Solving Polynomial Equations

Part IV

Binary Operations on a Set

One of the obvious features of the reals is that we can perform algebraic operations on them (addition, multiplication, etc.) We start by reviewing some of the general terminology associated with these operations.

A ***binary operation on a set S*** is a function : $S \times S \rightarrow S$.

Many binary operations can be defined on the same set. We will use a generic symbol for a binary operation, namely $\odot$, but this could stand for addition or multiplication or any other binary operation. So, for a, b $\in$ S, the binary operation maps

$$(a,b) \rightarrow a \odot b \in S.$$

Properties of Binary Operations

A binary operation on a set S may (but does not have to) satisfy any of these properties.

Associative Law: $a \odot (b \odot c) = (a \odot b) \odot c$ for all $a,b,c \in S$.

Commutative Law: $a \odot b = b \odot a$ for all $a,b \in S$.

Closure on a s/set. Let $A \subseteq S$. If for all $a,b \in A$, $a \odot b \in A$, then we say that the binary operation is ***closed*** on A.

Example: Let S be the set of natural numbers with binary operation of addition (+). If A is the subset of even natural numbers then + is closed on A. On the other hand, if B is the subset of odd natural numbers, then + is not closed on B.

The History of Mathematics Special Interest Group of the Mathematical Association of America

Is pleased to announce its fourth annual

Student Paper Contest in the History of Mathematics

This contest is open to all undergraduate students$^{\pi}$

The purpose of this contest is to increase awareness and interest in the history of mathematics among undergraduates, and to encourage students to learn more about an area in the history of mathematics of their choosing.

A grand prize and two runner-ups will be chosen.
Winners will receive a one year student membership to the MAA which includes a one year subscription to Math Horizons Magazine and one journal, the grand prize winner will also receive a $30 dollar gift certificate to the MAA bookstore.

Submission Guidelines and Deadlines:

- Topics can be drawn from any field of mathematics.
- Papers can address a single person or topic, or be an historical survey of a topic or school of thought.
- Submissions should be approximately 5000 words (approximately 12 double spaced 12 pt. pages) in length
- Papers should include a full citation list
- Papers should not draw too heavily from web sources
- Please include a cover sheet with: your name, the paper's title, your institution, supervising instructor if applicable, and email and permanent postal address.
- Please submit electronic copy to the addresses below.
- Students submitting a paper need not be currently taking a history of mathematics course.
- Single authored papers only please.

Deadline for submission is March 31, 2007

Papers will be judged by a panel of specialists for content, presentation, and grammar.

Properties of Binary Operations

Identity elements: If there exists an element $i \in S$ such that for all $a \in S$, $i \odot a = a \odot i = a$, then we say that i is an ***identity element*** for $\odot$.

Example: For $S = \mathbb{R}$, 0 is the identity element for addition and 1 is the identity element for multiplication.

Inverse elements: If a set S has a binary operation with an identity element i, then for a in S, the ***inverse*** of a with respect to the binary operation is an element $b \in S$ with the property that

$$a \odot b = b \odot a = i.$$

Example: For $S = \mathbb{R}$, the inverse of 5 with respect to addition is -5, while the inverse of 5 with respect to multiplication is 1/5. -5 is called the *additive inverse* and 1/5 is called the *multiplicative inverse* in this case.

Groups

Def: A ***group*** is a set G together with a binary operation $\odot$ (a binary operation is a mapping from $G \times G \to G$) such that

1. $a \odot (b \odot c) = (a \odot b) \odot c$ for all a, b, c in G.

2. There is a unique element I in G so that
   $a \odot I = I \odot a = a$ for all a in G. I is called the identity.

3. For each a in G, there exists a unique a^{-1} in G so that
   $a \odot a^{-1} = a^{-1} \odot a = I$. a^{-1} is called the inverse of a.

A group is called ***abelian*** if it satisfies the commutative law,
$a \odot b = b \odot a$ for all a, b in G.

Examples

Some common examples of groups:

1. The real numbers under addition.
2. The rational numbers under addition.
3. The integers under addition.
4. The real numbers except for 0, under multiplication.
5. The rational numbers except for 0, under multiplication.
6. 2x2 matrices over the reals under matrix addition.
7. 2x2 non-singular matrices over the reals under matrix multiplication.

Some non-groups:

1. The reals under multiplication.
2. The natural numbers under addition.

Fields

A ***field*** is a set F together with two binary operations, called addition and multiplication, which satisfy the following axioms:

1. F under addition is an abelian group with additive identity 0 and the additive inverse of a denoted by $-a$.

2. F - {0} under multiplication is an abelian group with multiplicative identity 1 and the multiplicative inverse of a denoted by a^{-1}.

3. $\forall a, b, c \in F$ we have $a(b + c) = ab + ac$ (*The distributive law of multiplication over addition*).

4. $0a = a0 = 0 \quad \forall a \in F$.

Examples

Examples of fields are given by the reals, the rationals, the complex numbers and the integers modulo p where p is a prime.

The first three examples above are infinite fields (the sets on which they are based are infinite sets) while the last examples are finite fields.

Field Extensions

A ***subfield*** of a field $(E,+,\times)$ is a subset F of E which is itself a field with the same binary operations. If $(F,+,\times)$ is a subfield of $(E,+,\times)$, then we say that E is an ***extension*** of F.

Example:

The rationals, $\mathbb{Q}$, form a subfield of the reals, $\mathbb{R}$. In turn, $\mathbb{R}$ is a subfield of the complex numbers, $\mathbb{C}$. We would say that $\mathbb{R}$ is an extension of $\mathbb{Q}$, and that $\mathbb{C}$ is an extension of $\mathbb{R}$. $\mathbb{C}$ is also an extension of $\mathbb{Q}$.

A sequence of fields, where each is an extension of the previous one is called a ***tower*** of fields. So, for example,

$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a tower of fields.

Field Extensions

Given a field $(F,+,\times)$ and a polynomial f which is irreducible over F (meaning that its coefficients are in F, but it has no root in F), we can form an extension of F by "adjoining" a root of f. That is, if $f(\alpha) = 0$,

$$F(\alpha) = \{a + b\alpha \mid a, b \in F\}$$

is a field extension of F, called a ***simple algebraic*** extension.

If some power of α is in F (i.e., $\alpha^n \in F$) then the simple algebraic extension of F by α is called a ***radical*** extension.

Field Extensions

This is a generalization of a familiar construction.

The complex numbers $\mathbb{C}$ are a radical extension of the reals $\mathbb{R}$.

In this case, the irreducible polynomial is $f(x) = x^2 + 1$, with root $i = \sqrt{-1}$, satisfying $i^2 = -1$. Thus, $\mathbb{C} = \mathbb{R}(i)$.

A less familiar example is given by the irreducible polynomial $f(x) = x^3 - 2$ over the rationals. (This is irreducible because none of its roots are rational numbers.) With $\alpha = 2^{1/3}$, we get the simple extension $\mathbb{Q}(\alpha) = \{a + b\alpha | \ a, b \in \mathbb{Q}\}$ which is a radical extension since $\alpha^3 = 2$ which is in $\mathbb{Q}$.

The Splitting Field

Given a polynomial f with coefficients in a field F, the smallest extension of F which contains all the roots of f is called the ***splitting field*** of f over F. Another way to say this is that the splitting field of a polynomial is smallest extension of F in which the polynomial factors completely (into linear factors).

Examples: Consider the polynomial $f(x) = x^2 + 1$ having coefficients in the field of rationals $\mathbb{Q}$.

The splitting field for this f is $\mathbb{Q}(i)$, a radical extension of $\mathbb{Q}$ which contains i and -i.

In this field we have $f(x) = (x + i)(x – i)$. This factorization is also valid over $\mathbb{C}$, but $\mathbb{C}$ is not the smallest field for which this is true, so it is not the splitting field.

The Splitting Field

Now consider $f(x) = x^3 - 2$, again with coefficients in $\mathbb{Q}$.

The splitting field for this f is not $\mathbb{Q}(\sqrt[3]{2})$ since this field does not contain the complex roots of the equation. It's splitting field is

$\mathbb{Q}(\sqrt[3]{2}, \omega) = [\mathbb{Q}(\sqrt[3]{2})](\omega)$ where $\omega^3 = 1, \omega \neq 1$.

This example shows a radical extension of a radical extension. In this field we have:

$$f(x) = (x - 2^{\frac{1}{3}})(x - \omega 2^{\frac{1}{3}})(x - \omega^2 2^{\frac{1}{3}}).$$

Solution by Radicals

We can now state, in modern terminology, what a solution by radicals of a polynomial means.

Let f be a polynomial with coefficients in the field F. Suppose that there exists a tower of field extensions,

$$F = F_0 \subset F_1 \subset F_2 \subset .... \subset F_n$$

where each F_{i+1} is a radical extension of F_i (i = 0, ..., n-1). Then the polynomial f has a ***solution by radicals*** iff the splitting field E of f satisfies $E \subseteq F_n$.

Automorphisms of Fields

Given a field E which is an extension of F, an ***automorphism of E over F*** is a bijection $\varphi: E \to E$ which preserves the field operations:

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$

and **fixes** every element of F, i.e., $\varphi(c) = c$ if $c \in F$.

Consider the map on complex numbers called *conjugation*:

$$\varphi(a + bi) = a - bi.$$

One easily checks that this map is a bijection which satisfies the two properties and $\varphi(a) = \varphi(a + 0i) = a - 0i = a$ for all real numbers a. Thus, conjugation is an automorphism of $\mathbb{C}$ over $\mathbb{R}$.

Automorphisms of Fields

The only automorphism of $\mathbb{R}$ is the identity map, so you may not be familiar with this type of map unless you've studied more abstract algebraic settings.

The automorphisms of E over F form a group under composition which is denoted ***Aut(E/F)*** and called the ***Galois group*** of the extension.

The Galois group of $\mathbb{C}$ over $\mathbb{R}$ is just the cyclic group with 2 elements (the identity and conjugation).

The Galois Correspondence

If E is a finite extension of F and every irreducible polynomial over F which has one root in E has all its roots in E, then E is called a ***normal*** extension of F. (Splitting fields are examples of normal extensions.)

If E is a normal extension of F, there is a one-to-one correspondence between the intermediate fields K, $E \supset K \supset F$ and the subgroups of Aut(E/F). This correspondence associates K with Aut(E/K) and reverses inclusion relations: $K_1 \subset K_2$ iff $Aut(E/K_1) \supset Aut(E/K_2)$.

This result permits us to translate questions about field extensions into questions about groups (which are easier objects to work with.)

Galois' Theorem

The essence of Galois' theorem (without the details) is this:

For a polynomial to be solvable by radicals, the splitting field of the polynomial has to have a subfield structure of a certain kind (the radical extensions). By using the Galois correspondence, this structure must be reflected in the subgroup structure of the Galois group of the splitting field.

Galois identifies this subgroup structure, which we refer to today as the property that the group be ***solvable***. Thus, a polynomial is solvable by radicals iff the Galois group of its splitting field is a solvable group.

Abel's Theorem

What Abel proved (although this is not the way he proved it) is that for every degree at least 5, there is a polynomial whose splitting field has a Galois group which is not solvable. (A polynomial with a factor of degree 5 over $\mathbb{Q}$ which has exactly 3 real (but not rational) roots will do the trick, for instance $2x^5 - 5x^4 + 5$.)

This means that no general formula giving the roots in terms of radicals of the coefficients can exist for polynomials of degree 5 or greater, since there are always polynomials whose roots can not be so expressed.

For polynomials of smaller degree, the Galois groups are too small to fail to be solvable, so general formulas exist for them.

Postscript

As with other mathematical problems whose solutions turn out to be impossible, for example squaring the circle, the goal may be obtained by dropping some of the restrictions put on the problem. Thus, if we eliminate the requirement that constructions be done using only straightedge and compass, then squaring the circle is possible. Similarly, if we remove the condition that the roots of a polynomial be expressed in terms of radical expressions of the coefficients, we are able to obtain the roots. By 1870, Jordan was able to show that any polynomial equation, of whatever degree, could be solved by using ***elliptic modular functions*** (which involve trigonometric expressions).