Abel's Theorem DRP

Max Chien

January 2024

Introduction

The well-known quadratic formula expresses the roots of an arbitrary polynomial of degree two in terms of the coefficients a_1, a_2, a_3:

$$x_1 = \frac{-a_2 + \sqrt{a_2^2 - 4a_1a_3}}{2a_1}$$
$$x_2 = \frac{-a_2 - \sqrt{a_2^2 - 4a_1a_3}}{2a_1}$$

Similar but less well known formulas exist for expressing the roots of polynomials of degree three and four in terms of their coefficients. However, the Abel-Ruffini theorem shows that no formula may express the roots of an arbitrary polynomial of degree five or higher, using radicals in terms of its coefficients.

Drawing from *Abel's Theorem in Problems and Solutions*, by V.B. Alekseev, we will prove Abel's Theorem using results about the monodromy groups of functions expressible by radicals. This text will begin with a treatment of groups. Then, it will develop the theory of multivalued functions. Finally, it will define the monodromy group of a multivalued function in order to prove the Abel-Ruffini theorem. Proofs will generally be omitted throughout, except when particularly instructive.

Chapter 1

Groups

1.1 Motivations

Across mathematics, many mathematical structures permit the combination of two objects of a certain type to obtain another of the same type. For instance, given two functions f, g, if the range of g is contained in the domain of f, then the composition $f \circ g$ gives a new function. Given two integers $x, y \in \mathbb{Z}$, $x + y$ is also an integer (as is xy). The notion of a *binary operation* captures this process. The study of groups, therefore, is the study of mathematical structures where binary operations obey certain axioms.

1.2 Elementary Group Theory

Definition 1. *A **binary operation** on a set M is a function $M \times M \to M$. The result of applying a binary operation $*$ on $(a, b) \in M \times M$ is denoted $a * b$, though the $*$ is often omitted when unambiguous.*

Definition 2. *A **group** is a set G together with a binary operation $*$ on G that satisfies the following axioms:*

- *$*$ is associative: $(a * b) * c = a * (b * c)$ for any $a, b, c \in G$.*
- *There exists an **identity element** $e \in G$ such that $ae = ea = a$ for any $a \in G$.*
- *For any $a \in G$, there exists an **inverse element** $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.*

Example. $(\mathbb{Z}, +)$ is a group. $\mathbb{Z}$ is closed under addition and addition is associative. For any integer m, $m + 0 = 0 + m = m$, so 0 is the identity element. $-m$ is also an integer, so inverses exist. $\triangle$

Example. $(\mathbb{R}^+, *)$ is a group. It is closed under multiplication, which is associative. 1 is the identity element, and the multiplicative inverse of a positive real x is $1/x$, which is also a positive real. $\triangle$

Example. $(\mathbb{R}, *)$ is not a group, since there is no real number x such that $0x = 1$, so 0^{-1} does not exist. $\triangle$

The following properties are immediate consequences of the group axioms, and their proofs are omitted.

- The product $a_1 * a_2 * a_3 * \ldots * a_n$ is associative.
- The identity element of a group is unique.
- The inverse of an element $a \in G$ is unique.
- $(a^{-1})^{-1} = a$.
- $(ab)^{-1} = b^{-1}a^{-1}$.

Definition 3. *A **finite group** is a group with a finite number of elements. The number of elements is called its **order**. An **infinite group** is a group with an infinite number of elements.*

Definition 4. *Two elements $a, b \in G$ commute if $ab = ba$. A group where every pair of elements commutes is an **abelian group**.*

Definition 5. *Let $(G, *_G)$ be a group. If $(H, *_G)$ is a group, with $H \subseteq G$, then $(H, *_G)$ is a **subgroup** of $(G, *_G)$, denoted $H \leq G$. If $H = \{e\}$, then H is called **trivial**.*

The following properties are immediate consequences of the definition of a subgroup:

- If e is the identity element of G, then $e \in H$ for any $H \leq G$.
- If $a, b \in H \leq G$, then $a *_G b \in H$ and $a_G^{-1} \in H$.
- The arbitrary intersection of subgroups is a subgroup.

Example. The rotations of a triangle is a subgroup of the symmetries of a triangle. The even integers are a subgroup of the integers. $\triangle$

1.3 Symmetry Groups

Definition 6. *A bijection $\phi : M \to M$ is a **transformation** of M. A transformation of a geometric figure which preserves distance is a **symmetry**.*

Example. Rotating an equilateral triangle by 120 degrees is a symmetry of the triangle. $\triangle$

Definition 7. *Given a geometric figure K, the symmetry group S of K is the set of all symmetries of K, with composition as the group operation ($\phi_1\phi_2 = \phi_1 \circ \phi_2 = \phi_1(\phi_2)$).*

Remark. Composition is associative for all functions, so it is associative for symmetries. The composition of two symmetries is a symmetry. The identity transformation $\phi_{id} : x \mapsto x$ acts as the identity element, and since a symmetry is bijective, the inverse ϕ^{-1} is also a symmetry satisfying $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \phi_{id}$ for any ϕ. Thus, the symmetry group as defined above is indeed a group.

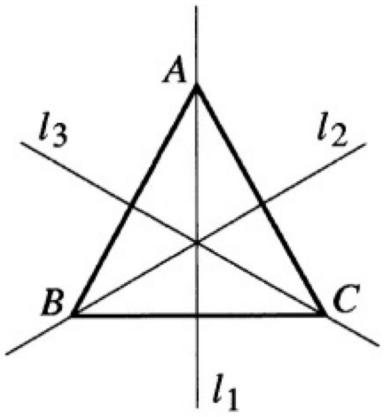

Figure 1.1:

Example. An equilateral triangle has six symmetries: rotation by 0, 120, and 240 degrees counterclockwise, which we denote e, r_1, r_2, and reflection over the axes of symmetry, which we denote l_1, l_2, l_3 according to Figure 1.1. When considered as a symmetry group, the symmetries have the composition table displayed in Table 1.1, where the column symmetry is performed first. Note that the group is not abelian; however, the subgroup of rotations is abelian. $\triangle$

	e	r_1	r_2	l_1	l_2	l_3
e	e	r_1	r_2	l_1	l_2	l_3
r_1	r_1	r_2	e	l_3	l_1	l_2
r_2	r_2	e	r_1	l_2	l_3	l_1
l_1	l_1	l_2	l_3	e	r_1	r_2
l_2	l_2	l_3	l_1	r_2	e	r_1
l_3	l_3	l_1	l_2	r_1	r_2	e

Table 1.1:

1.4 Cyclic Groups and Isomorphisms

Definition 8. *If $\{a_1, a_2, a_3 \ldots\} \subseteq G$, then the **generated subgroup**, denoted $\langle\{a_1, a_2, a_3 \ldots\}\rangle$, is the subset of G which can be obtained by finitely many multiplications and inversions of elements of $\{a_1, a_2, a_3 \ldots\}$. This subset is a subgroup of G.*

Definition 9. *A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$, and a is called a **generator** of G.*

Example. The group of rotations of a triangle is cyclic, with generators r_1 and r_2, but not e. △

Example. For any n, the set of integers $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$ with addition defined modulo n is a cyclic group of order n. △

In many cases, we are more interested with the structure of a group than the elements of the group themselves. The definition of an isomorphism formalizes the notion of two groups having identical structure.

Definition 10. *An **isomorphism** between two groups G_1, G_2 is a bijection $\phi : G_1 \to G_2$ such that for any $g_1, g_2 \in G_1$, $\phi(g_1 *_{G_1} g_2) = \phi(g_1) *_{G_2} \phi(g_2)$. G_1 and G_2 are isomorphic, denoted $G_1 \cong G_2$, if there is an isomorphism between them.*

The following are immediate consequences of the definition of an isomorphism:

- $G_1 \cong G_2, G_2 \cong G_3 \implies G_1 \cong G_3$.
- If $E \cong F$ under ϕ, then $\phi(e_E) = \phi(e_F)$.
- If $\phi : G \to F$ is an isomorphism, then $\phi(g_G^{-1}) = [\phi(g)]_F^{-1}$ for any $g \in G$.
- If G is abelian and $G \cong H$, then H is abelian.

Example. The group of rotations of a triangle is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. △

Lemma. For any $a, m, r, k \in \mathbb{Z}/n\mathbb{Z}$, $a^m * a^r = a^k$ if and only if $m + r \equiv k \mod n$.

Theorem 1. *If C is an arbitrary cyclic group of order n, then $C \cong \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let a generate C. For any $g \in C$, $g = a^m$ for some $m \in \{0, 1, \ldots, n-1\}$. Define $\phi : C \to \mathbb{Z}/n\mathbb{Z}$ such that ϕ maps $g = a^m$ to m. Let $b = a^x$, $c = a^y$ be elements of C. Then by the lemma, $\phi(bc) = \phi(a^{x+y}) = x +_n y$, where $+_n$ denotes addition modulo n. Moreover, $\phi(b) +_n \phi(c) = \phi(a^x) +_n \phi(a^y) = x +_n y$. Thus $\phi(b *_C c) = \phi(b) +_n \phi(c)$, and ϕ is bijective, so ϕ is an isomorphism and thus $C \cong \mathbb{Z}/n\mathbb{Z}$. □

Theorem 2. *If C is an arbitrary infinite cyclic group, then $C \cong \mathbb{Z}$.*

Corollary. If G is cyclic, it is abelian.

1.5 Direct Products, Cosets, Normal Subgroups, and Quotient Groups

Definition 11. *The **direct product** of two groups G, H, denoted $G \times H$, is the set of ordered pairs $\{(g, h) : g \in G, h \in H\}$, with the operation taken componentwise: $(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$.*

The following are immediate consequences of the definition of the direct product:

- $G \times H \cong H \times G$
- There exist $G', H' \leq G \times H$ such that $G' \cong G$ and $H' \cong H$.
- $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if and only if m, n are relatively prime.
- If G has order m and H has order n, then $G \times H$ has order mn.

Definition 12. *Let $H \leq G$. Then for any $g \in G$, the **left coset** of H in G is the set $gH = \{gh : h \in H\}$.*

The following are immediate consequences of the definition:

- If H has order n, then gH has order n for any $g \in G$.
- For $H \leq G$, for any $g \in G$, g is in at least one left coset of H in G.
- If $x \in yH$, then $xH = yH$.
- If $z \in xH$ and $z \in yH$, then $xH = yH$.

Definition 13. *The results above imply that any $H \leq G$ partitions G into a collection of left cosets, such that any two left cosets are either equal or disjoint, but the union is equal to G. We call this the **left partition** of G by H.*

Theorem 3 (Lagrange's Theorem)**.** *If $H \leq G$, G has order n, and H has order m, then m divides G.*

Proof. Suppose there are r cosets in the left partition of G by H. Then each has order m, so G has order $n = rm$, and thus m divides n. □

Definition 14. *The **order** of an element $x \in G$ is the least integer n, if it exists, such that $x^n = e$.*

Corollary. If $x \in G$ has order m and G has order n, then m divides n.

Corollary. If G has prime order p, then $G \cong \mathbb{Z}/p\mathbb{Z}$, and every element $g \neq e \in G$ generates G.

Definition 15. *Let $H \leq G$. If the left and right partitions of G by H are equal, then H is a **normal subgroup** of G, denoted $H \trianglelefteq G$.*

When $H \trianglelefteq G$, we refer to the partition of G by H rather than the left or right partition, since they are equal. The following are easy to prove:

- If G is abelian, then every subgroup of G is normal.
- If $H \leq G$, G has order n, and H has order $n/2$, then $H \trianglelefteq G$.

Theorem 4. *$N \trianglelefteq G$ if and only if for all $g \in G$ and $n \in N$, $g^{-1}ng \in N$.*

Corollary. If $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$, then $N_1 \times N_2 \trianglelefteq G_1 \times G_2$.

Example. The **center** C of a group G is the set of all $g \in G$ such that $xg = gx$ for any $x \in G$. For any $g \in G$ and $n \in C$, $g^{-1}ng = ng^{-1}g = n \in C$, so $C \trianglelefteq G$. $\triangle$

When G contains a normal subgroup, we can use the cosets of the normal subgroup to create a new group which "factors out" the structure of the normal subgroup, leaving only the other group structure.

Definition 16. *Let $N \trianglelefteq G$. Then the **quotient group** of G by N, denoted G/N, is the set of cosets in the partition of G by N. The binary operation of G/N is defined as follows: If $A = xN$ and $B = yN$, then $AB = (xy)N$.*

It can be verified that G/N as defined above is indeed a group. N is the identity element, the operation inherits associativity from G, and $(xN)^{-1} = (x^{-1})N$.

Theorem 5. *Let G_1, G_2 be groups. Then $G_1 \times \{e_2\} \trianglelefteq G_1 \times G_2$, and $(G_1 \times G_2)/(G_1 \times \{e_2\}) \cong G_2$.*

1.6 Homomorphisms

Under a group isomorphism, group structure is preserved precisely – that is, isomorphic groups have identical structure. By relaxing the condition of bijectivity, we define group homomorphisms. Under group homomorphisms, algebraic structure is preserved:

Definition 17. *A mapping $\phi : G \to F$ such that $\phi(xy) = \phi(x)\phi(y)$ for any $x, y \in G$ is a **homomorphism** from G into F.*

However, the existence of a homomorphism from G into F gives no information on the relationship between G and F, since $\phi(g) = e_F$ always exists. Moreover, we must specify which direction the homomorphism acts in. The following are immediate consequences of the definition of a homomorphism:

- Let $\phi : G \to F$ be a surjective homomorphism. If G is abelian, then F is abelian.
- Let $\phi : G \to F$ be a homomorphism. Then $\phi(e_G) = e_F$.

- Let $\phi : G \to F$ be a homomorphism. Then for any $u \in G$, $[\phi(u)]_F^{-1} = \phi(u_G^{-1})$.
- Let $\phi_1 : G \to F$ and $\phi_2 : F \to H$ be homomorphisms. Then $\phi_2 \circ \phi_1$ is a homomorphism.

Although the definition of a group homomorphism only requires the preservation of algebraic structure, it can be seen that other structure, namely subgroup and normal subgroup structure, is also preserved:

- Let $\phi : G \to F$ be a homomorphism. Let $X \leq G$, $Y \leq F$. Then $\phi(X) \leq F$ and $\phi^{-1}(Y) \leq G$. In particular, $\phi(G) \leq F$
- Let $\phi : G \to F$ be a homomorphism. Let $N \trianglelefteq G$. Then $\phi(N) \trianglelefteq F$.
- Let $\phi : G \to F$ be a surjective homomorphism. Let $N \trianglelefteq F$. Then $\phi^{-1}(N) \trianglelefteq G$.

As noted above, quotient groups allow us to preserve some group structure, while removing other structure. Similarly, we have seen that homomorphisms preserve some group structure, but not necessarily all. We now examine the relationship between these two notions. We first identify quotient groups with homomorphisms with the natural homomorphism:

Definition 18. *Let $N \trianglelefteq G$. Then the **natural homomorphism** $\phi : G \to G/N$ maps $g \in G$ to the unique coset $T \in G/N$ such that $x \in T$.*

In the other direction, each homomorhpism may be identified with a quotient group in a natural way.

Definition 19. *Let $\phi : G \to F$ be a homomorphism. The **kernel** of ϕ, denoted $\ker \phi$, is $\{g \in G : \phi(g) = e_F\}$.*

It can be shown that $\ker \phi \trianglelefteq G$. Moreover, we have the following lemma:

Lemma. For any $g_1 \in T_1 \in G/\ker \phi, g_2 \in T_2 \in G/\ker \phi$, we have $T_1 = T_2$ if and only if $\phi(g_1) = \phi(g_2)$.

Theorem 6. *Let $\phi : G \to F$ be a surjective homomorphism. Then $\psi : G/\ker \phi \to F$, with $\psi(x \ker \phi) = \phi(x)$, is an isomorphism.*

Proof. Let $x_1 \ker \phi, x_2 \ker \phi \in G/\ker \phi$. Denote $X_1 = x_2 \ker \phi, X_2 = x_2 \ker \phi$. Then $\psi(X_1) = \psi(X_2) \iff \phi(x_1) = \phi(x_2) \iff X_1 = X_2$ (with the last implication by the Lemma). So ψ is a bijection. We also have $\psi(X_1X_2) = \psi([x_1x_2] \ker \phi) = \phi(x_1x_2) = \phi(x_1)\phi(x_2) = \psi(X_1)\psi(X_2)$. So ψ is an isomorphism. □

In particular, we have the following result:

Corollary. Let $\phi : G \to F$ be a homomorphism. Let $\phi(G)$ denote the image of G under ϕ. Then $G/\ker \phi \cong \phi(G)$.

The previous discussion may be summarized with what is commonly referred to as the first isomorphism theorem:

Theorem 7 (First Isomorphism Theorem)**.** *Let G, H be groups, and $\phi : G \to H$ be a homomorphism. Then*

- $\ker \phi \trianglelefteq G$.
- $\phi(G) \leq F$.
- $\phi(G) \cong G/\ker \phi$.

1.7 Solvable Groups

Definition 20. *Let $a, b \in G$. Then the **commutator** of a and b, denoted $[a, b]$, is $aba^{-1}b^{-1}$.*

It can be seen that $[a, b]^{-1} = [b, a]$, and as a result, $[a, b] = e$ if and only if $ab = ba$.

Definition 21. *The **commutant** of a group G, denoted $K(G)$, is the set of elements $g \in G$ such that $g = x_1x_2x_3 \dots x_n$, where each $x_i = [a_i, b_i]$ for some $a_i, b_i \in G$.*

Example. Consider D_6, the symmetries of the triangle. Let l be a reflection. For any $s \in D_6$, $s = rl$ or $s = r$ for some rotation r. So s and s^{-1} have either 0 or 2 instances of reflection, and thus $[a, b]$ has either 0, 2, or 4 instances of reflection. In either case, the reflections cancel according to the group presentation rule $lrl = r^{-1}$ for any rotation r. So $[a, b]$ is always a rotation. Since D_6 is not abelian, $K(D_6) \neq \{e\}$, so we must have $K(D_6) = R_3$. In general, we have $K(D_{2n}) = R_n \cong \mathbb{Z}/n\mathbb{Z}$. △

It can be shown that $K(G) \trianglelefteq G$. It is also easily shown that $K(G) = \{e\}$ if and only if G is abelian. Then we have the following result:

Theorem 8. *Let G be a group. Then $G/K(G)$ is abelian.*

Proof. Consider $K(G/K(G))$. Take any two cosets $X, Y \in G/K(G)$. Suppose $X = xK(G), Y = yK(G)$. Then $[X, Y] = (xyx^{-1}y^{-1})K(G)$. But $(xyx^{-1}y^{-1}) = [x, y] \in K(G)$, so $[X, Y] = K(G)$. Since X, Y were arbitrary, $K(G/K(G)) = K(G)$. But $K(G) = e_{G/K(G)}$, so $G/K(G)$ is abelian. □

Intuitively, this means that when we factor out $K(G)$, we are factoring out all of the "nonabelian structure." Moreover, since $ab = ba \implies [a, b] = e$, $K(G)$ contains no abelian structure (again, intuitively). Thus, $K(G)$ contains exactly the nonabelian structure of G.

Definition 22. *For any group G, consider the sequence $K_i(G)$, defined by $K_0(G) = G$ and $K_{i+1}(G) = K(K_i(G))$. If there exists N such that $K_N(G) = \{e\}$, then G is said to be **solvable**.*

Some basic properties of solvable groups:

- If $H \leq G$ and G is solvable, H is solvable.
- Let $N \trianglelefteq G$. Then G is solvable if and only if G/N is solvable.
- A group G is a **simple group** if the only normal subgroups of G are $\{e\}$ and G. A nonabelian simple group is not solvable.
- If G/N is abelian and N is solvable, then G is solvable.

Example. Consider the dihedral group D_2n. $K(D_{2n}) = R_n \cong \mathbb{Z}/n\mathbb{Z}$ (except in the case $n = 1, 2$, when $K(D_{2n}) = \{e\}$), which is abelian, so $K(K(D_{2n})) = \{e\}$. So D_{2n} is solvable. △

Example. Consider the group of rotations of the dodecahedron. It can be shown that this group is simple. However, it is not abelian, so it is not solvable. △

We also offer two equivalent conditions for solvability.

Theorem 9. *A group G is solvable if and only if there exists $G_1, G_2, G_3 \ldots G_n$ such that $G_n \trianglelefteq G_{n-1} \trianglelefteq \ldots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G$, G_n is abelian, and each G_{i-1}/G_i is abelian.*

Proof. ($\Longrightarrow$) By the definition of solvable groups, we set $G_1 = K_1(G), G_2 = K_2(G), \ldots, G_n = K_n(G) = \{e\}$. Then from Theorem 8, we have $G_{i+1} = K(G_i) \trianglelefteq G_i$ for each i, with $G_i/G_{i+1} = G_i/K(G_i)$ abelian. Lastly, $G_n = \{e\}$ which is abelian.

($\Longleftarrow$) Proved inductively using the fact that if G/N is abelian and N is solvable, then G is solvable. Since G_n is solvable, and each quotient is abelian, G is solvable. □

Theorem 10. *A group G is solvable if and only if there exists $G_1, G_2, G_3 \ldots G_n$ such that every G_i contains $N_i \trianglelefteq G_i$ such that $G_i/N_i \cong G_{i+1}$, and G_n is commutative.*

1.8 Permutation Groups

Chapter 2

Complex Numbers