Polynomial rings

Coefficients in a domain

Coefficients in a field

Abstract Algebra, Lecture 12

Polynomial rings

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Linköping, fall 2019

Lecture notes availabe at course homepage

http://courses.mai.liu.se/GU/TATA55/

Summary

1. Polynomial rings
   - Zero-divisors, nilpotents, units
   - Degree
   - Evaluation
2. Coefficients in a domain
   - Divisibility
   - Polynomial rings in several variables
3. Coefficients in a field
   - Division algorithm
   - $K[x]$ is a PID
   - GCD
   - Zeroes of polynomials and linear factors
   - Prime and maximal ideals in $K[x]$
   - Unique factorization
   - Ideal calculus in $K[x]$
   - Quotients

Summary

1. **Polynomial rings**
   - Zero-divisors, nilpotents, units
   - Degree
   - Evaluation
2. **Coefficients in a domain**
   - Divisibility
   - Polynomial rings in several variables
3. **Coefficients in a field**
   - Division algorithm
   - $K[x]$ is a PID
   - GCD
   - Zeroes of polynomials and linear factors
   - Prime and maximal ideals in $K[x]$
   - Unique factorization
   - Ideal calculus in $K[x]$
   - Quotients

Summary

1. **Polynomial rings**
   - Zero-divisors, nilpotents, units
   - Degree
   - Evaluation
2. **Coefficients in a domain**
   - Divisibility
   - Polynomial rings in several variables
3. **Coefficients in a field**

- Division algorithm
- $K[x]$ is a PID
- GCD
- Zeroes of polynomials and linear factors
- Prime and maximal ideals in $K[x]$
- Unique factorization
- Ideal calculus in $K[x]$
- Quotients

Definition

Let L be a unitary, commutative ring. The polynomial ring $L[x]$ is the set of all maps $c : \mathbb{N} \to L$ whose support

$$\mathrm{Supp}(c) = \{ n \in \mathbb{N} | c(n) \neq 0 \}$$

is finite. Two such maps are added component-wise, and multiplied using *Cauchy convolution*

$$(c * d)(n) = \sum_{i=0}^{n} c(i) d(n-i)$$

This makes $L[x]$ into a commutative, unitary ring; via the injection

$$L \ni \ell \mapsto (\mathbb{N} \ni n \mapsto \ell \in L)$$

one can regard L as a subring.

One usually uses the indeterminate x as a "placeholder" for the coefficients, so the map $c : \mathbb{N} \to L$ is displayed as

$$f(x) = \sum_{j=0}^{\infty} c(j)x^j,$$

where x^j can be thought of as the indicator function on $\{j\}$. The "Cauchy convolution" is then explained by the rule

$$x^i * x^j = x^{i+j}$$

and distributivity.

Example

Let $L = \mathbb{Z}$, and let $c : \mathbb{N} \to L$ be given by $c(0) = 2$, $c(1) = -3, c(2) = 1$, and $c(n) = 0$ for $n > 2$.
Let $d : \mathbb{N} \to L$ be given by $d(0) = -1$, $d(1) = 0, d(2) = 5$, and $d(n) = 0$ for $n > 2$.
The corresponding polynomials, and their product, are

$$(2 - 3x + 1x^2) * (-1 + 0x + 5x^2) = -2 + 3x + 9x^2 - 15x^3 + 5 * x^4$$

Theorem

$L[x]$ is an integral domain iff L is.

Proof.

If $ab = 0$ in L, then the same holds in $L[x]$.
If

$$0 = (a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_n b_m x^{n+m}$$

then $a_n b_m = 0$. □

Example

$\mathbb{Z}[x]$ is a domain, $\mathbb{Z}_6[x]$ is not.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Polynomial rings
Zero-divisors, nilpotents, units
Degree
Evaluation
Coefficients in a domain
Coefficients in a field

Theorem

$f = a_0 + a_1 x \cdots + a_n x^n \in L[x]$ is invertible iff a_0 is a unit in L and $a_1, \ldots, a_n$ are nilpotent in L.

Proof

We will make use of the fact (proved later) that

- nilpotent + nilpotent = nilpotent
- unit + nilpotent = unit

If a_0 unit, $a_1, \ldots, a_n$ nilpotent, then $r = a_1 x + \cdots + a_n x^n$ nilpotent, so $f = a + r$ unit.

Proof (cont)

Conversely, if $f = a_0 + a_1 x + \cdots + a_n x^n$ is a a unit, then there exists $g = b_0 + b_1 x + \cdots + b_m x^m$ with $fg = 1$, thus $a_0 b_0 = 1$, so a_0 and b_0 are units. We need to prove that $a_1, \ldots, a_n$ are nilpotent.
Since $fg = 1$, except for the constant coefficient, the coefficients of fg are zero, in particular

$$\begin{aligned} a_n b_m &= 0 \\ a_{n-1} b_m + a_n b_{m-1} &= 0 \\ a_{n-2} b_m + a_{n-1} b_{m-1} + a_n b_{m-2} &= 0 \\ &\vdots \\ a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 &= 0 \end{aligned}$$

Proof (cont)

Multiply the eqn

$$a_{n-1}b_m + a_n b_{m-1} = 0$$

by a_n to conclude that $a_n^2 b_{m-1} = 0$.
Multiply the eqn

$$a_{n-2}b_m + a_{n-1}b_{m-1} + a_n b_{m-2} = 0$$

by a_n^2 to conclude (using $a_n^2 b_{m-1} = 0$) that $a_n^3 b_{m-2} = 0$.
Continue until you reach $a_n^{m+1} b_0 = 0$. Since b_0 is a unit, $a_n^{m+1} = 0$, so a_n is nilpotent.
Now $f - a_n x^n$ is a unit, so repeat the previous procedure to conclude that a_{n-1} is nilpotent, and so on.

Lemma

If x, y are nilpotent, then so is $x + y$.

Proof.

Suppose that $x^n = y^n = 0$. Then

$$(x+y)^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} x^j y^{2n-j},$$

and either j or $2n - j$ are $\geq n$. □

Lemma

If x unit, y nilpotent, then $x-y$ (and $x+y$) is a unit.

Proof.

Assume $xx^{-1}=1$, $y^n=0$. Then

$$(1-y)(1+y+\cdots+y^{n-1}) = 1-y^n = 1,$$

so $x^{-1}(x-y) = x^{-1}(1-yx^{-1})$ has inverse

$$x^{-1}(1+(yx^{-1})+\cdots+(yx^{-1})^{n-1}),$$

hence $(x-y)$ has inverse

$$1+(yx^{-1})+\cdots+(yx^{-1})^{n-1}.$$

□

Definition

If $f = a_0 + a_1 x + \cdots + a_n x^n \in L[x]$, with $a_n \neq 0$, then the *degree* of f is

$$\deg f = \max(\mathrm{Supp}\,(f)) = n.$$

The degree of the zero polynomial is $-\infty$.
We define the

- *leading term* as $a_n x^n$,
- *leading monomial* as x^n,
- *leading coefficient* as a_n

Example

If $\mathbb{Z}[x] = 1 - 3x^4 + 17x^5$ then the degree is 5, the l.t. is $17x^5$, the l.c. is 17, and the l.m. is x^5.

Polynomial rings
Zero-divisors, nilpotents, units
Degree
Evaluation
Coefficients in a domain
Coefficients in a field

Theorem

Let $f, g \in L[x]$.

- $\deg(f+g) \le \max(\deg(f), \deg(g))$,
- $\deg(fg) \le \deg(f) + \deg(g$.

If L is a domain then

- $\deg(fg) = \deg(f) + \deg(g)$,
- $\mathrm{lt}(fg) = \mathrm{lt}(f)\mathrm{lt}(g)$

Example

In $\mathbb{Z}_4[x]$,

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

so the degree of products can drop in the presence of zero-divisors. In $\mathbb{Q}[x]$,

$$(2x^2+x+1) + (-2x^2 - x + 1) = 2,$$

so the degree of sums may drop even with field coefficients.

Definition

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in L[x]$. Let $u \in L$. We define the evaluation of f at u by

$$f(u) = a_0 + a_1 u + \cdots + a_n u^n \in L$$

Theorem

For $u \in L$, the map

$$\begin{aligned} \mathrm{ev}_u : L[x] &\to L \\ f(x) &\mapsto f(u) \end{aligned}$$

is a ring homomorphism.

Example

A fixed polynomial $f(x) \in L[x]$ defines a polynomial function

$$
\begin{aligned}
f : L &\to L \\
u &\mapsto f(u)
\end{aligned}
$$

That is an importan topic that we will only touch upon in this course. We note the following oddity: for polynomials in $\mathbb{Q}[x]$, different polynomials give rise to different functions $\mathbb{Q} \to \mathbb{Q}$. However, already for polynomials with field coefficients this need not hold. In $\mathbb{Z}_2[x]$, if $f(x) = (x^2 + x)g(x)$ for any $g(x) \in \mathbb{Z}_2[x]$, then

$$
\begin{aligned}
f([0]_2) &= ([0]_2^2 + [0]_2)(g([0]_2) = [0]_2 \\
f([1]_2) &= ([1]_2^2 + [1]_2)(g([1]_2) = [0]_2
\end{aligned}
$$

so infinitely many polynomials represent the constantly zero polynomial function.

Corollary

The set

$$I_u = \{ f(x) \in L[x] \,|\, f(u) = 0 \}$$

is an ideal in $L[x]$, *and*

$$\frac{L[x]}{I_u} \simeq L$$

The ideals containing I_u *are in bijection with the ideals of* L.

Recall:

Theorem

Suppos that L is a domain, and that $f = a_0 + a_1 x + \cdots + a_n x^n \in L[x]$.

1. *$L[x]$ is a domain*
2. *f is invertible iff a_0 is a unit and $\deg(f) = 0$.*

Definition

Let $f, g \in L[x]$.

1. We write $f|g$ if there exists $h \in L[x]$ such that $g = fh$
2. We say that f and g are associate, $f \sim g$, if $f|g$ and $g|h$
3. We say that f is irreducible if it lacks non-trivial divisors, i.e., any divisor of f is either associate to f or a unit
4. We say that f is prime if $f|gh$ implies that $f|g$ or $f|h$

Lemma

1. *$f|g$ iff $(f) \supseteq (g)$.*
2. *$f \sim g$ iff $f = cg$, with c a unit.*
3. *A non-trivial divisor g of f has degree $0 < \deg(g) < \deg(f)$.*
4. *A prime element is irreducible*

Proof.

1. Suppose that $g = fh$. Then $u \in (g) \implies u = gv = fhv \implies u \in (f)$. Conversely, if $(g) \subseteq (f)$ then $g \in (f)$, hence $f|g$.
2. If $f = cg$ with c a unit, then $g = c^{-1}f$. Conversely, if $f = ug$, $g = vf$ then $f = uvf$, so $f(1 - uv) = 0$, so (since we're in a domain) $uv = 1$, and u, v are units.
3. If $f = gh$ then $\deg(f) = \deg(g) + \deg(h)$; since units have degree zero and non-zero degree zeros are units, $\deg(g), \deg(h) > 0$. Hence $\deg(g), \deg(h) < \deg(f)$.
4. If $p = ab$ then $p|ab$ hence $p|a$, say; hence $\deg a = \deg p$ and $p \sim a$.

□

Definition

We put $L[x,y] = (L[x])[y]$.

To expound, $L[x]$ is a ring (a domain, even) so we can form polynomials with coeffiecients in it. An element

$$f(y) = a_0(x) + a_1(x)y + \cdots + a_n(x)y^n,$$

where

$$a_i(x) = \sum_{j=0}^{m_j} b_{i,jj}x^j,$$

is usually written in distributed form as

$$f(x,y) = \sum_{i,j} b_{i,j}x^i y^j,$$

and is the regarded as an element in the semigroup ring $L[\mathbb{N}^2]$.

Example

$$\begin{aligned}\mathbb{Q}[x][y] \ni f &= (5+13x) + (2-x^2)y + (11 - x + 13x^2 + 17x^3)y^2 \\ &= 5 + 13x + 2y - x^2y + 11y^2 - xy^2 + 13x^2y^2 + 17x^3y \in \mathbb{Q}[x,y]\end{aligned}$$

has support $1, y, y^2$ or $1, x, y, x^2y, y^2, xy^2, x^2y^2, x^3y$, depending on one's point of view.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Polynomial rings
Coefficients in a domain
Coefficients in a field
Division algorithm
$K[x]$ is a PID
GCD
Zeroes of polynomials and linear factors
Prime and maximal ideals in $K[x]$
Unique factorization
Ideal calculus in $K[x]$
Quotients

We henceforth assume that K is a field.

Theorem (Division thm)

If $f(x), g(x) \in K[x]$, with $g(x)$ not the zero polynomial, then there is a unique quotient $a(x)$ and remainder $r(x)$ such that

$$f(x) = a(x)g(x) + r(x), \qquad \deg(r(x)) < \deg(g(x)) \tag{1}$$

Proof.

Put $r_0(x) = f(x)$, $a_0(x) = 0$, and then put $a_{i+1}(x) = \frac{\mathtt{lt}(r_i(x))}{\mathtt{lt}(g(x))} g(x)$, $r_{i+1}(x) = r_i(x) - a_{i+1}(x)$ as long as $\deg(a_i(x)) \geq \deg(g(x))$. $\square$

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Example

If $f(x) = 3x^3 + 5x^2 - 7x + 11 \in \mathbb{Q}[x]$, $g(x) = 2x^2 + 1$, then

$$\begin{aligned}
f(x) &= 3x^3 + 5x^2 - 7x + 11 \\
&= (3x^3 + 5x^2 - 7x + 11) - \frac{3x^3}{2x^2}g + \frac{3x^3}{2x^2}g \\
&= 3x^3 + 5x^2 - 7x + 11 - \frac{3}{2}x(2x^2 + 1) + \frac{3}{2}xg \\
&= 5x^2 - \frac{17}{2}x + 11 + \frac{3}{2}xg \\
&= 5x^2 - \frac{17}{2}x + 11 - \frac{5x^2}{2x^2}g + \frac{5x^2}{2x^2}g + \frac{3}{2}xg \\
&= 5x^2 - \frac{17}{2}x + 11 - \frac{5}{2}(2x^2 + 1) + \left(\frac{5}{2} + \frac{3}{2}x\right) g \\
&= -11x + 11 + \left(\frac{5}{2} + \frac{3}{2}x\right) g
\end{aligned}$$

Theorem

Let $I \subset K[x]$ be a proper non-zero ideal (hence containing no non-zero constants), and let $f \in I$ have degree d, the minimal degree of n.z. pols in I. Then $I = (f)$, and any other generator of the principal ideal I is associate to f. In particular, there is a monic (i.e. having lc 1) generator of I.

Proof.

Take $g \in I$, and use the division thm to write

$$g = af + r, \qquad \deg(r) < \deg(f) = d.$$

Since $g \in I \ni af$, we have that $r \in I$. But $\deg(r) < d$, the minimal degree of nonzero pols in I, so r is the zero pol. Thus $g \in (f)$.

If $I = (h) = (f)$, then $f|h$ and $h|f$, so $f \sim h$. □

Polynomial rings
Coefficients in a domain
Coefficients in a field
Division algorithm
$K[x]$ is a PID
GCD
Zeroes of polynomials and linear factors
Prime and maximal ideals in $K[x]$
Unique factorization
Ideal calculus in $K[x]$
Quotients

Definition

Let $f, g \in K[x]$. A generator of the principal ideal $(f) + (g)$ is called a greatest common divisor of f and g; the unique monic generator is called the greatest common divisor.

Lemma

If $h = \gcd(f, g)$ then $h|f$, $h|g$, and if $h'|f$, $h'|g$, then $h'|h$. Conversely, if h satisfies the above, then $(h) = (f) + (g)$.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Theorem (Euclidean algorithm)

If $f = ag + r$ *then* $\gcd(f, g) = \gcd(g, r)$.

Proof.

Exactly as for the integers. □

Theorem

If $h = \gcd(f, g)$ *then there are (not necessarily unique) polynomials* u, v *such that*

$$h = uf + vg.$$

Proof.

$(h) = (f) + (g)$ so $h = uf + vg$. □

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Example

```
R.<x> = PolynomialRing(QQ)
f = 3*x^4 + 13*x^3 + 5*x^2+3
g = 5*x^3 + 5*x+1
h,u,v =xgcd(f,g)
u*f+v*g
```

yields

$$h = 1$$

$$u = \frac{14700}{45529}x^2 + \frac{725}{91058}x + \frac{14225}{45529}$$

$$v = -\frac{8820}{45529}x^3 - \frac{76875}{91058}x^2 - \frac{30715}{91058}x + \frac{2854}{45529}$$

$$uf + vg = 1$$

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Theorem (Factor theorem)

Let $f(x) \in K[x]$, $a \in K$. Then a is a zero of f, i.e., $f(a) = 0$, iff $(x-a)|f(x)$.

Proof.

If $f(x) = (x-a)g(x)$, then $f(a) = (a-a)g(a) = 0$.
If $f(a) = 0$, use division theorem to get

$$f(x) = k(x)(x-a) + r, \qquad \deg r \leq 0$$

and then evaluate at a:

$$0 = k(a)(a-a) + r,$$

so $r = 0$, and $(x-a)|f(x)$. □

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm
$K[x]$ is a PID
GCD
Zeroes of polynomials and linear factors
Prime and maximal ideals in $K[x]$
Unique factorization
Ideal calculus in $K[x]$
Quotients

Theorem

Let $I = (f) \subseteq K[x]$.

1. *I is a prime ideal if f is the z.p. or if f is irreducible.*
2. *I is a maximal ideal iff f is a non-zero irreducible polynomial.*

Proof.

(0) is prime (in any domain) but not maximal (since it is for instance contained in $(x-1)$).
If $f = gh$ with $\deg(g), \deg(h) < \deg(f)$ then I is not prime.
If f is irreducible, then I is maximal, since $(f) \subsetneq (g)$ means that g is a proper, non-trivial divisor of f.
Maximal ideals are always prime. □

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Theorem (Unique factorization)

1. *Any non-zero polynomial $f \in K[x]$ can be written as a product of irreducible polynomials.*
2. *This factorization is unique, up to ordering and associate factors (we can permute the factors, and move constants between factors; or move the constants out and assume the remaining factors to be monic, i.e. having l.c. 1)*

Proof.

Existence: either f is irreducible, or it factors non-trivially as $f = gh$ with $\deg(g), \deg(h) < \deg(f)$. By induction on the degree, we can assume that g, h are both products of irreducibles.

Uniqueness: We have seen that irreducible polynomials (beeing the generators of prime ideals) are prime elements in $K[x]$. Thus, if

$$f = p_1 \cdots p_r = q_1 \cdots q_s$$

are two factorizations into irreducibles, then since p_1 divides the RHS, it divides som q_i. Cancel and continue, just like for the integers. □

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Theorem

1. *In $\mathbb{C}[x]$, irreducible polynomials have degree 1*
2. *In $\mathbb{R}[x]$, irreducible polynomials have degree 1 or 2*
3. *In $\mathbb{Q}[x]$, there are irreducible polynomials of any degree*
4. *In $\mathbb{Z}_p[x]$, there are irreducible polynomials of any degree*
5. *In $F[x]$, where F is a finite field, there are irreducible polynomials of any degree*

Proof.

The first assertion is topological in nature, and hard. We will skip the proof!

Real polynomials have complex zeroes that occur in complex conjugated pairs $\alpha, \overline{\alpha}$, and

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - 2\mathfrak{Re}(\alpha)x + |\alpha|$$

is irreducible as a real polynomial.

For any odd prime p, $x^p - 1 \in \mathbb{Q}[x]$ is irreducible.

The last two assertions will be proved in due time. □

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Theorem

Let $f, g \in K[x] \setminus \{0\}$ (as in the the z.p.)

1. $(f) \subseteq (g)$ *iff* $g|f$
2. $(f) + (g) = (\gcd(f, g))$
3. $(f) \cap (g) = (lcm(f, g))$
4. $(f)(g) = (fg)$
5. $\sqrt{(f)} = (\mathrm{sqfp}(f))$, *where* $\mathrm{sqfp}\left(\prod_j p_j^{a_j}\right) = \prod_j p_j$
6. (f) *is prime iff* (f) *maximal iff* (f) *is irreducible*
7. (f) *is primary iff* $f = p^r$ *with* p *irreducible*

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Polynomial rings
Coefficients in a domain
Coefficients in a field
Division algorithm
$K[x]$ is a PID
GCD
Zeroes of polynomials and linear factors
Prime and maximal ideals in $K[x]$
Unique factorization
Ideal calculus in $K[x]$
Quotients

Theorem

Let $f = a_0 + a_1 x + \dots a_{n_1} x^{n-1} + x^n \in K[x]$, *with* $\deg(f) = n > 0$. *Let* $I = (f)$, *and put* $R = K[x]/I$.

1. *R is a domain iff it is a field iff f is irreducible.*
2. *R is a K-vector space of dimension n. A natural basis is*
$$1, \overline{x}, \dots, \overline{x}^{n-1}$$
where $\overline{x} = x + I$, the image of x in the quotient R/I
3. *Multiplication of basis vectors are determined by*
$$\overline{x}^i \overline{x}^j = \overline{x}^{i+j}$$
$$\overline{x}^n = -\sum_{j=0}^{n-1} a_j \overline{x}^j$$

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Example

Put $R = \mathbb{Q}[x]/(x^2 - 1)$. Then any element in R can be written as

$$a + b\overline{x},$$

and the elements multiply subject to the relation

$$\overline{x}^2 = 1,$$

so there are zero divisors, e.g.

$$(\overline{x} + 1)(\overline{x} - 1) = \overline{x}^2 - 1 = 0$$

Are there nilpotent elements?

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Example

The polynomial $f = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$ is irreducible, so $R = \mathbb{Z}_2[x]/(f)$ is a field. Hence $g = \overline{x}^3 \in R$ is invertible. Find the inverse!

1. (Bezout): in $\mathbb{Z}_2[x]$,

$$\gcd(f, x^3) = 1 = (x^2 + 1)f + (x^4 + x^2 + x)g,$$

so

$$(\overline{x}^4 + \overline{x}^2 + \overline{x})g = 1 - \overline{f} * \overline{x^2 + 1} = 1 \in R$$

2. (Linear algebra) Make the Ansatz

$$h = a_0 + a_1\overline{x} + a_2\overline{x}^2 + a_3\overline{x}^3 + a_4\overline{x}^4$$

and solve

$$hg = 1,$$

using

$$\overline{x}^5 = \overline{x}^2 + 1, \qquad \overline{x}^6 = \overline{x}^3 + \overline{x}, \qquad \overline{x}^7 = \overline{x}^4 + \overline{x}^2$$

Polynomial rings

Coefficients in a domain

Coefficients in a field

Division algorithm

$K[x]$ is a PID

GCD

Zeroes of polynomials and linear factors

Prime and maximal ideals in $K[x]$

Unique factorization

Ideal calculus in $K[x]$

Quotients

Example

The ideals of $\mathbb{Q}[x]/(x^4 - 1)$ correspond to the ideals of $\mathbb{Q}[x]$ that contain $(x^4 - 1)$; those are principal ideals with generators that divide $x^4 - 1$. Thus, the non-zero, proper ideals of the quotient are

$$(\overline{x}^2 + 1), \; (\overline{x} + 1), \; (\overline{x} - 1).$$

Example

Show that $\mathbb{Q}[x]/(x^4 + 2x^2 + 1)$ is a local ring, and that the non-units are precisely the images of those polynomials $f(x)$ which vanish at $\pm i$ (imaginary unit).