) = \left(t - \frac{-b+\sqrt{\Delta}}{2}\right)\left(t - \frac{-b-\sqrt{\Delta}}{2}\right)$$

would not be irreducible.
Note: $2\delta + b = \pm\sqrt{\Delta}$. So

$$K = F(\delta) = F(2\delta + b) = F(\sqrt{\Delta})$$

April 15, 2024

Remarks on Ruler and Compass Construction

Game

Start with some "known" points in the plane and then we construct new points using a ruler and compass.
The ruler you may draw lines between two known points.
With the compass you may draw a circle with known center and known radius (distance between two known points).

Example Problems

Squaring the circle: given a circle, construct, using ruler and compass, a square with the same area.
Trisecting a given angle.
Can you construct a regular n-gon using ruler and compass?
Doubling the cube: given a cube, construct a cube with double the volume.

Remark

Starting with two given points, call one zero and the other one. Then we can construct a coordinate system system which identfies the plane with $\mathbb{R}^2 = \mathbb{C}$.
One can readily check that the constructible points (the points which are constructible starting from zero and one) form a subfield of $\mathbb{C}$.
One can readily check that every point whose coordinates are rational is constructible.
This transforms the geometric problems into problems of field theory.
That is, the field of constructible numbers is some field extension of $\mathbb{Q}(i)$.

Key Point

Let K be a subfield of $\mathbb{C}$ which contains i and is closed under complex conjugation.
e.g. $K = \mathbb{Q}(i)$. Then $z = x + iy \in K$ if and only if $x, y \in K$.
Consider the intersection of two lines. Then the point of intersection is in K.
The coordinates of the points of intersection are rational expressions of the coordinates of the points which determine the lines.
Consider instead the intersection of a circle $(x-a)^2 + (y-b)^2 = r^2$ and a line $px + qy = h$ $(p \neq 0)$.
Then $x = \frac{h-qy}{p}$ and

$$\left(\frac{h-qy}{p} - a\right)^2 + (y-b)^2 = r^2$$

is a quadratic equation in y. So y may be expressed as a rational expression, including square roots, of the coordinates of the points which determine the line and the circle.

Therefore, the point of intersection is contained in a quadratic extension of K.
Finally, the intersection of two circles is the same as the intersection of line and circle.

Theorem:

A point $z \in \mathbb{C}$ is constructible if and only if there exists a tower of field extension $\mathbb{Q} = F_0 \subseteq \cdots \subseteq F_m$ such that $z \in F_m$ and each F_i/F_{i-1} is a quadratic extension.
That is, $F_i = F_{i-1}(u_i)$ where $u_i^2 \in F_{i-1}$.

Corollary

If $z \in \mathbb{C}$ is constructible, then z is algebraic and $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of 2.

Proof

$$[F_m : \mathbb{Q}(z)][\mathbb{Q}(z) : \mathbb{Q}] = [F_m : F_0] = 2^m$$

Corollary

It is impossible to square the circle.

Proof

A square of side length $\sqrt{\pi}$, $\sqrt{\pi}$ and π would be constructible. But Lindemann demonstrated that π is transcendental.

Remark

Note that some angles can be trisected (e.g. $\pi/2$).

Corollary

Not every angle may be trisected.
In particular, $2\pi/3$ cannot be trisected.

Proof

If we could trisect $2\pi/3$, then we could construct $e^{2\pi i/9}$.
Let $\xi = e^{2\pi i/9}$. If ξ were constructible, then $\alpha := \xi + \xi^{-1}$ would be constructible.
Observe that $\xi^3 = e^{2\pi i/3}$. Then $(\xi^3)^2 + \xi^3 = -1$.
Given that

$$\alpha^3 = (\xi + \xi^{-1})^3 = \xi^3 + 3\xi + 3\xi^{-1} + \overbrace{\xi^{-3}}^{\xi^6} = 3(\xi + \xi^{-1}) - 1 = 3\alpha - 1$$

we have that $\alpha^3 - 3\alpha + 1 = 0$. That is, α is a root of $x^3 - 3x + 1$ which is irreducible (check directly that it is irreducible over $\mathbb{Z}$ and then Gauss implies it is irreducible over $\mathbb{Q}$).
Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and we are done.

Proposition

We can construct a regular n-gon using ruler and compass if and only if $e^{2\pi i/n}$ is constructible.

Corollary

We cannot construct a regular 9-gon using ruler and compass.

Definition: Algebraic Independence

Let K/F be a field extension.
A collection of distinct elements $a_1,\dots,a_n \in K$ are said to be algebraically independent over F if $\forall f \in F[x_1,\dots,x_n]$, $f(a_1,\dots,a_n) = 0$ implies $f = 0$.
A subset $S \subseteq K$ is said to be algebraically independent over F if every finite subset of S is algebraically independent over F.

Definition: Purely Transcendental Extension

K/F is a purely transcendental extension if $K = F(S)$ for some algebraically independent $S \subseteq K$.

Example

$F(t_1,\dots,t_n)/F$ is a purely transcendental extension.

Exercise

K/F is purely transcendental if and only if $K \cong F(\{t_i\}_{i\in S}) = \mathrm{Frac}(F[\{t_i\}_{i\in S}])$.

Definition: Transcendence Basis

Let K/F be a field extension.
A transcendence basis for K/F an algebraically independent subset $S \subseteq K$ such that $K/F(s)$ is an algebraic extension.

Theorem:

Let K/F be a field extension and $S \subseteq K$. The following are equivalent

1. S is a transcendence basis for K/F.
2. S is maximal among all algebraically independent subsets of K/F.
3. S is minimal among all subsets of K such that $K/F(S)$ is algebraic.

Lemma:

A subset $S \subseteq K$ is algebraically independent over F if and only if every element $u \in S$ is transcendental over $F(S \setminus \{u\})$.

Exercise

Using this lemma, prove the previous theorem.

Theorem:

Let K/F be a field extension.

1. Any algebraically independent subset $S \subseteq K$ is contained in the transcendence basis.

2. Any subset $S \subseteq K$ such that $K/F(S)$ is algebraic contains a transcendence basis.

In particular, a transcendence basis exists.

Remark

Every field extension is an algebraic extension of a purely transcendental extension.

Corollary / Exercise

Every finitely generated field extension K/F is an algebraic extension of $F(t_1, \ldots, f_n)$ for some n.

Theorem:

Any two transcendence bases of K/F have the same cardinality.

Definition: Transcendence Degree

Let K/F be a field extension.
The cardinaity of a transcendence basis is called the transcendence degree of K/F.

$$\text{trdeg}_F(K) \quad \text{or} \quad \text{trdeg}(K/F)$$

Examples

$\text{trdeg}_F(F(t_1, \ldots, t_n)) = n$.
$\text{trdeg}_F(K) = 0$ if and only if K/F is algebraic.

Exercise

Given $L/K/F$, $\text{trdeg}(L/F) = \text{trdeg}(L/K) + \text{trdeg}(K/F)$.

Example

Let X be a compact Riemann surface.
Then we have a field $M(x)$ of meromorphic functions, $M(x)/\mathbb{C}$.
e.g. $X = \mathbb{P}^1_{\mathbb{C}} = S^2$. Then, since every meromorphic function is rational, $M(x) \cong \mathbb{C}(t)$.
In general, $\text{trdeg}_{\mathbb{C}}(M(x)) = 1$.
For every finite extension, $K/\mathbb{C}(t)$, there exists a compact Riemann surface X such that $M(x) = K$.
There is an equivalence of categories between the compact Riemann surfaces with nonconstant holomorphic maps and the opposite category of finite extensions of $\mathbb{C}(t)$.

April 17, 2023

Definition: Splitting Field

Given a polynomial, $f \in F[t]$ we want to construct a field extension K/F in which f splits into linear factors:

$$f(t) = c(t - a_1)(t - a_2)\cdots(t - a_n)$$

where $c \in F$, $a_1, \ldots, a_n \in K$.
A splitting field for $f \in F[t]$ is a field extension K/F such that f splits completely into linear factors as above over K and K is generated by the roots of f in K such that $K = F(a_1, \ldots, a_n)$.

Theorem:

Every polynomial $f \in F[t]$ admits a splitting field.

Proof

Key: if $f \in F[t]$ is irreducible, then $F[t]/(f(t))$ is a field which is an extension of F

$$F \hookrightarrow F[t] \to F[t]/(f(t))$$

and $f(t)$ has a root in it, namely $\overline{t} \in F[t]/(f(t))$ ($f(\overline{t}) = \overline{f(t)} = 0$).
For a general polynomial $f(t) \in F[t]$,

$$f = cf_1 f_2 \cdots f_m$$

with $c \in F$, f_i irreducible ($F[x]$ a UFD).
Take $K_1 := F[t]/(f_1)$. Over K_1, one of the irreducible factors (namely f_1) gets a root.
Then consider the factorization of f into irreducibles over K_1 and continue. Then

$$F = K_0 \hookrightarrow K_1 \hookrightarrow K_2 \hookrightarrow \cdots$$

By injection on the sum of the degrees of the nonlinear irreducible factors, this implies that we eventually obtain a field K_N in which f splits completely.

Remark

Note that if $K = F(a_1, \ldots, a_n)$ is a splitting field of f where $a_1, \ldots, a_n$ are the roots of f in K, then K is a finite, hence algebraic, extension of F.

Remark

Be careful. Even if $f \in F[t]$ is irreducible, it is not enough in general just to go to $K := F[t]/(f(t))$ in order to obtain a complete splitting.

Example

Let $F = \mathbb{Q}$, $f(X) = X^4 - 2 \in \mathbb{Q}[X]$.
This is irreducible by Eisenstein.
Take $K := \mathbb{Q}[X]/(X^4 - 2)$. Then $x := \overline{X}$ is a root of the polynomial.
In K, we have that $x^4 = 2$; in $K[X]$, $X^4 - 2 = x^4 - x^4 = (X^2 - x^2)(X^2 + x^2) = (X - x)(X + x)(X^2 + x^2)$.
The last polynomial, $X^2 + x^2$ is irreducible in $K[X]$.
We still need to do one more quadratic extension (adjoining $i = \sqrt{-1}$) for $X^2 + x^2$ to split as $(X - ix)(X + ix)$.
A splitting field of $X^4 - 2$ over $\mathbb{Q}$ is a degree 8 extension $\mathbb{Q}(\sqrt[4]{2}, i)$.

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}, i) \\ \Big| 2 \\ \mathbb{Q}(\sqrt[4]{2}) \\ \Big| 4 \\ \mathbb{Q} \end{array}$$

Corollary

Let $f_1, f_2, \ldots, f_s \in F[t]$ be a finite collection of polynomials.
Then there exists a field extension K/F in which each polynomial $f_1, \ldots, f_s$ splits completely.

Proof

Apply the theorem to $f := f_1 f_2 \cdots f_s$.

Definition: Algebraically Closed Field

A field F is algebraically closed if it admits no non-trivial algebraic extension.
That is, K/F algebraic $\implies K = F$.

Proposition:

A field F is algebraically closed if and only if every polynomial in $F[t]$ splits completely into linear factors.

Proof

($\implies$) Let $f \in F[t]$.
By the theorem above, there exists a splitting field K of f. So K/F is algebraic, and therefore $K = F$.
So f splits completely over F.
($\impliedby$) Suppose K/F is algebraic.
Let $a \in K$. The minimal polynomial of a over F is irreducible, hence linear. Therefore $a \in F$.
So $K = F$.

Remark / Exercise

Every polynomial in $F[t]$ splits completely if and only if every non-constant polynomial in $F[t]$ has a root in F.

Theorem:

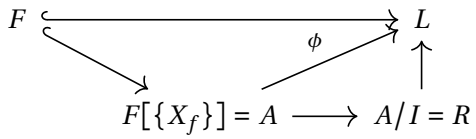
Let F be a field.
There exists a field extension E/F with E algebraically closed.

Aside: Zorn's Lemma

Take $S := \{\text{proper ideals } I \underset{\neq}{\subset} R\}$ ordered by inclusion, $S \neq \varnothing$ since $R \neq \varnothing$.
If $\{I_i\}$ a chain, then $\bigcup I_i$ is an ideal.
Further, it is a proper ideal since $1 \in \bigcup I_i \implies 1 \in I_i \implies I_i = R$ a contraduction.
Zorn's lemma implies that S contains a maximal ideal.

Proof

Zorn's lemma implies that every non-zero commutative ring has a maximal ideal.
Therefore, every non-zero commutative ring admits a ring homomorphism $R \to K$ to a field.
Let $A := F[X_f]_{f \in F[X] \setminus F}$, the (huge) polynomial algebra in infinitely many indeterminates, one for each non-constant polynomial $f \in F[t] \setminus F$.
Consider the ideal $I := (f(X_f))_{f \in F[x] \setminus F} \subseteq A$.
Here $f(X_f)$ is the single-variable polynomial f in the variable X_f.
Key: $I \neq A$. Let $Q = \sum_{i=1}^{n} Q_i f_i(X_{f_i}) \in I$, for some $Q_i \in A$ and $f_i \in F[t] \setminus F$.
There exists a field K/F in which $f_1, \ldots, f_n$ split completely.
In particular, $\exists \alpha_1, \ldots, \alpha_n \in K$ such that $f_i(\alpha_i) = 0$, $\forall\, i = 1, \ldots, n$.
Evaluate $Q(X_{f_1}, \ldots, X_{f_n}, X_{q_1}, \ldots, X_{q_k})$ by setting $X_{f_i} \mapsto \alpha_i$ and $X_{q_j} \mapsto 0$ (for example).
Then $Q \mapsto 0$. Therefore, $Q \neq 1$ because $1 \mapsto 1$ in K.
So $1 \notin I$ (i.e. $I \neq A$), hence $R := A/I$ is a non-zero ring and there exists a ring homomorphism $R \to L$ for some field L.
This field L is an extension of F.



Let $f \in F[t] \setminus F$.
Consider $\alpha_f := \phi(X_f) \in L$.
Well

$$f(\alpha_f) = f(\phi(X_f)) = \phi(\underbrace{f(X_f)}_{\in I}) = 0$$

That is, every non-constant polynomial in $F[t]$ has a root in L.
Repeat this process inductively,

$$F = L_0 \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_n \hookrightarrow \cdots$$

with the property that every non-constant polynomial with coefficients in L_n has a root in L_{n+1}.
Take $L := \operatorname{colim}_{n \to \infty} L_n = \bigcup_{n \geq 1} L_n$. This L is algebraically closed.

$$L[T] = \bigcup_{n \geq 1} L_n[T]$$

Every non-constant polynomial over L is realized over L_n, hence has a root in L_{n+1} and therefore has a root in L.

Definition: Algebraic Closure

Let F be a field.
An algebraic closure of F is an algebraic extension E/F with E algebraically closed.

Corollary

Every field ad mits an algebraic closure.

Proof

By the theorem, $F \hookrightarrow L$ with L algebraically closed.
Consider $E := \{a \in L : a \text{ is algebraic over } F\}$. We previously proved that E is a subfield of L.
By construction, E/F is algebraic.
We claim E is algebraically closed.
Let $f \in E[t]$ be a polynomial. Well

$$f(t) = c(t-\alpha_1)\cdots(t-\alpha_n)$$

in $L[t]$ with $c \in E$ and $\alpha_1, \ldots, \alpha_n \in L$.
Each α_i is algebraic over E (since $f(\alpha_i) = 0$).
So $E(\alpha_i)/E$ is algebraic and E/F is an algebraic extension.
Therefore $E(\alpha_i)/F$ is algebraic. Therefore α_i is algebraic over F so $\alpha_i \in F$.
So f splits on E.

Example

The Fundemental Theorem of Algebra asserts that $\mathbb{C}$ is algebraically closed.

Example

$\overline{\mathbb{Q}} = \{z \in \mathbb{C} : z \text{ is algebraic over } \mathbb{Q}\}$ is an algebraic closure of $\mathbb{Q}$.

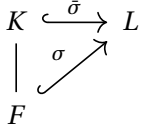
Example

$\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

April 22, 2024

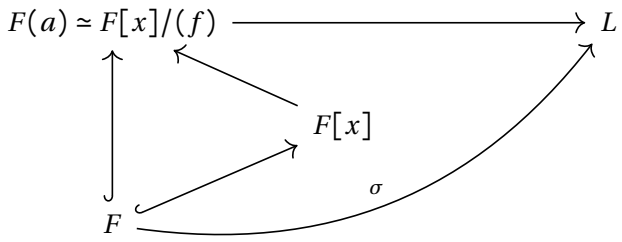
Proposition

Let K/F be an aglgebraic extension.
Any embedding $\sigma : F \hookrightarrow L$ with L algebraically closed can be exteneded to an embedding



Proof

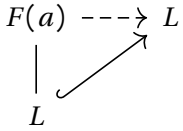
First, consider the case where $K = F(a)$ for some $a \in K$.
Let $f \in F[t]$ be the minimal polynomial of $a \in K$.
We know that $F(a) \simeq F[t]/(f)$.
The embedding $F \overset{\sigma}{\hookrightarrow} L$ induces a ring homomorphism $F[x] \hookrightarrow L[x]$.
Let $f^\sigma \in L[x]$ denote the polynomial obtained by applying σ to the coefficient of f.
Now L is algebraically closed, so f^σ splits completely.
Choose some root $\beta \in L$ of f^σ. Then consider the unique homomorphism $F[x] \to L$ which does σ to F and sends $X \mapsto \beta$, $F[x] \to L$, $f \mapsto f^{\sigma(\beta)=0}$.



Now for an arbitrary algebraic extension K/F, consider $S = \{(F_1, \sigma_1) : F \subseteq F_1 \subseteq K, \sigma_1 : F_1 \to L, \text{ such that } s_1|_F = \sigma\}$.
Define a partial order on S by $(F_1, \sigma_1) \leq (F_2, \sigma_2)$ if $F_1 \subseteq F_2$ and $\sigma_2|F_1 = \sigma_1$.
Note that $S \neq \varnothing$ since $(F, \sigma) \in S$.
Suppose $\{(F_\alpha, \sigma_\alpha)\}_\alpha$ is a totally ordered subset. Then $\bigcup_\alpha F_\alpha$ is a field and we can define $\tau : \bigcup_\alpha F_\alpha \to L$ by $\tau|_{F_\alpha} := \sigma_\alpha$.
Thus every totally ordered subset has an upper bound.
Then, by Zorn's lemma, this implies there is a maximal extension (F_0, σ_0).
Claim: $F_0 = K$. Otherwise, consider $\alpha \in K$ with $\alpha \in F_0$.
We can extend $\sigma_0 : F_0 \hookrightarrow L$ to a homomorphism $F_0(\alpha) \hookrightarrow L$ which contradicts the maximality of (F_0, σ_0).
Therefore, $F_0 = K$.

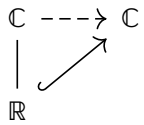
Remark

The extension is not unique.



We chose a root β in L of the minimum polynomial of a.
A different choice of root will gives a different extension.

Example



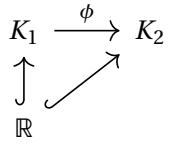
We have that $\mathbb{C} = \mathbb{R}(i)$ amd $X^2 + 1 = (x - i)(x + i)$.
So there are two such extension, $i \mapsto i$ the identity map and $z \mapsto \overline{z}$ $(i \mapsto -i)$ the complex conjugate.

Definition: F-Homomorphism

Let K_1/F and K_2/F be field extensions.
An F-homomorphism or homomorphism over F is a field homomorphism

$$K_1 \xrightarrow{\phi} K_2$$

such that $\phi(a) = a$ for all $a \in F$.



If ϕ is an isomorphism of fields, we call it an F-isomoprhism or an isomorphism over F.

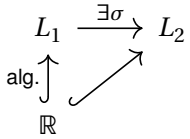
Example

Complex conjugation $z \mapsto \overline{z}$ is an $\mathbb{R}$-isomorphism of the field $\mathbb{C}$.

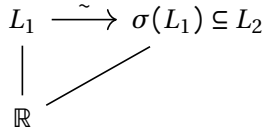
Corollary: Uniqueness of Algebraic Closure

Let L_1/F and L_2/F be algebraic closures.
Then there is an F-isomorphism $L_1 \tilde{\to} L_2$.

Proof



So there exists an F-homomorphism $\sigma : L_1 \to L_2$ by the proposition.
Claim: σ is an isomorphism.
It is automatically injective.



Since L_2/F is algebraic, $L_2/\sigma(L_1)$ is algebraic.
Hence $L_2 = \sigma(L_1)$ since $\sigma(L_1) \simeq L_1$ is algebraically closed.

Remark

Thus, “the” algebraic closure of a field F is unique up to a non-unique isomorphism.

Remark

Any algebraic extension K/F can be realized as (i.e. is F-isomorphic to) a subfield of the algebraic closure $\overline{F}$.
But again there can be many such embeddings.

Definition: Splitting Field

Let $\mathcal{F} \subseteq F[t]$ be a family of polynomials.
A splitting field for $\mathcal{F}$ is a field extension K/F such that every $f \in \mathcal{F}$ splits completely over K and $K = F(S)$ where $S := \{a \in K : a \text{ is a root of some } f \in \mathcal{F}\}$.

Proposition:

Let $\mathcal{F} \subseteq F[t]$ be a family of polynomials.

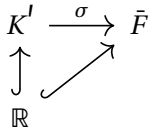
1. A splitting field for $\mathcal{F}$ exists. For example, $K := F(\{a \in \overline{F} : a \text{ is a root of some } f \in \mathcal{F}\}$ is such a splitting field.
2. Any 2 splitting fields for $\mathcal{F}$ are F-isomorphic.

Proof of 1

Over K, every polynomial $f \in \mathcal{F}$ splits completely and K is generated by these roots.

Proof of 2

Consider $F \hookrightarrow \overline{F}$, and let K'/F be a splitting field for $\mathcal{F}$.
We can extend the embedding $F \hookrightarrow \overline{F}$ to and embedding



Observe that $\alpha \in K'$ is a root of $f \in \mathcal{F}$ if and only if $\sigma(\alpha) \in \sigma(K') \subseteq \overline{F}$ is a root of $f \in \mathcal{F}$.
We know that $K' = F(S)$ where $S = \{\alpha \in K' : f(\alpha) = 0 \text{ for some } f \in \mathcal{F}\}$.
So $\sigma(K') = \sigma(F(S)) = F(\sigma(S)) = K$. That is $K' \tilde{\to} \sigma(K') = K \subseteq \overline{F}$.

Definition: Normal Extensions

A normal extension K/F is an algebraic extension such that for every irreducible polynomial $f \in F[t]$, if f has a root in K, then f splits completely in K.

Examples

- F/F is a normal extension.
- $\overline{F}/F$ is a normal extension.
- $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not a normal extension.

  $X^4 - 2 \in \mathbb{Q}[x]$ is irreducible which has a root but does not split completely (roots $\pm\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ and $\pm i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$).

Proposition

Let K/F be an algebraic extension and choose an algebraic closure $K \hookrightarrow \overline{K} = \overline{F}$.

1. K/F is a normal extension.
2. For any F-homomorphism $\sigma : K \to \overline{K}$, we have $\sigma(K) \subseteq K$.

3. For any F-homomorphism $\sigma : \overline{K} \to \overline{K}$, we have $\sigma(K) \subseteq K$.

Proof 1 Implies 2

Take $\sigma : K \to \overline{K}$.
Let $x \in K$ and consider its minimal polynomial $f \in F[t]$.
Then $\sigma(x)$ is also a root of f.
But f is an irreducible polynomial which has a root x in K, so every root of f in $\overline{K}$ is contained in K (since K/F is normal).
Therefore $\sigma(x) \in K$.

Proof 2 Implies 3

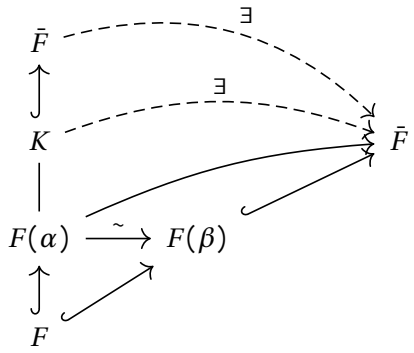
Trivial.

Proof 3 Implies 1

Let $f \in F[t]$ be an irreducible polynomial which has a root $\alpha \in K$.
We want to claim that all the roots of f (which exist in $\overline{K} = \overline{F}$) also lie in K.
Let $\beta \in \overline{K}$ be such a root. We have that

$$K \supseteq F(\alpha) \simeq F[t]/(f(t)) \simeq F(\beta) \subseteq \overline{F} = \overline{K}$$

with the F-isomorphism $\alpha \mapsto \beta$.



By hypothesis, $\sigma(K) \subseteq K$. Hence, $\sigma(\alpha) = \beta \in K$.

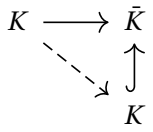
Remark

The intuition is that an F-homomorphism $\overline{K} \to \overline{K}$ must send $a \in K$ to a root of the minimal polynomial of a.
Normality of K/F ensures that all these roots are also in K.

Remark

$$K \overset{\iota}{\hookrightarrow} \Longrightarrow \operatorname{Hom}_F(K,K) \overset{\iota\circ -}{\hookrightarrow} \operatorname{Hom}_F(K,\overline{K})$$

is injective since ι is a monomorphism.
K/F is normal if and only if the map above is a bijection.



Proposition

Let K/F be a field extension. The following are equivalent

1. K/F is a normal extension.
2. K is the splitting field of a family of polynomials $\mathcal{F} \subseteq F[t]$.

Proof 1 Implies 2

Let $\mathcal{F} = \{\text{the minimal polynomials of all } x \in K\}$.
Then $K = F(S)$ where $S = \{a \in K : f(a) = 0 \text{ for some } f \in \mathcal{F}\}$.
Moreover, every polynomial $f \in \mathcal{F}$ splits completely in K since K/F is normal.
Therefore K is the splitting field of $\mathcal{F}$.

Proof 2 Implies 1

Choosing $F \hookrightarrow \overline{F}$, we know

$$K \xrightarrow{\sim} F(S) \subseteq \overline{F}$$

where $S = \{a \in \overline{F} : f(a) = 0 \text{ for some } f \in \mathcal{F}\}$.
Claim: $F(S)/F$ is a normal extension.
Consider an F-homomorphism $F(S) \xrightarrow{\sigma} \overline{F}$.
If $a \in S$, then $f(a) = 0$ for some $f \in \mathcal{F}$. Hence $f(\sigma(a)) = 0$ and $\sigma(a) \in S$.
Therefore $\sigma(F(S)) \subseteq F(\sigma(S)) \subseteq F(S)$.

Corollary

Finite normal extensions are precisely splitting fields of single polynomials.

Remark

Let $L/K/F$ be algebraic extensions.
Then L/F normal implies L/K normal.
On the other hand, L/F normal does not imply K/F normal.
e.g. $\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$
L/K and K/F normal does not imply L/F normal.
e.g. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

Definition: Normal Closure

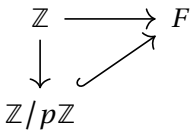
Let K/F be an algebraic extension.
Then there exists an extension L/K such that L/F is normal (hence L/K is normal) and which is minimal for this property.
We call L/F the normal closure of the extension K/F.

Moreover, if K/F is finite then L/F is finite.
Also, the normal closure L/F is unique up to F-isomorphism.
Proof left as an exercise.

April 24, 2024

Recall

For any prime p, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field of order p.
Note that if F is a finite field – i.e. a field with only finitely many elements – then $\mathrm{char}(F) = p > 0$.



It contains $\mathbb{F}_p$ as a subfield. We can regard F as an $\mathbb{F}_p$-vector space.
Since F is finite, its dimensions as an $\mathbb{F}_p$-vector space is finite.
That is, the degree $[F : \mathbb{F}_p] = n$ is finite.
As an $\mathbb{F}_p$-vector space, $F \simeq \mathbb{F}_p^n$. So $|F| = p^n$.
It is customary to use $q = p^n$ for the order of a finite field.
How can we construct finite fields? If $f \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n, then $\mathbb{F}_p[x]/(f)$ is a field of order p^n.

- Example
  $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible, hence $\mathbb{F}_2[x]/(x^2 + x + 1)$ is a field of order 4.

But it is not obvious whether there exists an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

Definition: Frobenius Homomorphism

Let F be a field of characteristic $p > 0$.
The Frobenius homomorphism is the map $F \xrightarrow{\text{Frob}} F$ defined by $a \mapsto a^p$.
This is obviously multiplicative $(ab)^p = a^p b^p$.
It is additive, since $(a+b)^p = a^p + b^p$ in characteristic p since $p \mid \binom{p}{i}$ for $i \neq 0, p$.
That is, the Frobenius is a field homomorphism.

Remark

The Frobenius is injective: $a^p = b^p \implies a = b$.

Remark

We can also consider iterates of the Frobenius

$$F \xrightarrow{\text{Frob}} F \xrightarrow{\text{Frob}} F \xrightarrow{\text{Frob}} \cdots \xrightarrow{\text{Frob}} F$$

which maps $a \mapsto a^{p^m}$.

Exercise

Since the Frobenius is a homomorphism, for any $m \geq 1$,

$$\left\{a \in F \,:\, a^{p^m} = a\right\}$$

is a subfield of F.

Theorem: (Kroenecker)

Let F be a field and let $G \leq F^*$ be a finite subgroup of the multiplicative group of units of F.
Then G is cyclic.

Proof

G is a finite, abelian group, therefore

$$G \simeq \mathbb{Z}/a_1 \oplus \mathbb{Z}_{a_2} \oplus \cdots \oplus \mathbb{Z}/a_s$$

where $a_1|a_2|\cdots|a_s$.
Written multiplicatively,

$$G \simeq C_{a_1} \times C_{a_2} \times \cdots \times C_{a_s}$$

where C_{a_i} is the cyclic group of order a_i.
If $x \in G$, then $x^{as} = 1$. It follows that

$$G \subseteq \left\{x \in F \,:\, x^{as} = 1\right\}$$

which are the roots of the polynomial $X^{as} - 1$. This polynomial has at most a_s roots in F.
Therefore, $a_1 a_2 \cdots a_s = |G| \leq a_s$ which implies $s = 1$ and $G \simeq C_{a_s}$ is cyclic.

Corollary

If F is a finite field, then the multiplicative group of units F^* is cyclic.

Remark

Let F be a finite field of order $q = p^n$.
Then F^* is a cyclic group of order $q - 1$ and for any $a \in F^*$ we have $a^{q-1} = 1$.
That is, for any $a \in F$, we have $a^q = a$. Thus every element of F is a root of the polynomial $X^q - X$.
In particular, $X^q - X$ has q distinct roots in F

$$X^q - X = \prod_{a \in F} (X - a)$$

in $F[x]$. Therefore F is a splitting field of $X^q - X$ over $\mathbb{F}_p$.

Proposition

If a finite field of order $q = p^n$ exists, then it is uniquely determined up to isomorphism as the splitting field of $X^q - X$ over $\mathbb{F}_p$.

Remark

Let F be a splitting field of $X^q - X$ over $\mathbb{F}_p$ ($q = p^n$). That is, $F = \mathbb{F}_p(\{\text{roots of } X^q - X \text{ in } \overline{\mathbb{F}_p}\}$.
The derivative of $X^q - X$ is $qX^{q-1} - 1 = -1$. Thus, $X^q - X$ has no multiple roots. That is, there are precisely q distinct roots in $\overline{\mathbb{F}_p}$.
Moreover, from the Frobenius homomorphism, these q roots form a subfield of $\overline{\mathbb{F}_p}$. Thus

$$F = \mathbb{F}_p(\{\text{roots of } X^q - X\}) = \{\text{roots of } X^q - X \text{ in } \mathbb{F}_p\}$$

is a field of order q.

Theorem:

For any prime p and integer $n \geq 1$, there exists a unique up to isomorphism field of order p^n, denoted $\mathbb{F}_{p^n}$, which is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.
Every finite field is isomorphic to a unique such $\mathbb{F}_{p^n}$.

Corollary

In a fixed algebraic closure $\overline{\mathbb{F}_p}$, there is a unique $\mathbb{F}_{p^n}$, namely the set of roots in $\overline{F_p}$ of $X^{p^n} - X$.

Definition: Roots of Unity

Let F be a field and $n \geq 1$.
An nth root of unity in F is an element $a \in F$ such that $a^n = 1$.
That is, a root of the polynomial $X^n - 1$.

Remark

If $\mathrm{char}(F) = p > 0$, then we have the Frobenius map which is injective: $a^{p^m} = b^{p^m} \implies a = b$.
Thus, the only p^mth root of unity in F is 1. Indeed, $X^{p^m} - 1 = (x-1)^{p^m}$.

Remark

Let F be a field with $\mathrm{char}(F) \nmid n$.
The derivative of $X^n - 1$ is nX^{n-1} whose only root is 0.
Thus $X^n - 1$ has no multiple roots. There are exactly n distinct roots of unity in $\overline{F}$.
Kronecker's Theorem implies that they form a cyclic group of order n.
The generators of this cyclic group are called the primitive nth roots of unity.

Example

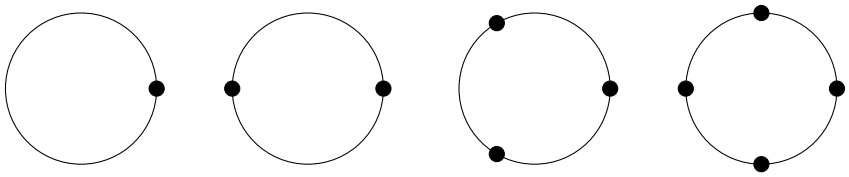
The nth roots of unity in $\overline{\mathbb{Q}} \subset \mathbb{C}$ are

$$\left\{e^{2\pi ik/n} : 0 \leq k < n\right\}$$

and $e^{2\pi ik/n}$ is primitive if and only if $\gcd(k, n) = 1$.
e.g. $\xi = e^{2\pi i/n}$ is a primitive nth root of unity.

$$1 = \xi^0, \xi^1, \ldots, \xi^{n-1}$$

Take, for example, $n = 1, 2, 3, 4$.



Remark

$$X^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots X + 1)$$

If $\xi \neq 1$ is an nth root of unity, then $1 + \xi + \xi^2 + \cdots + \xi^{n-1} = 0$.

Note

$X^n - 1 = \prod_{\xi\ n\text{th root of unity}} (X - \xi)$ in $\mathbb{C}[x]$.

Definition: Cyclotomic Polynomial

Let $n \geq 1$. The nth cyclotomic polynomial is

$$\Phi_n(X) := \prod_{\substack{\xi \text{ primitive} \\ n\text{th root of unity}}} (X - \xi) \in \mathbb{C}[X]$$

Examples

$n = 1$ gives $\Phi_1(X) = X - 1$.
$n = 2$ gives $\Phi_2(X) = X + 1$.
$n = 3$ gives

$$\Phi_3(X) = (X-\xi)(X-\xi^2) = X^2 - (\overbrace{\xi + \xi^2}^{-1}) + \xi^3 = X^2 + X + 1$$

with $\xi = e^{2\pi i/3}$.
$n = 4$ gives $\Phi_4(X) = (X - i)(X + i) = X^2 + 1$.

Remark

If p prime, $X^p - 1 = (X-1)(X^{p-1} + \cdots + X + 1)$.
Therefore, $\Phi_p(X) = X^{p-1} + \cdots + X + 1$.

Proposition

$$X^n - 1 = \prod_{d|n} \Phi_d(x)$$

Proof

The nth roots of unity form a cyclic group of order n.
The primitive nth roots of unity are the nth roots of 1 of order n.
The nth roots of unity of order $d|n$ are dth roots of unity and, in fact, are the primitive dth roots of unity.

$$X^n - 1 = \prod_{\substack{\xi \ n\text{th} \\ \text{root of unity}}} (X - \xi) = \prod_{d|n} \prod_{\substack{\xi \ d\text{th} \\ \text{root of unity}}} (X - \xi) = \prod_{d|n} \Phi_d(X)$$

Proposition

Let $n \geq 1$.
The nth cyclotomic polynomial $\Phi_n(X)$ has integer coefficients

$$\Phi_n(X) \in \mathbb{Z}[X]$$

Proof

Recall the following consequence of Gauss' lemma: if $f \in \mathbb{Z}[X]$ monic and $f = gh$ with $g, h \in \mathbb{Q}[X]$, then $g, h \in \mathbb{Z}[X]$.
When $n = 1$, $\Phi_1(X) = X - 1$. Then we have

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = \Phi_n(X) \underbrace{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)}_{f(X)}$$

By the inductive hypothesis, $f(X) \in \mathbb{Z}[X]$ monic.
In the Euclidean domain $\mathbb{Q}[X]$, $X^n - 1 = f(X)q(X) + r(X)$ for some $q, r \in \mathbb{Q}[X]$ with $\deg(r) < \deg(f)$.
On the other hand, in $\mathbb{C}[x]$ we have that

$$X^n - 1 = \Phi_n(X) f(X)$$

Therefore

$$\begin{aligned} f(X)q(X) = r(X) &= \Phi_n(X) f(X) \\ (\Phi_n(X) - q(X)) f(X) &= r(X) \end{aligned}$$

which implies that $\Phi_n(X) = q(X) \in \mathbb{Q}[X]$.
Therefore, by the consequence of Gauss' lemma we have $\Phi_n(X) \in \mathbb{Z}[X]$.

Theorem: (Gauss, 1798)

Let $n \geq 1$.
The nth cyclotomic polynomial $\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible.

Proof

Let ξ be a primitive nth root of unity, and let f be the minimal polynomial of ξ over $\mathbb{Q}$.
Then $f|\Phi_n$ and $\Phi_n(X) = f(X)g(X)$ for some $g(X) \in \mathbb{Z}[X]$ monic.
Claim: if $p \nmid n$, then $f(\xi^p) = 0$.

Note that $p \nmid n$ implies that ξ^p is also a primitive nth root of unity.
Suppose, for sake of contradiction, that $f(\xi^p) \neq 0$. Then it must be that $g(\xi^p) = 0$
It follows that ξ would be a root of $g(X^p)$ and $f(X) | g(X^p)$. So

$$g(X^p) = f(X)h(X)$$

for some $h \in \mathbb{Z}[X]$ monic.
Apply the ring homomorphism $\mathbb{Z}[X] \to \mathbb{F}_p[X]$ which applies $\mathbb{Z} \to \mathbb{F}_p$ to the coefficients. In $\mathbb{F}_p[X]$

$$g(X)^p = g(X^p) = f(X)h(X)$$

Let $k(X)$ be an irreducible factor of $f(X)$ in $\mathbb{F}_p[X]$. Then $k(X)$ divides $g(X)$.
Then $k(X)^2 | X^n - 1$ in $\mathbb{F}_p$ and, consequently, $X^n - 1$ has multiple roots in $\overline{\mathbb{F}_p}$.
But the derivative of $X^n - 1$ is nX^{n-1} whose only root is 0 since $p \nmid n$ which is a contradiction.
We have therefore established that if $p \nmid n$, then $f(\xi^p) = 0$.
Recall that ξ^p is itself a primitive, nth root of unity. Repeating the process above with ξ replaced by ξ^p leads to

$$f(\xi^{p_1 p_2 \cdots p_r}) = 0$$

for any primes $p_1 p_2 \cdots p_r$ which do not divide n.
Therefore, $f(\xi^k) = 0$ for all k such that $\gcd(k, n) = 1$ and $f(\xi) = 0$ for every primitive nth root of unity.
This tells us that $\Phi_n | f$ so $f = \Phi_n$.

Remark

$\mathbb{Z}[X]$ is a UFD. So

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

is the unique factorization of $X^n - 1$ into irreducible polynomials.

Remark

If ξ is a primitive nth root of unity, then $\Phi_n(\xi) = 0$.
Since Φ_n is irreducible, Φ_n is the minimal polynomial of ξ.
Then $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \deg(\Phi_n) = |\xi^{0 \leq k < n}|$ such that $\gcd(k, n) = 1$.
That is, it is equal to Euler's totient function $\phi(n)$.
Note that every nth root of unity is contained in $\mathbb{Q}(\xi_n)$.
Thus, $\mathbb{Q}(\xi_n)$ is the splitting field of $X^n - 1$ over $\mathbb{Q}$ (and also the splitting field of $\Phi_n(X)$ over $\mathbb{Q}$).

May 8, 2024

Recall:

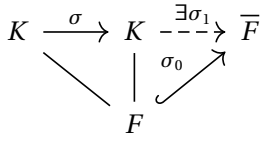
For K/F a field extension, $\mathrm{Gal}(K/F) = \{F\text{-automorphisms } \phi : K \xrightarrow{\sim} K\}$.

Remark:

If K/F is a finite extension, then every F-homomorphism $\phi : K \to K$ is an F-automorphism. Indeed, ϕ is an injective linear endomorphism of the finite-dimensional F-vector space K. Hence ϕ is surjective.
More generally, this is true for any algebraic extension.

Remark:

If K/F is a finite extension, $|\mathrm{Gal}(K/F)| \leq [K : F]_S \leq [K : F]$. Indeed



We have a map $\mathrm{Gal}(K/F) \to \mathrm{Hom}_F(K, \overline{F})$, $\sigma \to \sigma_1 \circ \sigma$ which is injective, since σ_1 is a monomorphism.

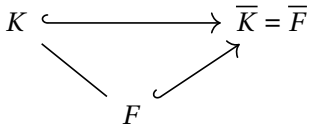
Proposition

Let K/F be a finite extension. The following are equivalent.

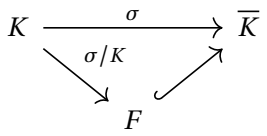
1. K/F is Galois.
2. $|\mathrm{Gal}(K/F)| = [K : F]$.

Proof

Note K/F is separable if and only if $[K : F]_S = [K : F]$.
On the other hand, we claim that K/F is normal if and only if $|\mathrm{Gal}(K/F)| = [K : F]_S$.
Well, choose an embedding



K/F is normal if and only if for every F-homomorphism, $\sigma : K \to \overline{K}$ we have $\sigma(K) \subseteq K$. That is



Movreover, note that $\sigma/K : K \to K$ is automatically an automorphism by the remark.
Thus K/F is normal if and only if the injective map $\mathrm{Gal}(K/F) \hookrightarrow \mathrm{Hom}_F(K, \overline{F})$ is surjective.
That is, if and only if $|\mathrm{Gal}(K/F)| = [K : F]_S$.

Theorem: Artin's Theorem

Let K be a field, and let $G \leq \mathrm{Aut}(K)$ be a finite subgroup.
Let $K^G := \{x \in K : \sigma(x) = x, \ \forall \sigma \in G\}$.
Then K/K^G is Galois with Galois group G.
In particular, $[K : K^G] = |G|$.

Proof: Galois

Let $x \in K$.
Consider the finite set $G.x = \{\sigma(x) : \sigma \in G\} \subseteq K$ (i.e. the orbit of x under the action of G).
Consider the polynomial $f = f_x = \prod_{y \in G.x}(t - y) \in K[t]$.
Note that f has only simple roots and $f_x(x) = 0$ since $x \in G.x$.
Now G acts on K, hence G acts on $K[t]$ by acting on the coefficients. Given $\sigma \in G$, this gives

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K \\ \downarrow & & \downarrow \\ K[t] & \dashrightarrow & K[t] \end{array}$$

$$f \longmapsto f^\sigma$$

This is an action on $K[t]$ by ring homomorphisms.
Therefore, $\forall \sigma \in G$,

$$f_x^\sigma = \prod_{y \in G.x} (t - \sigma(y)) \underset{(!)}{=} f_x$$

That is, the coefficients of f_x are fixed by σ for every $\sigma \in G$.
It follows that $f_x \in K^G[t]$. Since $f_x(x) = 0$, the minimal polynomial of x over K^G divides f_x and hence has simple roots.
This tells us that x is separable over K^G and therefore that K/K^G is a separable (and algebraic) extension.
Also, K is the splitting field over K^G of $\{f_x : x \in K\} \subseteq K^G[t]$. So K/K^G is a normal extension.
Since the extension is normal and separable, it is Galois.

Proof: Galois Group

Claim: $[K : K^G] \leq |G|$.
It will follow that the Galois extension K/K^G is a finite extension, hence $[K : K^G] = |\mathrm{Gal}(K/K^G)|$ by the previous proposition.
This will imply that $\mathrm{Gal}(K/K^G) = G$ since we have $G \subseteq \mathrm{Gal}(K/K^G)$ and

$$|G| \leq |\mathrm{Gal}(K/K^G)| = [K : K^G] \leq |G|$$

The remaineder of the proof is devoted to proving the claim.
Let $n := |G|$ and suppose for a contradiction that there are m linearly independent (over K^G) elements $x_1, \ldots, x_m \in K$ with $m > n$.
Let $G = \{\sigma_1, \ldots, \sigma_n\}$. Consider the matrix

$$A(\sigma_i(x_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in M_{n \times m}(K)$$

Consider the linear map $K^m \xrightarrow{A} K^n$. Since $m > n$, $\ker(A) \neq 0$. Let

$$\lambda = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix} \in \ker(A) \subseteq K^m$$

be such that $\lambda \neq 0$ and has the fewest number of nonzero entries.
Without loss of generality, we may assume $\lambda_1 \neq 0$ (e.g. by permuting the x_j if necessary). Note that $\lambda_1^{-1}\lambda$ satisfies the properties that λ has so we may assume without loss of generality that $\lambda_1 = 1$. Now we have that $A\lambda = 0$, so for each $1 \leq i \leq n$,

$$\sum_{j=1}^{m} \sigma_i(x_j)\lambda_j = 0$$

We can't have $\lambda_j \in K^G$ for all j, otherwise we would have

$$0 = \sum_{j=1}^{m} \sigma_1(x_j)\lambda_j = \sigma_1\left(\sum_{j=1}^{m} x_j\lambda_j\right) \implies \sum_{j=1}^{m} x_j\lambda_j = 0$$

which contradicts the linear independence of the x_j's.
Since $\lambda_1 = 1 \in K^G$, suppose without loss of generality that $\lambda_2 \in K^G$.
Hence, there is some $1 \leq k \leq n$ such that $\sigma_k(\lambda_2) \neq \lambda_2$ (i.e. there is a σ which does not fix λ_2). Consider

$$\sigma_k\lambda = \begin{pmatrix} \sigma_k(\lambda_1) \\ \vdots \\ \sigma_k(\lambda_m) \end{pmatrix}$$

Consider $A.\sigma_k(\lambda)$. For each $1 \leq i \leq n$, consider $\sum_{j=1}^{m} \sigma_j(x_j)\sigma_k(\lambda_j)$. There exists an l such that $\sigma_i = \sigma_k \circ \sigma_l$. Then

$$\sum_{j=1}^{m} \sigma_j(x_j)\sigma_k(\lambda_j) = \sum_{j=1}^{m} \sigma_k(\sigma_l(x_j))\sigma_k(\lambda_j) = \sigma_k\left(\underbrace{\sum_{j=1}^{m} \sigma_l(x_j)\lambda_j}_{0 \text{ since } A\lambda=0}\right) = 0$$

Therefore $\sigma_k\lambda \in \ker(A)$. Thus $\lambda - \sigma_k(\lambda) \in \ker(A)$. Obvserve

$$\lambda - \sigma_k(\lambda) = \begin{pmatrix} 1 - 1 = 0 \\ \lambda_2 - \sigma_k(\lambda_2) \neq 0 \\ \vdots \\ \lambda_m - \sigma_k(\lambda_m) \end{pmatrix}$$

Note that if $\lambda_j = 0$, then $\lambda_j - \sigma_k(\lambda_j) = 0$. This $\lambda - \sigma_k(\lambda)$ is a nonzero element of the kernel of A which has strictly fewer nonzero entries than λ which is a contradiction.
We conclude that $[K : K^G] \leq n = |G|$.

Corollary

If K/F is a finite Galois extension, then $F = K^{\mathrm{Gal}(K/F)}$.

Proof

Let $G := \mathrm{Gal}(K/F)$.
For K/F a finite Galois extension, $[K : F] = |G|$.
By Artin's Theorem, K/K^G is a finite Galois extension with GAlois group G. In particular, $[K : K^G] = G$. So

$$\underbrace{\underbrace{[K : K^G]}_{|G|}[K^G : F]}_{|G|} \implies [K^G : F] = 1 \implies K^G = F$$

Reminder

For $K/E/F$ algebraic extensions.
K/E separable and E/F separable implies that K/F is separable.
K/F separable implies that K/E and E/F are separable.
K/E normal and E/F normal does not imply that K/F is normal.
But K/F normal does imply that K/E is normal but not necessarily that E/F is normal.
We conclude that K/E Galois and E/F Galois does not imply K/F Galois.
Likewise, K/F Galois ensures K/E Galois but not necessarily E/F.

Theorem: Fundamental Theorem of Galois Theory

Let K/F be a finite Galois extension.
Then there are inclusion-reversing bijections of sets

$$\{\text{intermediate fields of } K/F\} \underset{\longleftarrow}{\overset{\sim}{\longrightarrow}} \{\text{subgroups of } \mathrm{Gal}(K/F)\}$$

$$E \longmapsto \mathrm{Gal}(K/E)$$

$$K^H \longmapsfrom H$$

Moreover, E/F is Galois if and only if E/F is normal if and only if $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$.
In this case, restriction induces an isomorphism

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \simeq \mathrm{Gal}(E/F)$$

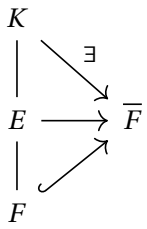
Proof: Bijection

$G := \mathrm{Gal}(K/F)$. Let $F \subseteq E \subseteq K$.
K/F Galois implies K/E Galois.
By the corollary of ARtin's Theorem, this implies that $E = K^{\mathrm{Gal}(K/E)}$.
On the other hand, let $H \leq G$.
Then Artin's theorem applied to K and H implies that K/K^H is Galois with Galois group H.
That is $\mathrm{Gal}(K/K^H) = H$. So we have an inverse bijection.

Proof: Normality

Note that K/F separable implies that E/F is separable.
So E/F is Galois if and only if E/F is normal.

Since K/F is normal, $\mathrm{Gal}(K/F) \simeq \mathrm{Hom}_F(K, \overline{F})$. Observe that



So every F-homomorphism $E \to \overline{F}$ is the restriction of an F-homomorphism $K \to \overline{F}$ and hence is the restriction of some $\sigma \in \mathrm{Gal}(K/F)$.
Consider $\sigma(E) \subseteq K$. This corresponds to some subgroup of $\mathrm{Gal}(K/F)$ by the correspondence theorem.
Let $G := \mathrm{Gal}(K/F)$ and $H := \mathrm{Gal}(K/E)$.
Claim: $\sigma(E)$ corresponds to the subgroup $\sigma H \sigma^{-1}$. That is, $\sigma(E) = K^{\sigma H \sigma^{-1}}$. Well

$$\begin{aligned} K^{\sigma H \sigma^{-1}} &= \{x \in K : \sigma(\tau(\sigma^{-1}(x))) = x,\ \forall \tau \in H\} \\ &= \{x \in K : \tau(\sigma^{-1}(x)) = \sigma^{-1}(x),\ \forall \tau \in H\} \\ &= \{x \in K : \sigma^{-1}(x) \in K^H = E\} = \sigma(E) \end{aligned}$$

Hence, E/F is normal if and only if $\sigma(E) \leq E,\ \forall \sigma \in G$; if and only if $\sigma(E) = E,\ \forall \sigma \in G$; if and only if $\sigma H \sigma^{-1} = H$, $\forall \sigma \in G$; if and only if $H \triangleleft G$.
Restricting from K to E gives a surjective map $\mathrm{Gal}(K/F) \twoheadrightarrow \mathrm{Gal}(E/F)$ by the discussion above whose kernel is $\mathrm{Gal}(K/E)$. Hence

$$\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \simeq \mathrm{Gal}(E/F)$$

Remark

The bijection is called the Galois correspondence.

Remark

If $F \subseteq E \subseteq F$, then K/E is Galois and $[K : E] = |\mathrm{Gal}(K/E)|$.

$$\{\text{intermediate fields of degree } d\ ([E : F] = d)\} \xleftrightarrow{\sim} \{\text{subgroups of index } d\}$$

May 13, 2024

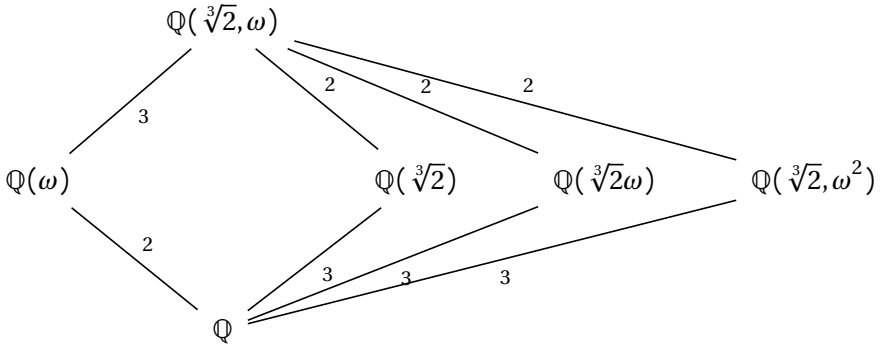
Example

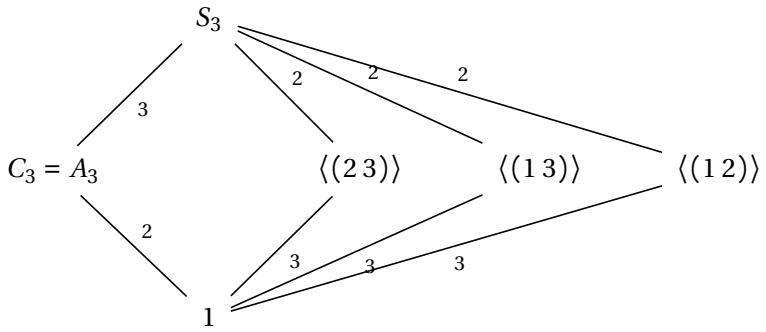
The splitting field of $X^3 - 2 \in \mathbb{Q}[X]$ is $K = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$ where $\omega = e^{2\pi i/3}$.
Since $[K : \mathbb{Q}] = 6$, $|\mathrm{Gal}(K/\mathbb{Q})| = 6$.
Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ must send each root of $X^3 - 2$ to another root. That is, each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ permutes the roots.

$$\mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow S_3$$

Since $|\mathrm{Gal}(K/\mathbb{Q})| = |S_3| = 6$, $\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} S_3$.

Alternatively, any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is complete determined by $\sigma(\sqrt[3]{2})$ and $\sigma(\omega)$.
There are at most three possibilities for $\sigma(\sqrt[3]{2})$, namely the three roots of its minimal polynomial $\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\}$.
On the other hand, there are at most two possibilities for $\sigma(\omega)$, namely the two roots of its minimal polynomial $\{\omega, \omega^2\}$.
So there are at most six possibilities, all of which aare actually realized.
If we set ρ to send $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$ and fix $\omega \mapsto \omega$, then $\sqrt[3]{2}\omega \mapsto \sqrt[3]{2}\omega^2$ and $\sqrt[3]{2}\omega^2 \mapsto \sqrt[3]{2}$. So ρ is an element of order three.
Letting τ be the guy $\omega \mapsto \omega^2$ and $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, an element of order two, we get that $\mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} D_6 \simeq S_3$.





So $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2})$ is a subgroup of S_3 of $[K : \mathbb{Q}(\sqrt[3]{2})] = 2$ which fixes 1. That is, $\mathrm{Gal}(K/\mathbb{Q}(\sqrt[3]{2}) = \langle(2\,3)\rangle$.
The only normal subgroups of S_3 are 1, A_3 and S_3.

Definition: Galois Group of a Separable Polynomial

The Galois group of a separable polynomial $f \in \mathbb{F}[t]$ is defined to be the Galois group of its splitting field:

$$\mathrm{Gal}(f) := \mathrm{Gal}(K/\mathbb{F})$$

where K is the splitting field of f over $\mathbb{F}$.

Remark

Any $\sigma \in \mathrm{Gal}(K/\mathbb{F})$ must send each root of f to another root of f.
That is, the Galois group permutes the roots of f. Said another way, the Galois group acts on the set of roots.

Remark

If f is irreducible, then it has $d := \deg(f)$ distinct roots and so we get a map

$$\mathrm{Gal}(K/\mathbb{F}) \hookrightarrow S_d$$

which is injective since K is generated over $\mathbb{F}$ by the roots.
On the other hand, if f is not irreducible then it might have fewer than d distinct roots.

Exercise:

The following are equivalent for a separable polynomial $f \in \mathbb{F}[t]$:

1. f has $\deg(f)$ distinct rootsin $\overline{\mathbb{F}}$.

2. $f = f_1 f_2 \cdots f_r$ with f_i irreducible and $f_i \neq f_j$ for $i \neq j$.

In this case, then certainly we have an embedding

$$\mathrm{Gal}(K/\mathbb{F}) \hookrightarrow S_d$$

where $d = \deg(f)$, but much more can be said. If a is a root of f_1, then $\forall \sigma \in \mathrm{Gal}(K/\mathbb{F})$ we have that $\sigma(a)$ is also a root of f_1.
So really $\mathrm{Gal}(K/\mathbb{F})$ is permuting the roots of the irreducible factors of f. We get an embedding

$$\mathrm{Gal}(K/\mathbb{F}) \hookrightarrow S_{d_1} \times S_{d_2} \times \cdots \times S_{d_r}$$

where $d_i = \deg(f_i)$. For $d = \sum d_i$, we have that

$$S_{d_1} \times S_{d_2} \times \cdots \times S_{d_r} \subseteq S_d$$

Remark

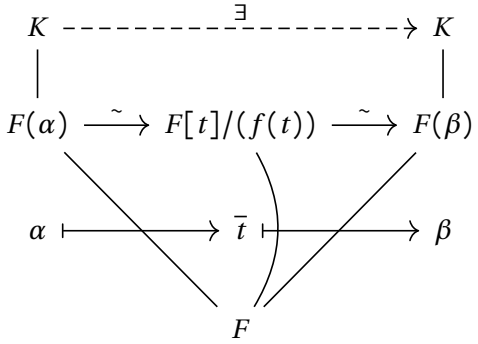
If $f = f_1^{m_1} f_2^{m_2} \cdots f_r^{m_r}$ with f_i irreducible, and $f_i \neq f_j$, $\forall\, i \neq j$, then the splitting field for f coincides with the splitting field for

$$g := f_1 f_2 \cdots f_r$$

and note that g is also separable.
By replacing f with g we can, without loss of generality, assume our separable polynomial f has $\deg(f)$ distinct roots in $\overline{F}$.

Remark

If f is irreducible, then the action of $\mathrm{Gal}(K/\mathbb{F})$ on the set of roots is transitive: for all roots $\alpha, \beta \in K$ of f, $\exists \sigma \in \mathrm{Gal}(K/\mathbb{F})$ such that $\sigma(\alpha) = \beta$.



Thus $\mathrm{Gal}(K/\mathbb{F}) \hookrightarrow S_d$ identifies $\mathrm{Gal}(K/\mathbb{F})$ with a transitive subgroup of S_d.

Definition:

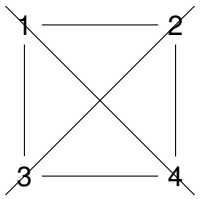
A subgroup $H \subseteq S_n$ is a transitive subgroup if the induced action of $\mathrm{Hom}\{1, \ldots, n\}$ is transitive.

Example

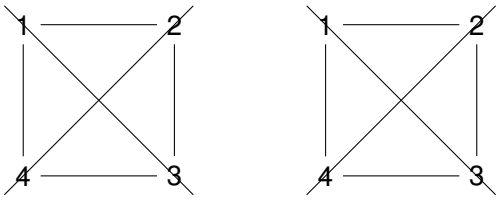
The splitting field of $X^4 - 2 \in \mathbb{Q}[X]$ is $K := \mathbb{Q}(\sqrt[4]{2}, i)$. The roots are

$$
\begin{aligned}
a_1 &= \sqrt[4]{2} \\
a_2 &= -\sqrt[4]{2} = -\alpha_1 \\
a_3 &= i\alpha_1 \\
a_4 &= -i\alpha_1
\end{aligned}
$$

Now $[K : \mathbb{Q}] = 8$. Hence $|\mathrm{Gal}(K/\mathbb{Q})| = 8$. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. $G \hookrightarrow S_4$ by permuting the roots.
$|S_4| = 4 \cdot 3 \cdot 2 = 24 = 8 \cdot 3$. Therefore, G is isomorphic a to a 2-Sylow subgroup of S_4.
What are the 2-Sylow subgroups of S_4?
Observe that D_8 acts faithfully on the vertices of $\square$. Therefore $D_8 \hookrightarrow S_4$.
It follows that $G \simeq D_8$, the dihedral group of order 8.
We have that $n_2 | 3$ and $n_2 \equiv 1 \pmod 2$, but $D_8 \subseteq S_4$ is not normal.
Therefore S_4 has 3 2-Sylow subgroups, each containing a pair of disjoint transpositions.



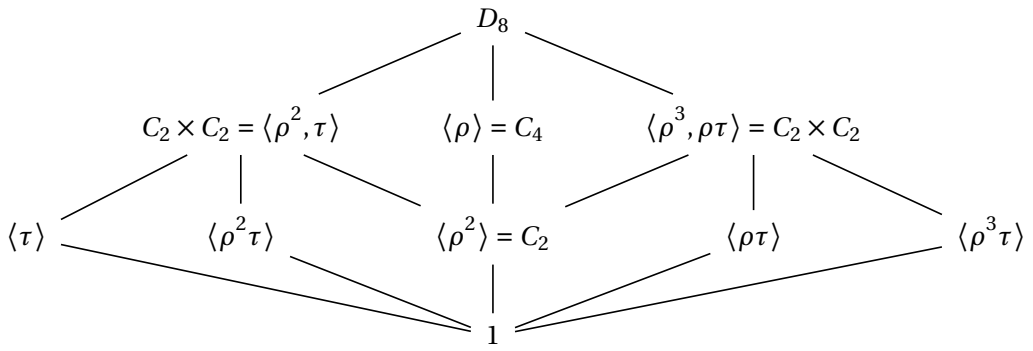
This copy of D_8 sitting inside S_4 contains $(1\,3)$ and $(2\,4)$ but no other transpositions. The other copies are given by



Back to the Galois group, $G \hookrightarrow S_4$. The complex conjugation gives $\sigma \in G$

$$
\begin{aligned}
\alpha_1 &\mapsto \alpha_1 \\
\alpha_2 &\mapsto \alpha_2 \\
\alpha_3 &\mapsto \alpha_4 \\
\alpha_4 &\mapsto \alpha_3
\end{aligned}
$$

That is, the transposition $(3\,4)$.
We conclude that $G \hookrightarrow S_4$ identifies G with the 2-Sylow D_8 in S_4 which contains $(3\,4)$.
Subgroups of $G \simeq D_8$.



Then $H \mapsto K^H$ should give (exercise) a picture like $\mathbb{Q}(\sqrt[4]{2}, i)$.

Example

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(X^2-2)(X^2-3) \in \mathbb{Q}[X]$.
Let us write the roots as

$$\begin{aligned} \alpha_1 &= \sqrt{2} \\ \alpha_2 &= -\sqrt{2} \\ \alpha_3 &= \sqrt{3} \\ \alpha_4 &= -\sqrt{3} \end{aligned}$$

$G := \mathrm{Gal}(\sqrt{2}, \sqrt{3}/\mathbb{Q})$, $|G| = 4$, $G \hookrightarrow S_4$. Let

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \text{and} \quad \tau : \begin{cases} \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{2} \mapsto \sqrt{2} \end{cases}$$

Then $G = \{1, \sigma, \tau, \sigma\tau\} = C_2 \times C_2 \simeq \langle (1\,2), (3\,4) \rangle \subseteq S_4$.
Alternatively, $G \hookrightarrow C_2 \times C_2$ isomorphically by direct means.

Example

Let $\mathbb{F}$ be any field and consider $\mathbb{F}[X_1, \ldots, X_n] \subseteq \mathbb{F}(X_1, \ldots, X_n)$.
We say that a rational function $f \in \mathbb{F}(X_1, \ldots X_n)$ if $f(X_{\sigma(1)}, X_{\sigma(2)}, \ldots X_{\sigma(n)}) = f(X_1, X_2, \ldots X_n)$ for all $\sigma \in S_n$.
Recall that S_n acts on $\mathbb{F}[X_1, X_2, \ldots X_n]$ by $\mathbb{F}$-algebra homomorphisms

$$\begin{array}{ccc} \mathbb{F}[X_1, \ldots, X_n] & \xrightarrow{\sigma} & \mathbb{F}[X_1, \ldots, X_n] \\ \downarrow & & \downarrow \\ \mathbb{F}(X_1, \ldots, X_n & \xrightarrow{\exists \sigma} & \mathbb{F}(X_1, \ldots, X_n) \end{array}$$

This action extends to an action of S_n on $\mathbb{F}(X_1, \ldots, X_n)$ by $\mathbb{F}$-algebra homomorphisms.

$$S_n \to \mathrm{Aut}_{\mathbb{F}-\mathrm{alg}}(\mathbb{F}(X_1, \ldots, X_n)) = \mathrm{Aut}_{\mathbb{F}}(\mathbb{F}(X_1, \ldots, X_n) = \mathrm{Gal}(\mathbb{F}(X_1, \ldots, X_n)/\mathbb{F})$$

Explicitly,

$$\frac{f(X_1,\ldots,X_n)}{g(X_1,\ldots,X_n)} \mapsto \frac{f(X_{\sigma(1)},\ldots,X_{\sigma(n)})}{g(X_{\sigma(1)},\ldots,X_{\sigma(n)})}$$

Therefore the collection $\mathbb{F}(X_1,\ldots,X_n)^{S_n}$ of symmetric rational functions is a subfield of $\mathbb{F}(X_1,\ldots,X_n)$.
Artin's Theorem implies that $\mathbb{F}(X_1,\ldots,X_n)/\mathbb{F}(X_1,\ldots,X_n)^{S_n}$ is a finite Galois extension with Galois group S_n.

Corollary

Let G be a finite group.
Then G is the Galois group of some finite Galois extension.

Proof

Caley's Theorem implies $G \hookrightarrow S_n$.
Let $K := \mathbb{F}(X_1,\ldots,X_n)^{S_n}$.

$$\begin{array}{c} \mathbb{F}(X_1,\ldots,X_n) \\ | \\ K \end{array}$$

is a finite Galois extension with Galois group S_n. So $\mathbb{F}(X_1,\ldots,X_n)/\mathbb{F}(X_1,\ldots,X_n)^{G}$ is a finite Galois extension with Galois group

$$\mathrm{Gal}(\mathbb{F}(X_1,\ldots,X_n)/\mathbb{F}(X_1,\ldots,X_n)^{G}) \simeq G$$

by the Fundemental Theorem of Galois Theory.

Remark

In algebraic number theory, one is primarily interested in "number fields" (i.e. finite extensions of $\mathbb{Q}$).

Inverse Galois Problem (Major Open Problem)

Does every finite group arise as the Galois group of some finite extension of $\mathbb{Q}$?

Proposition

Let $\mathbb{F}$ be a field and let $s_1,\ldots,s_n \in \mathbb{F}[X_1,\ldots,X_n]$ be the n elementary symmetric polynomials. Then

$$\mathbb{F}(X_1,\ldots,X_n)^{S_n} = \mathbb{F}(s_1,\ldots,s_n)$$

Proof

$$\begin{array}{c} \mathbb{F}(X_1,\ldots,X_n) \\ | \\ \mathbb{F}(X_1,\ldots,X_n)^{S_n} \\ | \\ \mathbb{F}(s_1,\ldots,s_n) \end{array}$$

Recall that

$$(t-X_1)(t-X_2)\cdots(t-X_n) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n \in \mathbb{F}(s_1,\ldots,s_n)[t]$$

Thus $\mathbb{F}(X_1,\ldots,X_n)$ is the splitting field of this polynomial over $\mathbb{F}(s_1,\ldots,s_n)$. Moreover, note that the polynomial is separabe (since the X_i are distinct). Therefore

$$\mathrm{Gal}(\mathbb{F}(X_1,\ldots,X_n)/\mathbb{F}(s_1,\ldots,s_n)) \hookrightarrow S_n$$

On the other hand, $S_n = \mathrm{Gal}(\mathbb{F}(X_1,\ldots,X_n)/\mathbb{F}(X_1,\ldots,X_n)^{S_n} \hookrightarrow \mathrm{Gal}(\mathbb{F}(X_1,\ldots,X_n)/\mathbb{F}(s_1,\ldots,s_n))$. Therefore

$$\mathrm{Gal}(\mathbb{F}(X_1,\ldots,X_n)/\mathbb{F}(s_1,\ldots,s_n)) = S_n$$

and $\mathbb{F}(s_1,\ldots,s_n) = \mathbb{F}(X_1,\ldots,X_n)^{S_n}$ by the Fundamental Theorem of Galois Theory.