Polynomial Rings

Yohana Solomon

November 15, 2016

Outline

1. Definitions and Basic Properties
2. Polynomial Rings over Fields
3. Polynomial Rings that are Unique Factorization Domains
4. Irreducibility Criteria

Definitions and Basic Properties

Basic Properties

The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and each $a_i \in R$.

Basic Properties

The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and each $a_i \in R$.

Addition of polynomials is componentwise:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

Basic Properties

The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and each $a_i \in R$.
Addition of polynomials is componentwise:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i .$$

Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ and then extending to all polynomials by the distributive laws so that in general

$$\left(\sum_{i=0}^{n} a_i x^i \right) \times \left(\sum_{i=0}^{m} b_i x^i \right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k .$$

Basic Properties

The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $n \geq 0$ and each $a_i \in R$. Addition of polynomials is componentwise:

$$\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n} (a_i + b_i)x^i.$$

Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ and then extending to all polynomials by the distributive laws so that in general

$$\left(\sum_{i=0}^{n} a_ix^i\right) \times \left(\sum_{i=0}^{m} b_ix^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_ib_{k-i}\right)x^k.$$

In this way $R[x]$ is a commutative ring with identity (the identity 1 from R) in which we identify R with the subring of constant polynomials.

Proposition:

Let R be an integral domain. Then

- degree $p(x)q(x) = $ degree $p(x) +$ degree $q(x)$ if $p(x)$, $q(x)$ are nonzero

Proposition:

Let R be an integral domain. Then

- degree $p(x)q(x) =$ degree $p(x) +$ degree $q(x)$ if $p(x)$, $q(x)$ are nonzero
- the units of $R[x]$ are just the units of R

Proposition:

Let R be an integral domain. Then

- degree $p(x)q(x) =$ degree $p(x) +$ degree $q(x)$ if $p(x)$, $q(x)$ are nonzero
- the units of $R[x]$ are just the units of R
- $R[x]$ is an integral domain.

Definition:

The polynomial ring in the variables $x_1, x_2, ..., x_n$ with coefficients in R, denoted

$$R[x_1, x_2, ..., x_n] = R[x_1, x_2, ..., x_{n-1}][x_n]$$

Example:

Let

$$p(x, y, z) = 2x^2y - 3xy^3z + 4y^2z^5$$

and

$$q(x, y, z) = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$$

be polynomials in $\mathbb{Z}[x, y, z]$.
Note: The polynomial ring $\mathbb{Z}[x, y, z]$ in three variables x, y and z with integers coefficients consists of all finite sums of monomial terms of the form $ax^iy^jz^k$ (of degree $i + j + k$).

```
sage:  R1 = QQ['x,y,z']
sage:  (x,y,z) = R1.gens()
sage:  px = 2*x^2*y - 3*x*y^3*z + 4*y^2*z^5;
sage:  qx = 7*x^2 + 5*x^2*y^3*z^4 - 3*x^2*z^3;
```

```
sage:  R1 = QQ['x,y,z']
sage:  (x,y,z) = R1.gens()
```
sage: px = $2 * x^2 * y - 3 * x * y^3 * z + 4 * y^2 * z^5$;
sage: qx = $7 * x^2 + 5 * x^2 * y^3 * z^4 - 3 * x^2 * z^3$;

Write each of p and q as a polynomial in x with coefficients in $\mathbb{Z}[y, z]$.

```
sage:  R2 = QQ['y,z']['x']
sage:  R2(px)
```
$$(2 * y) * x^2 - (3 * y^3 * z) * x + 4 * y^2 * z^5$$
```
sage:  R2(qx)
```
$$(5 * y^3 * z^4 - 3 * z^3 + 7) * x^2$$

```
sage:  R1 = QQ['x,y,z']
sage:  (x,y,z) = R1.gens()
```

sage: px = $2*x^2*y - 3*x*y^3*z + 4*y^2*z^5$;

sage: qx = $7*x^2 + 5*x^2*y^3*z^4 - 3*x^2*z^3$;

Find the degree of p and q.

```
sage:  px.degree()
    7
sage:  qx.degree()
    9
```

sage: R1 = QQ['x,y,z']
sage: (x,y,z) = R1.gens()
sage: px = $2*x^2*y-3*x*y^3*z+4*y^2*z^5$;
sage: qx = $7*x^2+5*x^2*y^3*z^4-3*x^2*z^3$;

Find the degree of p and q in each of the three variables x, y and z.

```
sage: px.exponents()
    [(0, 2, 5), (1, 3, 1), (2, 1, 0)]
sage: qx.exponents()
    [(2, 3, 4), (2, 0, 3), (2, 0, 0)]
```

```
sage: R1 = QQ['x,y,z']
sage: (x,y,z) = R1.gens()
```
sage: px = $2*x^2*y-3*x*y^3*z+4*y^2*z^5$;

sage: qx = $7*x^2+5*x^2*y^3*z^4-3*x^2*z^3$;

Compute *pq* and find the degree of *pq* in each of the three variables x, y and z.

sage: rx = px*qx; rx

$20*x^2*y^5*z^9-15*x^3*y^6*z^5+10*x^4*y^4*z^4-12*x^2*y^2*z^8+9*x^3*y^3*z^4+28*x^2*y^2*z^5-6*x^4*y*z^3-21*x^3*y^3*z+14*x^4*y$

```
sage: rx.degree()
    16
sage: rx.exponents()
    [(2, 5, 9), (3, 6, 5), (4, 4, 4), (2, 2, 8),
(3, 3, 4), (2, 2, 5), (4, 1, 3), (3, 3, 1), (4, 1, 0)]
```

```
sage: R1 = QQ['x,y,z']
sage: (x,y,z) = R1.gens()
```
sage: px = $2*x^2*y-3*x*y^3*z+4*y^2*z^5$;

sage: qx = $7*x^2+5*x^2*y^3*z^4-3*x^2*z^3$;

Write *pq* as a polynomial in the variable z with coefficients in $\mathbb{Z}[x,y]$.

```
sage: R3 = QQ['x,y']['z']
sage: R3(rx)
```

$$20*x^2*y^5*z^9-12*x^2*y^2*z^8+(-15*x^3*y^6+28*x^2*y^2)*z^5+(10*x^4*y^4+9*x^3*y^3)*z^4-6*x^4*y*z^3-21*x^3*y^3*z+14*x^4*y$$

Polynomial Rings over Fields

Theorem: Division Algorithm

Let F be a field. The polynomial $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x)$$

with $r(x) = 0$ or degree $r(x) <$ degree $b(x)$.

Example:

Determine the greatest common divisor of $a(x) = x^3 + 1$ and $b(x) = x^2 + 2x + 1$ in $\mathbb{Q}[x]$.

Example:

Determine the greatest common divisor of $a(x) = x^3 + 1$ and $b(x) = x^2 + 2x + 1$ in $\mathbb{Q}[x]$.

$$x^3 + 1 = (x^2 + 2x + 1)(x - 2) + 3(x + 1)$$
$$x^2 + 2x + 1 = (x + 1)(x + 1) + 0$$

Example:

Determine the greatest common divisor of $a(x) = x^3 + 1$ and $b(x) = x^2 + 2x + 1$ in $\mathbb{Q}[x]$.

$$\begin{aligned} x^3 + 1 &= (x^2 + 2x + 1)(x - 2) + 3(x + 1) \\ x^2 + 2x + 1 &= (x + 1)(x + 1) + 0 \end{aligned}$$

Thus, $\gcd(x^3 + 1, x^2 + 2x + 1) = x + 1.$

Definition:

- **Principal Ideal Domain (PID):**
  A *principal ideal domain* is an integral domain R in which every ideal has the form
  $$(a) = \{ra | r \in R\}$$
  for some a in R.

Definition:

- **Principal Ideal Domain (PID):**
  A *principal ideal domain* is an integral domain R in which every ideal has the form
  $$(a) = \{ra | r \in R\}$$
  for some a in R.

- **Unique Factorization Domain (UFD):**
  An integral domain D is a *unique factorization domain* if
  - every nonzero element of D that is not a unit can be written as a product of irreducibles of D; and
  - the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Corollary:

- If F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorization Domain.

Corollary:

- If F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorization Domain.
- If R is any commutative ring such that the polynomial ring $R[x]$ is a Principal Ideal Domain, then R is necessarily a field.

Example:

The ring $\mathbb{Z}$ of integers is a Principal Ideal Domain, but the ring $\mathbb{Z}[x]$ is not a Principal Ideal Domain, since $(2, x)$ is not principal in this ring.

Polynomial Rings that are Unique Factorization Domains

Proposition:

Let R be a Unique Factorization Domain. Suppose that g and h are elements of $R[x]$ and let $f(x) = g(x)h(x)$. Then the content of f is equal to the content of g times the content of h.

Proposition: Gauss' Lemma

Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if

$$p(x) = A(x)B(x)$$

for some non-constant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that

$$rA(x) = a(x) \text{ and } sB(x) = b(x)$$

both lie in $R[x]$ and

$$p(x) = a(x)b(x)$$

is a factorization in $R[x]$.

Proof: The coefficients of the polynomials on the right hand side of the equation $p(x) = A(x)B(x)$ are elements in the field F, hence are quotients of elements from the Unique Factorization Domains R. Multiplying through by a common denominator for all these coefficients, we obtain

$$dp(x) = a'(x)b'(x),$$

where now $a'(x)$ and $b'(x)$ are elements of $R[x]$ and d in a nonzero element of R. Now write

$$a'(x) = ra(x) \qquad \textit{and} \qquad b'(x) = sb(x).$$

We get

$$dp(x) = rsa(x)b(x).$$

By the proposition above, d divides rs, $rs = d\gamma$, where $\gamma \in R$. Thus, replacing $a(x)$ with $\gamma a(x)$, we have

$$p(x) = a(x)b(x).$$

Theorem:

R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Corollary:

If R is a Unique Factorization Domain, then a polynomial ring in any number of variables with coefficients in R is also a Unique Factorization Domain.

Example:

- $\mathbb{Z}[x]$, $\mathbb{Z}[x, y]$, etc. are Unique Factorization Domains. The ring $\mathbb{Z}[x]$ gives an example of a Unique Factorization Domain that is not a Principal Ideal Domain.

Example:

- $\mathbb{Z}[x]$, $\mathbb{Z}[x, y]$, etc. are Unique Factorization Domains.
  The ring $\mathbb{Z}[x]$ gives an example of a Unique Factorization Domain that is not a Principal Ideal Domain.
- $\mathbb{Q}[x]$, $\mathbb{Q}[x, y]$, etc. are Unique Factorization Domains.

Irreducibility Criteria

Propositions:

- Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, that is, there is an $\alpha \in F$ with $p(\alpha) = 0$.

Propositions:

- Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, that is, there is an $\alpha \in F$ with $p(\alpha) = 0$.
- A polynomial of degree two or three over a field F is reducible if and only if it has a root in F.

Example:

The polynomial $p(x) = x^2 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ since it does not have a root in $\mathbb{Z}/2\mathbb{Z}[x]$:

$$0^2 + 0 + 1 = 1$$

and

$$1^2 + 1 + 1 = 1$$

.

Propositions:

Let I be a proper ideal in the integral domain R and let $p(x)$ be a non-constant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ can't be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Example:

Consider the polynomial $p(x) = x^2 + x + 1$ in $\mathbb{Z}[x]$. Reducing modulo 2, we see from the last example that $p(x)$ is irreducible in $\mathbb{Z}[x]$.

Similarly, $x^3 + x + 1$ is irreducible in $\mathbb{Z}[x]$ because it is irreducible in $\mathbb{Z}[x]/2\mathbb{Z}[x]$.

Theorem:

Let $f(x) \in \mathbb{Z}[x]$.
If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Corollary: Eisenstein's Criterion for $\mathbb{Z}[x]$

Let p be a prime in $\mathbb{Z}$ and let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x],$$

where $n \geq 1$.
Suppose p divides a_i for all $i \in \{0, 1, \cdots n-1\}$ but that p^2 does not divide a_0.
Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Example:

Prove that the polynomial $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$.

Example:

Prove that the polynomial $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$.

The polynomial $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$ because $2 \nmid 1$ and $4 \nmid 6$ but 2 does divide -4, 0, and 6.

Example:

Let p be a prime, the p^{th} cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Z}$.

Let

$$\begin{aligned} f(x) = \Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{1}. \end{aligned}$$

Example:

Let p be a prime, the p^{th} cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Z}$.

Let

$$\begin{aligned} f(x) = \Phi_p(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{1}. \end{aligned}$$

Then, since every coefficient except that of x^{p-1} is divisible by p and the constant term is not divisible by p^2, by Eisensteins Criterion, $f(x)$ is irreducible over $\mathbb{Z}$.

Example:

Let p be a prime, the p^{th} cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Z}$.

So, if $\Phi_p(x) = g(x)h(x)$ were a nontrivial factorization of $\Phi_p(x)$ over $\mathbb{Z}$, then

$$f(x) = \Phi_p(x+1) = g(x+1) \cdot h(x+1)$$

would be a nontrivial factorization of $f(x)$ over $\mathbb{Z}$. Since this is impossible, we conclude that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$.