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 $\mathcal{C}$,

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

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

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{D}}(F(X), Y) & \tilde{\to} & \mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \\ g \circ - \downarrow & & \downarrow G(g) \circ - \\ \mathrm{Hom}_{\mathcal{D}}(F(X), Y') & \tilde{\to} & \mathrm{Hom}_{\mathcal{C}}(X, G(Y')) \end{array}$$

We write

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

Example 1

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

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

where

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

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.”

$$\begin{array}{c} \mathsf{Mod}_R \\ S \otimes_R - \Updownarrow \\ \mathsf{Mod}_S \end{array}$$

Recall

For commutative ring R, $\rightsquigarrow \mathsf{Mod}_R$.
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, $R[x_1, x_2, \ldots, x_n]$ 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.

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

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,

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

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

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

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

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

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."

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

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 $A \cong R[x, \ldots, x_n]/I$ for some $n \geq 1$ and ideal $I \subset R[x_1, \ldots, x_n]$.

April 3, 2024

Definition: Symmetric Polynomials

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

$$\begin{array}{rl} S_n \to & \mathsf{Set} \quad \overset{F}{\to} \mathsf{CAlg}_R \\ * \mapsto \{1, \ldots, n\} & \mapsto R[x_1, \ldots, x_n] \end{array}$$

Exercise 1

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

Example 1

Consider the polynomial

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

Write

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

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

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 $n = 3$.

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

Exercise 2

Show that the polynomials $s_1, \ldots, s_n \in R[x_1, \ldots, x_n]$ 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 $f(a) = 0$.

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

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,

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

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

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

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.