# Math 2550

## PSET 1

September 4 2025

# Contents

## Ex 1.1; Rudin 1.3

**Question**

Suppose $F$ is a field with $x, y, z \in F$. Prove carefully from the field axioms:

1. If $x \neq 0$ and $xy = xz$, then $y = z$
2. If $x \neq 0$ and $xy = x$, then $y = 1$.
3. If $xy = 1$, then $x \neq 0$ and $y = x^{-1}$.
4. If $x \neq 0$, then $(x^{-1})^{-1} = x$.

**Proof**

1. For all $x \in F$ with $x \neq 0$, we have $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. So this means that we can multiply $(xy)$ and $(yz)$ by the multiplicative inverse of $x$

$$xy = yz \implies x^{-1}(xy) = x^{-1}(yz)$$

   Also, fields are associative: $\forall x, y, z \in F,\ x(yz) = (xy)z$. So we can rewrite our expressions. And using the multiplicative inverse property simplify to 1.

$$(x^{-1} \cdot x)y = (x^{-1} \cdot x)z \implies 1 \cdot y = 1 \cdot z$$

   Since $\forall x \in F,\ 1 \cdot x = x$, it follows that $y = z$.

2. For all $x \in F$ with $x \neq 0$, we have $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. So this means that we can multiply $(xy)$ and 1 by the multiplicative inverse of $x$

$$xy = x \implies x^{-1}(xy) = x^{-1}(x)$$

   Also, fields are associative: $\forall x, y, z \in F,\ x(yz) = (xy)z$. So we can rewrite our expressions. And using the multiplicative inverse property simplify to 1.

$$(x^{-1} \cdot x)y = (x^{-1} \cdot x) \implies 1 \cdot y = 1$$

   Since $\forall x \in F,\ 1 \cdot x = x$, it follows that $y = 1$.

3. For all $x \in F$ with $x \neq 0$, we have $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. So this means that we can multiply $(xy)$ and 1 by the multiplicative inverse of $x$

$$xy = 1 \implies x^{-1}(xy) = x^{-1}(1)$$

   Also, fields are associative: $\forall x, y, z \in F,\ x(yz) = (xy)z$. So we can rewrite our expressions. And using the multiplicative inverse property simplify to 1.

$$(x^{-1} \cdot x)y = (x^{-1} \cdot 1) \implies 1 \cdot y = x^{-1}$$

4. Given the field axioms that for all $x \in F$ with $x \neq 0$, we have $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. we can take the multiplicative inverse of $\left(x^{-1}\right)^{-1}$, $x^{-1}$ and multiply both sides by it giving

$$\left(x^{-1}\right)^{-1}\left(x^{-1}\right) = x\left(x^{-1}\right)$$

$$\implies 1 = x \cdot x^{-1}$$

   and given the deifntion for multiplicative inverses, since $x \cdot x^{-1} = 1$ then x is an inverse of $x^{-1}$ which was the inverse of $\left(x^{-1}\right)^{-1}$ meaning $x = \left(x^{-1}\right)^{-1}$

## Ex 1.2, Rudin 1.3

**Question**

In this course we have not yet defined $\mathbb{R}$. For this exercise, all you need to know about $\mathbb{R}$ is that it is a field which contains the field $\mathbb{Q}$.
Suppose $r \in \mathbb{Q}$, $r \neq 0$, and $x \in \mathbb{R}$, $x \notin \mathbb{Q}$. Prove that $r + x \notin \mathbb{Q}$ and $rx \notin \mathbb{Q}$.

**Proof**

We know that $\mathbb{Q}$ is a field and $\mathbb{R}$ is a field, for the sake of contradiction, assume that there exists some $k = r + x \in \mathbb{Q}$. $\mathbb{Q}$ is a field with an addition rule, so $\forall x, y \in \mathbb{Q}$ we have some $x + y \in \mathbb{Q}$ but we also have the rule that $\forall x \in Q$ we have $-x + x = 0$ so since $k = r + x$ and $k \in \mathbb{Q}$ we can add the negation of $r$, $-r$ to both sides giving us $-r + k = -r + r + x$ and since both $-r$ and $k$ are in $\mathbb{Q}$ there sum must also be in $\mathbb{Q}$ but due to the negation rule that $\forall x \in \mathbb{Q} \exists -x$ such that $-x + x = 0$ we get $-r + k = x$ which implies that $x \in \mathbb{Q}$ which contradicts the statement that $x \notin \mathbb{Q}$.

for the second part $rx \notin \mathbb{Q}$, let us assume for the sake of contradiction that there exist some $n = r \cdot k \in Q$. Since $\mathbb{Q}$ is a field with a multiplicative rule, $\forall x, y \in \mathbb{Q}$ we have $xy \in \mathbb{Q}$ and $\mathbb{Q}$ also has the multiplicative inverse rule meaning $\forall x \in Q$ we have some $x^{-1}$ such that $x^{-1} \cdot x = 1$. so assuming $n \in Q$ and $n = rx$ we can multiply both sides by $r^{-1}$, since $n$ and $r^{-1}$ are both in meaning their product must also be. So $n \cdot r^{-1} = r^{-1} \cdot r \cdot x$ and using the multiplicative inverse rule $r \cdot r^{-1} = 1$ meaning $r^{-1} \cdot n = x \cdot 1$ and in a field $\forall x \in Q$ we have $1 \cdot x = x$, so this means $n \cdot r^{-1} = x$, which implies that $x \in \mathbb{Q}$ which contradicts the statement that $x \notin \mathbb{Q}$.

## Ex 1.3

**Question**

In this problem you may freely use without proof all the standard facts about arithmetic of rational numbers and integers.

1. Prove that $\mathbb{Q}$ does not contain any $x$ with $x^2 = 3$. (For this part it may be useful to use the fundamental theorem of arithmetic, which you may use without proof.)

2. Let $\mathbb{Q}(\sqrt{3})$ be the set of ordered pairs $(a, b)$ with $a, b \in \mathbb{Q}$. Informally, we think of each pair $(a, b)$ as representing a number "$a + b\sqrt{3}$." We can equip $\mathbb{Q}(\sqrt{3})$ with addition and product laws as follows:

$$(a, b) + (a', b') = (a + a', b + b'), \tag{1}$$
$$(a, b) \cdot (a', b') = (aa' + 3bb', ab' + ba'). \tag{2}$$

   (These rules are motivated by applying the usual rules of arithmetic to sums of the form "$a + b\sqrt{3}$".)

   Show that $\mathbb{Q}(\sqrt{3})$ can be made into a field, with these addition and product laws. (This means saying carefully what are the 0 and 1 elements, what is the negation law, what is the inversion law, and then proving that all the axioms of a field are satisfied. This will probably be the lengthiest part of your writeup.)

3. In solving part (2), did you use the result of part (1)? If so, where?

4. $\mathbb{Q}(\sqrt{3})$ contains an element 3, defined as $3 = 1 + 1 + 1$, where 1 is the 1 element you already defined in part (2). What is the element 3? Prove that $\mathbb{Q}(\sqrt{3})$ contains exactly two elements $x$ with $x^2 = 3$.

5. We could similarly consider the set $\mathbb{Z}(\sqrt{3})$, defined as above except that now we require $a, b \in \mathbb{Z}$. Show that $\mathbb{Z}(\sqrt{3})$ cannot be made into a field with the addition and product laws above.

**Proof**

1. For sake of contradiction, assume that $\sqrt{3} \in \mathbb{Q}$. Then we can express

$$\sqrt{3} = \frac{p}{q}$$

with integers $p, q$ such that they share no common factors other then 1. Squaring gives

$$3 = \frac{p^2}{q^2} \quad \Rightarrow \quad 3q^2 = p^2.$$

Hence $p^2$ is a multiple of 3, so $p$ is a multiple of 3 meaning that p can be expressed as multiple of 3, $p = 3k$. Substituting,

$$3q^2 = (3k)^2 \;\Rightarrow\; 3q^2 = 9k^2 \;\Rightarrow\; q^2 = 3k^2.$$

So $q$ is also a multiple of 3, contradicting the statement that they have no common factors other then 1. Therefore $\sqrt{3} \notin \mathbb{Q}$.

2. **Field structure of $\mathbb{Q}(\sqrt{3})$.**

   (a) The zero element is $(0, 0)$ since

$$(a, b) + (0, 0) = (a, b) \quad \text{for all } (a, b).$$

   (b) The additive inverse of $(a, b)$ is $-(a, b) = (-a, -b)$, because based on our defintion for addition in $\mathbb{Q}(\sqrt{3})$

$$(a, b) + (-a, -b) = (-a + a, -b + b) = (0, 0).$$

   (c) The unit element is $(1, 0)$, since

$$(1, 0) \cdot (a, b) = (1 \cdot a + 3 \cdot 0 \cdot b,\ 1 \cdot b + 0 \cdot a) = (a, b)$$

   and $(a, b) \cdot (1, 0) = (a, b)$ for all $(a, b)$.

   (d) multiplicative inverse for $(a, b) \neq (0, 0)$, we multiply by $(a, -b)$ since we need to get $(1, 0)$

$$(a, b) \cdot (a, -b) = (a^2 - 3b^2,\ 0).$$

   If $a^2 - 3b^2 = 0$, then $\frac{a}{b} = \sqrt{3}$, for $b \neq 0$, which is impossible since in part 1 we showed $\sqrt{3}$ is not in the set $\mathbb{Q}$. If $b = 0$, then $a = 0$ would contradict $(a, b) \neq (0, 0)$. So $a^2 - 3b^2 \neq 0$ for every nonzero $(a, b)$, and we can define

$$(a, b)^{-1} = \left( \frac{a}{a^2 - 3b^2},\ \frac{-b}{a^2 - 3b^2} \right).$$

   Then

$$(a, b) \cdot (a, b)^{-1} = (1, 0),$$

   Fields axioms:

   (a) For all $x, y \in \mathbb{Q}(\sqrt{3})$ we have $x + y = y + x$
   let $x = (a, b)$, $y = (c, d)$ with $a, b, c, d \in \mathbb{Q}$. Then

$$x + y = (a + c,\ b + d) = (c + a,\ d + b) = y + x,$$

   using commutativity in $\mathbb{Q}$ for each coordinate.

   (b) For all $x, y, z \in \mathbb{Q}(\sqrt{3})$ we have $(x + y) + z = x + (y + z)$
   Let $x = (a, b)$, $y = (c, d)$, $z = (e, f)$. Then

$$(x + y) + z = (a + c + e,\ b + d + f) = x + (y + z),$$

   by associativity in $\mathbb{Q}$ coordinatewise.

(c) For al $x \in \mathbb{Q}(\sqrt{3})$ we have $0 + x = x$
With $0 = (0,0)$ and $x = (a,b)$,

$$0 + x = (0 + a,\ 0 + b) = (a,b) = x.$$

(d) For all $x \in \mathbb{Q}(\sqrt{3})$ we have $-x + x = 0$
For $x = (a,b)$ we have $-x = (-a,-b)$, so

$$(-x) + x = (-a + a,\ -b + b) = (0,0) = 0.$$

(e) For all $x, y \in \mathbb{Q}(\sqrt{3})$ we have $xy = yx$
With $x = (a,b)$, $y = (c,d)$,

$$xy = (ac + 3bd,\ ad + bc) = (ca + 3db,\ cb + da) = yx,$$

using commutativity in $\mathbb{Q}$.

(f) For all $x, y, z \in \mathbb{Q}(\sqrt{3})$ we have $(xy)z = x(yz)$
Let $x = (a,b)$, $y = (c,d)$, $z = (e,f)$.

$$(xy)z = \big(ac + 3bd,\ ad + bc\big)(e,f) = \big(ace + 3bde + 3adf + 3bcf,\ acf + ade + bce + 3bdf\big),$$

and

$$x(yz) = (a,b)\big(ce + 3df,\ cf + de\big) = \big(ace + 3adf + 3bcf + 3bde,\ acf + ade + bce + 3bdf\big),$$

(g) For all $x \in \mathbb{Q}(\sqrt{3})$ we have $1\ 1 \cdot x = x$
With $1 = (1,0)$ and $x = (a,b)$,

$$1 \cdot x = (1,0)(a,b) = (1 \cdot a + 3 \cdot 0 \cdot b,\ 1 \cdot b + 0 \cdot a) = (a,b) = x.$$

(h) For all $x \in \mathbb{Q}(\sqrt{3})$ with $x \neq 0$ we have $x \cdot x^{-1} = 1$
For $x = (a,b) \neq (0,0)$, we use our defintion of the multiplicative inverse

$$x^{-1} = \left(\frac{a}{a^2 - 3b^2},\ \frac{-b}{a^2 - 3b^2}\right).$$

Since $(a,b)(a,-b) = (a^2 - 3b^2, 0)$ and part (1) implies $a^2 - 3b^2 \neq 0$ for $x \neq 0$,

$$x \cdot x^{-1} = (a,b)\left(\frac{a}{a^2 - 3b^2},\ \frac{-b}{a^2 - 3b^2}\right) = (1,0) = 1.$$

(i) For all $x, y, z \in \mathbb{Q}(\sqrt{3})$ we have $x(yz) = xy + xz$
With $x = (a,b)$, $y = (c,d)$, $z = (e,f)$,

$$x(y + z) = (a,b)(c + e,\ d + f) = \big(a(c + e) + 3b(d + f),\ a(d + f) + b(c + e)\big)$$
$$= (ac + 3bd,\ ad + bc) + (ae + 3bf,\ af + be) = xy + xz.$$

3. I did use part (1). It came up when I was trying to write down the formula for the inverse. To make sure the denominator $a^2 - 3b^2$ isn't zero, I argued that if it were, then $\frac{a}{b} = \sqrt{3}$ (as long as $b \neq 0$). But part (1) told me that can't happen in $\mathbb{Q}$. And if $b = 0$ we'd just be left with $a = 0$, which makes the whole element $(a,b)$ the zero element.

4. The unit element, 1 is $(1,0)$, so 3 is $(3,0)$. Now suppose $(a,b)$ squares to 3:

$$(a,b)^2 = (a^2 + 3b^2,\ 2ab) = (3,0).$$

We see that $2ab = 0$. So either $a = 0$ or $b = 0$. If $a = 0$, then the first coordinate is $3b^2 = 3$, so $b = \pm 1$. If $b = 0$, then we'd need $a^2 = 3$, but that would force $a$ to be $\sqrt{3}$, which is not rational. So that case doesn't work. So the only square roots of 3 in this field are $(0,1)$ and $(0,-1)$.

5. Let $u = (0,1)$. If $\mathbb{Z}(\sqrt{3})$ were a field, then $u$ would have an inverse $(c,d)$ with integers $c, d$. But

$$(0,1) \cdot (c,d) = (3d,\ c).$$

For this to be our unit element we need $3d = 1$ and $c = 0$. That's impossible with $d \in \mathbb{Z}$. So $u$ has no inverse here. Since every nonzero element has to have an inverse in a field, $\mathbb{Z}(\sqrt{3})$ can't be a field.

## Ex 1.4

**Question**

Let $A$ be a nonempty subset of an ordered set $S$. If $\alpha \in S$ and, for all $x \in A$, we have $\alpha \leq x$, then we call $\alpha$ a *lower bound* for $A$. Similarly, if $\beta \in S$ and, for all $x \in A$, we have $x \leq \beta$, then we call $\beta$ an *upper bound* for $A$.
Suppose $\alpha$ is a lower bound of $A$ and $\beta$ is an upper bound of $A$.

1. Prove that $\alpha \leq \beta$.
2. Note that in the statement of the problem we require $A$ to be nonempty. Would the statement $\alpha \leq \beta$ still hold even if we allow $A$ to be empty? Explain why. In solving part (1), did you use the fact that $A$ is nonempty? If so, where did you use it?

**Proof**

1. Let us suppose that $\alpha$ is a lower bound of $A$ and $\beta$ is an upper bound of $A$. $A$ is a subset of $S$ where $S$ is an ordered set, now let us take an arbitrary element $x_1 \in A$ and then by definition $\alpha \leq x_1$ and since $\beta$ is an upper bound, then $x_1 \leq \beta$ then since $A$ is a subset of an ordered set and the relation $\leq$ is transitive, then $\alpha \leq x_1$ and $x_1 \leq \beta$ means $\alpha \leq \beta$

2. I did use the statement that $A$ was non-empty so that I could find an arbitrary $x$ to compare $\alpha$ and $\beta$ so that I could use the rule of transitivity to imply $\alpha \leq \beta$. If $A = \varnothing$, then every $\alpha \in S$ would count as a lower bound and every $\beta \in S$ would count as an upper bound, but they wouldn't necessarily satisfy $\alpha \leq \beta$. For example, in $\mathbb{R}$ with $A = \varnothing$, both $\alpha = 1$ and $\beta = 0$ are bounds, but clearly $1 \not\leq 0$. So the statement fails.