Handout #6 INTRODUCTION TO ALGEBRAIC STRUCTURES: Prof. Moseley
Chap. 2 AN ALGEBRAIC FIELD

To introduce the notion of an **abstract algebraic structure** we consider (algebraic) **fields**. (These should not to be confused with vector and scalar fields in vector analysis.) Examples of other abstract algebraic structures are: Groups, Rings, Integral Domains, Modules and Vector Spaces. Informally, a **field** is a number system where we can add, subtract, multiply, and divide (except by zero). Abstractly, we think of addition and multiplication as the two defined binary operations and subtraction and division as inverse operations. Our objective is to see what kinds of equations we can solve by using only the algebraic (i.e., field) structure of the real numbers and then examine other fields (e.g., **Q** and **C**) to verify that the same solution procedure works.

DEFINITION. Let F be a set (of numbers) together with two **binary operations** (which we call addition and multiplication), denoted by + and $\cdot$ (or juxtaposition), which satisfy the following list of properties.:

F1) $\forall$ x,y $\in$ F $x + y = y + x$ Addition is commutative

F2) $\forall$ x,y $\in$ F $x + (y + z) = (x + y) + z$ Addition is associative

F3) $\exists$ a unique element $0 \in F$ such that.$\forall$ $x \in F$, $x + 0 = x$ Existence of a right additive identity

F4) $\forall$ $x \in F$, $\exists$ a unique $y \in F$ s.t. $x + y = 0$ Existence of a right additive inverse for each element
We usually denote y by $-x$ for each element in F.

F5) $xy = yx$ $\forall$ x,y $\in$ F Multiplication is commutative

F6) $x(yz) = (xy)z$ $\forall$ x,y,z $\in$ F Multiplication is associative

F7) $\exists$ a unique element $1 \in F$ such that $\forall$ $x \in F$, $x1 = x$ Existence of a a right multiplicative identity

F8) $\forall$ x s.t. $x \neq 0$, $\exists$ a unique $y \in F$ s.t. $xy = 1$ Existence of a right multiplicative inverse for each element except 0 for each nonzero element in F.
We usually denote y by (x^{-1}) or (1/x)

F9) $x(y + z) = xy + xz$ $\forall$ x,y,z $\in$ F (Multiplication distributes over addition)

Then the ordered 5-tuple consisting of the set F and the structure defined by the two operations of addition and multiplication as well as the two identity elements mentioned in the definition, $K = (F,+,\cdot,0,1)$, is an algebraic **field**.

Although technically not correct, we often refer to the set F as the (algebraic) field. The elements of a field (i.e. the elements in the set F) are often called **scalars**. Since the letter F is used a lot in mathematics, the letter K is also used for a field of scalars. The real numbers **R** and the complex numbers **C** are examples of fields. The rational numbers **Q** also form a field. Hence it will be convenient to use the notation **K** to represent (the set of elements for) any field $K = (\mathbf{K},+,\cdot,0,1)$.

The properties in the definition of a field constitute the fundamental axioms for **field theory**. Other field properties can be proved based only on these properties. Once we proved that **Q**, **R**, and **C** are fields (or believe that someone else has proved that they are) then, by the **principle of abstraction**, we need not prove these properties for these fields individually, one proof has done the work of three. In fact, for every (concrete) structure that we can establish as a field, all of the field properties apply.

We prove an easy property of fields. As a **field property**, this property must hold in every algebraic field. It is an identity and we use the standard form for proving identities.

THEOREM #1. Let K = (**K**,+,·,0,1) be a field.. Then ∀x∈**K**, 0 + x = x.
Proof. Let x∈**K**. Then

STATEMENT	REASON
0 + x = x + 0	F1. Addition is commutative
= x	F3 0 is the right additive identity element.(and properties of equality)

Hence ∀x∈K, 0 + x = x. Q.E.D.

Thus 0 is not only a **right additive identity** by Axiom F3 in the definition of an abstract field, we have proved that it is a **left additive identity**. Hence we may say that 0 is an **additive identity**. (We can also prove that it is unique. Then we can say that 0 is the additive identity.) Although this property appears "obvious" (and it is) a formal proof can be written. This is why mathematicians may disagree about what axioms to select, but once the selection is made, they rarely disagree about what follows logically from these axioms. Actually, the first four properties establish a field with addition as an **Abelian (or commutative) group** (another abstract algebraic structure). **Group Theory**, particularly for Abelian groups have been well studied by mathematicians. Also, if we delete 0, then the nonzero elements of **K** along with multiplication also form an Abelian group. We list some (Abelian) group theory properties as they apply to fields. Some are identities, some are not. These properties all hold for **Q**, **R**, and **C** since they are all fields.

THEOREM #2. Let K = (**K**,+,·,0,1) be a field. Then
1. The identity elements 0 and 1 are unique.
2. For each nonzero element in **K**, its additive and multiplicative inverse element is unique.
3. 0 is its own additive inverse element (i.e., 0 = 0 = 0) and it is unique, but it has no multiplicative inverse element.
4. The additive inverse of an additive inverse element is the element itself. (i.e., if -a is the additive inverse of a, then −(−a) = a).
5. −(a + b) = −a + (−b). (i.e., the additive inverse of a sum is the sum of their additive inverses.)
7. (−a)b = −(ab)
8. (−a)(−b) = ab
9. The multiplicative inverse of a multiplicative inverse element is the element itself. (i.e., if a^{-1} is the multiplicative inverse of a, then $(a^{-1})^{-1}$ = a).
10 $(a\,b)^{-1} = a^{-1}\,b^{-1}$. (i.e., the multiplicative inverse of a product is the product of their multiplicative inverses.)
11. Sums and products can be written in any order you wish.
12. If a + b = a + c, then b = c. (Cancellation Law for Addition)
13. If ab = ac and a ≠ 0, the b = c. (Cancellation Law for Multiplication.)
14. If ab = 0, then either a = 0 or b = 0. (Zero Product Theorem)

These properties, along with **properties of equality**, result in the following **Elementary Equation Operations** (EEO's)

EEO#1. Interchange the two sides of an equation ($a=b \Leftrightarrow b=a$).
EEO#2. Replace an algebraic expression by an equivalent algebraic expression. (e.g., If $a = b+c$ and $c =d$, then $a = b+d$.)
EEO#3. Adding the same number or algebraic expression to both sides of an equation. ($a = b \Rightarrow a + c = b + c$)
EEO#4. Multiply (or divide) both sides of the equation by the same nonzero expression.
EEO#5. If the right hand side (RHS) equals zero and the left hand side (LHS) can be written as a
product (i.e., factored), then the solutions of the equation are the zeros of the two factors
(i.e., the two factors can be set equal to zero).

All fields contain the elements 0 and 1 (although they may have other names). Using induction, we define 2 as 1 + 1, 3 as 2 + 1, 4 as 3+1, and so forth. It can be shown that unless there exists an n defined in this manner such that n = 0, we have an **infinite field**. In this case we have embedded **N** in the infinite field **K**. The algebraic structure of **N** can also be embedded. Since it can be shown that this is possible for any infinite field, for any infinite field **K**, we may assume $\mathbf{N} \subseteq \mathbf{K}$. Then for any nonzero element $a\in\mathbf{K}$, we may define $2a = a + a$, $3a = 2a + a$, and so forth so that na is well defined. In fact, we may not only embed **N** in **K**, but also **Z** and **Q** as well. Can you imagine how this might be done? How would you define -1?

<u>THEOREM #3.</u> Let $K = (\mathbf{K},+,\cdot,0,1)$ be an infinite field. If $n\in\mathbf{N}\subseteq\mathbf{K}$, then $na = 0$ if and only if $a = 0$.

Suppose $K = (\mathbf{K},+,\cdot,0,1)$ is a field and that we can do exact arithmetic. That is, suppose that we can compute $x + y$ (and $x - y$) and xy (and x/y if $y \neq 0$) exactly. Then we have algorithms for solving equations such as $a x + b = c x + d$ that can be used to find x exactly in a finite number of steps for any values of the constants (parameters) a, b, c, and d.

Now suppose that our field has an absolute value function $|\cdot|\to R$ such that
1. $\forall x\in\mathbf{K}$, $|x| \geq 0$ and $|x|=\geq 0$ if and only if $x = 0$.
2. $\forall x,y\in\mathbf{K}$, $|x + y| \leq |x| + |y|$ triangle inequality
3. $\forall x,y\in\mathbf{K}$, $|xy| =|x|\,|y|$

We say **K** is a **field with absolute value**. We claim that $\rho(x,y) = |x - y|$ gives a measure of the distance from x to y. This function $\rho:\mathbf{K}\times\mathbf{K} \to \mathbf{R}$ is an example of a **metric**. Let x_e be the exact solution to a problem. Even if we are not able to obtain an algorithm to find x_e in a finite number of steps, we may be able to obtain an algorithm that yields an infinite sequence of numbers, $\{x_n\}_{n=1}^{\infty}$, such that x_n gets closer and closer to x_e; that is, such that $\lim_{n\to\infty} |x_n - x_e| = 0$. We say $\lim_{n\to\infty} x_e = x_e$ and that x_n is a sequence of **approximate solutions** to the problem. $\rho(x_n,x_e) = |x_n - x_e|$ tells us how good the approximation is.

Handout # 7 SOLVING EQUATIONS IN AN ALGEBRAIC FIELD Prof. Moseley
Chap. 2

A scalar equation in the variable x in a field **K** is a statement in which two algebraic expressions, say f(x) and g(x) (algebraic expressions do indeed define functions) that contain constants in **K** (or parameters) and the variable x, are asserted to be equal. The expressions are often called the sides of the equation (left hand side, LHS, and right hand side, RHS,). Since the equation $f(x) = g(x)$ is an **open statement**, it may or may not be true depending on the value of the variable x. Let D_f and D_g be the domains of the functions f and g respectively. The set Σ of admissible values of the variable x are those elements in **K** for which both expressions "make sense" (i.e., for which a value can be computed). Thus $\Sigma = D_f \cap D_g$. A **solution** is an element in Σ that satisfies the equation $f(x) = g(x)$. Thus the solution set is $S = \{x \in \Sigma: f(x) = g(x)\}$ and **the solution process** is whatever algorithms are used to obtain an explicit description of S. Since Σ and $f(x) = g(x)$ define the problem Prob, we sometimes let $\text{Prob}(\Sigma,f{=}g) = \{x \in \Sigma: f(x) = g(x)\}$ and think of $\text{Prob}(\Sigma,f{=}g)$ as an implicit description of the **solution set**. We then use $\text{Soln}(\Sigma,f{=}g)$ to mean the explicit description of the solution set obtained by the solution process. Since as sets we have $\text{Prob}(\Sigma,f{=}g) = \text{Soln}(\Sigma,f{=}g)$, for brevity in working examples we usually just let $S = \{x \in \Sigma: f(x) = g(x)\} \subseteq \Sigma$ be the solution set during the solution process.

For $\text{Prob}(\Sigma,f{=}g)$, there is a clearly defined and easily implemented algorithm to determine if an element x in Σ is a solution to the problem, we say that the solutions to the problem are **testable** (and that the problem Prob is testable). We denote this algorithm to test possible solutions by T so that the operation T(x) results in a yes if s is a solution and in a no if x is not a solution. Thus the collection of elements x in Σ such that T(x) results in a yes is the solution set S for the problem Prob defined by the set Σ and the equation $f(x) = g(x)$. The need for clearly defining the set Σ is illustrated by the equation $x^2 + 1 = 0$. The existence of a solution depends on whether we choose the real numbers **R** or the complex numbers **C** as the field which must contain the solution.

Normally Σ is large or infinite (e.g. **R** and **C**) so that it is not possible to use the algorithm T to test each element in Σ individually. Problems where Σ is small enough so that a check of its elements by hand is possible are considered to be trivial. On the other hand, some problems where Σ is large but not to large (e.g. Which students at a university have brown eyes?) yield to the technique of testing each element in Σ by using computers and data bases.

Examples of equations in the field **K** that we would like to establish a solution procedure for are 1) $ax = b$, 2) $ax + b = c$, 3) $ax + b + cx + d = ex + f$, 4) $ax^2 = 0$, 5) $ax^2 + bx = 0$, 6)$(ax+b)(cx + d) = 0$, and 7) $ax^2 + b\,x + c = 0$. For any values of the parameters, we wish to determine when these problems have solutions, how many solutions does each have, and can we find formulas for these. Recall that in any field, we have the following **Elementary Equation Operations** (EEO's) which can be used to solve these equations.

EEO#1. Interchange the two sides of an equation ($a=b \Leftrightarrow b=a$).

EEO#2. Replace an algebraic expression by an equivalent algebraic expression. (e.g., If $a = b+c$ and $c = d$, then $a = b+d$.)

EEO#3. Adding the same number or algebraic expression to both sides of an equation. ($a = b \Rightarrow a + c = b + c$)

EEO#4. Multiply (or divide) both sides of the equation by the same nonzero expression.

EEO#5. If the right hand side (RHS) equals zero and the left hand side (LHS) can be written as a product (i.e., factored), then the solutions of the equation are the zeros of the two factors (i.e., the two factors can be set equal to zero).

Although we can solve $ax^2 + b\,x = 0$ by factoring it into $x(ax + b) = 0$ and using EEO#5, we can not develop a solution algorithm for $ax^2 + b\,x + c = 0$ until we determine for which elements a in K we can solve (the nonlinear equation) $x^2 = a$. That is, we need to establish which elements in **K** have a square root. Although all positive rational numbers do not have rational square roots, the least upper bound axiom guarantees that all positive real numbers have exactly two square roots. (0 has only one square root. No negative real numbers have real square roots so that $x^2 = -1$ has no solution.) The point is that, just as we extended **N** to **Z** so that we may solve $x+4 = 0$, we need structure in addition to being able to add, subtract, multiply and divide (ie., structure in addition to the field structure) in order to solve the equation $ax^2 + b\,x + c = 0$ for all values of the parameters a, b. and c. We need to know what numbers have square roots, how many there are, and how to find them(or at least how to find approximations to them).

All "equation operations" are not EEO's. Some may introduce **extraneous roots** (that is, we may obtain answers that are not solutions).

THEOREM. For all a,b∈**R**, if a = b, then $a^2 = b^2$. However, if $a^2 = b^2$, then we do not know that a = b unless we know (by some other means) that a and b have the same sign.

EXAMPLE: Solve $x + 2\sqrt{x} - 3 = 0$.
Solution: First note that $\Sigma = R^+ = [0,\infty) = \{x\in\mathbf{R}: x\geq 0\}$; that is, we only look for nonnegative solutions. Suppose $x\in[0,\infty)$ is a solution. Then

STATEMENT	REASON
$x + 2\sqrt{x} - 3 = 0$	Given
$(x + 2\sqrt{x} - 3) + 3 = 0 + 3$	If a=b, then a+3 = b+3.
$(x + 2\sqrt{x}) + (-3 + 3) = 3$	−3 is the additive inverse of 3, associativity of addition, and 0 is the additive identity element..
$(x + 2\sqrt{x}) = 3$	−3 is the additive inverse of 3 and 0 is the additive identity element..
$2\sqrt{x} = 3 - x$	For any x∈**R**, there exists −x such that. x + (−x) = 0.
$(2\sqrt{x})^2 = (3 - x)^2$	Theorem above. (This new problem has more solutions than the old.)
$4x = 9 - 6x + x^2$	Properties of square and square root functions
$x^2 - 10x + 9 = 0$	Properties similar to above.
$(x - 9)(x - 1) = 0$	Theorems about factoring
$x - 9 = 0$ or $x - 1 = 0$	If ab = 0, then a = 0 or b = 0.
$x = 9$ or $x = 1$	Additive inverse properties
$x \in \{1,9\}$	Definition of set notation.

Since the implications only go one way (the forward direction), we only have that if x is a solution of the original problem, then it must be either 1 or 9. Since the solution process only proves uniqueness, not existence, we prove (check) existence by substituting into the original equation.

$(9) + 2\sqrt{(9)} - 3 = 9 + 2(3) - 3 = 12 \neq 0$ so that 9 is not a solution.

$(1) + 2\sqrt{(1)} - 3 = 1 + 2(1) - 3 = 0$ so that 1 is a solution.

Hence $x = 1$ is the unique solution. $x = 9$ is an **extraneous solution**; that is, a solution to the new problem after we squared both sides, but not a solution to the original problem.

Handout # 9 SOLVING INEQUALITIES IN AN ORDERED FIELD Professor Moseley
Chap. 2

Suppose **K** is a field with a (positive) subset P that satisfies the following:

O1. $x,y \in P$ implies $x+y \in P$
O2. $x,y \in P$ implies $xy \in P$
O3. $x \in P$ implies $-x \notin P$
O4. $x \in \mathbf{K}$ implies exactly one of $x = 0$ or $x \in P$ or $-x \in P$ holds (trichotomy).

Note that the order properties involve the binary operations of addition and multiplication and are therefore linked to the field properties. To establish a positive set, we need to be able to add and multiply all numbers. Other order properties follow from the four fundamental properties. The relations usually denoted by the symbols <, >, ≤, and ≥ can be defined in terms of the set of positive numbers P and the binary field operation of addition. The properties of these relations can then be established. In fact, ≤ can be shown to be a **linear ordering** on **K**.

THEOREM #1. The relation ≤ on **K** is a linear ordering; that is
a) $\forall x \in \mathbf{K}$, $(x,x) \in \leq$ $(x \leq x)$. (≤ is reflexive.)
b) $\forall x,y \in \mathbf{K}$, $(x,y) \in \leq$ and $(y,x) \in \leq$ implies $x=y$ ($x \leq y$ and $y \leq x$ implies $x=y$). (≤ is antisymmetric.)
c) $\forall x,y,z \in \mathbf{K}$, $(x,y) \in \leq$ and $(y,z) \in \leq$ implies $x \leq z$ ($x \leq y$ and $y \leq z$ implies $x \leq z$). (≤ is transitive).
d) $\forall x,y \in \mathbf{K}$, $(x,y) \in \leq$ or $(y,x) \in \leq$ ($x \leq y$ or $y \leq x$). (all x and y in **K** are comparable).

If **K** has a (positive) subset P that satisfies O1, O2, O3, and O4 so that it has a linear ordering ≤, it is referred to as an **ordered field**. Alternatively, we could assume the existence of the linear ordering ≤ on **K** (i.e., a relation≤ having the properties listed in Theorem#1), instead of O1, O2, O3, and O4. The resulting ordered field would be the same. Note that **Q** and **R** have a subset P satisfying O1, O2, O3, and O4, but that **C** does not. Hence **Q** and **R** are ordered fields, but **C** is not.

An **absolute value function** can be defined on an ordered field **K** with (positive) set P satisfying O1, O2, O3, and O4 as follows:

DEFINITION#1. If **K** is a field with a positive set, then we define the **absolute value function** as

$$f(x) = |x| = \begin{cases} x & \text{if} \quad x \in P \\ -x & \text{if} \quad x \notin P \end{cases} \quad \text{where } -x \text{ is the additive inverse of x.} \qquad (1.1)$$

Then **K** is a field with absolute value. Thus **Q** and **R** have absolute value functions. Recall that **C** also has an absolute value function, but that it is not defined by (1.1). Hence a field does not have to be ordered in order to have an absolute value function. Do you recall the defining properties of an absolute value function? Do they include $|\cdot|:\mathbf{K}\to\mathbf{R}$ (as **R** is an ordered field), $|x| \in P_{\mathbf{R}} = \{x \in \mathbf{R} : x > 0\}$ if $x \neq 0$ and $|0| = 0 \in \mathbf{R}$? Does the absolute value function give us the notion of the **magnitude** of a number?

Often application problems require the solution of **inequalities** for **R**. Recall that our framework for find problems (FFP's) includes inequalities (e.g. $|x - 3| < 4$) which in an ordered field may be reformulated as $f(x) < 0$ (e.g. $|x - 3| - 4 < 0$ so that $f(x) = |x - 3| - 4$), and the "less than" symbol < may instead be any of ≤, >, or ≥. The set Σ is the domain of f (e.g., it may be a subset of **Q** or **R**, unlike the rational and the real numbers, the complex numbers do not have a natural ordering). The algorithm T(x) yields a yes if the inequality is satisfied and is effected by first evaluating the function f. The solution set is S = {x ∈ Σ: f(x) < (alternately, ≤, >, or ≥) 0} and is the set of numbers x in Σ such that f(x) is less than (alternately, less than or equal to, greater than, or greater than or equal to) zero. Although there might be no solution (e.g. $x^2 < -1$) or one solution (e.g. $x^2 \leq 0$), the solution set when $\Sigma \subseteq \mathbf{R}$ is usually a portion of the real number line and hence is usually an infinite set. A simple description of the portion of **R** that satisfies the inequality is the objective of the solution process.

As with equalities, operations on inequalities can be developed that result in **equivalent inequalities** (i.e., ones that have the same solution set). These are called **Equivalent Inequality Operations** or EIO's. In any ordered field we have the following:

EIO#1. Interchange the two sides of an inequality by reversing the inequality sign.
($a<b \Leftrightarrow b>a$ or $a \leq b \Leftrightarrow b \geq a$).

EIO#2. Replace an algebraic expression by an equivalent algebraic expression. (e.g., If $a < b+c$ and
$c = d$, then $a < b+d$.)

EIO#3. Adding the same number or algebraic expression to both sides of an inequality.
(e.g., $a < b \Rightarrow a + c < b + c$)

EIO#4. Multiply (or divide) both sides of the inequality by the same positive expression.

EIO#5. If the right hand side (RHS) of the inequality is zero, the inequality is >, and the left hand side (LHS) can be written as a product (i.e., factored), then the solutions of the inequality occur when either both terms are positive or when both terms are negative.