BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India

Programme	:	M. Sc. Mathematics
Course Title	:	Algebra - II
Course Code	:	21S3M08CC

Unit - I

Prime and Maximal Ideals & Irreducible Polynomials

Dr. C. Durairajan

Professor

Department of Mathematics

Introduction

- Galois theory is the interplay between polynomials, fields, and groups.
- The quadratic formula giving the roots of a quadratic polynomial was essentially known by the Babylonians. By the middle of the sixteenth century, the cubic and quartic formulas were known.
- Almost three hundred years later, Abel (1824) proved, using ideas of Lagrange and Cauchy, that there is no analogous formula (involving only algebraic operations on the coefficients of the polynomial) giving the roots of a quintic polynomial (actually Ruffini (1799) outlined a proof of the same result, but his proof had gaps and it was not accepted by his contemporaries).

Continue ...

- In 1829, Abel gave a sufficient condition that a polynomial (of any degree) have such a formula for its roots (this theorem is the reason that, nowadays, commutative groups are called abelian).
- Shortly thereafter, Galois (1831) invented groups, associated a group to each polynomial, and used properties of this group to give, for any polynomial, a necessary and sufficient condition that there be a formula of the desired kind for its roots, thereby completely settling the problem.

Rings

A nonempty set R with two binary operations (usually written as addition and multiplication) is said to be a **ring** if

1. $(R, +)$ is an abelian group
2. $(R, \times)$ is a semigroup
3. two distributive laws hold

It is denoted by $(R, +, \times)$.

Example 1.

$\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R}), 2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ rings with respect to usual addition and multiplication.

Example 2.

The set $R = C[0, 1]$ of all real valued functions on the closed interval $[0, 1]$ is a ring with pointwise addition and multiplication.

Continue ...

- A ring R is said to be a **commutative ring** if the second operation satisfies the commutative property.
- In Example 1 and 2, all are commutative ring except $M_n(\mathbb{R}), n > 1$. A ring with identity is a ring R that contains a multiplicative identity element. We usually write the multiplicative identity as 1. In the Example 1 and 2, all are ring with identity except $2\mathbb{Z}$.
- A nonzero element a in a ring R is said to be a zero-divisor or divisor-of-zero if there exists a nonzero element $b \in R$ such that $ab = 0$.

Example 3.

Let n be a composite integer. Then the divisor d of n in $\mathbb{Z}_n$ is a zero-divisor.

Continue ...

- $\mathbb{Z}_n$ for n is composite integer , $M_n(\mathbb{R})$ for $n > 1$ have zero-divisors whereas $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ does not have zero-divisor but it is a commutative ring with no identity.
- A subset of a ring is said to be a **subring** if itself is a ring. A subring I of a ring R is said to be an **ideal** if for ever $r \in R, a \in I, ra \in I$.

Example 5.

Let R be a ring, then

- $\{0\}$ and R are ideals of R
- $aR = \{ar \mid r \in R\}$ is an ideal for all $a \in R$.

$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for all $n \in \mathbb{Z}$.

Prime Ideals

A proper ideal P in a ring R is called a **prime ideal** if $ab \in P$ implies $a \in P$ or $b \in P$.

Example 6.

1. $\langle x \rangle$ is a prime ideal in the ring $\mathbb{Z}[x]$
2. In any integral domain, $\{0\}$ is a prime ideal.
3. $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ for all prime integer p

Theorem 7.

A proper ideal P in R is a prime ideal if and only if $\frac{R}{P}$ is a domain.

Using this theorem, we can prove the above example.

Maximal Ideals

A proper ideal M in a ring R is said to be a **maximal ideal** if there is no ideal J with $M \subsetneqq J \subsetneqq R$.

Example 8.

1. In a field, $\{0\}$ is a maximal ideal
2. $\langle 2, x\rangle$ is a maximal ideal in $\mathbb{Z}[x]$.
3. Let p be a prime integer. Then $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$.

Theorem 9.

A proper ideal M in a ring R is a maximal ideal if and only if $\frac{R}{M}$ is a field.

Using this theorem, we can prove first problem in the above example.

Corollary 10.

Every maximal ideal I in a commutative ring R is a prime ideal.

- The converse of the above theorem need not be true. For example, in the Example 6, $\langle x\rangle$ is a prime ideal in $\mathbb{Z}[x]$ but not a maximal because $\langle x\rangle \subset \langle 2, x\rangle \subset \mathbb{Z}[x]$.
- If the ring is a principal ideal domain, then every prime ideal is a maximal ideal. That is, in a prinicpal ideal ring, the prime ideal and maximal ideal are the same.
- A polynomial $f(x) \in F[x]$ is said to be **splits over** $\mathbb{F}$ if it is a product of linear factors in $F[x]$.

Continue ...

Example 11.

1. The polynomial $f(x) = x^2 + 1 \in \mathbb{R}[x]$ can not split over $\mathbb{Q}$ but splits over $\mathbb{C}$ since $x^2 + 1 = (x - i)(x + i)$.
2. The polynomial $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ can not split over $\mathbb{Q}$ but splits over $\mathbb{R}$ since $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Theorem 12 (Kronecker).

Let $f(x)$ be a polynomial over a field $\mathbb{F}[x]$. There exists a field $\mathbb{E}$ containing $\mathbb{F}$ over which $f(x)$ splits.

The **prime field** of a field $\mathbb{F}$ is the intersection of all the subfields of F.

Theorem 13.

If $\mathbb{F}$ is a field, then its prime field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p.

Characteristic of a Field

1. A field has **characteristic** 0 if its prime field is isomorphic to $\mathbb{Q}$; it has **characteristic** p if its prime field is isomorphic to $\mathbb{Z}_p$.
2. A field of characteristic 0 has infinite number of elements.
3. The characteristic of a finite field is a prime integer.
4. It is noted that the characteristic of infinite field is either o or some prime inter p.
5. Galois proved the existence of finite field and the following theorem.

Theorem 14.

For every prime p and every positive integer n, there exists a field having exactly p^n elements.

Irreducible Polynomials

- A nonzero polynomial $p(x)$ over a field $\mathbb{F}[x]$ is said to be an **irreducible polynomial** over $\mathbb{F}$ if it can not be written as a product of two polynomials of degree greater than or equal to 1.

Theorem 15.

If $\mathbb{F}$ is afield, then a nonzero polynomial $p(x) \in F[x]$ is irreducible if and only if the ideal $(p(x))$ is a prime ideal.

- Since $\mathbb{F}[x]$ is a principal ideal domain, the prime ideal and maximal ideal are the same. Therefore, $\langle p(x) \rangle$ is a maximal ideal and hence by Theorem 9, $\frac{\mathbb{F}[x]}{\langle p(x) \rangle}$ is a field for any irreducible polynomial $p(x) \in \mathbb{F}[x]$.

continue ....

1. Let $(R_1, \Delta_1, \star_1)$ and $(R_2, \Delta_2, \star_2)$ be two rings. A map $\sigma : R_1 \to R_2$ is said to be a **ring homomorphism** if
    1. $\sigma(x \Delta_1 y) = \sigma(x) \Delta_2 \sigma(y)$
    2. $\sigma(x \star_1 y) = \sigma(x) \star_2 \sigma(y)$

    for all $x, y \in R_1$.
2. In a ring, hereafter we take the first operation as $+$, addition, the second operation as $\times$, multiplication and additive identity as 0 and mutiplicative identity as 1.
3. $\sigma(0) = 0, \sigma(-x) = -\sigma(x)$
4. If the ring homomorphism is from an integral domain into an integral domain, then $\sigma(1) = 1'$ where1 and $1'$ are identity elements with respect to the second operations of R_1 and R_2, respectively.

continue ....

If $\sigma : R \to S$ is a ring homomorphism, then $\sigma^* : R[x] \to S[x]$, defined by $\sigma^* : \sum r_i x^i \mapsto \sum \sigma(r_i) x^i$ is a ring homomorphism.

Theorem 16.

Let R be a domain and $\mathbb{F}$ be a field, let $\sigma : R \to \mathbb{F}$ be a ring map, and let $p(x) \in R[x]$. If $deg(\sigma^*(p)) = deg(p)$ and if $\sigma^*(p(x))$ is irreducible in $\mathbb{F}[x]$, then $p(x)$ is not a product of two polynomials in $R[x]$ each of degree less than $deg(p)$.

- A polynomial is said to be a **monic polynomial** if its leading coefficient is 1.
- Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. Then the gcd of its coefficients is called the content of $f(x)$. A polynomial is said to a **primitive** polynomial if the gcd of its coefficients is 1.

continue ...

From the above definition of primitive polynomial, it is clear that every monic polynomial is primitive but primitive polynomial need not be monic.

Example 17.

For example, $x^9 + 5x + 4$ monic and hence primitive but $3x^{111} + 2x^{25} - 111$ is primitive, not a monic.

Lemma 18 (Gauss's Lemma).

The product of two primitive polynomials $f(x)$ and $g(x)$ is itself primitive.

continue ...

Lemma 19.

Every nonzero $f(x) \in \mathbb{Q}[x]$ has a unique factorization $f(x) = c(f)f^*(x)$ where $c(f) \in \mathbb{Q}$ is positive and $f^*(x) \in \mathbb{Z}[X]$ is primitive.

The positive rational $c(f)$ of the above theorem is called the **content of** $f(x)$.

If a polynomial can not be written as a product of two polynomial of positive degree in an algebraic structure, then there is a possibility to write in the bigger algebraic structure containing it. But Gauss proved

Theorem 20.

If $p(x) \in \mathbb{Z}[X]$ is not a product of two polynomials in $\mathbb{Z}[x]$ each of degree $< deg(p)$, then $p(x)$ is irreducible in $\mathbb{Q}[x]$.

Cyclotomic Polynomials

- The set G of all n^{th} roots of unity form a cyclic group under multiplication.
- Its generator is called the **primitive n^{th} root of unity.**
- The polynomial

  $$\Phi_n(x) = \prod (x - \alpha)$$

  where the product is running over all primitive n^{th} root α of unity.
- Since G is cyclic group of order n, the degree of $\Phi_n(x)$ is $\phi(n)$, the Euler ϕ-function.
- If p is a prime, then the p^{th} cyclotomic polynomial is $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1.$

Cyclotomic Polynomials

Theorem 21 (Eisenstein Criterion).

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$. If there is a prime p dividing a_i for all $i < n$, but with p not dividing a_n and p^2 not dividing a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Using this theorem, we can prove

- The p^{th} cyclotomic polynomial $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$ for every prime p.
- If an integer a is not a petfect square, then $x^n - a$ is irreducible in $\mathbb{Q}[x]$ for every $n \geq 2$.

REFERENCES

- M. Artin, **Algebra**, Prentice Hall of India, New Delhi, 1994.
- David S. Dummit and Richard M. Foote,**Abstract Algebra**, 2nd Edition, Wiley Student Edition, 2008.
- I. N. Herstein, **Topics in Algebra**, John Wiley, 2nd Edition, 1975.
- Ian Stewart, **Galois Theory**, Chapman and Hall, 1973.
- Joseph Gallian, **Contemporary Abstract Algebra** , 9th Edition
- Joseph Rotman, **Galois Theory**, 2nd edition, Springer Verlag, 1990.
- C. Lanski, **Concepts in Abstract Algebra**, AMS Indian edition, 2010.
- Serge Lang, **Algebra** - Revised third edition, Springer, Verlag - 2002.
- R. Solomon, **Abstract Algebra**, AMS Indian edition, 2010.
- John B. Fraleigh, **A First course in Abstract Algebra**, Narosa Publishing House, 2003.