BHARATHIDASAN UNIVERSITY

Tiruchirappalli- 620024

Tamil Nadu, India

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

UNIT - II

CLASSICAL FORMULAS AND SPLITTING FIELDS

Dr. C. Durairajan

Professor

Department of Mathematics

Reduced Polynomials

In this Unit, we study the classical formulas for the roots of quadratics, cubics, and quartics.

Definition 1.

A polynomial $f(x)$ of degree n is called **reduced** if it has no x^{n-1} term; that is, $f(x) = a_n x^n + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \cdots$.

Example 2.

$f(x) = x^3 - 15x - 126$ be a reduced polynomial of degree 3.

Theorem 3.

If $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n_2}x^{n-2} + \cdots + a_1 x + a_0$, then replacing x by $x - \frac{a_{n-1}}{na_n}$ gives a reduced polynomial $\tilde{f}(x) = f(x - a_n/n)$. If α is a root of $f(x)$, then $\alpha - \frac{a_{n-1}}{na_n}$ is a root of its corresponding reduced polynomial.

Formula for the Roots of Polynomials

Lemma 4.

If α is a root of $f(X) = a_nX^n + a_{n-1}X^{n-1} + a_{n-2}x^{n-2} + \cdots$, then α is also a root of $\frac{1}{a_n}f(x)$.

To finding a formula for the polynomial, it is enough to find a formula monic reduced polynomial.

- The roots of quadratic polynomial $x^2 + bx + c$ are $\frac{-b\pm\sqrt{b^2-4c}}{2}$
- The roots of cubic polynomial $x^3 + qx + r$ are $y + z, \omega y + \omega^2 z, \omega^2 y + \omega z$ where $y^3 = \frac{1}{2}(-r + \sqrt{r^2 + 4q^3/27}), z = \frac{-q}{3y}$ and ω is a cube root of unity.

Continue ...

Consider the quartic polynomial $x^4 + qx^2 + rx + s$.

$$x^4 + qx^2 + rx + s = (x^2 + kx + l)(x^2 - kx + m)$$

Expanding the right side and equating coefficients of like terms gives:

$$l + m - k^2 = q, k(m - l) = r, lm = s.$$

The first two equations yield: $2m = k^2 + q + r/k, 2l = k^2 + q - r/k$.

Substituting these values of m and l into the third equation gives

$$k^6 + 2qk^4 + (q^2 - 4s)k^2 - r^2 = 0.$$

This is a cubic in k^2 and one can solve for k^2 using the cubic formula.

Substitute k, l, m values in the quadratic products, we get roots.

Exercises

Find the roots of the following polynomials $f(x) \in \mathbb{R}[x]$

1. $f(x) = x^3 - 3x + 1.$
2. $f(x) = x^3 - 9x + 28.$
3. $f(x) = x^3 - 24x^2 - 24x - 25.$
4. $f(x) = x^3 - 15x - 4.$
5. $f(x) = x^3 - 6x + 4.$
6. $f(x) = x^3 + x^2 - 36.$
7. $f(x) = x^4 - 15x^2 - 20x - 6.$
8. $f(x) = x^4 - 2x^2 + 8x - 3,$
9. $f(x) = x^4 - 2x^2 + 8x - 3.$

Field Extensions

If $\mathbb{F}$ is a subfield of a field $\mathbb{E}$, then $\mathbb{E}$ is called an **extension field of** $\mathbb{F}$ and we writes $\mathbb{E} \mid \mathbb{F}$ is a field extension.

Lemma 5.

Let $\mathbb{E} \mid \mathbb{F}$ be a field extension, let $\alpha \in \mathbb{E}$ and let $p(x) \in \mathbb{F}[x]$ be a monic irreducible having α as a root. Then

1. *$deg(p) < deg(f)$ for every $f(x) \in \mathbb{F}[x]$ having α as a root.*
2. *$p(x)$ is the only monic polynomial in $\mathbb{F}[x]$ of degree $deg(p(x))$ that has α as a root.*

The dimension of $\mathbb{E}$ viewed as a vector space over $\mathbb{F}$ is called the **degree** of $\mathbb{E}$ over $\mathbb{F}$ and it is denoted by $[\mathbb{E} : \mathbb{F}]$. One says that $\mathbb{E} \mid \mathbb{F}$ is a **finite extension** if $[\mathbb{E} : \mathbb{F}]$ is finite. Otherwise, we call it an infinite extension.

Continue ...

The following lemma is known as the Tower Lemma

Lemma 6.

If $\mathbb{F} \subseteq \mathbb{B} \subseteq \mathbb{E}$ are fields with $[\mathbb{E} : \mathbb{B}]$ and $[\mathbb{B} : \mathbb{F}]$ finite, then $\mathbb{E} \mid \mathbb{F}$ is finite and $[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{B}][\mathbb{B} : \mathbb{F}]$.

Theorem 7.

Let $p(x) \in \mathbb{F}[x]$ be an irreducible polynomial of degree d. Then $\mathbb{E} = \frac{\mathbb{F}[x]}{\langle p(x) \rangle}$ is a field extension of $\mathbb{F}$ of degree d.

Indeed, $\mathbb{E}$ contains a root α of $p(x)$, and a basis of $\mathbb{E}$ as a vector space over $\mathbb{F}$ is $\{1, \alpha, \alpha^2, \cdots, \alpha^{d-1}\}$.

- Let $\mathbb{E} \mid \mathbb{F}$ be a field extension, and let $\alpha_1, \cdots, \alpha_n \in \mathbb{E}$. Then $\mathbb{F}(\alpha_1, \cdots, \alpha_n)$ is called the field obtained by **adjoining** $\alpha_1, \cdots, \alpha_n$ to $\mathbb{F}$.

Continue ...

- In fact, it is the intersection of all the subfields of $\mathbb{E}$ which contain $\mathbb{F}$ and $\{\alpha_1, \cdots, \alpha_n\}$. That is , the smallest field containing both $\mathbb{F}$ and $\{\alpha_1, \cdots, \alpha_n\}$.
- An extension $\mathbb{E} \mid \mathbb{F}$ is called a **simple extension** if it is obtained by adjoining just one element α to $\mathbb{F}$.
- That is, $\mathbb{E} = \mathbb{F}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in \mathbb{F}[x] \text{ and } g(\alpha) \neq 0 \right\}$. In fact $[\mathbb{F}(\alpha) : \mathbb{F}] = \deg(irr(\alpha, \mathbb{F}))$, the degree of monic irreducible polynomial over $\mathbb{F}$ with α as a root.

  Let $\mathbb{E} \mid \mathbb{F}$ be a field extension, and let $\alpha \in \mathbb{E}$. Then α is said to be **algebraic over** $\mathbb{F}$ if α is a root of some nonzero polynomial in $\mathbb{F}[x]$. Otherwise α is called **transcendental over** $\mathbb{F}$. A field extension $\mathbb{E} \mid \mathbb{F}$ is called **algebraic** if every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$.

Continue ...

Theorem 8.

Every finite extension is an algebraic extension.

The converse of this theorem is false.

Example 9.

Let $\mathbb{A}$ to be the set of all complex numbers which are algebraic over $\mathbb{Q}$. Then $\mathbb{A} \mid \mathbb{Q}$ is an algebraic extension that is not finite.

Suppose it is $\mathbb{A} \mid \mathbb{Q}$ finite, say $n > 1$. Then By Eisenstein Criterion, $x^{n+1} - 2$ is irreducible over $\mathbb{Q}$ and hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n + 1$ where α is a root of the irreducible polynomial $x^{n+1} - 2$. By Tower Lemma, $[\mathbb{A} : \mathbb{Q}] > n + 1$, a contradiction.

Continue ...

Theorem 10.

Let $\mathbb{E} \mid \mathbb{F}$ be a field extension and let $\alpha \in \mathbb{E}$ be algebraic over $\mathbb{F}$. Then

1. *there is a monic irreducible polynomial $p(x) \in \mathbb{F}[x]$ having α as a root;*
2. $\frac{\mathbb{F}[x]}{\langle p(x) \rangle} \cong \mathbb{F}(\alpha)$; *in fact, there is an isomorphism* $\Phi : \frac{\mathbb{F}[x]}{\langle p(x) \rangle} \to \mathbb{F}(\alpha)$, *fixing $\mathbb{F}$ pointwise, with* $\Phi(x + (p(x))) = \alpha$.
3. *$p(x)$ is the unique monic polynomial of least degree in $\mathbb{F}[x]$ having α as a root;*
4. $[\mathbb{F}(\alpha) : \mathbb{F}] = deg(p(x))$.

Splitting Fields

A **splitting field** of $f(x) \in \mathbb{F}[x]$ is a field extension $\mathbb{E} \mid \mathbb{F}$ in which $f(x)$ splits (it is a product of linear factors) but $f(x)$ does not split in any proper subfield of $\mathbb{E}$.

Note that if $\mathbb{E}$ is a splitting of $f(x)$, then it is the smallest field containing all roots of $f(x)$.

Example 11.

If ω is a primitive cube root of unity, then $x^3 - 1 \in \mathbb{Q}[x]$ splits over $\mathbb{C}$, but its splitting field is $\mathbb{Q}(\omega)$.

By Kronecker's theorem, we have the following

Theorem 12.

If $\mathbb{F}$ is a field, then every polynomial $f(x) \in \mathbb{F}[x]$ has a splitting field.

Continue ...

An irreducible polynomial is said to a **separable polynomial** if all of its roots are distinct. A polynomial $f(x)$ is said to be a **separable polynomial** if its irreducible factors (not necessarily distinct) are separable.

Theorem 13.

Let $\sigma : \mathbb{F} \to \mathbb{F}'$ *be an isomorphism of fields, let* $f(x) \in \mathbb{F}[x]$*, and let* $f^*(x) = \sigma^*(f(x))$ *be the corresponding polynomial in* $\mathbb{F}'[x]$*; let* $\mathbb{E}$ *be a splitting field of* $f(x)$ *over* $\mathbb{F}$ *and let* $\mathbb{E}'$ *be a splitting field of* $f^*(x)$ *over* $\mathbb{F}'$*. Then*

1. *there is an isomorphism* $\tilde{\sigma} : \mathbb{E} \to \mathbb{E}'$ *extending* σ*.*
2. *If* $f(x)$ *is separable, then* σ *has exactly* $[\mathbb{E} : \mathbb{F}]$ *extensions* $\tilde{\sigma}$*.*

Continue ...

Definition 14.

If $\mathbb{E} \mid \mathbb{F}$ is an extension, then $\alpha \in \mathbb{E}$ is called **separable** if either it is transcendental or its irreducible polynomial is separable. An extension is called **separable** if every one of its elements is separable.

Corollary 15.

If $f(x) \in \mathbb{F}[x]$, then any two splitting fields of $f(x)$ over $\mathbb{F}$ are isomorphic by an isomorphism fixing $\mathbb{F}$ pointwise.

Theorem 16 (E.H. Moore).

If $f(x) \in \mathbb{F}[x]$, then any two splitting fields of $f(x)$ over $\mathbb{F}$ are isomorphic by an isomorphism fixing $\mathbb{F}$ pointwise.

One calls the field of order p^n the **Galois field** of this order and denotes it by $GF(p^n)$, although $GF(p)$ is usually denoted by $\mathbb{Z}_p$.

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.