4

Ruler and Compass Construction

Structure

4.1. Introduction. In this chapter, possibility to construct some geometrical figures using ruler and compass are discussed by the help of some algebraic structures. Also the solvability by radicals of generic polynomial is discussed

4.1.1. Objective. The objective of these contents is to provide some important results to the reader like:

(i) Normal Extensions.

(ii) Fixed Fields, Galios Groups

(iii) Norms and Traces.

4.1.2. Keywords. Normal Extensions, Galois Group, Fixed Fields.

4.2. Ruler-and-compasses constructions.

Three main problem of Geometry are:

Using the traditional geometrical instruments ruler and compasses can we

1. Trisect an arbitrary given angle.
2. Construct a cube having volume double to that of a given cube.
3. Construct a square with area equal to that of a given circle.

We shall show that these three problems are insolvable.

Consider the Euclidean plane and two straight lines intersecting at right angles in this plane meeting at a point O. Assume I is an arbitrary point on one of those lines. Then, by taking O as origin and I to be the point $(1,0)$, we can set up a Cartesian coordinate system in the plane. Let B be a collection of points in this plane, including O and I. With the points in B we can start our construction and so these points will be called basic points.

By ruler-and-compasses construction based on B we mean a finite sequence of operations of the following types:

(1) Drawing a straight line through two points which are either basic points or points previously constructed in the sequence of operations.

(2) Drawing a circle with center at a basic point or a point previously constructed with radius equal to the distance between two points, each of which is either a basic point or a point previously constructed.

(3) Obtaining points of intersection of any two obtained in (1) and (2), which are (a) points of straight lines, (b) pairs of circles, (c) straight lines and circles.

Any point P which is obtained by (3) based on B is said to be **constructible from** B. If B consists of the points O and I and no others, we simply say that B is **constructible.**

Let P be any point of the plane with coordinates (α, β) determined by O and I. The subfield of $\mathbf{R}$ obtained by adjoining α and β to $\mathbf{B}$ will be denoted by $\mathbf{B}(P)$.

4.2.1. Theorem. If the point P is constructible from B, then the $[\mathbf{B}(P) : \mathbf{B}] = 2^n$ for some non-negative integer n.

Proof. To obtain P from B in ruler-and-compasses construction let the sequence is $P_1, P_2, \dots, P_n = P$ of operations of type (3). Suppose that P_1 is one of the basic points and the co-ordinates of $P_i (i = 1, \dots, n)$ be (α_i, β_i).

Let $K = \mathbf{B}(P_1, \dots, P_n)$. We claim that $[\mathbf{K} : \mathbf{B}] = 2^n$. Then the result follows directly as $\mathbf{B}(P)$ is a subfield of K and hence $[\mathbf{B}(P) : \mathbf{B}]$ is a factor of $[K : \mathbf{B}]$.

We prove by induction on n.

If $n = 1$, then $K = \mathbf{B}(P_1) = \mathbf{B}$, thus $[K : \mathbf{B}] = 1 = 2^0$.

Now assume result holds for $n = k\text{-}1$, that is, if L is the subfield of $\mathbf{R}$ obtained by adjoining to $\mathbf{B}$ the coordinates of $P_1, \dots, P_{k-1}$ then $[L : \mathbf{B}] = 2^s$ for some s.

If P_i and P_j are distinct points $(1 \le i, j \le k-1)$ then the equation of straight line λ_{ij} joining them is

$$(\alpha_j - \alpha_i)(y - \beta_i) = (\beta_j - \beta_i)(x - \alpha_i).$$

Similarly, if P_r and P_s are distinct points and P_t is any point $(1 \le r, s, t \le k-1)$, then the equation of circle $\sum_{rs}^{t}$, with center P_t and radius equal to the distance between P_r and P_s is

$$(x - \alpha_t)^2 + (y - \beta_t)^2 = (\alpha_r - \alpha_s)^2 + (\beta_r - \beta_s)^2. \qquad (1)$$

Let T $= \mathbf{B}\,(P_1, \ldots, P_k)$ =L(P_k). If P_k is obtained from $P_1, \ldots, P_{k-1}$ by intersection of two lines like λ_{ij}, then its coordinates are obtained by solving two linear equations with coefficients in L and so its coordinates lie in L Thus, T = L and so $[L : \mathbf{B}] = [T : \mathbf{B}] = 2^s$.

Similarly, in other cases $[T : \mathbf{B}] = 2^t$ for some *t* (Left as an exercise to the reader).

This completes the Proof.

4.2.2. Theorem. Let P be a point in the plane and $\mathbf{B}(P)$ has a sequence of subfields, $\mathbf{B}(P) = K_n, K_{n-1}, \ldots, K_1, K_0 = \mathbf{B}$ such that K_i includes K_{i-1} and$[K_i : K_{i-1}] = 2 (i = 1, \ldots, n),$ then P is constructible from B.

Proof. We proceed by induction on $n.$

If $n = 0$ then$\mathbf{B}(P) = \mathbf{B}.$ Hence, P is constructible from B. Now, let result holds for *n = k-1*.

Assume that K has a sequence of subfields $K = K_k, K_{k-1}, \ldots, K_1, K_0 = \mathbf{B}$. Since $[K_k : K_{k-1}] = 2,$ it follows that K_k is a normal extension of K_{k-1}. If $\beta \in K_k$ such that $\beta \notin K_{k-1}$, then $K_k = K_{k-1}(\beta)$. If minimum polynomial of β over K_{k-1} is $X^2 + aX + b = (X + \frac{1}{2}a)^2 + (b - \frac{1}{4}a^2)$. Considering$\alpha = \beta + \frac{1}{2}a$, we have $\alpha^2 = \frac{1}{4}a^2 - b \ge 0;$ thus α^2 is a positive element of K_{k-1} and clearly $K_k = K_{k-1}(\beta) = K_{k-1}(\alpha)$.

Now, since $(\alpha^2, 0)$ has coordinates in K_{k-1}, it is constructible from **B,** by the induction hypothesis. Hence every point with coordinates in K_k is constructible from B. This completes the induction.

4.2.3. Corollary. Let P be a point in the plane. If the field$\mathbf{B}(P)$ is a normal extension of $\mathbf{B}$ such that $[\mathbf{B}(P) : \mathbf{B}]$ is a power of 2, then the point P is constructible from B.

Proof. Let G be the Galois group of $\mathbf{B}(P)$ over $\mathbf{B}$, Then |G| = [$\mathbf{B}(P)$: $\mathbf{B}$] = 2^s. Then, G has a sequence of subgroups, $G = A_0, A_1, A_2, ..., A_n = \{e\}$ each of index 2 in the preceding. Thus, $\mathbf{B}(P)$ has a sequence of subfields $\mathbf{B}(P) = K_0, K_1, K_2, ..., K_n = \mathbf{B}$ each of degree 2 over the next. Hence P is constructible from B.

4.3. Solution by radicals.

Let F be a field of characteristic zero and E is an extension of F, then E is said to be an **extension** of F by **radicals** if there exists a sequence of subfields $F = E_0$, E_1 , … , E_{r-1}, $E_r = E$ such that

$$E_{i+1} = E_i(\alpha_i),$$

for i = 0 , …, r -1, where α_i is a root of an irreducible polynomial in $P(E_i)$ of the form $X^{ni} - a_i$. A polynomial f(x) in F[x] is said to be **solvable by radicals** if the splitting field of f(x) over F is contained in an extension of F by radicals.

4.3.1. Theorem. Let F be a field of characteristic zero, K a normal extension of F with G(K,F) is abelian. If [K : F] = n and the polynomial $k_n = X^n - 1$ splits completely in F[X], then K is an extension of F by radicals.

Proof. Let *G* = G(K,F). Then, G may be expressed as a direct product of cyclic groups, say

$$G = C_1 \text{ x } ... \text{ x } C_r.$$

Define, $G_i = C_1 \text{ x } C_2 \text{ x } ... \text{ x } C_{r-i}$, for $i = 0, ..., r - 1$, and $G_r =< I >$, where I is the identity element of *G*. Then G_{i+1} is a normal subgroup of G_i and

$$G_i/G_{i+1} \cong C_i \qquad \text{for } i = 0, ..., r - 1.$$

Let E_i be the subfield of K left fixed by G_i for i = 0, …, r. Then, E_{i+1} is a normal extension of E_i with cyclic Galois group, isomorphic to C_{r-1} for i = 0, …, r-1. Since the degree n_i of E_{i+1} over E_i is a factor of n and k_n splits completely in F[X] and hence in E_i[X], it follows that k_n splits completely in E_i[X]. So $E_{i+1} = E_i(\alpha_i)$ where α_i is a root of an irreducible polynomial in E_i[X] of the form $X^{ni} - a_i$ for i = 0, …, r -1.

Thus K is an extension of F by radicals, as asserted.

4.3.2. Theorem. Let F be a field of characteristic zero. For every positive integer n, the polynomial $k_n = X^n – 1$ in F[X] is solvable by radicals.

Proof. We prove the result by induction on n.

If n = 1, then the splitting field for k_n over F is F itself, which is an extension of itself by radicals.

Now, suppose that every polynomial k_l with $l < m$ is solvable by radicals.

Let K_m be a splitting field of k_m over F containing F. If $[K_m : F] = r$, then $r \leq \varphi(m) < m$. According to induction hypothesis, k_r is solvable by radicals and so there is a splitting field K_r of k_r over F which is contained in an extension E of F by radicals. Without loss of generality assume that E and K_m are contained in the same algebraic closure C of F, then consider $L = E(K_m) \subseteq C$.

Then, L is a separable normal extension of E and the Galois group G(L, E) of L over E is isomorphic to a subgroup of the Galois group $G(K_m, F)$ of K_m over F. Hence G(L, E) is Abelian. It follows that s = [L : E] is a factor of $r = [K_m : F]$. Since k_r splits completely in E[X], so too does k_s. Thus L is an extension of E by radicals. Since E is also an extension of F by radicals it follows that L is also an extension of F by radicals and hence k_m is solvable by radicals.

This completes the induction.

Before proceeding further, we discuss some results of solvable groups.

4.4. Solvable Group. A group G is said to be solvable if there exists a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = <e>$$

such that (i) $G_{i+1} \trianglelefteq G_i$ for $0 \leq i \leq n-1$

(ii) G_i / G_{i+1} is abelian for $0 \leq i \leq n-1$.

Results.

1. Every subgroup of a solvable group is solvable.
2. Every quotient group of a solvable group is solvable.
3. Let G be a group and H be a normal subgroup of G. Then if H and G/H both are solvable, then prove that G is also a solvable group.
4. A finite p-group is solvable.
5. Direct product of two solvable groups is solvable .
6. Let H and K are solvable subgroups of G and $H \trianglelefteq G$ then HK is also solvable.
7. Show that every group of order pq is solvable where p , q are prime numbers not necessarily distinct.
8. Prove that every group of order p^2q , p and q are primes , is solvable .
9. S_n is solvable for $n \leq 4$.
10. S_n is not solvable for $n > 4$.
11. If a subgroup G of S_n ($n > 4$) contains every 3 – cycle and H be any normal subgroup of G such that G/H is abelian then H contains all the 3 – cycles.
12. Homomorphic image of a solvable group is solvable.
13. A finite group G is solvable iff there exist a sequence of subgroups
$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = < e >$$
such that $G_{i+1} \trianglelefteq G_i$ and G_i / G_{i+1} is cyclic group of prime order for $0 \leq i \leq n$.
14. A group G in is solvable iff $G^{(n)} = < e >$ for some $n \geq 0$.
15. A_n is not solvable for $n \geq 5$ and hence S_n is also not solvable for $n \geq 5$.

We now state a criterion for a polynomial to be solvable by radicals.

4.4.1. Exercise. Let F be a field of characteristic zero. A polynomial f(x) in F[x] has splitting field over F with a solvable Galois group iff f(x) is solvable by radicals.

4.5. Solution of Polynomial Equations by Radicals.

An extension field K of F is called a radical extension of F if there exist elements $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$ such that

1. $K = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$
2. $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$ for $i = 1, 2, \ldots, m$ and integers $n_1, n_2, \ldots, n_m$

For $f(x) \in F[x]$ the polynomial equation f(x) = 0 is said to be solvable by radicals if there exists a radical extension K of F that contains all roots of f(x).

If now $\{x_1, \ldots, x_n\}$ is asubset of a field E algebraically independent over the subfield F of E, the polynomial

$$g_n = X^n - x_1 X^{n-1} + x_2 X^{n-2} - \ldots + (-1)^n x_n$$

in $P(F(x))$ is called a **generic polynomial** of degree n over F. So a generic polynomial over F is one which has no polynomial relations with coefficients in F connecting its coefficients

4.5.1. Theorem. Let $g_n = X^n - x_1 X^{n-1} + \ldots + (-1)^n x_n$ be a generic polynomial of degree n over a field F of characteristic zero. Then the Galois group of any splitting field of g_n over $F(x_1, \ldots, x_n) = F(x)$ is isomorphic to the symmetric group on n digits. **(Left as an exercise for students)**

4.5.2. Theorem. The generic polynomial of degree $n \geq 5$ is not solvable by radicals.

Proof. Since the Galois group of any splitting field of g_n over $F(x_1, \ldots, x_n) = F(x)$ is isomorphic to the symmetric group S_n,. But S_n is not solvable group when $n \geq 5$. Hence f(x) is not solvable by radicals over $F(x_1, \ldots, x_n) = F(x)$ when $n \geq 5$.

4.6. Check Your Progress.

1. Design fields of order 27, 16, 25, 49.
2. Compute ϕ_{30}.

4.7. Summary.

Constructing a cube having volume double to that of a given cube is equivalent to the construction from the basic points O and I of the point $(\alpha, 0)$, where α is the real number such that $\alpha^3 = 2$. Since the polynomial $X^3 - 2$ is irreducible in $P(\mathbf{Q})$, the field $\mathbf{Q}(\alpha)$ has degree 3 over $\mathbf{Q}$ and hence, since 3 is not a power of 2, the point $(\alpha, 0)$ is not constructible from O and I. Constructing a square with area equal to that of a given circle is equivalent to the construction of the point $(\sqrt{\pi}, 0)$. However, π is not algebraic over the field of rational numbers. Hence $(\mathbf{Q}(\pi) : \mathbf{Q})$ is infinite and hence cannot a power of 2.

Books Suggested:

1. Stewart, I., Galios Theory, Chapman and Hall/CRC, 2004.
2. Adamson, I. T., Introduction to Field Theory, Cambridge University Press, 1982.