MAT205: Abstract Algebra II

Rings, Polynomial Rings, and Polynomial Functions

Ma, Jia-Jun - Xiamen University Malaysia

Part I

Rings and Ring Homomorphisms

Definition: Ring

Definition. A **ring** R is a set with two binary operations

$$+ : R \times R \to R, \qquad \cdot : R \times R \to R$$

such that:

1. $(R, +)$ is an abelian group;
2. multiplication is associative;
3. multiplication distributes over addition:

$$a(b + c) = ab + ac, \qquad (a + b)c = ac + bc.$$

The additive identity is written 0.

Example: Basic Rings

Ring	Comment
$\mathbb{Z}$	integers
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$	fields
$\mathbb{Z}_n$	modular arithmetic
$M_n(F)$	matrices over a field
$\mathcal{F}(\mathbb{R}, \mathbb{R})$	real-valued functions
$R_1 \times R_2$	product ring

In $M_n(F)$, multiplication is usually not commutative.

Definition: Commutative Rings and Unity

Commutative ring.

$$ab = ba \qquad \text{for all } a, b \in R.$$

Ring with unity. There is an element 1_R such that

$$1_R a = a 1_R = a.$$

For most of this course, our default examples are commutative rings with unity.

Definition: Units

Let R be a ring with unity.

An element $u \in R$ is a **unit** if there exists $v \in R$ such that

$$uv = vu = 1_R.$$

The units form a group:

$$R^\times.$$

Examples:

$$\mathbb{Z}^\times = \{\pm 1\}, \qquad \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}.$$

Definition: Fields

Definition. A **field** is a commutative ring with unity $1 \neq 0$ in which every nonzero element is a unit.

Examples:

$$\mathbb{Q}, \qquad \mathbb{R}, \qquad \mathbb{C}, \qquad \mathbb{F}_p = \mathbb{Z}_p.$$

Non-example:

$$\mathbb{Z}$$

is not a field, because 2 has no inverse in $\mathbb{Z}$.

Definition: Zero Divisors

Definition. A nonzero element $a \in R$ is a **zero divisor** if there exists nonzero $b \in R$ such that

$$ab = 0.$$

Example in $\mathbb{Z}_6$:

$$\bar{2} \cdot \bar{3} = \bar{0}.$$

So $\mathbb{Z}_6$ has zero divisors.

Definition: Integral Domains

A ring has **no zero divisors** if

$$ab = 0 \quad \Longrightarrow \quad a = 0 \text{ or } b = 0.$$

A commutative ring with unity $1 \neq 0$ and no zero divisors is an **integral domain**.

Examples:

$$\mathbb{Z}, \qquad F, \qquad F[x], \qquad F[x_1, \ldots, x_n], \qquad F[t, t^{-1}].$$

Example: More Zero Divisors

Product rings usually have zero divisors:

$$(1,0)(0,1) = (0,0) \quad \text{in } R \times S.$$

Matrix rings have zero divisors:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Quotient rings can have nilpotents:

$$\bar{x}^2 = 0 \quad \text{in } F[x]/(x^2).$$

Definition: Ring Homomorphisms

Let R, S be rings.

Definition. A map $\varphi : R \to S$ is a **ring homomorphism** if

$$\varphi(a + b) = \varphi(a) + \varphi(b),$$

and

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Modern convention often also requires

$$\varphi(1_R) = 1_S.$$

Proposition: Kernels Are Ideals

Let $\varphi : R \to S$ be a ring homomorphism. Then

$$\ker \varphi = \{r \in R : \varphi(r) = 0\}$$

is an ideal of R.

Example:

$$\pi : \mathbb{Z} \to \mathbb{Z}_n, \qquad a \mapsto \bar{a}, \qquad \ker \pi = n\mathbb{Z}.$$

This is the guiding model for quotient rings:

$$\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}.$$

Proposition: Point Evaluation of Functions

Let

$$\mathcal{F}(\mathbb{R}, \mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}.$$

Use pointwise operations:

$$(f + g)(x) = f(x) + g(x), \qquad (fg)(x) = f(x)g(x).$$

For each $a \in \mathbb{R}$, the map

$$\mathrm{ev}_a : \mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}, \qquad f \mapsto f(a).$$

is a ring homomorphism.

Example: Additive Isomorphism Need Not Preserve Multiplication

As abelian groups,

$$\mathbb{Z} \simeq 2\mathbb{Z}$$

by

$$\phi(x) = 2x.$$

But this is not a ring homomorphism:

$$\phi(xy) = 2xy, \qquad \phi(x)\phi(y) = 4xy.$$

A ring homomorphism must preserve both addition and multiplication.

Part II

Ideals and Quotient Rings

Example: Historical Motivation for Ideals

Kummer introduced **ideal numbers** while studying Fermat's Last Theorem.

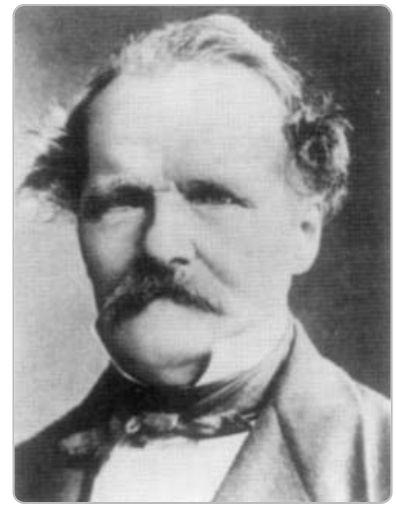
The obstruction was failure of unique factorization in some rings of algebraic integers.

Dedekind later replaced ideal numbers by **ideals**:

> subsets that behave like generalized multiples.

For us today:

> ideals are the right kernels for ring homomorphisms.



Ernst Eduard Kummer

Definition: Ideals

Let R be a commutative ring.

Definition. An **ideal** $I \subseteq R$ is a subset such that:

1. I is an additive subgroup of $(R, +)$;
2. for every $r \in R$ and every $a \in I$,

$$ra \in I.$$

If $I \neq R$, then I is a **proper ideal**.

Slogan:

$$\boxed{\text{ideals are kernels of ring homomorphisms.}}$$

Definition: Principal Ideals

Let R be a commutative ring and $a \in R$.

The **principal ideal generated by a** is

$$(a) = Ra = \{ra : r \in R\}.$$

Examples:

$$(n) = n\mathbb{Z} \subset \mathbb{Z}, \qquad (x - a) \subset F[x].$$

This notation also appears inside quotient rings such as $\mathbb{Z}_n$.

Whenever I is an ideal, we can form the quotient ring R/I.

Definition: Principal Ideal Domains

Let D be an integral domain.

A **principal ideal domain**, or **PID**, is an integral domain in which every ideal is principal.

That is, for every ideal $I \subseteq D$, there exists $a \in D$ such that

$$I = (a).$$

Examples:

$$\mathbb{Z}, \qquad F[x].$$

A typical non-example is

$$F[x, y],$$

where the ideal (x, y) is not principal.

Definition: Quotient Rings

Let $I \subseteq R$ be an ideal.

The quotient ring R/I is the set of cosets

$$r + I = \{r + i : i \in I\}.$$

Addition and multiplication are defined by

$$(r + I) + (s + I) = (r + s) + I,$$

$$(r + I)(s + I) = rs + I.$$

The quotient map

$$\pi : R \to R/I, \qquad r \mapsto r + I$$

is a ring homomorphism with $\ker \pi = I$.

Example: Quotient Rings

For $n \geq 1$,

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$$

The coset $a + n\mathbb{Z}$ corresponds to $\bar{a}$.

In polynomial rings,

$$F[x]/(x - a) \simeq F$$

by evaluation at a.

Proposition: Ideals in $\mathbb{Z}_n$

Ideals of $\mathbb{Z}_n$ correspond to divisors of n.

For $d \mid n$,

$$(d) = d\mathbb{Z}_n = \{\bar{0}, \bar{d}, \overline{2d}, \dots\}.$$

Every ideal of $\mathbb{Z}_n$ has this form.

The larger d is, the smaller (d) is.

Example: Ideals of $\mathbb{Z}_{12}$

The divisors of 12 are

$$1, \quad 2, \quad 3, \quad 4, \quad 6, \quad 12.$$

So the ideals are

$$(1), \quad (2), \quad (3), \quad (4), \quad (6), \quad (12).$$

Question:

$$\boxed{\text{Which of these are maximal? Which are prime?}}$$

Definition: Maximal Ideals

Let R be a commutative ring with unity.

An ideal $\mathfrak{m} \subsetneq R$ is **maximal** if there is no ideal I with

$$\mathfrak{m} \subsetneq I \subsetneq R.$$

Key test:

$$\boxed{\mathfrak{m} \text{ is maximal} \iff R/\mathfrak{m} \text{ is a field.}}$$

Definition: Prime Ideals

Let R be a commutative ring with unity.

An ideal $\mathfrak{p} \subsetneq R$ is **prime** if

$$ab \in \mathfrak{p} \quad \Longrightarrow \quad a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}.$$

Key test:

$$\boxed{\mathfrak{p} \text{ is prime} \quad \Longleftrightarrow \quad R/\mathfrak{p} \text{ is an integral domain.}}$$

Always:

$$\text{maximal} \Longrightarrow \text{prime}.$$

Example: Maximal Ideals in $\mathbb{Z}_{12}$

In $\mathbb{Z}_{12}$:

$$(2) \quad \text{and} \quad (3)$$

are maximal.

Indeed,

$$\mathbb{Z}_{12}/(2) \simeq \mathbb{Z}_2, \qquad \mathbb{Z}_{12}/(3) \simeq \mathbb{Z}_3.$$

They are also prime.

In general:

$$(d) \subset \mathbb{Z}_n \text{ is maximal} \quad \iff \quad n/d \text{ is prime.}$$

Proposition: Ideals in $F[x]$

For $a \in F$,

$$(x - a) \subset F[x]$$

is maximal because

$$F[x]/(x - a) \simeq F.$$

More generally, if $p(x) \in F[x]$ is irreducible, then

$$(p(x))$$

is maximal.

Example: Prime But Not Maximal

In a commutative ring with unity:

$$\text{maximal} \implies \text{prime}.$$

But prime need not imply maximal.

Example:

$$(x) \subset F[x, y].$$

Since

$$F[x, y]/(x) \simeq F[y],$$

(x) is prime but not maximal.

Example: Point Ideals in $F[x, y]$

For a point $(a, b) \in F^2$,

$$\mathfrak{m}_{(a,b)} = (x - a, y - b).$$

This is maximal because

$$F[x, y]/(x - a, y - b) \simeq F.$$

Geometric meaning:

$$(x - a, y - b) = \text{polynomials vanishing at } (a, b).$$

Definition: Radical of an Ideal

Let $I \subseteq R$ be an ideal in a commutative ring.

The **radical** of I is

$$\sqrt{I} = \{r \in R : r^n \in I \text{ for some } n \geq 1\}.$$

If $\sqrt{I} = I$, then I is a **radical ideal**.

The radical $\sqrt{I}$ is again an ideal.

Definition: Nilradical

The radical of the zero ideal is the **nilradical**:

$$\sqrt{(0)} = \{r \in R : r^n = 0 \text{ for some } n \geq 1\}.$$

It is the set of nilpotent elements of R.

Example: Radical Ideals

In $F[x]$:

$$\sqrt{((x-a)^m)} = (x-a).$$

In $F[x, y]$:

$$\sqrt{(x^2, y)} = (x, y).$$

Radical removes repeated or nilpotent behavior.

Example: Radical in $\mathbb{Z}_{12}$

In $\mathbb{Z}_{12}$,

$$\sqrt{(4)} = (2).$$

Reason:

$$\bar{2}^2 = \bar{4} \in (4),$$

so $\bar{2} \in \sqrt{(4)}$.

This is another way nilpotent-like behavior appears in quotient rings.

Part III

Polynomial Rings

Definition: Polynomial Rings

Let R be a commutative ring with unity.

The polynomial ring over R is

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_i \in R\}.$$

The symbol x is an **indeterminate**, not an element of R.

The inclusion $R \to R[x]$ sends r to the constant polynomial r.

Definition: Formal Polynomial Viewpoint

A polynomial can be modeled as a formal sum

$$\sum_{i=0}^{\infty} a_i x^i$$

where all but finitely many a_i are zero.

This avoids ambiguity:

$$1 + x = 1 + x + 0x^2 = 1 + x + 0x^2 + 0x^3 + \cdots .$$

Definition: Addition in $R[x]$

Add coefficients:

$$(a_0 + a_1x + \cdots) + (b_0 + b_1x + \cdots)$$

$$= (a_0 + b_0) + (a_1 + b_1)x + \cdots.$$

Example in $\mathbb{Z}_5[x]$:

$$(3x^2 + 4x + 1) + (4x^2 + 2) = 2x^2 + 4x + 3.$$

Definition: Multiplication in $R[x]$

Let

$$f = \sum_{i=0}^{m} a_i x^i, \qquad g = \sum_{j=0}^{n} b_j x^j.$$

The product is

$$fg = \sum_{k=0}^{m+n} c_k x^k,$$

where

$$c_k = \sum_{i+j=k} a_i b_j.$$

This is the usual distributive multiplication:

$$(a_i x^i)(b_j x^j) = a_i b_j x^{i+j}.$$

Example: Multiplication Depends on R

Multiply as usual, using coefficients in F:

$$(x+1)(x^2+2) = x^3 + x^2 + 2x + 2.$$

In $\mathbb{Z}_2[x]$:

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1.$$

The coefficient ring matters.

Lemma: Degree over Domains

Let D be an integral domain.

For a nonzero polynomial

$$f(x) = a_n x^n + \cdots + a_1 x + a_0, \qquad a_n \neq 0,$$

the **degree** is

$$\deg f = n.$$

If $f, g \in D[x]$ are nonzero, then

$$\deg(fg) = \deg f + \deg g.$$

Proposition: Polynomial Rings Preserve Domains

Let D be an integral domain.

Then $D[x]$ is an integral domain.

Indeed, if $0 \neq f, g \in D[x]$, then

$$\deg(fg) = \deg f + \deg g.$$

So $fg \neq 0$.

$$\boxed{D[x] \text{ has no zero divisors.}}$$

Proposition: Units in $F[x]$

Let F be a field.

The units are exactly the nonzero constants:

$$F[x]^\times = F^\times.$$

Indeed, if $f(x)g(x) = 1$, then $\deg f + \deg g = 0$.

In particular, $F[x]$ is not a field, because x has no inverse.

Counterexample: Zero Divisors in $R[x]$

If the coefficient ring has zero divisors, then the polynomial ring does too.

In $\mathbb{Z}_6$:

$$\bar{2} \cdot \bar{3} = \bar{0}.$$

So in $\mathbb{Z}_6[x]$:

$$(2x + 2)(3x + 3) = 0.$$

The good behavior of $F[x]$ comes from no zero divisors in F.

Definition: Multivariable Polynomial Rings

For a commutative ring with unity R,

$$R[x_1, \ldots, x_n]$$

is the ring of finite R-linear combinations of monomials

$$x_1^{a_1} \cdots x_n^{a_n}.$$

For example,

$$R[x, y] = (R[x])[y].$$

Part IV

Algebras, Free Algebras, and Evaluation

Definition: R-Modules

Let R be a commutative ring with unity.

An **R-module** is an abelian group M with scalar multiplication

$$R \times M \to M, \qquad (r, m) \mapsto rm,$$

such that

$$(r+s)m = rm + sm, \quad r(m+n) = rm + rn,$$

$$(rs)m = r(sm), \qquad 1m = m.$$

Examples: vector spaces, R^n, and ideals $I \subseteq R$.

Definition: R-Algebras

Let R be a commutative ring with unity.

A **commutative R-algebra** is a commutative ring A with unity together with a unital ring homomorphism

$$R \to A.$$

Convention: after choosing this map, we write elements of R as scalars in A.

Then A is an R-module by

$$r \cdot a = ra.$$

Examples:

$$R, \qquad R[x], \qquad R[x_1, \ldots, x_n], \qquad F \leq E.$$

Definition: R-Algebra Homomorphisms

Let A and B be commutative R-algebras.

An **R-algebra homomorphism** is a unital ring homomorphism $\varphi : A \to B$ such that

$$\varphi(r) = r \qquad (r \in R),$$

using the scalar convention in both A and B.

Equivalently, φ fixes the scalars from R.

Theorem: Universal Property of Polynomial Algebras

Let $R[x_s \mid s \in S]$ be the polynomial ring whose variables are indexed by S.

Its elements are finite R-linear combinations of finite monomials

$$r\, x_{s_1}^{e_1} \cdots x_{s_m}^{e_m}.$$

Let

$$i : S \to R[x_s \mid s \in S], \qquad s \mapsto x_s.$$

For every commutative R-algebra A, precomposition with i gives a bijection

$$i^* : \mathrm{Hom}_{R\text{-alg}}(R[x_s \mid s \in S], A) \longrightarrow \mathrm{Map}(S, A).$$

Corollary: Polynomial Algebras Are Free

The universal property says:

every set map $a : S \to A$ extends uniquely to an R-algebra homomorphism

$$\Phi_a : R[x_s \mid s \in S] \to A.$$

This is what it means to say:

$$R[x_s \mid s \in S]$$

is the **free commutative R-algebra on the set S**.

In particular, $R[x]$ is free on one generator, and $R[x_1, \ldots, x_n]$ is free on n generators.

Proof: Polynomial Rings Are Free

Given a set map $a : S \to A$, define Φ_a by

$$\Phi_a(x_s) = a(s), \qquad \Phi_a(r) = r.$$

On a monomial,

$$\Phi_a\left(r\, x_{s_1}^{e_1} \cdots x_{s_m}^{e_m}\right) = r\, a(s_1)^{e_1} \cdots a(s_m)^{e_m}.$$

Extend by finite sums. This gives an R-algebra homomorphism because multiplication of monomials corresponds to adding exponents.

Uniqueness: every polynomial is built from scalars, addition, multiplication, and the generators x_s.

Definition: Evaluation Homomorphism

Let A be a commutative R-algebra and let $a : S \to A$ be a set map.

The unique homomorphism

$$\mathrm{ev}_a : R[x_s \mid s \in S] \to A, \qquad x_s \mapsto a(s)$$

is called the **evaluation homomorphism** at a.

If $S = \{1, \ldots, n\}$, then $a : S \to A$ is the same data as a tuple

$$(a_1, \ldots, a_n) \in A^n,$$

and

$$\mathrm{ev}_a : R[x_1, \ldots, x_n] \to A, \qquad x_i \mapsto a_i.$$

Definition: Polynomial Functions from Evaluation

Let A be a commutative R-algebra.

For $f \in R[x_1, \ldots, x_n]$, the **polynomial function defined by f on A** is

$$f_A : A^n \to A, \qquad (a_1, \ldots, a_n) \mapsto \mathrm{ev}_{(a_1,\ldots,a_n)}(f).$$

In one variable, if $f = r_0 + r_1 x + \cdots + r_d x^d$, then

$$\mathrm{ev}_a(f) = r_0 + r_1 a + \cdots + r_d a^d.$$

Proposition: Evaluation Preserves Operations

Let A be a commutative R-algebra and let $a : S \to A$.

For $f, g \in R[x_s \mid s \in S]$,

$$\mathrm{ev}_a(f + g) = \mathrm{ev}_a(f) + \mathrm{ev}_a(g),$$

$$\mathrm{ev}_a(fg) = \mathrm{ev}_a(f)\,\mathrm{ev}_a(g).$$

This is not an extra calculation: it is exactly the statement that $\mathbf{ev}_a$ is an R-algebra homomorphism.

Example: A Point Ideal in Two Variables

Take $R = A = F$ and the point $(2, 3) \in F^2$.

The evaluation map is

$$\mathrm{ev}_{(2,3)} : F[x, y] \to F, \qquad x \mapsto 2, \quad y \mapsto 3.$$

Its kernel is the point ideal

$$(x - 2, y - 3).$$

This is the multivariable analogue of $\ker(\mathrm{ev}_a) = (x - a)$.

Part V

Division, Kernels, and Root Bounds

Definition: Zeros

Let $F \leq E$, let $\alpha \in E$, and let $f \in F[x]$.

The element α is a **zero** of f if

$$\mathrm{ev}_\alpha(f) = 0.$$

Equivalently, if $f_E : E \to E$ is the polynomial function defined by f, then

$$f_E(\alpha) = 0.$$

Example: Computing Zeros

In $\mathbb{Q}[x]$, let

$$f = x^2 + x - 6.$$

Then

$$f_{\mathbb{R}}(2) = 2^2 + 2 - 6 = 0.$$

Thus 2 is a zero of f over $\mathbb{R}$.

$$x^2 + 1 \in \mathbb{Q}[x]$$

has zero i over $\mathbb{C}$, but not over $\mathbb{Q}$.

Theorem: Division Algorithm

Let R be a commutative ring with unity.

If $g \in R[x]$ has leading coefficient a unit, then for every $f \in R[x]$ there exist unique $q, r \in R[x]$ such that

$$f = qg + r, \qquad r = 0 \text{ or } \deg r < \deg g.$$

In particular, division by any **monic** polynomial works over any commutative ring.

Proof: Division by a Monic Polynomial

Let $g = x^d + \text{lower terms}$.

If $\deg f = m \geq d$ and the leading term of f is cx^m, subtract

$$cx^{m-d}g.$$

This cancels the leading term of f and lowers the degree.

Repeating gives $f = qg + r$ with $\deg r < d$.

Uniqueness follows because multiplying by a monic polynomial raises degree by d.

Theorem: Kernel of Evaluation

Let R be a commutative ring with unity and let $a \in R$.

$$\mathrm{ev}_a : R[x] \to R$$

Then

$$\boxed{\ker(\mathrm{ev}_a) = (x - a).}$$

Proof: Kernel of Evaluation

By division by the monic polynomial $x - a$, write

$$f = q(x)(x - a) + r$$

with $r \in R$.

Evaluating at a gives

$$f(a) = q(a)(a - a) + r = r.$$

So $f \in \ker(\mathrm{ev}_a)$ if and only if $r = 0$.

This is exactly $f \in (x - a)$.

Corollary: Factor Theorem

Let R be a commutative ring with unity, $a \in R$, and $f \in R[x]$.

Then

$$f(a) = 0 \iff f \in (x - a).$$

$$\boxed{a \text{ is a zero of } f \iff x - a \text{ divides } f.}$$

Lemma: Root Ideals over a Field

Let F be a field and let $a_i \neq a_j$ in F.

Then

$$(x - a_i) + (x - a_j) = F[x].$$

Indeed,

$$(x - a_i) - (x - a_j) = a_j - a_i \in F^\times.$$

So $1 \in (x - a_i) + (x - a_j)$.

Lemma: Comaximal Ideals

Let I, J be ideals in a commutative ring R.

If $I + J = R$, then

$$I \cap J = IJ.$$

More generally, if $I_1, \ldots, I_k$ are pairwise comaximal, then

$$\bigcap_{i=1}^{k} I_i = \prod_{i=1}^{k} I_i.$$

Proof: Comaximal Ideals

It is always true that

$$IJ \subseteq I \cap J.$$

For the reverse inclusion, choose $u \in I$ and $v \in J$ with

$$u + v = 1.$$

If $x \in I \cap J$, then

$$x = x(u + v) = xu + xv.$$

Here $xu \in JI = IJ$ and $xv \in IJ$, so $x \in IJ$.

Proof: Pairwise Comaximal Case

Assume $I_1, \ldots, I_k$ are pairwise comaximal.

By induction, set

$$P = \prod_{i=1}^{k-1} I_i = \bigcap_{i=1}^{k-1} I_i.$$

For each $i < k$, choose

$$u_i \in I_i, \qquad v_i \in I_k, \qquad u_i + v_i = 1.$$

Expanding $\prod_{i<k}(u_i + v_i) = 1$ shows

$$1 \in P + I_k.$$

Thus

Theorem: Root Bound over a Field

Let F be a field and let $0 \neq f \in F[x]$ have degree n.

Then f has at most n zeros in F.

Ideal translation:

$$a \text{ is a zero of } f \iff (f) \subseteq (x - a).$$

Proof: Root Bound over a Field

Suppose $a_1, \ldots, a_k$ are distinct zeros of f.

Then

$$f \in \bigcap_{i=1}^{k} (x - a_i).$$

The ideals $(x - a_i)$ are pairwise comaximal, so

$$\bigcap_{i=1}^{k} (x - a_i) = \prod_{i=1}^{k} (x - a_i) = \left(\prod_{i=1}^{k} (x - a_i) \right).$$

Hence $\prod_i (x - a_i) \mid f$, so $k \leq \deg f$.

Definition: Fraction Field

Let D be an integral domain.

The **fraction field** of D is

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

where

$$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad ad = bc.$$

There is an injective ring homomorphism

$$D \hookrightarrow \mathrm{Frac}(D), \qquad a \mapsto \frac{a}{1}.$$

Example: Fraction Fields

The standard example is

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

If F is a field, then

$$\mathbf{Frac}(F[x]) = F(x),$$

the field of rational functions.

This construction is possible because D has no zero divisors.

Corollary: Root Bound over Domains

Let D be an integral domain and let $0 \neq f \in D[x]$ have degree n.

Then f has at most n zeros in D.

Proof: embed D into its fraction field $K = \mathbf{Frac}(D)$ and view f in $K[x]$.

The field theorem applies in $K[x]$, so the same bound holds for zeros lying in D.

Counterexample: Rings with Zero Divisors

In $\mathbb{Z}_{12}$,

$$x^2 - 5x + 6 = (x-2)(x-3).$$

But this degree 2 polynomial has four zeros:

$$2, \quad 3, \quad 6, \quad 11.$$

In $\mathbb{Z}_6$,

$$x^2 - x = x(x-1).$$

The roots are

$$0, \quad 1, \quad 3, \quad 4.$$

Both examples have degree 2 and four roots.

Part VI

Local, Laurent, and Simple Rings

Definition: Local Rings

Definition. A commutative ring with unity R is **local** if it has a unique maximal ideal.

The main example today:

$$F[x]_{(x-a)} = \left\{ \frac{f(x)}{g(x)} : g(a) \neq 0 \right\}.$$

Think:

$$\text{rational functions defined at } a.$$

Proposition: The Maximal Ideal of $F[x]_{(x-a)}$

The unique maximal ideal is

$$\mathfrak{m}_a = \left\{ \frac{f(x)}{g(x)} : f(a) = 0,\ g(a) \neq 0 \right\}.$$

So

$$\mathfrak{m}_a = \text{functions vanishing at } a.$$

This is the local version of the ideal $(x - a) \subset F[x]$.

Definition: Valuation as Order of Vanishing

For $0 \neq f \in F[x]$, define

$$v_a(f) = \max\{m : (x-a)^m \mid f(x)\}.$$

We also set

$$v_a(0) = \infty.$$

Examples:

$$v_0(x^3(x+1)) = 3,$$

$$v_2((x-2)^4(x+5)) = 4.$$

Proposition: Valuation Rules

The order of vanishing satisfies:

$$v_a(fg) = v_a(f) + v_a(g),$$

and

$$v_a(f+g) \geq \min\{v_a(f), v_a(g)\}.$$

This introduces valuation language.

Definition: Laurent Polynomial Ring

The **Laurent polynomial ring** is

$$F[t, t^{-1}] = \left\{ \sum_{i=m}^{n} a_i t^i : m, n \in \mathbb{Z},\ a_i \in F \right\}.$$

It is obtained from $F[t]$ by making t invertible.

So it contains

$$t^{-1}, t^{-2}, t^{-3}, \ldots .$$

Proposition: Units in $F[t, t^{-1}]$

The units are exactly

$$F[t, t^{-1}]^{\times} = \{ct^n : c \in F^{\times},\ n \in \mathbb{Z}\}.$$

In particular, t is a unit.

So

$$(t) = F[t, t^{-1}].$$

Example: Maximal Ideals in $F[t, t^{-1}]$

For $a \in F^{\times}$, evaluation at a gives

$$F[t, t^{-1}] \to F, \qquad t \mapsto a.$$

Its kernel is

$$(t - a).$$

But $a = 0$ is not allowed, because t^{-1} cannot be evaluated at 0.

Example: Valuation on Laurent Polynomials

For a nonzero Laurent polynomial, define v_t as the lowest exponent of t, and set $v_t(0) = \infty$.

Example:

$$v_t(3t^{-2} + 5 + t^4) = -2.$$

Negative valuation means a pole at $t = 0$.

Definition: Simple Rings

A nonzero ring R is **simple** if its only two-sided ideals are

$$\{0\} \quad \text{and} \quad R.$$

Analogy:

$$\text{simple group} \quad \leftrightarrow \quad \text{simple ring}.$$

Example: Simple Rings

If F is a field, then F is a simple ring.

In commutative rings with unity:

$$R \text{ simple} \iff R \text{ is a field.}$$

Noncommutative example:

$$M_n(F)$$

is simple as a ring, but not a field when $n \geq 2$.