Algebra III

April 1, 2024

Chapter 0: Review

Definition: Category

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

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

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

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 $X \in$ Obj$(\mathcal{C})$, there exists a morphism $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ such that

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

Example 1

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

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 Obj$(\mathcal{C}) = \{*\}$, $\mathrm{Hom}_{\mathcal{C}}(*, *) = G$ and

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

the group operator.

Example 4

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

$$\mathrm{Hom}_{\mathcal{C}}(x, y) = \begin{cases} \varnothing & \text{if } x \nleq y \\ \{f_{xy}\} & \text{if } x \leq y \end{cases}$$

Notation

If $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ 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 $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.

Definition: Endomorphism

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

Definition: Automorphism

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

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

Example 2

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

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 $X \in \mathrm{Obj}(\mathcal{C})$, a chosen object $F(X) \in \mathrm{Obj}(\mathcal{D})$.

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

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

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 $\mathcal{C}$,

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(F(X'), Y) \arrow[r, "\sim"] \arrow[d, "- \circ F(f)"] & \mathrm{Hom}_{\mathcal{C}}(X', G(Y)) \arrow[d, "- \circ f"] \\
\mathrm{Hom}_{\mathcal{D}}(F(X), Y) \arrow[r, "\sim"] & \mathrm{Hom}_{\mathcal{C}}(X, G(Y))
\end{tikzcd}$$

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

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

Example 1

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

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

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 $\mathsf{Mod}_S \to \mathsf{Mod}_R$ called a “restriction of scalars”, which has a left adjoint called “extension of scalars.”

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

Recall

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

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, $R[x_1, x_2, \dots, x_n]$ 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.

$$\begin{tikzcd} \mathsf{Set} \arrow[d, shift right, "f"'] \\ \mathsf{Mod}_R \arrow[u, shift right, "\mathcal{U}"'] \end{tikzcd}$$

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,

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

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

$$\begin{tikzcd} \mathsf{Set} \arrow[d, shift right, "f"'] \\ \mathsf{CAlg}_R \arrow[u, shift right, "\mathcal{U}"'] \end{tikzcd}$$

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

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

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."

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

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

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

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 $n = 2$.

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

Let $n = 3$.

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

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, Frac(R), is the set of all “formal fractions”

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

More precisely, 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

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

Example 1

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

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 $f(a) = 0$.

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

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 $a_1, \dots, a_n \in \mathbb{C}$. Then

$$\begin{aligned} a_1 &= -s_1(\alpha_1, \dots, \alpha_n) = -(\alpha_1 + \cdots + \alpha_n) \\ a_k &= (-1)^k s_k(\alpha_1, \dots, \alpha_n) \\ a_n &= (-1)^n \alpha_1 \cdots \alpha_n \end{aligned}$$

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 $\text{char}(F) = \begin{cases} 0 & \text{if } \mathbb{Q} \subseteq F \\ p & \text{if } \mathbb{F}_p \subseteq F \end{cases}$.

Remark

Note that the kernel of $\mathbb{Z} \to F$ is $\text{char}(F)\mathbb{Z} \subseteq \mathbb{Z}$.
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.

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook] \arrow[d] & \mathbb{Q} \\ \mathbb{F}_p & \end{tikzcd}$$

Examples

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

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

Notation

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

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

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

Notation

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

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 $F[t] \hookrightarrow F(t)$.