EE 441: Axioms and Lemmas for a Field $\mathbb{F}$

I. Axioms for a field

Let $\mathbb{F}$ be a set of objects that we call "scalars." We assume that $\mathbb{F}$ has at least two distinct elements. We say that $\mathbb{F}$ is a *field* if there are rules for addition and multiplication of the elements of $\mathbb{F}$ such that for any $\alpha \in \mathbb{F}, \beta \in \mathbb{F}$, we have:

- $\alpha + \beta \in \mathbb{F}$
- $\alpha\beta \in \mathbb{F}$

Further, the addition and scalar multiplication must satisfy the following properties (for any $\alpha, \beta, \gamma \in \mathbb{F}$):

1) $\alpha + \beta = \beta + \alpha$, $\alpha\beta = \beta\alpha$ (Commutative)

2) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (Associative)

3) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ (Distributive)

4) (Existence of 0) There is an element "0" such that $\alpha + 0 = \alpha$ for any $\alpha \in \mathbb{F}$.

5) (Existence of 1) There is an element "1" such that $\alpha 1 = \alpha$ for any $\alpha \in \mathbb{F}$.

6) (Additive inverse) For every $\alpha \in \mathbb{F}$, there exists an additive inverse $-\alpha$ such that $\alpha + -\alpha = 0$.

7) (Multiplicative inverse) For every $\alpha \in \mathbb{F}$ such that $\alpha \neq 0$, there exists a multiplicative inverse α^{-1} such that $\alpha\alpha^{-1} = 1$.

II. Lemmas

Suppose we have a field $\mathbb{F}$. Recall that the field must contain at least two elements. We have the following arithmetic facts for any field (the proofs are on the back page).

Note: For any values $a \in \mathbb{F}$, $b \in \mathbb{F}$, the following fact holds: If $a = b$, then for any $c \in \mathbb{F}$ we have $a + c = b + c$ and $ac = bc$. That is, we can add any value c to both sides of a true equation to yield another true equation, and we can multiply any value c to both sides to yield another true equation. The proof is obvious (For addition: If $a = b$ then $a + c = b + c$, done). (For multiplication: If $a = b$ then $ac = bc$, done).

Lemma 1: $\alpha 0 = 0$ for any $\alpha \in \mathbb{F}$.

Lemma 2: $0 \neq 1$.

Lemma 3: For any element $a \in \mathbb{F}$, the additive inverse $-a$ is unique.

Lemma 4: For any element $a \in \mathbb{F}$ such that $a \neq 0$, the multiplicative inverse a^{-1} is unique.

Lemma 5: For any element $a \in \mathbb{F}$, we have that $-a = (-1)a$.

Lemma 6: $(-1)(-1) = 1$.

Lemma 7: For any elements a, b in $\mathbb{F}$, we have:

$$a(-b) = -(ab) = (-a)b \quad , \quad (-a)(-b) = ab$$

Definition 1: (Subtraction) If $a \in \mathbb{F}$ and $b \in \mathbb{F}$, then the *subtraction operator* $a - b$ produces another element in $\mathbb{F}$, defined as follows:

$$a - b \triangleq a + (-b)$$

From this subtraction rule, it immediately follows that $a(b - c) = ab - ac$.

Definition 2: (Integer Powers) For any element $a \in \mathbb{F}$, we define the *square* of a (written a^2), to be aa. Similarly, for any positive integer k, we use the notation a^k to represent a multiplied by itself k times (so that $a^1 \triangleq a$, $a^2 \triangleq aa$, $a^3 \triangleq aaa$, etc.). For any $a \neq 0$ and for any positive integer k, we define a^{-k} to be the product of a^{-1} with itself k times (so that $a^{-2} = a^{-1}a^{-1}$). For any $a \neq 0$, the power a^0 is defined to be 1. The power 0^{-k} is not defined for any integers $k \geq 0$.

Lemma 8: For any two elements a, b in $\mathbb{F}$, if $ab = 0$ then either $a = 0$ or $b = 0$ (or both).

Lemma 9: For any element $a \in \mathbb{F}$, if $a^2 = 1$, then $a \in \{-1, 1\}$.

Lemma 10: (Polynomial Factoring) Suppose $a \in \mathbb{F}$ and $b_1, b_2, \ldots, b_n$ are n additional elements of $\mathbb{F}$. Suppose the following equation holds: $\Pi_{i=1}^{n}(a - b_i) = 0$. Then $a \in \{b_1, b_2, \ldots, b_n\}$.

The proof of Lemma 1 (that $\alpha 0 = 0$) is given below. The proofs of the remaining lemmas are given on the next page. For fun, you are encouraged to prove the lemmas yourself and then check the proofs on the back if you need help or want to compare proof methodologies.

Proof: (*Lemma 1:* $\alpha 0 = 0$.) Note that $1 + 0 = 1$. Therefore, for any $\alpha \in \mathbb{F}$, we have:

$$\begin{aligned} \alpha &= \alpha 1 \\ &= \alpha(1 + 0) \\ &= \alpha 1 + \alpha 0 \\ &= \alpha + \alpha 0 \end{aligned}$$

Thus, we have:

$$\alpha = \alpha + \alpha 0$$

Adding $-\alpha$ to both sides of the above equation yields:

$$-\alpha + \alpha = -\alpha + \alpha + \alpha 0$$

and therefore we have $0 = 0 + \alpha 0 = \alpha 0$, and we are done. □

Proof: (*Lemma 2:* $0 \neq 1$.)
Let $a \in \mathbb{F}$. If $0 = 1$, then $0 = a0 = a1 = a$, and hence $a = 0$. Thus, if $0 = 1$, then all elements a of $\mathbb{F}$ are equal to 0, contradicting the fact that $\mathbb{F}$ has at least two elements. □

Proof: (*Lemma 3:* $-a$ *is unique.*)
Suppose that $a + b = 0$. Then adding $-a$ to both sides, we get $a + (-a) + b = -a$ and hence $0 + b = -a$. That is, $b = -a$. In other words, the only element that can be added to a to get 0 is the element $-a$. □

Proof: (*Lemma 4: If* $a \neq 0$*, then* a^{-1} *is unique.*)
Suppose $a \neq 0$ and there is a $b \in \mathbb{F}$ such that $ab = 1$. Because $a \neq 0$, a^{-1} exists. Multiplying both sides of the equation $ab = 1$ by a^{-1} yields: $a^{-1}ab = a^{-1}1 = a^{-1}$. But $a^{-1}a = 1$, and hence $b = a^{-1}$. □

Proof: (*Lemma 5:* $-a = (-1)a$.)
Note that $0 = a(1 + -1) = a1 + a(-1) = a + a(-1)$. Adding $-a$ to both sides yields $-a = 0 + a(-1)$, and hence $-a = (-1)a$. □

Proof: (*Lemma 6:* $(-1)(-1) = 1$.)

$$0 = (-1)(1 + -1) = (-1)1 + (-1)(-1) = -1 + (-1)(-1)$$

Adding 1 to both sides of the equation yields:

$$0 + 1 = -1 + 1 + (-1)(-1) = (-1)(-1)$$

Therefore, $1 = (-1)(-1)$. □

Proof: (*Lemma 7:* $a(-b) = -(ab) = (-a)b$ *and* $(-a)(-b) = ab$.)
We have by the previous lemmas and by commutativity of multiplication:

$$a(-b) = a(-1)b = (-1)ab = -(ab)$$

Similarly, $(-a)b = (-1)ab = -(ab)$. Finally: $(-a)(-b) = (-1)a(-1)b = (-1)(-1)ab = ab$. □

Proof: (*Lemma 8: If* $ab = 0$*, then either* $a = 0$ *or* $b = 0$.)
Suppose $ab = 0$, but that both a and b are nonzero. We reach a contradiction. If $a \neq 0$ and $b \neq 0$, then there exist multiplicative inverses a^{-1} and b^{-1}. Thus, multiplying the equation $ab = 0$ by the product $a^{-1}b^{-1}$ yields:

$$aba^{-1}b^{-1} = 0$$

and hence: $0 = aa^{-1}bb^{-1} = (1)(1) = 1$. Thus, $0 = 1$. This is a contradiction, as we know that $0 \neq 1$. □

Proof: (*Lemma 9: If* $a^2 = 1$*, then* $a \in \{-1, 1\}$.)
Suppose $a^2 = 1$. Then we have:

$$(a + 1)(a - 1) = a^2 - a + a - 1 = 1 - 1 = 0$$

Therefore, either $(a + 1) = 0$ or $(a - 1) = 0$. Equivalently, either $a = -1$ or $a = 1$. □

Proof: (*Lemma 10:* $\Pi_{i=1}^{n}(a - b_i) = 0$ *implies* $a \in \{b_1, \ldots, b_n\}$.)
This fact follows by using induction together with Lemma 8. □

III. EXAMPLES

Basic examples of fields are $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$ (the real numbers, rational numbers, and complex numbers, respectively). Interesting *finite field* examples are the binary field $\mathbb{F}_2 = \{0, 1\}$, where all arithmetic is taken mod 2, and $\mathbb{F}_3 = \{0, 1, 2\}$, where all arithmetic is taken mod 3. Thus, in $\mathbb{F}_3$, we have $-1 = 2$, $-2 = 1$, and $2^{-1} = 2$. It can be shown that $\mathbb{F}_p$, consisting of all integers from 0 to $p - 1$ (where p is prime) and with mod p arithmetic, is a field. There exist finite fields of size p^k (where k is an integer power, and p is a prime), but arithmetic needs to be redefined for these fields (mod p^k arithmetic will not work!). Example: Show that the 4-element set $\{0, 1, 2, 3\}$ with mod 4 arithmetic is *not* a field.