Abstract Algebra II

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 342

Subsection 1

Definitions and Basic Properties

Polynomials

- Let R be a commutative ring with identity $1 \neq 0$.
- 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 $a_i \in R$.
- If $a_n \neq 0$, then:
  - the polynomial is of **degree** n;
  - $a_n x^n$ is the **leading term**;
  - a_n is the **leading coefficient**;
    the leading coefficient of the zero polynomial is defined to be 0.
- The polynomial is **monic** if $a_n = 1$.

Polynomial Rings

- **Addition of polynomials** is "componentwise":
$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i b_i) x^i,$$
where a_n or b_n may be zero in order for addition of polynomials of different degrees to be defined.
- **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
$$(\sum_{i=0}^{n} a_i x^i) \times (\sum_{i=0}^{m} b_i x^i) = \sum_{k=0}^{n+m} (\sum_{i=0}^{k} a_i b_{k-i}) x^k.$$
- $R[x]$ is a commutative ring with identity 1 in which we identify R with the subring of constant polynomials.

Properties of $R[x]$

- We have already noted that if R is an integral domain then the leading term of a product of polynomials is the product of the leading terms of the factors.

Proposition

Let R be an integral domain. Then:

(1) $\text{degree} p(x)q(x) = \text{degree} p(x) + \text{degree} q(x)$ if $p(x), q(x)$ are nonzero.

(2) The units of $R[x]$ are just the units of R.

(3) $R[x]$ is an integral domain.

- Recall also that if R is an integral domain, the quotient field of $R[x]$ consists of all quotients $\frac{p(x)}{q(x)}$, where $q(x)$ is not the zero polynomial; It is called the **field of rational functions** in x with coefficients in R.

Ideals of R and of $R[x]$

Proposition

Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I). Then $R[x]/(I) \cong (R/I)[x]$. In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.

- There is a natural map $\varphi : R[x] \to (R/I)[x]$ given by reducing each of the coefficients of a polynomial modulo I. The definition of addition and multiplication in these two rings shows that φ is a ring homomorphism. The kernel is precisely the set of polynomials each of whose coefficients is an element of I. I.e., $\ker\varphi = I[x] = (I)$.

  For the last statement, suppose I is a prime ideal in R. Then, R/I is an integral domain. Thus, by the preceding proposition, $(R/I)[x]$ is an integral domain. Hence, (I) is a prime ideal of $R[x]$.

More on Ideals

- It is not true that if I is a maximal ideal of R then (I) is a maximal ideal of $R[x]$.
- However, if I is maximal in R, then the ideal of $R[x]$ generated by I and x is maximal in $R[x]$.

  Example: Let $R = \mathbb{Z}$ and consider the ideal $n\mathbb{Z}$ of $\mathbb{Z}$. Then the isomorphism above can be written $\mathbb{Z}[x]/n\mathbb{Z}[x] \cong \mathbb{Z}/n\mathbb{Z}[x]$.

  The natural projection map of $\mathbb{Z}[x]$ to $\mathbb{Z}/n\mathbb{Z}[x]$ by reducing the coefficients modulo n is a ring homomorphism.

  - If n is composite, then the quotient ring is not an integral domain.
  - If n is a prime p, then $\mathbb{Z}/p\mathbb{Z}$ is a field and so $\mathbb{Z}/p\mathbb{Z}[x]$ is an integral domain (in fact, a Euclidean Domain, as we will show).

    We also see that the set of polynomials whose coefficients are divisible by p is a prime ideal in $\mathbb{Z}[x]$.

Polynomial Rings in Several Variables

Definition (Polynomial Rings in Several Variables)

The **polynomial ring in the variables** $x_1, x_2, \ldots, x_n$, **with coefficients in** R, denoted $R[x_1, x_2, \ldots, x_n]$, is defined inductively by $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$.

- Thus, we can consider polynomials in n variables with coefficients in R simply as polynomials in one variable (say x_n) but now with coefficients that are themselves polynomials in $n-1$ variables.
- Alternatively, a nonzero polynomial in $x_1, x_2, \ldots, x_n$ with coefficients in R is a finite sum of nonzero **monomial terms**, i.e., a finite sum of elements of the form $ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$, where $a \in R$ (the **coefficient** of the term) and the d_i are nonnegative integers.
- A monic term $x_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$ is called simply a **monomial**; it is the **monomial part** of the term $ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$.
- The exponent d_i is called the **degree** in x_i of the term and the sum $d = d_1 + d_2 + \cdots + d_n$ is called the **degree** of the term.

Polynomial Rings in Several Variables (Cont'd)

- Consider again the term $ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$.
- The ordered n-tuple $(d_1, d_2, \ldots, d_n)$ is the **multidegree** of the term.
- The **degree** of a nonzero polynomial is the largest degree of any of its monomial terms.
- A polynomial is called **homogeneous** or a **form** if all its terms have the same degree.
- If f is a nonzero polynomial in n variables, the sum of all the monomial terms in f of degree k is called the **homogeneous component** of f of degree k.
- If f has degree d then f may be written uniquely as the sum $f_0 + f_1 + \cdots + f_d$, where f_k is the homogeneous component of f of degree k, for $0 \leq k \leq d$ (where some f_k may be zero).

Polynomial Rings in Arbitrarily Many Variables

- A **polynomial ring in an arbitrary number of variables with coefficients in** R is formed by taking finite sums of monomial terms of the type above;

  The variables are not restricted to just $x_1, \ldots, x_n$.
- Alternatively, we could define this ring as the union of all the polynomial rings in a finite number of the variables being considered.

In the polynomial ring $\mathbb{Z}[x, y]$

- The polynomial ring $\mathbb{Z}[x, y]$ in two variables x and y with integer coefficients consists of all finite sums of monomial terms of the form $ax^i y^j$ (of degree $i + j$).
- E.g., $p(x, y) = 2x^3 + xy - y^2$ and $q(x, y) = -3xy + 2y^2 + x^2y^3$ are both elements of $\mathbb{Z}[x, y]$, of degrees 3 and 5, respectively. We have

$$\begin{aligned} p(x,y) + q(x,y) &= 2x^3 - 2xy + y^2 + x^2y^3; \\ p(x,y)q(x,y) &= -6x^4y + 4x^3y^2 + 2x^5y^3 - 3x^2y^2 + \\ & \quad 5xy^3 + x^3y^4 - 2y^4 - x^2y^5; \end{aligned}$$

The latter is a polynomial of degree 8. To view it as a polynomial in y with coefficients in $\mathbb{Z}[x]$, we write the polynomial in the form

$$(-6x^4)y + (4x^3 - 3x^2)y^2 + (2x^5 + 5x)y^3 + (x^3 - 2)y^4 - (x^2)y^5.$$

Its nonzero homogeneous components are $f_4 = -3x^2y^2 + 5xy^3 - 2y^4$ (degree 4), $f_5 = -6x^4y + 4x^3y^2$ (degree 5), $f_7 = x^3y^4 - x^2y^5$ (degree 7), and $f_8 = 2x^5y^3$ (degree 8).

Subsection 2

Polynomial Rings over Fields I

Division in Polynomial Rings Over Fields

- Suppose the coefficient ring is a field F.
- We can define a norm on $F[x]$ by defining $N(p(x)) = \text{degree} p(x)$ (where we set $N(0) = 0$).

Theorem

Let F be a field. The polynomial ring $F[x]$ 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 $\text{degree} r(x) < \text{degree} b(x)$.

- If $a(x)$ is the zero polynomial, then take $q(x) = r(x) = 0$.
- We may assume $a(x) \neq 0$ and prove the existence of $q(x)$ and $r(x)$ by induction on $n = \text{degree} a(x)$. Let $b(x)$ have degree m.
  - If $n < m$, take $q(x) = 0$ and $r(x) = a(x)$.
  - If $n \geq m$, write $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $b(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$.

Division in Polynomial Rings Over Fields (Cont'd)

- We assumed $n \geq m$,

$$\begin{array}{rcl} a(x) & = & a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0; \\ b(x) & = & b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0. \end{array}$$

Then the polynomial $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ is of degree less than n (we have arranged to subtract the leading term from $a(x)$).

Note that this polynomial is well defined because the coefficients are taken from a field and $b_m \neq 0$.

By induction then, there exist polynomials $q'(x)$ and $r(x)$, with $a'(x) = q'(x) b(x) + r(x)$, with $r(x) = 0$ or $\text{degree} r(x) < \text{degree} b(x)$. Let $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$. Then, we have:

  - $a(x) = a'(x) + \frac{a_n}{b_m} x^{n-m} b(x) = (q'(x) b(x) + r(x)) + \frac{a_n}{b_m} x^{n-m} b(x) = (q'(x) + \frac{a_n}{b_m} x^{n-m}) b(x) + r(x) = q(x) b(x) + r(x)$;
  - $r(x) = 0$ or $\text{degree} r(x) < \text{degree} b(x)$.

Division: The Uniqueness Part

- For uniqueness, suppose $q_1(x)$ and $r_1(x)$ also satisfied the conditions of the theorem, that is

$$a(x) = q(x)b(x) + r(x) = q_1(x)b(x) + r_1(x),$$

where $r_1(x) = 0$ or $\text{degree} r_1(x) < \text{degree} b(x)$.

Then both $a(x) - q(x)b(x)$ and $a(x) - q_1(x)b(x)$ are of degree less than $m = \text{degree} b(x)$.

The difference of these two polynomials $b(x)(q(x) - q_1(x))$ is also of degree less than m.

But the degree of the product of two nonzero polynomials is the sum of their degrees (since F is an integral domain), whence $q(x) - q_1(x)$ must be 0, that is, $q(x) = q_1(x)$.

This implies $r(x) = r_1(x)$, completing the proof.

The Coordinate Ring and the Ring of Polynomials

Corollary

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

- Recall, also, that if R is any commutative ring such that $R[x]$ is a Principal Ideal Domain (or Euclidean Domain) then R must be a field.
- We will see in the next section that $R[x]$ is a Unique Factorization Domain whenever R itself is a Unique Factorization Domain.

Examples

(1) The ring $\mathbb{Z}[x]$ is not a Principal Ideal Domain.

The ideal $(2, x)$ is not principal in this ring.

(2) $\mathbb{Q}[x]$ is a Principal Ideal Domain since the coefficients lie in the field $\mathbb{Q}$.

The ideal generated in $\mathbb{Z}[x]$ by 2 and x is not principal in the subring $\mathbb{Z}[x]$ of $\mathbb{Q}[x]$.

However, the ideal generated in $\mathbb{Q}[x]$ is principal; in fact it is the entire ring (so has 1 as a generator) since 2 is a unit in $\mathbb{Q}[x]$.

Examples (Cont'd)

(3) If p is a prime, the ring $\mathbb{Z}/p\mathbb{Z}[x]$ obtained by reducing $\mathbb{Z}[x]$ modulo the prime ideal (p) is a Principal Ideal Domain, since the coefficients lie in the field $\mathbb{Z}/p\mathbb{Z}$.

This example shows that the quotient of a ring which is not a Principal Ideal Domain may be a Principal Ideal Domain.

To follow the ideal $(2, x)$ above in this example, note that:

- if $p = 2$, then the ideal $(2, x)$ reduces to the ideal (x) in the quotient $\mathbb{Z}/2\mathbb{Z}[x]$, which is a proper (maximal) ideal;
- if $p \neq 2$, then 2 is a unit in the quotient, so the ideal $(2, x)$ reduces to the entire ring $\mathbb{Z}/p\mathbb{Z}[x]$.

(4) $\mathbb{Q}[x, y]$ is not a Principal Ideal Domain since this ring is $\mathbb{Q}[x][y]$ and $\mathbb{Q}[x]$ is not a field (any element of positive degree is not invertible).

It is an exercise to see that the ideal (x, y) is not a principal ideal in this ring.

We will see that $\mathbb{Q}[x, y]$ is a Unique Factorization Domain.

Quotient and Remainder in Field Extensions

- The quotient and remainder in the Division Algorithm applied to $a(x), b(x) \in F[x]$ are independent of field extensions:
  Suppose the field F is contained in the field E and
  $$a(x) = Q(x)b(x) + R(x),$$
  for $Q(x), R(x) \in E[x]$, with $R(x) = 0$ or $\text{degree} R(x) < \text{degree} b(x)$.
  Write $a(x) = q(x)b(x) + r(x)$, for some $q(x), r(x) \in F[x]$.
  Apply uniqueness in the ring $E[x]$ to deduce that $Q(x) = q(x)$ and $R(x) = r(x)$.
- In particular, $b(x)$ divides $a(x)$ in the ring $E[x]$ if and only if $b(x)$ divides $a(x)$ in $F[x]$.
- Also, the greatest common divisor of $a(x)$ and $b(x)$ (which can be obtained from the Euclidean Algorithm) is the same, once we make it unique by specifying it to be monic, whether these elements are viewed in $F[x]$ or in $E[x]$.

Subsection 3

Polynomial Rings that are U.F.D.s

Unique Factorization in $R[x]$

- If R is an integral domain, then $R[x]$ is also an integral domain:
  - R can be embedded in its field of fractions F so that $R[x] \subseteq F[x]$ is a subring;
  - $F[x]$ is a Euclidean Domain (hence a Principal Ideal Domain and a Unique Factorization Domain).
- Suppose $p(x)$ is a polynomial in $R[x]$. Since $F[x]$ is a Unique Factorization Domain we can factor $p(x)$ uniquely into a product of irreducibles in $F[x]$. In general $R[x]$ is not a Unique Factorization Domain, since the constant polynomials would have to be uniquely factored into irreducible elements of $R[x]$ and R would have to be a Unique Factorization Domain.
  - Thus if R is an integral domain which is not a Unique Factorization Domain, $R[x]$ cannot be a Unique Factorization Domain.
  - On the other hand, it turns out that if R is a Unique Factorization Domain, then $R[x]$ is also a Unique Factorization Domain.
    The method of proving this is to first factor uniquely in $F[x]$ and, then, "clear denominators" to obtain a unique factorization in $R[x]$.

Gauss' Lemma

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 nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$, such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

- The coefficients of the polynomials on the right in the equation $p(x) = A(x)B(x)$ are elements in the field F. Hence, they are quotients of elements from the Unique Factorization Domain R. Multiply by a common denominator for all these coefficients. We get an equation $dp(x) = a'(x)b'(x)$, where $a'(x)$ and $b'(x)$ are in $R[x]$ and d is a nonzero element of R.
    - If d is a unit in R, the proposition is true with $a(x) = d^{-1}a'(x)$ and $b(x) = b'(x)$.

Gauss' Lemma (Cont'd)

- We obtained $dp(x) = a'(x)b'(x)$, where $a'(x)$ and $b'(x)$ are elements of $R[x]$ and d is a nonzero element of R.
  - Suppose d is not a unit. Write d as a product of irreducibles in R, say $d = p_1 \cdots p_n$. Since p_1 is irreducible in R, the ideal (p_1) is prime. Thus, the ideal $p_1R[x]$ is prime in $R[x]$. Hence, $(R/p_1R)[x]$ is an integral domain. Reducing the equation $dp(x) = a'(x)b'(x)$ modulo p_1, we obtain the equation $0 = \overline{a'(x)}\overline{b'(x)}$ in this integral domain. Hence one of the two factors, say $\overline{a'(x)}$ must be 0. But this means all the coefficients of $a'(x)$ are divisible by p_1. So $\frac{1}{p_1}a'(x)$ also has coefficients in R. In other words, in the equation $dp(x) = a'(x)b'(x)$ we can cancel a factor of p_1 from d (on the left) and from either $a'(x)$ or $b'(x)$ (on the right) and still have an equation in $R[x]$. But now the factor d on the left hand side has one fewer irreducible factors.
    Proceeding similarly with each of the remaining factors of d, we can cancel all of the factors of d into the two polynomials on the right hand side. This gives an equation $p(x) = a(x)b(x)$, with $a(x), b(x) \in R[x]$ and with $a(x), b(x)$ being F-multiples of $A(x), B(x)$, respectively.

Additional Comments

- We cannot prove that $a(x)$ and $b(x)$ are necessarily R-multiples of $A(x)$, $B(x)$, respectively:

  Example: Consider x^2 in $\mathbb{Q}[x]$.

  - It factors as $x^2 = A(x)B(x)$, with $A(x) = 2x$ and $B(x) = \frac{1}{2}x$;
  - However, no integer multiples of $A(x)$ and $B(x)$ give a factorization of x^2 in $\mathbb{Z}[x]$.

- The elements of the ring R become units in the Unique Factorization Domain $F[x]$ (the units in $F[x]$ being the nonzero elements of F).

  Example:

  - $7x$ factors in $\mathbb{Z}[x]$ into a product of two irreducibles: 7 and x;
    So $7x$ is not irreducible in $\mathbb{Z}[x]$;
  - $7x$ is the unit 7 times the irreducible x in $\mathbb{Q}[x]$;
    So $7x$ is irreducible in $\mathbb{Q}[x]$.

Irreducibility in $R[x]$ and in $F[x]$

Corollary

Let R be a Unique Factorization Domain, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

- By Gauss' Lemma above, if $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$. Conversely, the assumption on the greatest common divisor of the coefficients of $p(x)$ implies that, if it is reducible in $R[x]$, then $p(x) = a(x)b(x)$, where neither $a(x)$ nor $b(x)$ are constant polynomials in $R[x]$. This same factorization shows that $p(x)$ is reducible in $F[x]$.

U.F. Property for R and $R[x]$

Theorem

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

- We have indicated above that $R[x]$ a Unique Factorization Domain forces R to be a Unique Factorization Domain.

  Suppose conversely that R is a Unique Factorization Domain, F is its field of fractions and $p(x)$ is a nonzero element of $R[x]$. Let d be the greatest common divisor of the coefficients of $p(x)$. Then $p(x) = dp'(x)$, where the g.c.d. of the coefficients of $p'(x)$ is 1. Such a factorization of $p(x)$ is unique up to a change in d (so up to a unit in R). d can be factored uniquely into irreducibles in R which are also irreducibles in $R[x]$. So, it suffices to prove that $p'(x)$ can be factored uniquely into irreducibles in $R[x]$. Thus we may assume:
  - The greatest common divisor of the coefficients of $p(x)$ is 1;
  - $p(x)$ is not a unit in $R[x]$, i.e., degree $p(x) > 0$.

U.F. Property for R and $R[x]$ (Cont'd)

- Since $F[x]$ is a Unique Factorization Domain, $p(x)$ can be factored uniquely into irreducibles in $F[x]$. By Gauss' Lemma, such a factorization implies there is a factorization of $p(x)$ in $R[x]$ whose factors are F-multiples of the factors in $F[x]$. But the greatest common divisor of the coefficients of $p(x)$ is 1. Hence, the g.c.d. of the coefficients in each of these factors in $R[x]$ must be 1. By the corollary, each of these factors is an irreducible in $R[x]$. This shows that $p(x)$ can be written as a finite product of irreducibles in $R[x]$.

U.F. Property for R and $R[x]$ (Uniqueness)

- Suppose
$$p(x) = q_1(x) \cdots q_r(x) = q_1'(x) \cdots q_s'(x)$$
are two factorizations of $p(x)$ into irreducibles in $R[x]$. Since the g.c.d. of the coefficients of $p(x)$ is 1, the same is true for each of the irreducible factors above. In particular, each has positive degree.

  By the corollary, each $q_i(x)$ and $q_j'(x)$ is an irreducible in $F[x]$.

  By unique factorization in $F[x]$, $r = s$ and, possibly after rearrangement, $q_i(x)$ and $q_j'(x)$ are associates in $F[x]$, for all $i \in \{1, \ldots, r\}$.

  It remains to show they are associates in $R[x]$.

U.F. Property for R and $R[x]$ (Uniqueness Cont'd)

- $q_i(x)$ and $q'_j(x)$ are associates in $F[x]$.

  We want to show they are associates in $R[x]$.

  The units of $F[x]$ are precisely the elements of $F^\times$.

  Thus, we need to consider the case $q(x) = \frac{a}{b}q'(x)$, for some $q(x), q'(x) \in R[x]$ and nonzero elements a, b of R, where the greatest common divisor of the coefficients of each of $q(x)$ and $q'(x)$ is 1.

  In this case $bq(x) = aq'(x)$; the g.c.d. of the coefficients on the left hand side is b and on the right hand side is a.

  Since in a Unique Factorization Domain the g.c.d. of the coefficients of a nonzero polynomial is unique up to units, $a = ub$, for some unit u in R. Thus $q(x) = uq'(x)$. So $q(x)$ and $q'(x)$ are associates in R as well.

Rings of Polynomials of Many Variables and U.F.D.s

Corollary

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

- Recall that a polynomial ring in n variables can be considered as a polynomial ring in one variable with coefficients in a polynomial ring in $n-1$ variables. So, for finitely many variables, the conclusion follows by induction from the theorem.

  The general case follows from the definition of a polynomial ring in an arbitrary number of variables as the union of polynomial rings in finitely many variables.

  Examples:

  (1) $\mathbb{Z}[x], \mathbb{Z}[x,y]$, 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.

  (2) Similarly, $\mathbb{Q}[x], \mathbb{Q}[x,y]$, etc. are Unique Factorization Domains.

Irreducibility in Integral Domains and Fields of Fractions

- We saw that if R is a Unique Factorization Domain with field of fractions F and $p(x) \in R[x]$, then we can factor out the greatest common divisor d of the coefficients of $p(x)$ to obtain $p(x) = dp'(x)$, where $p'(x)$ is irreducible in both $R[x]$ and $F[x]$.
- Let R be an arbitrary integral domain with field of fractions F.
  In R the notion of greatest common divisor may not make sense, but we may ask if, say, a monic polynomial which is irreducible in $R[x]$ is still irreducible in $F[x]$.
  - If a monic polynomial $p(x)$ is reducible, it must have a factorization $p(x) = a(x)b(x)$ in $R[x]$, with both $a(x)$ and $b(x)$ monic, nonconstant polynomials.
    So, a nonconstant monic polynomial $p(x)$ is irreducible if and only if it cannot be factored as a product of two monic polynomials of smaller degree.
  - We are now able to see that it is not true that if R is an arbitrary integral domain and $p(x)$ is a monic irreducible polynomial in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

The Integral Domain $\mathbb{Z}[2i]$

- Example: Consider

$$R = \mathbb{Z}[2i] = \{a + 2bi : a, b \in \mathbb{Z}\}.$$

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

The fraction field of R is $F = \{a + bi : a, b \in \mathbb{Q}\}$.

The polynomial $p(x)$ factors uniquely into a product of two linear factors in $F[x]$:

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

In particular, $p(x)$ is reducible in $F[x]$.

Neither of these factors lies in $R[x]$.

So $p(x)$ is irreducible in $R[x]$.

By the corollary, $\mathbb{Z}[2i]$ is not a Unique Factorization Domain.

Subsection 4

Irreducibility Criteria

Investigating Irreducibility in $R[x]$

- 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.
- It is of interest to determine the irreducible elements in such a polynomial ring, particularly in the ring $R[x]$.
- In the one-variable case, a non constant monic polynomial is irreducible in $R[x]$ if it cannot be factored as the product of two other polynomials of smaller degrees.
- Determining whether a polynomial has factors is frequently difficult to check, particularly for polynomials of large degree in several variables.
- The purpose of irreducibility criteria is to give an easier mechanism for determining when some types of polynomials are irreducible.
- For polynomials in one variable where the coefficient ring is a Unique Factorization Domain, it suffices, by Gauss' Lemma, to consider factorizations in $F[x]$ where F is the field of fractions of R.

Existence of Linear Factors in $F[x]$

Proposition

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, i.e., there is an $\alpha \in F$, with $p(\alpha) = 0$.

- Suppose $p(x)$ has a factor of degree one. Since F is a field, we may assume the factor is monic, i.e., is of the form $(x - \alpha)$, for some $\alpha \in F$. But then $p(\alpha) = 0$.
  Conversely, suppose $p(\alpha) = 0$. By the Division Algorithm in $F[x]$, we may write $p(x) = q(x)(x - \alpha) + r$, where r is a constant. Since $p(\alpha) = 0$, r must be 0. Hence $p(x)$ has $(x - \alpha)$ as a factor.

Proposition

A polynomial of degree two or three over a field F is reducible if and only if it has a root in F.

- A polynomial of degree two or three is reducible if and only if it has at least one linear factor.

A Divisibility Criterion

Proposition

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $\frac{r}{s} \in \mathbb{Q}$ is in lowest terms (i.e., r and s are relatively prime integers) and $\frac{r}{s}$ is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$: $r \mid a_0$ and $s \mid a_n$.
In particular, if $p(x)$ is a monic polynomial with integer coefficients and $p(d) \neq 0$, for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

- By hypothesis, $0 = p(\frac{r}{s}) = a_n (\frac{r}{s})^n + a_{n-1} (\frac{r}{s})^{n-1} + \cdots + a_0$. Multiply by s^n. We get $0 = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n$. Thus $a_n r^n = s(-a_{n-1} r^{n-1} - \cdots - a_0 s^{n-1})$. So s divides $a_n r^n$. By assumption, s is relatively prime to r. Hence, $s \mid a_n$. Similarly, solving the equation for $a_0 s^n$, we get $r \mid a_0$.

  The last assertion of the proposition follows from the previous ones.

Examples

(1) The polynomial $x^3 - 3x - 1$ is irreducible in $\mathbb{Z}[x]$. To prove this, by Gauss' Lemma and a preceding proposition, it suffices to show it has no rational roots. By the last proposition, the only candidates are integers which divide the constant term 1, namely ± 1. Substituting both 1 and -1 into the polynomial shows that these are not roots.

(2) For p any prime the polynomials $x^2 - p$ and $x^3 - p$ are irreducible in $\mathbb{Q}[x]$. This is because they have degrees ≤ 3, so it suffices to show they have no rational roots. The only candidates for roots are ± 1 and $\pm p$. None of these give 0 when they are substituted into the polynomial.

(3) The polynomial $x^2 + 1$ is reducible in $\mathbb{Z}/2\mathbb{Z}[x]$, since it has 1 as a root. It factors as $(x+1)^2$.

(4) The polynomial $x^2 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ since it does not have a root in $\mathbb{Z}/2\mathbb{Z}$: $0^2 + 0 + 1 = 1$ and $1^2 + 1 + 1 = 1$.

(5) Similarly, the polynomial $x^3 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$.

Reducibility in $R[x]$ and in $(R/I)[x]$

Proposition

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

- Suppose $p(x)$ cannot be factored in $(R/I)[x]$ but that $p(x)$ is reducible in $R[x]$. As noted at the end of the preceding section, this means there are monic, nonconstant polynomials $a(x)$ and $b(x)$ in $R[x]$, such that $p(x) = a(x)b(x)$. Reducing the coefficients modulo I gives a factorization in $(R/I)[x]$ with nonconstant factors, a contradiction.
- Thus, if it is possible to find a proper ideal I, such that the reduced polynomial cannot be factored, then the polynomial is itself irreducible.

Limitations of the Reduction Technique

- Unfortunately, there are examples of polynomials even in $\mathbb{Z}[x]$ which are irreducible but whose reductions modulo every ideal are reducible.

  So their irreducibility is not detectable by this technique.

  Example:
  - The polynomial $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every prime.
  - The polynomial $x^4 - 72x^2 + 4$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every integer.

Examples

(1) Consider the polynomial $p(x) = x^2 + x + 1$ in $\mathbb{Z}[x]$. Reducing modulo 2, we see from Example 4 above 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 $\mathbb{Z}/2\mathbb{Z}[x]$.

(2) The polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ since it is irreducible in $\mathbb{Z}/3\mathbb{Z}[x]$ (no root in $\mathbb{Z}/3\mathbb{Z}$), but is reducible mod 2.

This shows that the converse to Proposition 12 does not hold.

Examples in Several Variables

(3) The idea of reducing modulo an ideal to determine irreducibility can be used in several variables with some care:
$x^2 + xy + 1$ in $\mathbb{Z}[x, y]$ is irreducible since modulo the ideal (y) it is $x^2 + 1$ in $\mathbb{Z}[x]$, which is irreducible and of the same degree.
In general, we must be careful about "collapsing":
The polynomial $xy + x + y + 1$ (which is $(x + 1)(y + 1)$) is reducible, but appears irreducible modulo both (x) and (y). The reason is that non unit polynomials in $\mathbb{Z}[x, y]$ can reduce to units in the quotient. To take account of this, it is necessary to determine which elements in the original ring become units in the quotient.

- The elements in $\mathbb{Z}[x, y]$ which are units modulo (y), for example, are the polynomials in $\mathbb{Z}[x, y]$ with constant term ± 1 and all nonconstant terms divisible by y.

The fact that $x^2 + xy + 1$ and its reduction mod (y) have the same degree therefore eliminates the possibility of a factor which is a unit modulo (y), but not a unit in $\mathbb{Z}[x, y]$ and proves irreducibility.

The Eisenstein-Schönemann Criterion

Proposition (Eisenstein's Criterion)

Let P be a prime ideal of the integral domain R and let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial in $R[x]$ (here $n \geq 1$). If $a_{n-1}, \ldots, a_1, a_0$ are all elements of P and a_0 is not an element of P^2, then $f(x)$ is irreducible in $R[x]$.

- Suppose $f(x)$ were reducible, say $f(x) = a(x)b(x)$ in $R[x]$, where $a(x)$ and $b(x)$ are nonconstant polynomials. Reduce modulo P, using the assumptions on the coefficients. We get $x^n = \overline{a(x)}\ \overline{b(x)}$ in $(R/P)[x]$, where the bar denotes the polynomials with coefficients reduced mod P. Since P is a prime ideal, R/P is an integral domain. Thus, both $\overline{a(x)}$ and $\overline{b(x)}$ have 0 constant term. So, the constant terms of both $a(x)$ and $b(x)$ are elements of P. But then the constant term a_0 of $f(x)$ is an element of P^2, a contradiction.

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

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

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

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

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

Examples:

(1) The polynomial $x^4 + 10x + 5$ in $\mathbb{Z}[x]$ is irreducible by Eisenstein's Criterion applied for the prime 5.

(2) If a is any integer which is divisible by some prime p but not divisible by p^2, then $x^n - a$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Criterion.
In particular, $x^n - p$ is irreducible for all positive integers n.
So, for $n \geq 2$, the n-th roots of p are not rational numbers, i.e., this polynomial has no root in $\mathbb{Q}$.

Indirect Application of Eisenstein's Criterion

(3) Eisenstein's Criterion does not apply directly to $f(x) = x^4 + 1$.

Consider

$$\begin{aligned} g(x) &= f(x+1) \\ &= (x+1)^4 + 1 \\ &= x^4 + 4x^3 + 6x^2 + 4x + 2. \end{aligned}$$

Eisenstein's Criterion for the prime 2 shows that this polynomial is irreducible. It follows that $f(x)$ must also be irreducible, since any factorization for $f(x)$ would provide a factorization for $g(x)$ just by replacing x by $x + 1$ in each of the factors.

- Thus, Eisenstein's Criterion can sometimes be used to verify the irreducibility of a polynomial to which it does not immediately apply.

More Examples

(4) Let p be a prime and consider the polynomial

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

an example of a **cyclotomic polynomial**. Consider $\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p \in \mathbb{Z}[x]$. Eisenstein's Criterion applies for the prime p, since all the coefficients except the first are divisible by p by the Binomial Theorem. As before, this shows $\Phi_p(x)$ is irreducible in $\mathbb{Z}[x]$.

(5) Let $R = \mathbb{Q}[x]$ and let n be any positive integer.

Consider $X^n - x$ in the ring $R[X]$.

$R/(x) = \mathbb{Q}[x]/(x)$ is the integral domain $\mathbb{Q}$. Hence, the ideal (x) is prime in the coefficient ring R. Eisenstein's Criterion for the ideal (x) of R applies directly to show that $X^n - x$ is irreducible in $R[X]$.

Subsection 5

Polynomial Rings over Fields II

Quotients by Ideals Generated by Irreducible Polynomials

- Let F be a field.

Proposition

The maximal ideals in $F[x]$ are the ideals $(f(x))$ generated by irreducible polynomials $f(x)$. In particular, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

- A previous proposition applied to the Principal Ideal Domain $F[x]$.

Proposition

Let $g(x)$ be nonconstant in $F[x]$ and let $g(x) = f_1(x)^{n_1} f_2(x)^{n_2} \cdots f_k(x)^{n_k}$ be its factorization into irreducibles, with $f_i(x)$ distinct. Then as rings: $F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times F[x]/(f_2(x)^{n_2}) \times \cdots \times F[x]/(f_k(x)^{n_k})$.

- Suppose $f_i(x)$ and $f_j(x)$ are distinct and irreducible. Then, the ideals $(f_i(x)^{n_i})$ and $(f_j(x)^{n_j})$ are comaximal in $F[x]$. The conclusion now follows from the Chinese Remainder Theorem.

Roots and Factorization

- We look at the number of roots of a polynomial over a field F.
- A root a corresponds to a linear factor $(x - \alpha)$ of $f(x)$.
- If $f(x)$ is divisible by $(x - \alpha)^m$ but not by $(x - \alpha)^{m+1}$, then α is said to be a root of **multiplicity** m.

Proposition

If the polynomial $f(x)$ has roots $a_1, a_2, \ldots, a_k$ in F (not necessarily distinct), then $f(x)$ has $(x - a_1) \cdots (x - \alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in F, even counted with multiplicity.

- The first statement follows easily by induction from a preceding proposition.

  Since linear factors are irreducible, the second statement follows since $F[x]$ is a Unique Factorization Domain.

Finite Subgroups of Multiplicative Group of Fields

Proposition

A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^{\times}$ of nonzero elements of F is a cyclic group.

- We use the Fundamental Theorem of Finitely Generated Abelian Groups. By the Fundamental Theorem, the finite subgroup can be written as the direct product of cyclic groups

  $$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

  where $n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$.
  In general, if G is a cyclic group and $d \mid |G|$, then G contains precisely d elements of order dividing d.
  Since n_k divides the order of each of the cyclic groups in the direct product, it follows that each direct factor contains n_k elements of order dividing n_k.

Subgroups of Multiplicative Group of Fields (Cont'd)

- We wrote
$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$
where $n_k \mid n_{k-1} \mid \cdots \mid n_2 \mid n_1$.

  If k were greater than 1, there would therefore be a total of more than n_k elements of order dividing n_k.

  But then there would be more than n_k roots of the polynomial $x^{n_k} - 1$ in the field F, a contradiction. Hence $k = 1$ and the group is cyclic.

Corollary

Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes mod p is cyclic.

- This is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$.