MAT205: Abstract Algebra II

Fraction Fields, Localization, and Root Bounds

Ma, Jia-Jun - Xiamen University Malaysia

Part I

Division, Evaluation Kernels, and Root Bounds

Definition: Zeros

Let F be a field, let E be a field with $F \subseteq E$, and let $\alpha \in E$, $f \in F[x]$.

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.

Over a field, every nonzero leading coefficient is a unit, so division by any nonzero polynomial works.

Proof: Division by a Unit Leading Coefficient

Let $g = ux^d + \mathrm{lower\ terms}$ with $u \in R^\times$.

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

$$cu^{-1}x^{m-d}g.$$

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 g 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

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

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

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.

Definition. I and J are **comaximal** if $I + J = R$.

Lemma. If $I + J = R$, then

$$I \cap J = IJ.$$

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

$$1 \in P + I_k.$$

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

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:

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

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 $k \leq \deg f$.

Part II

Fraction Fields and Localization

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

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

Operations are defined by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

There is an injective ring homomorphism

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

Example: Fraction Fields

The standard example is

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

If F is a field, then

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

the field of rational functions.

This construction is possible because D has no zero divisors.

Fraction Fields as Localization

Let D be an integral domain and let

$$S = D \setminus \{0\}.$$

Then

$$\mathrm{Frac}(D) = S^{-1}D.$$

That is, the field of fractions is obtained by making every nonzero element of D invertible.

Definition: Multiplicative Set

Let R be a commutative ring with unity.

Definition. A subset $S \subseteq R$ is a **multiplicative set** if:

1. $1 \in S$;
2. for all $s, t \in S$, the product $st \in S$.

Examples.

- $S = D \setminus \{0\}$ for D an integral domain.
- $S = \{1, f, f^2, f^3, \dots\}$ for any $f \in R$.
- $S = R \setminus \mathfrak{p}$ for a prime ideal $\mathfrak{p} \subset R$.

Non-example. $R \setminus \{0\}$ for $R = \mathbb{Z}_6$ is **not** multiplicative: $\bar{2} \cdot \bar{3} = \bar{0}$.

Definition: Localization

Let R be a commutative ring and let $S \subseteq R$ be a multiplicative set.

The localization $S^{-1}R$ consists of formal fractions

$$\frac{r}{s} \qquad (r \in R,\ s \in S),$$

with the usual fraction rules.

Every element of S becomes a unit in $S^{-1}R$.

Universal Property of Localization

Let $\varphi : R \to A$ be a ring homomorphism such that $\varphi(s) \in A^\times$ for every $s \in S$.

Theorem. There exists a **unique** ring homomorphism

$$\tilde{\varphi} : S^{-1}R \to A, \qquad \tilde{\varphi}(r/s) = \varphi(r)\,\varphi(s)^{-1},$$

with $\tilde{\varphi} \circ \iota = \varphi$.

Interpretation. $\iota : R \to S^{-1}R$ is **initial** among ring homs from R that send S to units: $S^{-1}R$ is the smallest ring obtained from R by inverting S.

Universal Property of the Fraction Field

Let D be an integral domain and let $\varphi : D \to K$ be an **injective** ring homomorphism into a field K.

Theorem. φ extends uniquely to a ring homomorphism

$$\tilde{\varphi} : \mathrm{Frac}(D) \to K, \qquad \tilde{\varphi}(a/b) = \varphi(a)\,\varphi(b)^{-1}.$$

This is the case $S = D \setminus \{0\}$ of the previous slide; injectivity ensures $\varphi(S) \subseteq K^{\times}$.

$\mathrm{Frac}(D)$ is the **smallest** field containing D.

Examples of Localization

Ring	Multiplicative set	Localization
$\mathbb{Z}$	$\mathbb{Z} \setminus \{0\}$	$\mathbb{Q}$
$\mathbb{Z}$	$\{1, p, p^2, \ldots\}$	$\mathbb{Z}[1/p]$
$F[t]$	$\{1, t, t^2, \ldots\}$	$F[t, t^{-1}]$
$F[x]$	$\{g : g(a) \neq 0\}$	$F[x]_{(x-a)}$

Localization remembers which denominators are allowed.

Definition: Extension and Contraction

Localization map: $\iota : R \to S^{-1}R$, $r \mapsto r/1$.

Extension. For an ideal $I \subseteq R$:

$$S^{-1}I = \{a/s : a \in I,\ s \in S\} \subseteq S^{-1}R.$$

Contraction. For an ideal $J \subseteq S^{-1}R$:

$$\iota^{-1}(J) = \{r \in R : r/1 \in J\} \subseteq R.$$

Both are ideals.

Proposition: When Extension Collapses

Proposition. $S^{-1}I = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.

($\Leftarrow$): if $a \in I \cap S$, then $1 = a/a \in S^{-1}I$.

($\Rightarrow$): if $1/1 = a/s$ with $a \in I$, $s \in S$, the equivalence relation gives $u \in S$ with $us = ua$. Then $ua \in I \cap S$.

Slogan. Ideals meeting S get killed; ideals disjoint from S survive.

Theorem: Prime Ideal Correspondence

Extension and contraction give mutually inverse bijections

$$\{\,\mathfrak{p} \subset R \text{ prime},\ \mathfrak{p} \cap S = \emptyset\,\} \longleftrightarrow \{\,\text{primes of } S^{-1}R\,\}.$$

Forward: $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$. Inverse: $\mathfrak{q} \mapsto \iota^{-1}(\mathfrak{q})$.

Order-preserving: $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \iff S^{-1}\mathfrak{p}_1 \subseteq S^{-1}\mathfrak{p}_2$.

Maximal among survivors on the left $\leftrightarrow$ maximal on the right.

Proof: Prime Correspondence

Extension preserves primality. Suppose $(a/s)(b/t) \in S^{-1}\mathfrak{p}$. Write as c/r with $c \in \mathfrak{p}$, $r \in S$. The equivalence relation gives $w \in S$ with $wr \cdot ab = wc \cdot st$ in R.

The right side lies in $\mathfrak{p}$ (since $c \in \mathfrak{p}$), so $wr \cdot ab \in \mathfrak{p}$. But $wr \in S$ and $\mathfrak{p} \cap S = \emptyset$, so $wr \notin \mathfrak{p}$.

Primality forces $ab \in \mathfrak{p}$, hence $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Mutual inverses. Routine equivalence-class checks: $\iota^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$ and $S^{-1}(\iota^{-1}\mathfrak{q}) = \mathfrak{q}$.

Geometric Reading via Spec

Prime spectrum.

$$\mathrm{Spec}(R) = \{\mathfrak{p} \subset R : \mathfrak{p} \text{ prime}\}.$$

Prime correspondence says

$$\mathrm{Spec}(S^{-1}R) \;\cong\; \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \cap S = \emptyset\}.$$

Slogan. Localization **deletes** the primes that meet S and keeps the rest.

Examples.

- $\mathrm{Spec}(\mathbb{Z}_{(p)}) = \{(0), (p)\}$ – two points, **local**.
- $\mathrm{Spec}(\mathbb{Z}[1/p]) = \mathrm{Spec}(\mathbb{Z}) \setminus \{(p)\}$ – all primes except (p), **not local**.

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 $K = \mathrm{Frac}(D)$ 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 III

Local Rings and Laurent Polynomials

Definition: Local Rings

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

One main example today:

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

It consists of rational functions defined at a.

Example: $\mathbb{Z}$ Localized at p

Terminology. For a prime $\mathfrak{p} \subset R$, the **localization of R at $\mathfrak{p}$** is $R_{\mathfrak{p}} := S^{-1}R$ with $S = R \setminus \mathfrak{p}$.

Fix a prime number p. Apply with $R = \mathbb{Z}$, $\mathfrak{p} = (p)$, so $S = \mathbb{Z} \setminus (p) = \{n \in \mathbb{Z} : p \nmid n\}$:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}.$$

We invert every integer not divisible by p.

But we do **not** invert p.

The Maximal Ideal of $\mathbb{Z}_{(p)}$

The units are exactly

$$\left(\mathbb{Z}_{(p)}\right)^{\times} = \left\{\frac{a}{b} : p \nmid a,\ p \nmid b\right\}.$$

The non-units are exactly

$$p\mathbb{Z}_{(p)} = \left\{\frac{a}{b} : p \mid a,\ p \nmid b\right\}.$$

Thus $\mathbb{Z}_{(p)}$ is local, with unique maximal ideal $p\mathbb{Z}_{(p)}$.

$\mathbb{Z}_{(p)}$ vs. $\mathbb{Z}[1/p]$

The notation is easy to confuse.

Localizing **at** (p) means

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : p \nmid b \right\}.$$

Inverting p gives a different ring:

$$\mathbb{Z}[1/p] = \left\{ \frac{a}{p^n} : a \in \mathbb{Z},\ n \geq 0 \right\}.$$

Among ordinary primes, only p remains non-invertible in $\mathbb{Z}_{(p)}$.

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

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

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

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

Ideals After Inverting t

Think of

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

Every ideal of $F[t,t^{-1}]$ comes from an ideal of $F[t]$ after t is made invertible.

So factors of t no longer matter:

$$(t^k f(t)) = (f(t)) \quad \text{in } F[t,t^{-1}].$$

Principal Ideals in $F[t, t^{-1}]$

Since $F[t]$ is a PID, $F[t, t^{-1}]$ is also a PID.

Every nonzero ideal has the form

$$(f(t))$$

where $f(t) \in F[t]$ and $f(0) \neq 0$.

Example:

$$(t^3(t-2)(t^2+1)) = ((t-2)(t^2+1)).$$

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

The maximal ideals are

$$(q(t)),$$

where $q(t) \in F[t]$ is irreducible and $q(0) \neq 0$.

The condition $q(0) \neq 0$ says that q is not a multiple of t.

Equivalently, these are the maximal ideals of $F[t]$ that do not meet

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

Linear 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

$$(t - a).$$

So $(t - a)$ is maximal.

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

If F is algebraically closed, these are all maximal ideals.

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 $t = 0$.