Notation:

1. $\forall a$ - is read “for all a”
2. $\exists a$ - is read “there exists some a”
3. $a \in B$ - is read “a in B”

Definition-A field is a set , F ,with two binary operations addition , + , and multiplication , X , and two distinct special elements zero, 0 , and one, 1. Such that the following properties hold :

F1.Commutative Property - $\forall a, b \in F$ it follows that $a+b=b+a$ and $a \times b = b \times a$.

F2.Associative Property - $\forall a, b, c \in F$ it follows that $(a+b)+c=a+(b+c)$ and $(a \times b) \times c = a \times (b \times c)$.

F3.Additive Identity - $\forall a \in F$ it follows that $a+0=a$

Multiplicative Identity - $\forall a \in F$ it follows that $a \times 1 = a$

F4.Existence of Multiplicative Inverse - $\forall a \neq 0 \in F$ $\exists b \in F$ s.t. $a \times b = 1$.

Existence of Additive Inverse - $\forall a \in F$ $\exists b \in F$ s.t. $a - b = 0$.

F5.Distributive Property - $\forall a, b, c \in F$ it follows that $a \times (b+c) = a \times b + a \times c$

Note that as a result the following holds $\forall a, b \in F$ $(a-b)(a+b)=a^2-b^2$.

However the existence of a square root, which can be written as follows, cannot be inferred from these properties alone. $\forall a \in F \exists b \in F$ such that $a=x^2$ or $-a=x^2$

Examples of Fields

1. $\mathbb{R}$ - the real numbers.
2. $\mathbb{Q}=\{\frac{m}{n} | m, n \in \mathbb{Z}\}$ - the set of rational numbers
3. The set of Integers $\mathbb{Z}=\{..., -4, -3, -2, -1, 0, 1, 2, 3, 4...\}$ is **not** a field as F4 does not hold, e.g. given $a=3 \in \mathbb{Z}$ there is no $b \in Z$ such that $a \times b = 1$, in $\mathbb{R}$ b= $b=\frac{1}{3}$ but $\frac{1}{3} \notin \mathbb{Z}$.
4. $F=\{0,1\}$ the operations + and x are defined by:

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

It is necessary to test every possible case for each of the field properties, for example :

F1. $a+b=b+a$ one must test 4 times for ever possible value of a and b.

5. $\mathbb{C}=\{a+bi | a, b \in \mathbb{R}\}$ - the complex numbers

Theorem: $\forall a, b \in F \quad (a+b)(a-b)=a^2-b^2$

In order to prove the above theorem one must first prove the below lemma:

Lemma – I. $\forall a \in F$,a has a unique negative

Precisely $a+b_1=0, a+b_2=0$ it follows that $b_1=b_2$

II. $\forall a \neq 0 \in F$, a has a unique inverse.

Precisely $a \neq 0, a \times b_1=1, a \times b_2=1$ it follows that $b_1=b_2$

Proof of Part II:

Suppose $a \neq 0, ab_1=1=ab_2$

Take any c such that $ca=1$ (Exists by F4)

$c(ab_1)=c(ab_2)$

$(ca)b_1=(ca)b_2$ (by property F2)

$1 \times b_1=1 \times b_2$ (by choice of c)

$b_1=b_2$ (by F3)

For practice prove part I.

Definition: $\forall a \in F$ define $-a$ to be **<u>the</u>** b for which $a+b=0$, therefore $a+(-a)=0$

Likewise $\forall a \in F$ define a^{-1} to be **<u>the</u>** b for which $a \times b=1$ therefore $a \times a^{-1}=1$.

Definition: $a-b:=a+(-b)$ and $\frac{a}{b}:=a \times b^{-1}$ and $a^2:=a \times a$.

Lemma: $\forall a, b \quad a \times (-b)=-ab$, prove for practice.

Proof of the main theorem:

$(a-b)(a+b)=(a+(-b))(a+b)$ = (by definition)

$a(a+b)+(-b)(a+b)$ = (by property F5)

$(a \times a+a \times b)+((-b) \times a+(-b) \times b)$ = (by property F5)

$(a^2+ab)+((-b) \times a+(-b) \times b)$ = (by definition)

$(a^2+ab)+(-ab+(-b \times b))$ = (by above lemma)

$(a^2+ab)+(-ab+(-b^2))$ = (by above lemma)

$a^2+(ab+(-ab+(-b^2)))$ = (by property F2)

$a^2+((ab+-ab)-b^2)$ = (by property F2)

$a^2+((0)+(-b^2))$ (by above lemma and definition)

$a^2+-(b^2)$ = (by property F3)

a^2-b^2 (by definition)