# Field Theory Exercises

Jason Sass

July 30, 2021

**Exercise 1.** Let $F$ be a field.
Let $a, b \in F$.
If $b \neq 0$ and $ab = b$, then $a = 1$.

*Proof.* Suppose $b \neq 0$ and $ab = b$.
Since $b \neq 0$, then $\frac{1}{b} \in F$.
Therefore,

$$\begin{aligned} a &= a \cdot 1 \\ &= a \cdot (b \cdot \frac{1}{b}) \\ &= (ab) \cdot \frac{1}{b} \\ &= b \cdot \frac{1}{b} \\ &= 1. \end{aligned}$$

□

**Exercise 2.** Let $F$ be a field.
Let $a, b \in F$.
If $a \neq 0$ and $ab = 1$, then $b = \frac{1}{a}$.

*Proof.* Suppose $a \neq 0$ and $ab = 1$.
Since $a \neq 0$, then $\frac{1}{a} \in F$.
Therefore,

$$\begin{aligned} b &= 1 \cdot b \\ &= (\frac{1}{a} \cdot a) \cdot b \\ &= \frac{1}{a} \cdot (ab) \\ &= \frac{1}{a} \cdot 1 \\ &= \frac{1}{a}. \end{aligned}$$

□

**Exercise 3.** Let $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

Then $(S, +, *)$ is a commutative ring with unity $1 \neq 0$.

*Proof.* Observe that $S$ is a subset of the additive group of real numbers $(\mathbb{R}, +)$.

Since $0 = 0 + 0\sqrt{2}$, then 0 is an element of $S$, so $S$ is not empty.

Let $x, y \in S$.

Then there exist integers $a, b, c, d$ such that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$.

Thus,

$$\begin{aligned} x - y &= (a + b\sqrt{2}) - (c + d\sqrt{2}) \\ &= (a - c) + (b - d)\sqrt{2}. \end{aligned}$$

Hence, $x - y \in S$.

Therefore, $S$ is an additive subgroup of $\mathbb{R}$, so $S$ is closed under addition.

Since $\mathbb{R}$ is abelian and $S \subset \mathbb{R}$ and $S$ is closed under addition, then addition is commutative in $S$.

Hence, $S$ is abelian, so $(S, +)$ is an abelian group.

Let $x, y \in S$.

Then there exist integers $a, b, c, d$ such that $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$.

Thus,

$$\begin{aligned} xy &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= ac + ad\sqrt{2} + bc\sqrt{2} + 2bd \\ &= (ac + 2bd) + (ad + bc)\sqrt{2}. \end{aligned}$$

Hence, $xy \in S$, so $S$ is closed under multiplication.

Since $S$ is a subset of $\mathbb{R}$, then $xy \in \mathbb{R}$.

Since $\mathbb{R}$ is a ring, then multiplication is a binary operation on $\mathbb{R}$, so multiplication is well defined in $\mathbb{R}$.

Hence, $xy$ is unique.

Since $S$ is closed under multiplication and $xy$ is unique, then multiplication is a binary operation on $S$.

Since $(\mathbb{R}, +, *)$ is a commutative ring, then multiplication is associative and commutative in $\mathbb{R}$.

Since $S \subset \mathbb{R}$ and $S$ is closed under multiplication, then multiplication is associative and commutative in $S$.

Observe that $1 = 1 + 0\sqrt{2}$, so $1 \in S$ and $1 \neq 0$.

Since 1 is the unity of $\mathbb{R}$, then for every $r \in \mathbb{R}$, $r * 1 = 1 * r = r$.

Let $x \in S$.

Since $x \in S$ and $S \subset \mathbb{R}$, then $x \in \mathbb{R}$.

Hence, $x * 1 = 1 * x = x$. Therefore, 1 is a multiplicative identity of $S$. Thus, a multiplicative identity exists in $S$.

Since $\mathbb{R}$ is a ring, then the distributive laws hold in $\mathbb{R}$. Thus, for every $x, y, z \in \mathbb{R}, x(y + z) = xy + xz$ and $(x + y)z = xz + yz$. Let $a, b, c \in S$. Since $S \subset \mathbb{R}$, then $a, b, c \in \mathbb{R}$. Hence, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$. Therefore, the distributive laws hold in $S$.

Thus, $(S, +, *)$ is a commutative ring with unity $1 \neq 0$. $\square$

**Exercise 4.** Let $S = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Then $(S, +, *)$ is not a field.

*Proof.* Observe that $(S, +, *)$ is a commutative ring with unity $1 \neq 0$. Thus, $S$ is a field iff every nonzero element of $S$ is a unit. Hence, $S$ is not a field iff there exists a nonzero element of $S$ that is not a unit.

Let $x = \sqrt{2}$. Then $x = 0 + 1 * \sqrt{2}$, so $x \in S$ and $x \neq 0$. The element $x$ is a unit iff there exists $y \in S$ such that $xy = 1$. Hence, $x$ is not a unit iff there does not exist $y \in S$ such that $xy = 1$.

Suppose there exists $y \in S$ such that $xy = 1$. Then there exist integers $a, b$ such that $y = a + b\sqrt{2}$. Thus,

$$\begin{aligned} 1 &= xy \\ &= \sqrt{2}(a + b\sqrt{2}) \\ &= a\sqrt{2} + 2b. \end{aligned}$$

Hence, $1 + 0\sqrt{2} = 1 = 2b + a\sqrt{2}$, so $1 = 2b$ and $0 = a$. Thus, $b = \frac{1}{2}$, so $b \notin \mathbb{Z}$. But, we have $b \in \mathbb{Z}$ and $b \notin \mathbb{Z}$, a contradiction. Therefore, does not exist $y \in S$ such that $xy = 1$. Thus, $x$ is not a unit. Hence, there exists a nonzero element of $S$ that is not a unit. Therefore, $S$ is not a field. □

**Exercise 5.** The algebraic structure $(\mathbb{Z} \times \mathbb{Z}, +, *)$ is a commutative ring with unity $(1, 1)$ and is not a field.

**Solution.** The direct product of $n$ copies of a commutative ring is a commutative ring. Hence, the direct product of 2 copies of a commutative ring is a commutative ring. Observe that $(\mathbb{Z}, +, *)$ is a commutative ring and $(\mathbb{Z}\times\mathbb{Z}, +, *)$ is the direct product of 2 copies of $(\mathbb{Z}, +, *)$. Therefore, $(\mathbb{Z}^2, +, *)$ is a commutative ring. Observe that the unity of $\mathbb{Z}^2$ is $(1, 1)$ and the zero of $\mathbb{Z}^2$ is $(0, 0)$ and $(1, 1) \neq (0, 0)$.

The ring $\mathbb{Z}^2$ is a field iff $\mathbb{Z}^2$ is a commutative ring and the unity is distinct from the zero element and every nonzero element of $\mathbb{Z}^2$ is a unit. Since $\mathbb{Z}^2$ is a commutative ring with unity $(1, 1) \neq (0, 0)$, then $\mathbb{Z}^2$ is a field iff every nonzero element of $\mathbb{Z}^2$ is a unit. Hence, $\mathbb{Z}^2$ is not a field iff there exists a nonzero element of $\mathbb{Z}^2$ that is not a unit.

Let $x = (1, 2) \in \mathbb{Z}^2$. Then $(1, 2) \neq (0, 0)$, so $(1, 2)$ is a nonzero element of $\mathbb{Z}^2$.

Suppose $(1, 2)$ is a unit of $\mathbb{Z}^2$. Then there exists an element $y \in \mathbb{Z}^2$ such that $xy = (1, 1)$. Since $y \in \mathbb{Z}^2$, then there exist integers $a, b$ such that $y = (a, b)$.

Observe that

$$\begin{aligned} (1, 1) &= xy \\ &= (1, 2)(a, b) \\ &= (a, 2b). \end{aligned}$$

Thus, $1 = a$ and $1 = 2b$, so $b = \frac{1}{2}$. Hence, $b \notin \mathbb{Z}$. Thus, we have $b \in \mathbb{Z}$ and $b \notin \mathbb{Z}$, a contradiction. Therefore, $(1, 2)$ is not a unit of $\mathbb{Z}^2$.

Hence, there exists a nonzero element of $\mathbb{Z}^2$ that is not a unit of $\mathbb{Z}^2$. Therefore, $(\mathbb{Z}^2, +, *)$ is not a field. □

**Exercise 6.** What are all of the units in the ring $\mathbb{Z} \times \mathbb{Z}$?

**Solution.** We know that the ring $\mathbb{Z} \times \mathbb{Z}$ is not a field, so not every nonzero element is a unit. Hence, there are some nonzero elements of $\mathbb{Z} \times \mathbb{Z}$ which do not have multiplicative inverses in $\mathbb{Z} \times \mathbb{Z}$.

Let $S$ be the set of all units of $\mathbb{Z} \times \mathbb{Z}$. Then $S = \{a \in \mathbb{Z} \times \mathbb{Z} : (\exists a^{-1} \in \mathbb{Z}^2)(aa^{-1} = (1,1)\}$. Let $x \in S$. Then $x \in \mathbb{Z}^2$ and there exists $x^{-1} \in \mathbb{Z}^2$ such that $xx^{-1} = (1,1)$. Thus, there exist integers $a, b, c, d$ such that $x = (a, b)$ and $x^{-1} = (c, d)$. Hence,

$$\begin{aligned} (1,1) &= xx^{-1} \\ &= (a,b)(c,d) \\ &= (ac, bd). \end{aligned}$$

Thus, $1 = ac$ and $1 = bd$. Since $a, b, c, d$ are integers, then this implies either $a = c = 1$ or $a = c = -1$ and either $b = d = 1$ or $b = d = -1$. Hence, $a = c$ and $b = d$, so $x = x^{-1}$ and 4 possibilities exist. Thus, $x$ is either $(1,1)$ or $(1,-1)$ or $(-1,1)$ or $(-1,-1)$. Therefore, $S = \{(1,1),(1,-1),(-1,1),(-1,-1)\}$. □

**Exercise 7.** Let $F$ be a field.
Let $x \in F$ such that $x = x^{-1}$.
Then $x = 1$.
Is this true or false?

*Proof.* This is false.
Here is a counterexample. There are other counter examples as well.
Let $F$ be the field $(\mathbb{Z}_3, +, \cdot)$.
Then $2 = 2^{-1}$ since $2 \cdot 2 = 1$, but $2 \neq 1$.
Another counterexample is the field $(\mathbb{R}, +, \cdot)$.
Clearly, $-1 = (-1)^{-1}$ since $(-1)(-1) = 1$, but $-1 \neq 1$. □

**Exercise 8.** Let $F$ be a field.
Let $x \in F$ such that $x = -x$.
Then $x = 0$.
Is this true or false?

*Proof.* This is false.
Here is a counterexample.
Let $F$ be the field $(\mathbb{Z}_2, +, \cdot)$.
Then $1 = -1$ since $1 + 1 = 0$, but $1 \neq 0$. □

**Exercise 9.** Let $n$ be a positive integer.
Give an example of a field $F$ and nonzero element $x \in F$ such that $nx = 0$.

**Solution.** Let $F = (\mathbb{Z}_7, +, \cdot)$.
Since 7 is prime, then $F$ is a field.
Let $n = 7$ and $x = 5$.
Then

$$
\begin{aligned}
7*5 &= 6*5+5 \\
&= (5*5+5)+5 \\
&= ((4*5+5)+5)+5 \\
&= (((3*5+5)+5)+5)+5 \\
&= ((((2*5+5)+5)+5)+5)+5 \\
&= (((((1*5+5)+5)+5)+5)+5)+5 \\
&= (((((5+5)+5)+5)+5)+5)+5 \\
&= ((((3+5)+5)+5)+5)+5 \\
&= (((1+5)+5)+5)+5 \\
&= ((6+5)+5)+5 \\
&= (4+5)+5 \\
&= 2+5 \\
&= 0.
\end{aligned}
$$

□

**Exercise 10.** Let $(F, +, \cdot)$ be a field.

Let $a, b, c, x \in F$ and $a \neq 0$.

Then $ax + b = c$ iff $x = (c - b)a^{-1}$.

Therefore, a linear equation in one variable with coefficients in a field $F$ has a unique solution in $F$.

*Proof.* We prove if $ax + b = c$, then $x = (c - b)a^{-1}$.

Suppose $ax + b = c$.

Then $ax = c - b$.

Since $a \neq 0$, we divide by $a$ to get $x = \frac{c-b}{a} = (c - b)a^{-1}$.

Conversely, we prove if $x = (c - b)a^{-1}$, then $ax + b = c$.

Suppose $x = (c - b)a^{-1}$.

Then

$$
\begin{aligned}
ax + b &= a((c-b)a^{-1}) + b \\
&= a(a^{-1}(c-b)) + b \\
&= (aa^{-1})(c-b) + b \\
&= 1(c-b) + b \\
&= c - b + b \\
&= c.
\end{aligned}
$$

□

**Exercise 11.** Give an example linear equation in $\mathbb{Z}_8$ that has no solution and one that has more than one solution.

Give an example of elements $a, b$ of $\mathbb{Z}_8$ such that $a^2 = b^2$, but $a \neq b$ and $a \neq -b$.

**Solution.** $\mathbb{Z}_8$ is a commutative ring that has zero divisors.

For example, 4 is a zero divisor because $0 = 4 * 2$ and $2 \neq 0$.

Hence, $\mathbb{Z}_8$ is not an integral domain, so $\mathbb{Z}_8$ cannot be a field.

A linear equation $ax + b = c$ for $a, b, c \in \mathbb{Z}_8$ has at least one solution $x = (c - b)a^{-1}$ if $a^{-1}$ exists.

Therefore, if $ax + b = c$ for $a, b, c \in \mathbb{Z}_8$ has no solution, then $a^{-1}$ does not exist.

So, to provide an example of a linear equation in $\mathbb{Z}_8$ that has no solution, we want $a$ to not have a multiplicative inverse.

Since $4*0+5 = 5 \neq 6$ and $4*1+5 = 1 \neq 6$ and $4*2+5 = 5 \neq 6$ and $4*3+5 = 1 \neq 6$ and $4*4+5 = 5 \neq 6$ and $4*5+5 = 1 \neq 6$ and $4*6+5 = 5 \neq 6$ and $4*7+5 = 1 \neq 6$, then the linear equation $4x+5 = 6$ in $\mathbb{Z}_8$ has no solution.

Here is an example of a linear equation in $\mathbb{Z}_8$ that has more than one solution: $4x + 3 = 7$.

The solution set is $\{1, 3, 5, 7\}$ since $4*1+3 = 7 = 4*3+3 = 4*5+3 = 4*7+3$.

Let $a = 1$ and $b = 3$. Then $1^2 = 1 = 3^2$ and $1 \neq 3$ and $1 \neq -3$ since $-3 = 5$. □

**Exercise 12.** Let $F$ be a field. If $a \in F$, then there exists $x \in F$ such that $x^2 = a$. Is this true or false?

**Solution.** This is false. Here is a counterexample. Let $F$ be the field $(\mathbb{Q}, +, \cdot)$ with $a = 2 \in \mathbb{Q}$. Then there does not exist $x \in \mathbb{Q}$ such that $x^2 = 2$. □

**Exercise 13.** Let $S = \{a, b\}$. Define addition on $S$ by $a + a = a$ and $a + b = b = b + a$ and $b + b = b$. Define multiplication on $S$ by $aa = ab = ba = a$ and $bb = b$. Then $(S, +, *)$ is a field.

**Solution.** To prove $S$ is a field, we must prove $S$ is a commutative division ring. Thus, we must prove $(S, +, *)$ is a ring with $1 \neq 0$ and $*$ is commutative and every nonzero element of $S$ has a multiplicative inverse. Hence, we must prove

1. $(S, +)$ is an abelian group.

1a. addition is a binary operation on $S$.

1a1. $S$ is closed under addition.

1a2. $x + y$ is unique for all $x, y \in S$.

1b. $+$ is associative.

1c. $+$ is commutative.

1d. there exists an additive identity in $S$.

1e. each element of $S$ has an additive inverse.

2. multiplication is a binary operation on $S$.

2a1. $S$ is closed under multiplication.

2a2. $xy$ is unique for all $x, y \in S$.

2. $*$ is associative.

3. there exists a multiplicative identity 1

4. multiplication distributes over addition:

4a. left distributive : $a(b + c) = ab + ac$

4b. right distributive: $(a+b)c = ac+bc$.

5. $1 \neq 0$.

6. $*$ is commutative.

7. every nonzero element of $S$ has a multiplicative inverse.

We can write out the addition and multiplication tables for $S$. Since $|S| = 2$, then $|S \times S| = |S||S| = 2 * 2 = 2^2 = 4$. Thus, there are 4 ordered pairs mapped by addition and mapped by multiplication.

□

*Proof.* The sum of any pair of elements of $S$ is a unique element of $S$. Hence, addition is a binary operation on $S$.

Since $a+b = b = b+a$, then addition is commutative.

We prove addition is associative.

There are $2^3 = 8$ cases to consider.

**Case 1:** Observe that $(a+a)+a = a+a = a+(a+a)$.

**Case 2:** Observe that $(a+a)+b = a+b = a+(a+b)$.

**Case 3:** Observe that $(a+b)+a = b+a = b = a+b = a+(b+a)$.

**Case 4:** Observe that $(a+b)+b = b+b = a = a+a = a+(b+b)$.

**Case 5:** Observe that $(b+a)+a = b+a = b+(a+a)$.

**Case 6:** Observe that $(b+a)+b = b+b = b+(a+b)$.

**Case 7:** Observe that $(b+b)+a = a+a = a = b+b = b+(b+a)$.

**Case 8:** Observe that $(b+b)+b = a+b = b = b+a = b+(b+b)$.

Thus, addition is associative.

Since $a+a = a$ and $a+b = b = b+a$, then $a$ is an additive identity. Thus, $a$ is a zero element of $S$.

Since $a+a = a$, then $a$ is an additive inverse of $a$. Since $b+b = a$, then $b$ is an additive inverse of $b$. Hence, each element of $S$ has an additive inverse.

Therefore, $(S, +)$ is an abelian group.

The product of any pair of elements of $S$ is a unique element of $S$. Hence, multiplication is a binary operation on $S$.

Since $ab = a = ba$, then multiplication is commutative.

We prove multiplication is associative.

There are $2^3 = 8$ cases to consider.

**Case 1:** Observe that $(aa)a = aa = a(aa)$.

**Case 2:** Observe that $(aa)b = ab = a = aa = a(ab)$.

**Case 3:** Observe that $(ab)a = aa = a(ba)$.

**Case 4:** Observe that $(ab)b = ab = a(bb)$.

**Case 5:** Observe that $(ba)a = aa = a = ba = b(aa)$.

**Case 6:** Observe that $(ba)b = ab = a = ba = b(ab)$.

**Case 7:** Observe that $(bb)a = ba = b(ba)$.

**Case 8:** Observe that $(bb)b = bb = b(bb)$.

Thus, multiplication is associative.

Since $ba = a = ab$ and $bb = b$, then $b$ is a multiplicative identity. Since $a \neq b$, then the multiplicative identity is distinct from the additive identity. The only nonzero element in $S$ is $b$. Since $bb = b$, then the multiplicative inverse of $b$ is $b$. Hence, every nonzero element of $S$ has a multiplicative inverse.

We prove the left distributive law holds in $S$.

There are $2^3 = 8$ cases to consider.

**Case 1:** Observe that $a(a+a) = aa = a = a+a = aa+aa$.

**Case 2:** Observe that $a(a+b) = ab = a = a+a = aa+ab$.

**Case 3:** Observe that $a(b+a) = ab = a = a+a = ab+aa$.

**Case 4:** Observe that $a(b+b) = aa = a = a+a = ab+ab$.

**Case 5:** Observe that $b(a+a) = ba = a = a+a = ba+ba$.

**Case 6:** Observe that $b(a+b) = bb = b = a+b = ba+bb$.

**Case 7:** Observe that $b(b+a) = bb = b = b+a = bb+ba$.

**Case 8:** Observe that $b(b+b) = ba = a = b+b = bb+bb$.

Thus, the left distributive law holds in $S$.

Let $x, y, z \in S$. Then $(x+y)z = z(x+y) = zx+zy = xz+yz$. Thus, the right distributive law holds in $S$. Hence, multiplication is distributive over addition in $S$.

Therefore, $(S, +, *)$ is a field. □

*Proof.* Define $\phi : \mathbb{Z}_2 \to S$ by $\phi(0) = a$ and $\phi(1) = b$.

Clearly, $\phi$ is a function and $\phi$ is injective and surjective. Hence, $\phi$ is bijective.

We prove $\phi$ is a ring homomorphism. Observe that $\phi(0+0) = \phi(0) = a = a+a = \phi(0)+\phi(0)$ and $\phi(0+1) = \phi(1) = b = a+b = \phi(0)+\phi(1)$ and $\phi(1+0) = \phi(1) = b = b+a = \phi(1)+\phi(0)$ and $\phi(1+1) = \phi(0) = a = b+b = \phi(1)+\phi(1)$. Thus, $\phi$ preserves addition.

Observe that $\phi(0*0) = \phi(0) = a = aa = \phi(0)\phi(0)$ and $\phi(0*1) = \phi(0) = a = ab = \phi(0)\phi(1)$ and $\phi(1*0) = \phi(0) = a = ba = \phi(1)\phi(0)$ and $\phi(1*1) = \phi(1) = b = bb = \phi(1)\phi(1)$. Thus, $\phi$ preserves multiplication.

Since $\phi(1) = b$ and 1 is unity of $\mathbb{Z}_2$ and $b$ is unity of $S$, then $\phi$ preserves the unity element of the rings.

Therefore, $\phi$ is a ring homomorphism. Since $\phi$ is bijective, then $\phi$ is a bijective ring homomorphism, so $\phi$ is a ring isomorphism. Hence, $(\mathbb{Z}_2, +, *) \cong (S, +, *)$. Since 2 is prime, then $\mathbb{Z}_2$ is a field. Hence, $S$ is a field. □

**Exercise 14.** Let $(R, +, \cdot)$ be a ring.

If $(R^*, \cdot)$ is an abelian group, then $(R, +, \cdot)$ is a field.

*Proof.* Suppose $(R^*, \cdot)$ is an abelian group.

To prove $(R, +, \cdot)$ is a field, we prove multiplication is commutative and multiplicative identity $1 \neq 0$ and every nonzero element has a multiplicative inverse in $R$.

Since $R$ is a ring, then there is a zero of $R$.

Let 0 be the zero of $R$.

Since $(R^*, *)$ is a multiplicative group, then there is a multiplicative identity in $R^*$.

Let 1 be the multiplicative identity of $R^*$.

Then $1 \in R^*$, so $1 \in R$ and $1 \neq 0$.

Thus, $1 \neq 0$.

Since $(R^*, *)$ is a group, then each element of $R^*$ has a multiplicative inverse in $R^*$.

Let $a \in R^*$. Then $a \in R$ and $a \neq 0$ and there exists $b \in R^*$ such that $ab = ba = 1$. Since $b \in R^*$ and $R^* \subset R$, then $b \in R$. Hence, the multiplicative inverse of $a$ is in $R$. Thus, each nonzero element of $R$ has a multiplicative inverse in $R$.

We prove multiplication is commutative. Let $a, b \in R$. Either $a = 0$ or $a \neq 0$ and either $b = 0$ or $b \neq 0$.

Thus, there are 4 cases to consider.

**Case 1:** Suppose $a = 0$ and $b = 0$.

Then $ab = 0 * 0 = 0 = 0 * 0 = ba$.

**Case 2:** Suppose $a = 0$ and $b \neq 0$.

Then $ab = 0b = 0 = b0 = ba$.

**Case 3:** Suppose $a \neq 0$ and $b = 0$.

Then $ab = a * 0 = 0 = 0 * a = ba$.

**Case 4:** Suppose $a \neq 0$ and $b \neq 0$.

Then $a \in R^*$ and $b \in R^*$. Since $(R^*, *)$ is an abelian group, then multiplication is commutative in $R^*$. Thus, $ab = ba$.

Hence, in all cases, $ab = ba$, so multiplication is commutative in $R$. □

**Exercise 15.** Let $(F, F^+)$ be an ordered field. Let $x \in F$ and $x \neq 0$. Then $x^{2n} \in F^+$ for all $n \in \mathbb{N}$.

*Proof.* Define predicate $p(n) : x^{2n} \in F^+$ over $\mathbb{N}$.

We prove $p(n)$ for all $n \in \mathbb{N}$ by induction on $n$.

**Basis:** Since $x \in F$ and $x \neq 0$, then $x^2 = x^{2*1} \in F^+$. Therefore, $p(1)$ is true.

**Induction:** Let $n \in \mathbb{N}$ such that $p(n)$ is true. Then $x^{2n} \in F^+$. To prove $p(n+1)$ is true, we must prove $x^{2(n+1)} \in F^+$.

Observe that $x^{2(n+1)} = x^{2n+2} = x^{2n}x^2$.

Since $x^{2n} \in F^+$ and $x^2 \in F^+$, then by closure of $F^+$ under multiplication of $F$, $x^{2n}x^2 \in F^+$.

Thus, $x^{2(n+1)} \in F^+$.

Therefore, $p(n)$ implies $p(n+1)$ for all $n \in \mathbb{N}$.

Hence, by induction, $p(n)$ is true for all $n \in \mathbb{N}$.

Therefore, $x^{2n} \in F^+$ for all $n \in \mathbb{N}$. □

**Exercise 16.** Let $(F, F^+)$ be an ordered field. Let $x, y, a \in F$. Then

1. if $x \leq y$, then $x + a \leq y + a$.
2. if $x \leq y$ and $a \geq 0$, then $ax \leq ay$.
3. if $x \leq y$ and $a \leq 0$, then $ax \geq ay$.

*Proof.* We prove 1.

Suppose $x \leq y$. Then either $x < y$ or $x = y$.

We consider these cases separately.

**Case 1:** Suppose $x = y$.

Then $x + a = y + a$.

**Case 2:** Suppose $x < y$.

Then $y - x \in F^+$.

To prove $x + a < y + a$, we must prove $(y + a) - (x + a) \in F^+$.
Observe that $y - x = y - x + a - a = y + a - x - a = (y + a) - (x + a)$.
Therefore, $(y + a) - (x + a) \in F^+$.
We prove 2.
Suppose $x \leq y$ and $a \geq 0$.
Then both $x < y$ or $x = y$ and $a > 0$ or $a = 0$. Thus, either $x < y$ and $a > 0$ or $x < y$ and $a = 0$ or $x = y$ and $a > 0$ or $x = y$ and $a = 0$.
We consider these cases separately.
**Case 1:** Suppose $x < y$ and $a = 0$.
Then $ax = 0x = 0 = 0y = ay$.
**Case 2:** Suppose $x = y$ and $a = 0$.
Then $ax = ax = ay$.
**Case 3:** Suppose $x = y$ and $a > 0$.
Then $ax = ax = ay$.
**Case 4:** Suppose $x < y$ and $a > 0$.
Then $y - x \in F^+$ and $a \in F^+$.
To prove $ax < ay$, we prove $ay - ax \in F^+$.
By closure of $F^+$ under multiplication of $F$, we have $a(y - x) \in F^+$.
Therefore, $ay - ax \in F^+$.
We prove 3.
Suppose $x \leq y$ and $a \leq 0$.
Then both $x < y$ or $x = y$ and $a < 0$ or $a = 0$. Thus, either $x < y$ and $a < 0$ or $x < y$ and $a = 0$ or $x = y$ and $a < 0$ or $x = y$ and $a = 0$.
We consider these cases separately.
**Case 1:** Suppose $x < y$ and $a = 0$.
Then $ax = 0x = 0 = 0y = ay$.
**Case 2:** Suppose $x = y$ and $a = 0$.
Then $ax = ax = ay$.
**Case 3:** Suppose $x = y$ and $a < 0$.
Then $ax = ax = ay$.
**Case 4:** Suppose $x < y$ and $a < 0$.
Then $y - x \in F^+$ and $-a \in F^+$.
To prove $ax > ay$, we prove $ax - ay \in F^+$.
By closure of $F^+$ under multiplication of $F$, we have $-a(y - x) \in F^+$. Since $-a(y - x) = -ay - a(-x) = -ay + ax = ax - ay$, then $ax - ay \in F^+$, as desired. □

**Exercise 17.** Let $(F, +, \cdot, \leq)$ be an ordered field.
Let $x, y, a, b \in F$.
Then
1. if $a \leq x$ and $b < y$, then $a + b < x + y$.
2. if $a \leq x$ and $b \leq y$, then $a + b \leq x + y$.
3. if $0 \leq a < x$ and $0 \leq b < y$, then $ab < xy$.
4. if $0 \leq a \leq x$ and $0 \leq b < y$, then $ab \leq xy$.
5. if $0 \leq a \leq x$ and $0 \leq b \leq y$, then $ab \leq xy$.

*Proof.* We prove 1.

Suppose $a \leq x$ and $b < y$.

Since $b < y$, then $y - b \in F^+$.

Since $a \leq x$, then either $a < x$ or $a = x$.

We consider these cases separately.

To prove $a + b < x + y$, we must prove $(x + y) - (a + b) \in F^+$.

**Case 1:** Suppose $a < x$.

Then $x - a \in F^+$.

Since $x - a \in F^+$ and $y - b \in F^+$, then by closure of $F^+$ under addition of $F$, we have $(x - a) + (y - b) \in F^+$.

Observe that

$$\begin{aligned}(x-a)+(y-b) &= x-a+y-b \\ &= x+y-a-b \\ &= (x+y)-(a+b).\end{aligned}$$

Therefore, $(x + y) - (a + b) \in F^+$.

**Case 2:** Suppose $a = x$.

Then $x - a = 0$.

Observe that

$$\begin{aligned}y-b &= (y-b)+0 \\ &= (y-b)+(x-a) \\ &= y-b+x-a \\ &= y+x-b-a \\ &= x+y-a-b \\ &= (x+y)-(a+b).\end{aligned}$$

Therefore, $(x + y) - (a + b) = y - b \in F^+$. □

*Proof.* We prove 2.

Suppose $a \leq x$ and $b \leq y$.

Then $a \leq x$ and either $b < y$ or $b = y$. Hence, $a \leq x$ and $b < y$ or $a \leq x$ and $b = y$.

We consider these cases separately.

To prove $a + b \leq x + y$, we must prove either $a + b < x + y$ or $a + b = x + y$. Hence, we must prove either $(x + y) - (a + b) \in F^+$ or $a + b = x + y$.

**Case 1:** Suppose $a \leq x$ and $b < y$.

Then $a + b < x + y$.

**Case 2:** Suppose $a \leq x$ and $b = y$.

Then either $a < x$ or $a = x$ and $b = y$. Hence, either $a < x$ and $b = y$ or $a = x$ and $b = y$.

**Case 2a:** Suppose $a < x$ and $b = y$.

Then $x - a \in F^+$ and $y - b = 0$.

Observe that

$$\begin{aligned} x - a &= (x-a) + 0 \\ &= (x-a) + (y-b) \\ &= x - a + y - b \\ &= x + y - a - b \\ &= (x+y) - (a+b). \end{aligned}$$

Therefore, $(x+y)-(a+b) \in F^+$.

**Case 2b:** Suppose $a = x$ and $b = y$.

Then

$$\begin{aligned} a + b &= x + b \\ &= x + y. \end{aligned}$$

We prove 3.

Suppose $0 \leq a < x$ and $0 \leq b < y$. Then $0 \leq a$ and $a < x$ and $0 \leq b$ and $b < y$. Since $0 \leq a$ and $0 \leq b$, then either $0 < a$ or $0 = a$ and either $0 < b$ or $0 = b$. Thus, either $0 < a$ and $0 < b$ or $0 < a$ and $0 = b$ or $0 = a$ and $0 < b$ or $0 = a$ and $0 = b$.

We consider these cases separately.

**Case 1:** Suppose $0 = a$ and $0 = b$.

Since $0 = a$ and $a < x$, then $0 < x$. Since $0 = b$ and $b < y$, then $0 < y$. Hence, $x > 0$ and $y > 0$, so $xy > 0$. Therefore, $ab = 0 \cdot 0 = 0 < xy$, so $ab < xy$.

**Case 2:** Suppose $0 = a$ and $0 < b$.

Since $0 = a$ and $a < x$, then $0 < x$. Since $0 < b$ and $b < y$, then $0 < y$. Hence, $x > 0$ and $y > 0$, so $xy > 0$. Therefore, $ab = 0 \cdot b = 0 < xy$, so $ab < xy$.

**Case 3:** Suppose $0 < a$ and $0 = b$.

Since $0 < a$ and $a < x$, then $0 < x$. Since $0 = b$ and $b < y$, then $0 < y$. Hence, $x > 0$ and $y > 0$, so $xy > 0$. Therefore, $ab = a \cdot 0 = 0 < xy$, so $ab < xy$.

**Case 4:** Suppose $0 < a$ and $0 < b$.

Since $a < x$ and $b > 0$, then $ab < xb$, so $ab < bx$. Since $0 < a$ and $a < x$, then $0 < x$. Since $b < y$ and $x > 0$, then $bx < yx$, so $bx < xy$. Thus, $ab < bx$ and $bx < xy$, so $ab < xy$.

We prove 4.

Suppose $0 \leq a \leq x$ and $0 \leq b < y$. Then $0 \leq a$ and $a \leq x$ and $0 \leq b$ and $b < y$. Since $a \leq x$, then either $a < x$ or $a = x$.

We consider these cases separately.

**Case 1:** Suppose $a < x$.

If $0 \leq a < x$ and $0 \leq b < y$, then $ab < xy$.

Since $0 \leq a$ and $a < x$, then $0 \leq a < x$.

Since $0 \leq b$ and $b < y$, then $0 \leq b < y$.

Therefore, we conclude $ab < xy$.

**Case 2:** Suppose $a = x$.

Since $0 \leq a$, then either $0 < a$ or $0 = a$.

**Case 2a:** Suppose $0 = a$.
Then $ab = 0b = 0 = 0y = ay = xy$.
**Case 2b:** Suppose $0 < a$.
Then $a \in F^+$. Since $b < y$, then $y - b \in F^+$. Thus, $a(y - b) \in F^+$. Since $a(y - b) = ay - ab = xy - ab$, then $xy - ab \in F^+$. Therefore, $ab < xy$.
We prove 5.
Suppose $0 \leq a \leq x$ and $0 \leq b \leq y$. Then $0 \leq a$ and $a \leq x$ and $0 \leq b$ and $b \leq y$. Since $b \leq y$, then either $b < y$ or $b = y$.
We consider these cases separately.
**Case 1:** Suppose $b < y$.
If $0 \leq a \leq x$ and $0 \leq b < y$, then $ab \leq xy$.
Since $0 \leq a$ and $a \leq x$, then $0 \leq a \leq x$.
Since $0 \leq b$ and $b < y$, then $0 \leq b < y$.
Therefore, we conclude $ab \leq xy$.
**Case 2:** Suppose $b = y$.
Since $a \leq x$, then either $a < x$ or $a = x$.
**Case 2a:** Suppose $a = x$.
Then $ab = xb = xy$.
**Case 2b:** Suppose $a < x$.
Since $0 \leq b$, then either $0 < b$ or $0 = b$.
If $0 = b$, then $ab = a0 = 0 = x0 = xb = xy$.
If $0 < b$, then $b \in F^+$. Since $a < x$, then $x - a \in F^+$. Hence, $(x - a)b \in F^+$.
Since $(x - a)b = xb - ab = xy - ab$, then $xy - ab \in F^+$.
Therefore, $ab < xy$. □

**Exercise 18.** Let $F$ be a field.
Let $a, b \in F$.
If $a^2 + b^2 = 0$, then $a = b = 0$.
Is this true or false?

**Solution.** This is false.
Here is a counterexample.
Let $F$ be the field $(\mathbb{Z}_5, +, \cdot)$ with $a = 1$ and $b = 2$.
Then $1^2 + 2^2 = 1 * 1 + 2 * 2 = 1 + 4 = 0$, but $1 \neq 0$ and $2 \neq 0$. □

**Exercise 19.** Let $F$ be an ordered field.
Let $a, b \in F$.
If $a^2 + b^2 = 0$, then $a = 0$ and $b = 0$.

*Proof.* We prove by contrapositive.
Suppose either $a \neq 0$ or $b \neq 0$.
If $a \neq 0$, then $a^2 > 0$.
Since $b^2 \geq 0$, then $a^2 + b^2 > 0$, so $a^2 + b^2 \neq 0$.
If $b \neq 0$, then $b^2 > 0$.
Since $a^2 \geq 0$, then $a^2 + b^2 > 0$, so $a^2 + b^2 \neq 0$.
Therefore, in either case, $a^2 + b^2 \neq 0$, as desired. □

**Exercise 20.** Let $F$ be an ordered field.

Let $a, b \in F$ such that $a \geq 0$ and $b \geq 0$.

Then $a < b$ iff $a^2 < b^2$.

*Proof.* We must prove $a < b$ iff $a^2 < b^2$.

We prove if $a < b$, then $a^2 < b^2$.

Suppose $a < b$.

Then $b - a$ is positive. Since $a^2 < b^2$ iff $b^2 - a^2$ is positive iff $(b-a)(b+a)$ is positive, to prove $a^2 < b^2$, we prove $(b-a)(b+a)$ is positive.

The product $(b-a)(b+a)$ is positive iff $b-a$ and $b+a$ are either both positive or both negative. Therefore, we must prove $b-a$ and $b+a$ are either both positive or both negative. Since $b-a$ is positive, then we need only prove $b+a$ is positive.

Since $b \geq 0$ and $a \geq 0$, then $b + a \geq 0$. Hence, either $b + a > 0$ or $b + a = 0$.

Suppose $b + a = 0$. Then $a = -b$.

Since $b \geq 0$, then either $b > 0$ or $b = 0$.

If $b = 0$, then $a < b = 0$, so $a < 0$. But, $a \geq 0$. Therefore, $b \neq 0$.

If $b > 0$, then $-b < 0$, so $a < 0$. But, again, $a \geq 0$. Therefore, $b$ is not positive.

Hence, $b + a \neq 0$. Therefore, $b + a > 0$, so $b + a$ is positive, as desired.

Conversely, we prove if $a^2 < b^2$, then $a < b$.

Suppose $a^2 < b^2$.

To prove $a < b$, we must prove $b - a$ is positive.

Since $a^2 < b^2$, then $b^2 - a^2$ is positive, so $(b-a)(b+a)$ is positive.

Hence, $b - a$ and $b + a$ are either both positive or both negative.

Since $a \geq 0$ and $b \geq 0$, then $b + a \geq 0$, so $b + a$ is not negative.

Thus, we conclude $b - a$ and $b + a$ must be both positive.

Therefore, $b - a$ is positive, as desired. □

**Exercise 21.** If $R$ is a field, then the only ideals of $R$ are the zero ring and $R$ itself.

*Proof.* Let $R$ be a field.

Let $I$ be an ideal in $R$.

Then either $I$ is the zero ring or $I$ is not the zero ring.

Suppose $I$ is not the zero ring.

Since $I$ is an ideal, then $(I, +)$ is an abelian subgroup of $(R, +)$.

Since $I$ is not the zero group, then $I$ must contain a nonzero element.

Let $a$ be some nonzero element of $I$.

Then $a \in I$ and $a \neq 0$.

Since $R$ is a field, then every nonzero element of $R$ is a unit of $R$.

Hence, in particular, $a$ is a unit of $R$.

Therefore, there exists $a^{-1} \in R$ such that $aa^{-1} = e$, where $e$ is the unity of $R$. Since $I$ is an ideal, then for every $x \in I, IR \subset I$. Thus, $aR \subset I$, where $aR = \{ar : r \in R\}$. Since $a^{-1} \in R$, then $aa^{-1} \in aR$. Hence, $e \in aR$. Thus, $e \in aR$ and $aR \subset I$, so $e \in I$. Therefore, $eR \subset I$, where $eR = \{er : r \in R\} =$

$\{r : r \in R\} = R$. Hence, $R \subset I$. Since $I$ is an ideal, then $I \subset R$. Thus, $I \subset R$ and $R \subset I$, so $I = R$.

Therefore, either $I$ is the zero ring or $I$ is the field $R$ itself. $\square$