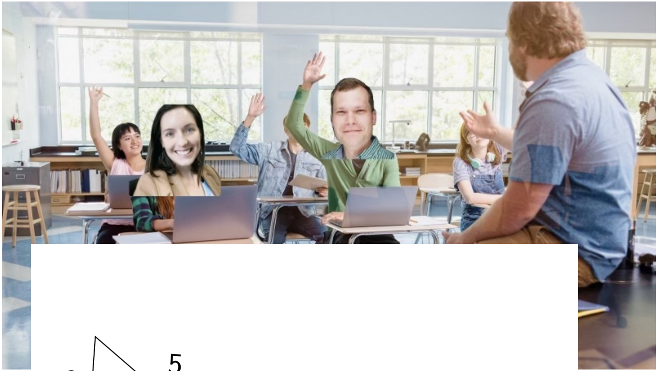
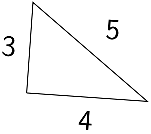
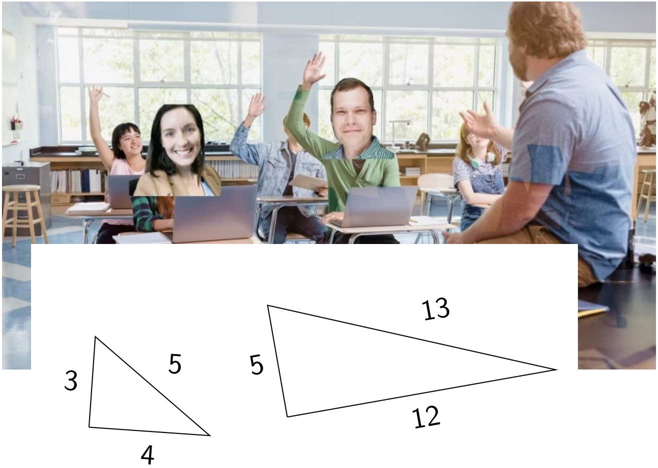
An Introduction to
Algebraic Number Theory

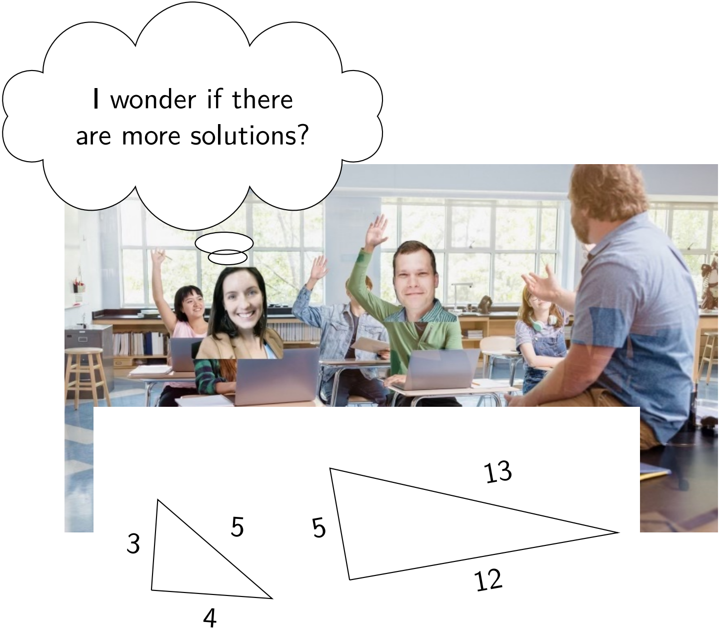
Alistair Pattison

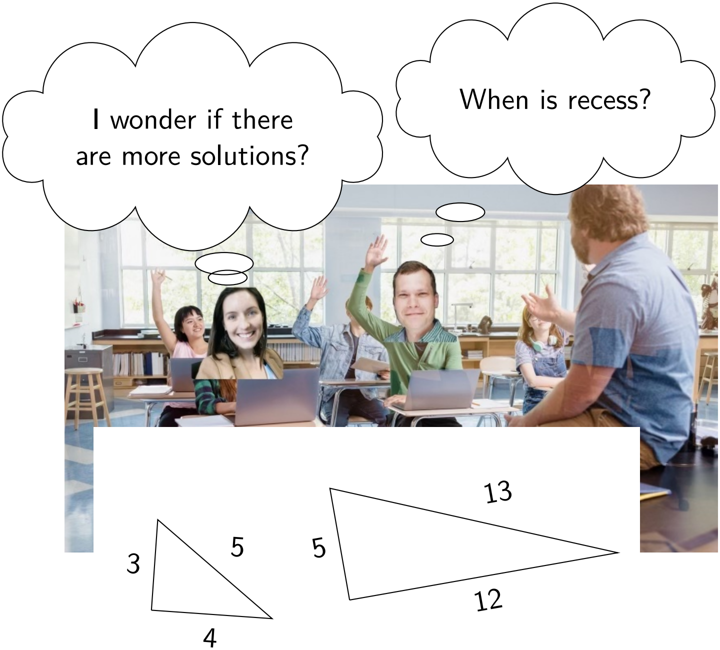
November 2, 2023




5
3
4


3
5
4
13
5
12


I wonder if there
are more solutions?
3
5
4
5
13
12


I wonder if there
are more solutions?
When is recess?
3
5
4
5
13
12

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$z^2 = x^2 + y^2$$

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= \underbrace{(x+iy)}_{\alpha}\underbrace{(x-iy)}_{\beta} \qquad \text{over } \mathbb{Z}[i] \end{aligned}$$

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= \underbrace{(x + iy)}_{\alpha} \underbrace{(x - iy)}_{\beta} \qquad \text{over } \mathbb{Z}[i] \end{aligned}$$

x and y relatively prime $\implies \alpha$ and β relatively prime

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$z^2 = x^2 + y^2 = \underbrace{(x+iy)}_{\alpha}\underbrace{(x-iy)}_{\beta} \qquad \text{over } \mathbb{Z}[i]$$

x and y relatively prime $\implies \alpha$ and β relatively prime

$$z^2 = \alpha\beta \implies \alpha = \gamma^2 \quad \gamma \in \mathbb{Z}[i]$$

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= \underbrace{(x + iy)}_{\alpha} \underbrace{(x - iy)}_{\beta} \qquad \text{over } \mathbb{Z}[i] \end{aligned}$$

$$\alpha = \gamma^2$$

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= \underbrace{(x + iy)}_{\alpha} \underbrace{(x - iy)}_{\beta} \qquad \text{over } \mathbb{Z}[i] \end{aligned}$$

$$\begin{aligned} \alpha &= \gamma^2 \\ &= (a + bi)^2 \end{aligned}$$

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= \underbrace{(x + iy)}_{\alpha}\,\underbrace{(x - iy)}_{\beta} \qquad \text{over } \mathbb{Z}[i] \end{aligned}$$

$$\begin{aligned} \alpha &= \gamma^2 \\ &= (a + bi)^2 \\ &= \underbrace{(a^2 - b^2)}_{x} + \underbrace{2ab}_{y}\, i \end{aligned}$$

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= \underbrace{(x+iy)}_{\alpha}\,\underbrace{(x-iy)}_{\beta} \end{aligned}$$

over $\mathbb{Z}[i]$

$$\begin{aligned} \alpha &= \gamma^2 \\ &= (a+bi)^2 \\ &= \underbrace{(a^2-b^2)}_{x} + \underbrace{2ab}_{y}\, i \end{aligned}$$

$$\begin{aligned} x &= a^2 - b^2 \\ y &= 2ab \\ z &= a^2 + b^2 \end{aligned}$$

Generating Primitive Pythagorean Triples

Goal: find all relatively prime $x, y, z \in \mathbb{Z}$ such that

$$z^2 = x^2 + y^2$$

a	b	
2	1	$3^2 + 4^2 = 5^2$
3	2	$5^2 + 12^2 = 13^2$
4	3	$7^2 + 24^2 = 25^2$
4	2	$12^2 + 16^2 = 20^2$
4	1	$15^2 + 8^2 = 17^2$

Algebraic Number Theory

ALGEBRAIC NUMBER THEORY

Using tools from algebra like rings and field extensions

Algebraic Number Theory

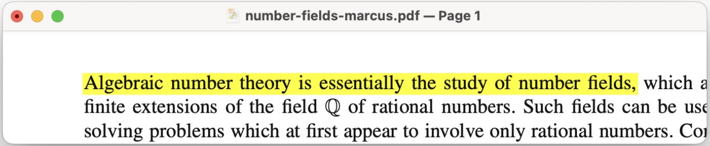
Using tools from algebra like rings and field extensions

Generating insight about the integers and the primes

Algebraic Number Theory

Using tools from algebra like rings and field extensions

Generating insight about the integers and the primes


number-fields-marcus.pdf — Page 1

Algebraic number theory is essentially the study of number fields, which a
finite extensions of the field $\mathbb{Q}$ of rational numbers. Such fields can be use
solving problems which at first appear to involve only rational numbers. Co

Outline

1. MATH 342 in 3:42

Outline

1. MATH 342 in 3:42

2. Number Fields and Number Rings

Outline

1. MATH 342 in 3:42
2. Number Fields and Number Rings
3. The Ideal Class Group

MATH 342 in 3:42

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Commutative Ring)

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Commutative Ring)

"Things like the integers"

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Commutative Ring)

"Things like the integers"

- Addition/subtraction: $a + b, a - b \in R$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Commutative Ring)

"Things like the integers"

- Addition/subtraction: $a + b, a - b \in R$
- Multiplication: $ab = ba \in R$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Commutative Ring)

"Things like the integers"

- Addition/subtraction: $a + b, a - b \in R$
- Multiplication: $ab = ba \in R$
- Distributive property: $a(b + c) = ab + bc$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Commutative Ring)

"Things like the integers"

- Addition/subtraction: $a + b, a - b \in R$
- Multiplication: $ab = ba \in R$
- Distributive property: $a(b + c) = ab + bc$
- *Not* division: $a/b \notin R$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Ideal)

An (additive) subgroup, I, such that $ra \in I$ for all $r \in R$, $a \in I$.

Ring Hierarchy

Rings ⟶ Integral Domains ⟶ Integrally Closed Domains ⟶ Unique Factorization Domains ⟶ Principal Ideal Domains ⟶ Fields

Definition (Ideal)

An (additive) subgroup, I, such that $ra \in I$ for all $r \in R$, $a \in I$.

- **Example**: Even integers ($8 \cdot 7$ is even)

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Ideal)

An (additive) subgroup, I, such that $ra \in I$ for all $r \in R$, $a \in I$.

- **Example**: Even integers ($8 \cdot 7$ is even)
- **Non-example**: Odd integers ($7 \cdot 8$ is not odd)

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Ideal)

An (additive) subgroup, I, such that $ra \in I$ for all $r \in R$, $a \in I$.

- **Example**: Even integers ($8 \cdot 7$ is even)
- **Non-example**: Odd integers ($7 \cdot 8$ is not odd)

Definition (Prime Ideal)

An ideal, P, such that $ab \in P$ implies $a \in P$ or $b \in P$.

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Ideal)

An (additive) subgroup, I, such that $ra \in I$ for all $r \in R$, $a \in I$.

- **Example**: Even integers ($8 \cdot 7$ is even)
- **Non-example**: Odd integers ($7 \cdot 8$ is not odd)

Definition (Prime Ideal)

An ideal, P, such that $ab \in P$ implies $a \in P$ or $b \in P$.

- This is a generalization of Euclid's Lemma

Ring Hierarchy

Rings $\longrightarrow$ **Integral Domains** $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Ring Hierarchy

Rings $\longrightarrow$ **Integral Domains** $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition

A commutative ring is an *integral domain* if $ab = 0$ implies $a = 0$ or $b = 0$. (No zero divisors.)

Ring Hierarchy

Rings $\longrightarrow$ **Integral Domains** $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition

A commutative ring is an *integral domain* if $ab = 0$ implies $a = 0$ or $b = 0$. (No zero divisors.)

- **Example**: $\mathbb{Z}$, $\mathbb{Z}[i]$

Ring Hierarchy

Rings $\longrightarrow$ **Integral Domains** $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition

A commutative ring is an *integral domain* if $ab = 0$ implies $a = 0$ or $b = 0$. (No zero divisors.)

- **Example**: $\mathbb{Z}$, $\mathbb{Z}[i]$
- **Non-example**: in $\mathbb{Z}/8\mathbb{Z}$, we have $4 \cdot 2 = 0$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ **Integrally Closed Domains** $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Ring Hierarchy

$$\boxed{\text{Rings}} \longrightarrow \boxed{\text{Integral Domains}} \longrightarrow \boxed{\textbf{Integrally Closed Domains}} \longrightarrow \boxed{\text{Unique Factorization Domains}} \longrightarrow \boxed{\text{Principal Ideal Domains}} \longrightarrow \boxed{\text{Fields}}$$

Definition (Integrally Closed Domain)

A ring R is *integrally closed* if for all $\alpha/\beta \in \operatorname{Frac} R$ that are integral over R, then $\beta \mid \alpha$, i.e., $\alpha/\beta \in R$.

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ **Integrally Closed Domains** $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Integrally Closed Domain)

A ring R is *integrally closed* if for all $\alpha/\beta \in \operatorname{Frac} R$ that are integral over R, then $\beta \mid \alpha$, i.e., $\alpha/\beta \in R$.

- $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$; $\operatorname{Frac} \mathbb{C}[x]$ is the field of rational functions, $\mathbb{C}(x)$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ **Integrally Closed Domains** $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Integrally Closed Domain)

A ring R is *integrally closed* if for all $\alpha/\beta \in \operatorname{Frac} R$ that are integral over R, then $\beta \mid \alpha$, i.e., $\alpha/\beta \in R$.

- $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$; $\operatorname{Frac} \mathbb{C}[x]$ is the field of rational functions, $\mathbb{C}(x)$
- If $f(p/q) = 0$ with monic $f \in \mathbb{Z}[x]$, then $q \mid p$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ **Integrally Closed Domains** $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (Integrally Closed Domain)

A ring R is *integrally closed* if for all $\alpha/\beta \in \operatorname{Frac} R$ that are integral over R, then $\beta \mid \alpha$, i.e., $\alpha/\beta \in R$.

- $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$; $\operatorname{Frac} \mathbb{C}[x]$ is the field of rational functions, $\mathbb{C}(x)$
- If $f(p/q) = 0$ with monic $f \in \mathbb{Z}[x]$, then $q \mid p$
- **Example**: $\mathbb{Z}$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ **Unique Factorization Domains** $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ **Unique Factorization Domains** $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (UFD)

A commutative ring R is a *unique factorization domain* if every element factors uniquely into irreducible elements.

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ **Unique Factorization Domains** $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ Fields

Definition (UFD)

A commutative ring R is a *unique factorization domain* if every element factors uniquely into irreducible elements.

- **Example**: $\mathbb{Z}$

Ring Hierarchy

$$\boxed{\text{Rings}} \longrightarrow \boxed{\begin{array}{c}\text{Integral}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Integrally}\\\text{Closed}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\textbf{Unique}\\\textbf{Factorization}\\\textbf{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Principal}\\\text{Ideal}\\\text{Domains}\end{array}} \longrightarrow \boxed{\text{Fields}}$$

Definition (UFD)

A commutative ring R is a *unique factorization domain* if every element factors uniquely into irreducible elements.

- **Example**: $\mathbb{Z}$
- **Non-example**: $\mathbb{Z}[i\sqrt{5}]$:

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

Ring Hierarchy

Rings ⟶ Integral Domains ⟶ Integrally Closed Domains ⟶ Unique Factorization Domains ⟶ **Principal Ideal Domains** ⟶ Fields

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ **Principal Ideal Domains** $\longrightarrow$ Fields

Definition (PID)

A commutative ring R is a *principal ideal domain* if every ideal is generated by a single element.

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ **Principal Ideal Domains** $\longrightarrow$ Fields

Definition (PID)

A commutative ring R is a *principal ideal domain* if every ideal is generated by a single element.

- **Example**: $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{Z}[i]$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ **Principal Ideal Domains** $\longrightarrow$ Fields

Definition (PID)

A commutative ring R is a *principal ideal domain* if every ideal is generated by a single element.

- **Example**: $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{Z}[i]$
- **Non-example**: $\mathbb{Z}[x]$ because of $(2, x)$

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ **Fields**

Ring Hierarchy

Rings $\longrightarrow$ Integral Domains $\longrightarrow$ Integrally Closed Domains $\longrightarrow$ Unique Factorization Domains $\longrightarrow$ Principal Ideal Domains $\longrightarrow$ **Fields**

Definition (Field)

"Things like the rationals" or "rings where you can divide".

Ring Hierarchy

$$\boxed{\text{Rings}} \longrightarrow \boxed{\begin{array}{c}\text{Integral}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Integrally}\\\text{Closed}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Unique}\\\text{Factorization}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Principal}\\\text{Ideal}\\\text{Domains}\end{array}} \longrightarrow \boxed{\textbf{Fields}}$$

Definition (Field)

"Things like the rationals" or "rings where you can divide".

- **Example**: $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$

Ring Hierarchy

$$\boxed{\text{Rings}} \longrightarrow \boxed{\begin{array}{c}\text{Integral}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Integrally}\\\text{Closed}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Unique}\\\text{Factorization}\\\text{Domains}\end{array}} \longrightarrow \boxed{\begin{array}{c}\text{Principal}\\\text{Ideal}\\\text{Domains}\end{array}} \longrightarrow \boxed{\textbf{Fields}}$$

Definition (Field)

"Things like the rationals" or "rings where you can divide".

- **Example**: $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$
- **Non-example**: $\mathbb{Z}$, $\mathbb{Z}[x]$

$$f(x) = x^2 + 5$$

Field Extensions

$$f(x) = x^2 + 5$$

- Over $\mathbb{Q}$, f is irreducible

Field Extensions

$$\begin{aligned} f(x) &= x^2 + 5 \\ &= (x - i\sqrt{5})(x + i\sqrt{5}) \end{aligned}$$

- Over $\mathbb{Q}$, f is irreducible
- Over $\mathbb{C}$, f factors

$$e \qquad \pi \qquad \sqrt{7} \qquad 1 + 2\sqrt{17}$$

Field Extensions

$$f(x) = x^2 + 5$$
$$= (x - i\sqrt{5})(x + i\sqrt{5})$$

- Over $\mathbb{Q}$, f is irreducible
- Over $\mathbb{C}$, f factors

$$e \qquad \pi \qquad \sqrt{7} \qquad 1 + 2\sqrt{17}$$

- But f is equally happy living in

$$\mathbb{Q}(i\sqrt{5}) = \{a + bi\sqrt{5} : a, b \in \mathbb{Q}\}$$

Number Fields and Number Rings

Number Fields

Definition (Number Field)

A *number field* $K \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$.

Number Fields

Definition (Number Field)

A *number field* $K \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$.

Theorem

Any number field can be written in the form

$$K = \mathbb{Q}[\alpha] = \mathrm{span}_{\mathbb{Q}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

where n is the degree of the minimal polynomial of α.

Number Fields

Definition (Number Field)

A *number field* $K \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$.

Theorem

Any number field can be written in the form

$$K = \mathbb{Q}[\alpha] = \mathrm{span}_{\mathbb{Q}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

where n is the degree of the minimal polynomial of α.

Examples

- $\mathbb{Q}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Q}\}$

Number Fields

Definition (Number Field)

A *number field* $K \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$.

Theorem

Any number field can be written in the form

$$K = \mathbb{Q}[\alpha] = \operatorname{span}_{\mathbb{Q}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

where n is the degree of the minimal polynomial of α.

Examples

- $\mathbb{Q}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Q}\}$
- $\mathbb{Q}[\omega]$, $\omega = e^{2\pi i/p}$ (cyclotomic fields)

Number Fields

Definition (Number Field)

A *number field* $K \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$.

Theorem

Any number field can be written in the form

$$K = \mathbb{Q}[\alpha] = \mathrm{span}_{\mathbb{Q}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

where n is the degree of the minimal polynomial of α.

Examples

- $\mathbb{Q}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Q}\}$
- $\mathbb{Q}[\omega]$, $\omega = e^{2\pi i/p}$ (cyclotomic fields)
- $\mathbb{Q}[\sqrt{m}]$, m squarefree (quadratic fields)

Number Fields

Definition (Number Field)

A *number field* $K \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$.

Theorem

Any number field can be written in the form

$$K = \mathbb{Q}[\alpha] = \mathrm{span}_{\mathbb{Q}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

where n is the degree of the minimal polynomial of α.

Examples

- $\mathbb{Q}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Q}\}$
- $\mathbb{Q}[\omega]$, $\omega = e^{2\pi i/p}$ (cyclotomic fields)
- $\mathbb{Q}[\sqrt{m}]$, m squarefree (quadratic fields)

Number Fields

Definition (Number Field)

A *number field* $K \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$.

Theorem

Any number field can be written in the form

$$K = \mathbb{Q}[\alpha] = \mathrm{span}_{\mathbb{Q}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

where n is the degree of the minimal polynomial of α.

Examples

- $\mathbb{Q}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Q}\}$
- $\mathbb{Q}[\omega]$, $\omega = e^{2\pi i/p}$ (cyclotomic fields)
- $\mathbb{Q}[\sqrt{m}]$, m squarefree (quadratic fields)

Non-examples

- $\mathbb{Q}[\pi]$ because π is transcendental

Definition (Algebraic Integer)

An *algebraic integer* is a complex number α that is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

Number Rings

Definition (Algebraic Integer)

An *algebraic integer* is a complex number α that is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

We use $\mathbb{A}$ to denote the set of all algebraic integers.

Definition (Algebraic Integer)

An *algebraic integer* is a complex number α that is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

We use $\mathbb{A}$ to denote the set of all algebraic integers.

- Any integer k is an algebraic integer because of $f(x) = x - k$

Number Rings

Definition (Algebraic Integer)

An *algebraic integer* is a complex number α that is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

We use $\mathbb{A}$ to denote the set of all algebraic integers.

- Any integer k is an algebraic integer because of $f(x) = x - k$
- $i\sqrt{5} \in \mathbb{A}$ because of $f(x) = x^2 + 5$

Definition (Algebraic Integer)

An *algebraic integer* is a complex number α that is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

We use $\mathbb{A}$ to denote the set of all algebraic integers.

- Any integer k is an algebraic integer because of $f(x) = x - k$
- $i\sqrt{5} \in \mathbb{A}$ because of $f(x) = x^2 + 5$
- $2 + \sqrt[3]{17} \in \mathbb{A}$ because of $f(x) = x^3 - 6x^2 + 12x - 25$

Number Rings

Definition (Algebraic Integer)

An *algebraic integer* is a complex number α that is the root of some monic polynomial $f \in \mathbb{Z}[x]$.

We use $\mathbb{A}$ to denote the set of all algebraic integers.

- Any integer k is an algebraic integer because of $f(x) = x - k$
- $i\sqrt{5} \in \mathbb{A}$ because of $f(x) = x^2 + 5$
- $2 + \sqrt[3]{17} \in \mathbb{A}$ because of $f(x) = x^3 - 6x^2 + 12x - 25$
- $\mathbb{A}$ is a subring of $\mathbb{C}$

Number Rings

Definition (Number Ring)

The *number ring* of a number field $K = \mathbb{Q}(\alpha)$ is the set

$$\mathcal{O}_K = \mathbb{A} \cap K.$$

Number Rings

Definition (Number Ring)

The *number ring* of a number field $K = \mathbb{Q}(\alpha)$ is the set

$$\mathcal{O}_K = \mathbb{A} \cap K.$$

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$

Number Rings

Definition (Number Ring)

The *number ring* of a number field $K = \mathbb{Q}(\alpha)$ is the set

$$\mathcal{O}_K = \mathbb{A} \cap K.$$

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$
- $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$

Number Rings

Definition (Number Ring)

The *number ring* of a number field $K = \mathbb{Q}(\alpha)$ is the set

$$\mathcal{O}_K = \mathbb{A} \cap K.$$

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$
- $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$
- $\mathcal{O}_{\mathbb{Q}[\zeta]} = \mathbb{Z}[\zeta]$ for primitive roots ζ

Number Rings

Definition (Number Ring)

The *number ring* of a number field $K = \mathbb{Q}(\alpha)$ is the set

$$\mathcal{O}_K = \mathbb{A} \cap K.$$

- $\mathcal{O}_{\mathbb{Q}} = \mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$
- $\mathcal{O}_{\mathbb{Q}[i]} = \mathbb{Z}[i]$
- $\mathcal{O}_{\mathbb{Q}[\zeta]} = \mathbb{Z}[\zeta]$ for primitive roots ζ
- $\mathcal{O}_{\mathbb{Q}[\sqrt{5}]} = \mathbb{Z}[1, \frac{1}{2} + \frac{1}{2}\sqrt{5}]$

Dedekind Domains

Theorem

Number rings are Dedekind domains.

Definition (Dedekind domain)

A *Dedekind domain* is an integrally closed domain R such that

1. every ideal is finitely generated and
2. every nonzero prime ideal is maximal.

Dedekind Domains

Factoring ideals

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

- Allows replacing unique factorization of elements with unique factorization of ideals.

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

- Allows replacing unique factorization of elements with unique factorization of ideals.
- In $R = \mathbb{Z}[i\sqrt{5}]$,

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned}$$

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

- Allows replacing unique factorization of elements with unique factorization of ideals.
- In $R = \mathbb{Z}[i\sqrt{5}]$,

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned}$$

$$(6) = (2, 1 + i\sqrt{5})^2 \, (3, 1 + i\sqrt{5}) \, (3, 1 - i\sqrt{5})$$

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

- Allows replacing unique factorization of elements with unique factorization of ideals.
- In $R = \mathbb{Z}[i\sqrt{5}]$,

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned}$$

$$(6) = (2, 1 + i\sqrt{5})^2\,(3, 1 + i\sqrt{5})\,(3, 1 - i\sqrt{5})$$

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

- Allows replacing unique factorization of elements with unique factorization of ideals.
- In $R = \mathbb{Z}[i\sqrt{5}]$,

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned}$$

$$(6) = (2, 1 + i\sqrt{5})^2 \, (3, 1 + i\sqrt{5}) \, (3, 1 - i\sqrt{5})$$

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

- Allows replacing unique factorization of elements with unique factorization of ideals.
- In $R = \mathbb{Z}[i\sqrt{5}]$,

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned}$$

$$(6) = (2, 1 + i\sqrt{5})^2 \, (3, 1 + i\sqrt{5}) \, (3, 1 - i\sqrt{5})$$

Theorem

Every ideal of a Dedekind domain R uniquely factors into prime ideals.

- Allows replacing unique factorization of elements with unique factorization of ideals.
- In $R = \mathbb{Z}[i\sqrt{5}]$,

$$\begin{aligned} 6 &= 2 \cdot 3 \\ &= (1 + i\sqrt{5})(1 - i\sqrt{5}) \end{aligned}$$

$$(6) = (2, 1 + i\sqrt{5})^2 \, (3, 1 + i\sqrt{5}) \, (3, 1 - i\sqrt{5})$$

Theorem

A Dedekind domain has unique factorization iff it's a PID.

Dedekind Domains

In the class hierarchy

Theorem

A Dedekind domain has unique factorization iff it's a PID.

$$\begin{tikzcd}
 & \text{Integrally Closed Domains} \arrow[dl] \arrow[dr] & \\
\text{UFDs} \arrow[dr] & & \text{Dedekind Domains} \arrow[dl] \\
 & \text{PIDs} &
\end{tikzcd}$$

Dedekind Domains

In the class hierarchy

Theorem

A Dedekind domain has unique factorization iff it's a PID.

$$\begin{tikzcd}[column sep=tiny] & \text{Integrally Closed Domains} \arrow[dl] \arrow[dr] & \\ \text{UFDs} \arrow[dr] & & \text{Dedekind Domains} \arrow[dl] \\ & \text{PIDs} & \end{tikzcd}$$

- **DD, not UFD**
  $\mathbb{Z}[i\sqrt{5}]$

Dedekind Domains

In the class hierarchy

Theorem

A Dedekind domain has unique factorization iff it's a PID.

$$\begin{tikzcd}[column sep=small]
& \text{Integrally Closed Domains} \arrow[dl] \arrow[dr] & \\
\text{UFDs} \arrow[dr] & & \text{Dedekind Domains} \arrow[dl] \\
& \text{PIDs} &
\end{tikzcd}$$

- **DD, not UFD**
  $\mathbb{Z}[i\sqrt{5}]$
- **UFD, not DD**
  $\mathbb{R}[x_1, x_2, \ldots]$, $\mathbb{Q}[x, y]$

The Ideal Class Group

The Ideal Class Group

Definition (Ideal Class Group)

Let $K = \mathbb{Q}[\alpha]$ be a number field. The *class group* of K is the set of ideals of $\mathcal{O}_K$, modulo the equivilence relation

$$I \sim J \text{ iff } \alpha I = \beta J \text{ for some nonzero } \alpha, \beta \in R.$$

THE IDEAL CLASS GROUP

DEFINITION (IDEAL CLASS GROUP)

Let $K = \mathbb{Q}[\alpha]$ be a number field. The *class group* of K is the set of ideals of $\mathcal{O}_K$, modulo the equivilence relation

$$I \sim J \text{ iff } \alpha I = \beta J \text{ for some nonzero } \alpha, \beta \in R.$$

- Back to $K = \mathbb{Q}[i\sqrt{5}]$ and $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$

$$(2) \sim (3) \qquad\qquad 2(3) = (6) = 3(2)$$

The Ideal Class Group

Definition (Ideal Class Group)

Let $K = \mathbb{Q}[\alpha]$ be a number field. The *class group* of K is the set of ideals of $\mathcal{O}_K$, modulo the equivilence relation

$$I \sim J \text{ iff } \alpha I = \beta J \text{ for some nonzero } \alpha, \beta \in R.$$

- Back to $K = \mathbb{Q}[i\sqrt{5}]$ and $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$

$$(2) \sim (3) \qquad 2(3) = (6) = 3(2)$$

$$(2) \not\sim (2, 1 + i\sqrt{5})$$

The Ideal Class Group

Definition (Ideal Class Group)

Let $K = \mathbb{Q}[\alpha]$ be a number field. The *class group* of K is the set of ideals of $\mathcal{O}_K$, modulo the equivilence relation

$$I \sim J \text{ iff } \alpha I = \beta J \text{ for some nonzero } \alpha, \beta \in R.$$

- Back to $K = \mathbb{Q}[i\sqrt{5}]$ and $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$

$$(2) \sim (3) \qquad\qquad 2(3) = (6) = 3(2)$$

$$(2) \not\sim (2, 1 + i\sqrt{5})$$

- That's it.

The Ideal Class Group

Definition (Ideal Class Group)

Let $K = \mathbb{Q}[\alpha]$ be a number field. The *class group* of K is the set of ideals of $\mathcal{O}_K$, modulo the equivilence relation

$$I \sim J \text{ iff } \alpha I = \beta J \text{ for some nonzero } \alpha, \beta \in R.$$

- Back to $K = \mathbb{Q}[i\sqrt{5}]$ and $\mathcal{O}_K = \mathbb{Z}[i\sqrt{5}]$

$$(2) \sim (3) \qquad 2(3) = (6) = 3(2)$$

$$(2) \not\sim (2, 1 + i\sqrt{5})$$

- That's it.
- The class group of $\mathbb{Q}[i\sqrt{5}]$ is $\mathbb{Z}/2\mathbb{Z}$.

The Class Number

Definition (Class Number)

The class number of a number field $K = \mathbb{Q}[\alpha]$ is the size of its ideal class group.

The Class Number

Definition (Class Number)

The class number of a number field $K = \mathbb{Q}[\alpha]$ is the size of its ideal class group.

- $\mathbb{Q}[i\sqrt{5}]$ has class number 2

The Class Number

Definition (Class Number)

The class number of a number field $K = \mathbb{Q}[\alpha]$ is the size of its ideal class group.

- $\mathbb{Q}[i\sqrt{5}]$ has class number 2
- K has class number 1 iff $\mathcal{O}_K$ is a UFD

The Class Number

Definition (Class Number)

The class number of a number field $K = \mathbb{Q}[\alpha]$ is the size of its ideal class group.

- $\mathbb{Q}[i\sqrt{5}]$ has class number 2
- K has class number 1 iff $\mathcal{O}_K$ is a UFD
- Measures "how far away" $\mathcal{O}_K$ is from achieving unique factorization

The Class Number

Definition (Class Number)

The class number of a number field $K = \mathbb{Q}[\alpha]$ is the size of its ideal class group.

- $\mathbb{Q}[i\sqrt{5}]$ has class number 2
- K has class number 1 iff $\mathcal{O}_K$ is a UFD
- Measures "how far away" $\mathcal{O}_K$ is from achieving unique factorization

The Class Number

Definition (Class Number)

The class number of a number field $K = \mathbb{Q}[\alpha]$ is the size of its ideal class group.

- $\mathbb{Q}[i\sqrt{5}]$ has class number 2
- K has class number 1 iff $\mathcal{O}_K$ is a UFD
- Measures "how far away" $\mathcal{O}_K$ is from achieving unique factorization

Theorem

Class numbers are always finite.

Thank you!

Thank you!

Slides/paper