Definition: The Field of Quotients of an Integral Domain

The **field of quotients** (or field of fractions) of an integral domain D is the smallest field that contains D as a subring. It consists of elements of the form $\frac{a}{b}$, where $a, b \in D$ and $b \neq 0$, subject to the equivalence relation:

$$\frac{a}{b} = \frac{c}{d} \quad \text{if and only if} \quad ad = bc.$$

The field of quotients allows division by any nonzero element of D, making it a field.

Construction

Let D be an integral domain. Define:

$$F = \left\{ \frac{a}{b} \mid a, b \in D,\, b \neq 0 \right\}.$$

Addition and multiplication are defined as:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

One can verify that F satisfies the field axioms and contains D as a subring (identifying each $a \in D$ with $\frac{a}{1}$).

Non-Trivial Examples

1. **Rational Numbers**:
   - Let $D = \mathbb{Z}$, the ring of integers.
   - The field of quotients of $\mathbb{Z}$ is $\mathbb{Q}$, the field of rational numbers, where each fraction $\frac{a}{b}$ (with $a, b \in \mathbb{Z}$, $b \neq 0$) corresponds to a rational number.
2. **Rational Function Field**:
   - Let $D = k[x]$, the ring of polynomials over a field k.
   - The field of quotients is $k(x)$, the field of rational functions, consisting of fractions of polynomials $\frac{f(x)}{g(x)}$ with $f(x), g(x) \in k[x]$ and $g(x) \neq 0$.
3. **Gaussian Rational Numbers**:
   - Let $D = \mathbb{Z}[i]$, the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.
   - The field of quotients is $\mathbb{Q}(i)$, the field of Gaussian rational numbers, which consists of all numbers of the form $\frac{a+bi}{c+di}$ (where $a, b, c, d \in \mathbb{Z}$ and $c + di \neq 0$).
4. **p-adic Valuation Domains**:
   - Let $D = \mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at a prime p, which consists of fractions $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and b is not divisible by p.
   - The field of quotients is $\mathbb{Q}$, since every rational number can be expressed as a fraction with denominator coprime to p.

Let L be a field and D a subring of L that contains the unity. The ring D is an integral domain since it has no zero divisors.

Yes, that's correct! Let's break it down step by step to understand why D is an integral domain.

1. **Field L:**
   - A field L is a commutative ring with unity (1) where every non-zero element has a multiplicative inverse. This means that for any $a \in L$ with $a \neq 0$, there exists an element $a^{-1} \in L$ such that $a \cdot a^{-1} = 1$.
2. **Subring D:**
   - A subring D of L is a subset of L that is itself a ring under the operations of addition and multiplication defined in L. Since D is a subring of L, it inherits the addition and multiplication operations from L.
3. **Unity in D:**
   - The unity (1) of L is contained in D. This means that $1 \in D$, and for any $d \in D$, $1 \cdot d = d \cdot 1 = d$.
4. **No Zero Divisors:**
   - Since L is a field, it has no zero divisors. That is, if $a \cdot b = 0$ in L, then either $a = 0$ or $b = 0$. Because D is a subring of L, this property is inherited by D. Therefore, D also has no zero divisors.
5. **Integral Domain:**
   - An integral domain is a commutative ring with unity that has no zero divisors. Since D is a subring of L containing the unity and has no zero divisors, D satisfies the definition of an integral domain.

In summary, D is an integral domain because it is a commutative ring with unity (inherited from L) and it has no zero divisors (also inherited from L).

Example 1: $\mathbb{Z}$ as a subring of $\mathbb{Q}$

- **Field L:** $\mathbb{Q}$, the field of rational numbers.
- **Subring D:** $\mathbb{Z}$, the ring of integers.
- **Explanation:**
  - $\mathbb{Z}$ is a subring of $\mathbb{Q}$ because it is closed under addition, subtraction, and multiplication, and it contains the unity 1.
  - $\mathbb{Z}$ has no zero divisors: if $a \cdot b = 0$ in $\mathbb{Z}$, then either $a = 0$ or $b = 0$.
  - Thus, $\mathbb{Z}$ is an integral domain.

Example 2: $\mathbb{Z}[i]$ as a subring of $\mathbb{C}$

- **Field L:** $\mathbb{C}$, the field of complex numbers.
- **Subring D:** $\mathbb{Z}[i]$, the ring of Gaussian integers (complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$).
- **Explanation:**
  - $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$ because it is closed under addition, subtraction, and multiplication, and it contains the unity $1 = 1 + 0i$.
  - $\mathbb{Z}[i]$ has no zero divisors: if $(a + bi)(c + di) = 0$ in $\mathbb{Z}[i]$, then either $a + bi = 0$ or $c + di = 0$.
  - Thus, $\mathbb{Z}[i]$ is an integral domain.

Example 3: $\mathbb{Z}[\sqrt{2}]$ as a subring of $\mathbb{R}$

- **Field L:** $\mathbb{R}$, the field of real numbers.
- **Subring D:** $\mathbb{Z}[\sqrt{2}]$, the ring of numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Z}$.
- **Explanation:**
  - $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$ because it is closed under addition, subtraction, and multiplication, and it contains the unity $1 = 1 + 0\sqrt{2}$.
  - $\mathbb{Z}[\sqrt{2}]$ has no zero divisors: if $(a + b\sqrt{2})(c + d\sqrt{2}) = 0$ in $\mathbb{Z}[\sqrt{2}]$, then either $a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$.
  - Thus, $\mathbb{Z}[\sqrt{2}]$ is an integral domain.

Example 4: Polynomial ring $\mathbb{Q}[x]$ as a subring of $\mathbb{Q}(x)$

- **Field L:** $\mathbb{Q}(x)$, the field of rational functions (ratios of polynomials with coefficients in $\mathbb{Q}$).
- **Subring D:** $\mathbb{Q}[x]$, the ring of polynomials with coefficients in $\mathbb{Q}$.
- **Explanation:**
  - $\mathbb{Q}[x]$ is a subring of $\mathbb{Q}(x)$ because it is closed under addition, subtraction, and multiplication, and it contains the unity 1 (the constant polynomial).
  - $\mathbb{Q}[x]$ has no zero divisors: if $f(x) \cdot g(x) = 0$ in $\mathbb{Q}[x]$, then either $f(x) = 0$ or $g(x) = 0$.
  - Thus, $\mathbb{Q}[x]$ is an integral domain.

Section 21: The Field of Quotients of an Integral Domain

Example 5: $\mathbb{Z}_p$ as a subring of itself (for prime p)

- **Field L:** $\mathbb{Z}_p$, the field of integers modulo a prime p.
- **Subring D:** $\mathbb{Z}_p$, which is trivially a subring of itself.
- **Explanation:**
  - $\mathbb{Z}_p$ is a field, so it has no zero divisors: if $a \cdot b = 0$ in $\mathbb{Z}_p$, then either $a = 0$ or $b = 0$.
  - Thus, $\mathbb{Z}_p$ is an integral domain.

Example 6: $\mathbb{Z}[\sqrt{-5}]$ as a subring of $\mathbb{C}$

- **Field L:** $\mathbb{C}$, the field of complex numbers.
- **Subring D:** $\mathbb{Z}[\sqrt{-5}]$, the ring of numbers of the form $a + b\sqrt{-5}$, where $a, b \in \mathbb{Z}$.
- **Explanation:**
  - $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$ because it is closed under addition, subtraction, and multiplication, and it contains the unity $1 = 1 + 0\sqrt{-5}$.
  - $\mathbb{Z}[\sqrt{-5}]$ has no zero divisors: if $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 0$ in $\mathbb{Z}[\sqrt{-5}]$, then either $a + b\sqrt{-5} = 0$ or $c + d\sqrt{-5} = 0$.
  - Thus, $\mathbb{Z}[\sqrt{-5}]$ is an integral domain.

Key Observations:

1. In each case, D is a subring of a field L, and D contains the unity of L.
2. Since L has no zero divisors, D inherits this property and is therefore an integral domain.
3. These examples demonstrate how integral domains arise naturally as subrings of fields.

To show that $F = \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$ is a field, we need to verify that F satisfies all the field axioms. Specifically, we need to show that:

1. F is closed under addition and multiplication.
2. Addition and multiplication are associative and commutative.
3. There exist additive and multiplicative identities in F.
4. Every element in F has an additive inverse.
5. Every non-zero element in F has a multiplicative inverse.
6. Multiplication distributes over addition.

Let's go through each of these properties step by step.

---

1. Closure under addition and multiplication

- **Addition:** Let $a = r_1 + s_1\sqrt{2}$ and $b = r_2 + s_2\sqrt{2}$ be two elements of F. Then:

$$a + b = (r_1 + r_2) + (s_1 + s_2)\sqrt{2}.$$

  Since $r_1 + r_2$ and $s_1 + s_2$ are rational numbers (as $\mathbb{Q}$ is closed under addition), $a + b \in F$.
- **Multiplication:** Let $a = r_1 + s_1\sqrt{2}$ and $b = r_2 + s_2\sqrt{2}$ be two elements of F. Then:

$$a \cdot b = (r_1 + s_1\sqrt{2})(r_2 + s_2\sqrt{2}) = r_1r_2 + r_1s_2\sqrt{2} + r_2s_1\sqrt{2} + s_1s_2(\sqrt{2})^2.$$

  Simplifying, we get:

$$a \cdot b = (r_1r_2 + 2s_1s_2) + (r_1s_2 + r_2s_1)\sqrt{2}.$$

  Since $r_1r_2 + 2s_1s_2$ and $r_1s_2 + r_2s_1$ are rational numbers (as $\mathbb{Q}$ is closed under addition and multiplication), $a \cdot b \in F$.

---

2. Associativity and commutativity

- **Addition and multiplication are associative and commutative** because F is a subset of $\mathbb{R}$, and addition and multiplication in $\mathbb{R}$ are associative and commutative. Thus, these properties are inherited by F.

---

3. Additive and multiplicative identities

- **Additive identity:** The additive identity is $0 = 0 + 0\sqrt{2}$, which is in F.
- **Multiplicative identity:** The multiplicative identity is $1 = 1 + 0\sqrt{2}$, which is in F.

---

4. Additive inverses

- For any $a = r + s\sqrt{2} \in F$, the additive inverse is $-a = -r - s\sqrt{2}$. Since $-r$ and $-s$ are rational numbers, $-a \in F$.

Section 21: The Field of Quotients of an Integral Domain

5. Multiplicative inverses

- For any non-zero $a = r + s\sqrt{2} \in F$, we need to find a^{-1} such that $a \cdot a^{-1} = 1$.
- Let $a^{-1} = \frac{r - s\sqrt{2}}{r^2 - 2s^2}$. This is well-defined because $r^2 - 2s^2 \neq 0$ (since $\sqrt{2}$ is irrational, $r^2 - 2s^2 = 0$ would imply $r = s = 0$, but $a \neq 0$).
- Multiplying a and a^{-1}:

$$(r + s\sqrt{2}) \cdot \left(\frac{r - s\sqrt{2}}{r^2 - 2s^2}\right) = \frac{r^2 - 2s^2}{r^2 - 2s^2} = 1.$$

  Thus, $a^{-1} \in F$.

---

6. Distributivity

- Multiplication distributes over addition in F because F is a subset of $\mathbb{R}$, and distributivity holds in $\mathbb{R}$. Thus, this property is inherited by F.

Conclusion

Since F satisfies all the field axioms, F is a field. It is an example of a **quadratic field**, which is a field extension of $\mathbb{Q}$ obtained by adjoining a square root of a non-square integer (in this case, $\sqrt{2}$).

26.4 Lemma For $[(a,b)]$ and $[(c,d)]$ in F, the equations

$$[(a,b)]+[(c,d)]=[(ad+bc,bd)]$$

and

$$[(a,b)][(c,d)]=[(ac,bd)]$$

give well-defined operations of addition and multiplication on F.

Explanation of Well-Defined Operations in the Field of Quotients

Let D be an integral domain and F be its field of quotients. Elements of F are equivalence classes of pairs $[(a,b)]$ where $a,b\in D$ and $b\neq 0$, subject to the equivalence relation:

$$(a,b)\sim(c,d)\quad\text{if and only if}\quad ad=bc.$$

The operations of **addition** and **multiplication** in F are defined as:

$$[(a,b)]+[(c,d)]=[(ad+bc,bd)]$$

$$[(a,b)]\cdot[(c,d)]=[(ac,bd)].$$

To claim that these operations are **well-defined**, we must show that if we replace (a,b) and (c,d) with equivalent pairs, the results do not change.

Proof of Well-Definedness

Addition

Suppose $(a,b)\sim(a',b')$ and $(c,d)\sim(c',d')$, meaning:

$$ab'=a'b,\quad cd'=c'd.$$

We want to show:

$$(ad+bc,bd)\sim(a'd'+b'c',b'd').$$

Expanding the equivalence condition:

$$(ad+bc)b'd'=(a'd'+b'c')bd.$$

Expanding both sides:

$$adb'd'+bcb'd'=a'd'bd+b'c'bd.$$

Since $ab'=a'b$ and $cd'=c'd$, we substitute:

$$(a'bd)d'+(bcd)b'=(a'bd)d'+(bcd)b'.$$

This confirms the equality, meaning $[(ad+bc,bd)]=[(a'd'+b'c',b'd')]$, so addition is well-defined.

Section 21: The Field of Quotients of an Integral Domain

Multiplication

Similarly, suppose $(a,b)\sim(a',b')$ and $(c,d)\sim(c',d')$, so:

$$ab'=a'b,\quad cd'=c'd.$$

We need to verify:

$$(ac,bd)\sim(a'c',b'd').$$

That is:

$$(ac)b'd'=(a'c')bd.$$

Using $ab'=a'b$ and $cd'=c'd$, we rewrite:

$$(ab'cd')=(a'bc'd).$$

Since multiplication in an integral domain is associative and commutative, both sides are equal, confirming multiplication is well-defined.

Non-Trivial Examples

1. **Field of Rational Numbers $\mathbb{Q}$ as the Field of Quotients of $\mathbb{Z}$**
   - Consider $(2,3)$ representing $\frac{2}{3}$ and $(4,6)$ representing $\frac{4}{6}$.
   - Since $2\cdot 6=4\cdot 3$, we have $(2,3)\sim(4,6)$.
   - Addition:
     $$(2,3)+(1,2)=(2\cdot 2+1\cdot 3,3\cdot 2)=(4+3,6)=(7,6)\Rightarrow\frac{7}{6}.$$
   - Multiplication:
     $$(2,3)\cdot(1,2)=(2\cdot 1,3\cdot 2)=(2,6)\Rightarrow\frac{2}{6}=\frac{1}{3}.$$
2. **Field of Rational Functions $k(x)$ as the Field of Quotients of $k[x]$**
   - Consider polynomials $(x+1,x^2+1)$ and (x^2+2x+1,x^3+x).
   - The operations are performed as:
     $(x+1,x^2+1)+(x^2+2x+1,x^3+x)=((x+1)(x^3+x)+(x^2+2x+1)(x^2+1),(x^2+1)(x^3+x))$.
3. **Gaussian Rational Numbers $\mathbb{Q}(i)$**
   - Consider $(1+i,2)$ and $(3-i,4)$ in $\mathbb{Z}[i]$.
   - Their sum:
     $(1+i,2)+(3-i,4)=((1+i)\cdot 4+(3-i)\cdot 2,2\cdot 4)=(4+4i+6-2i,8)=(10+2i,8)\Rightarrow\dfrac{10+2i}{8}$.
   - Their product:
     $(1+i,2)\cdot(3-i,4)=((1+i)(3-i),2\cdot 4)=(3-i+3i-i^2,8)=(4+2i,8)\Rightarrow\dfrac{4+2i}{8}$.

26.5 Lemma The map $i : D \to F$ given by $i(a) = [(a, 1)]$ is an isomorphism of D with a subring D' of F.

Proof For a and b in D, we have

$$i(a + b) = [(a + b, 1)].$$

Also,

$$i(a) + i(b) = [(a, 1)] + [(b, 1)] = [(a1 + 1b, 1)] = [(a + b, 1)]$$

while

$$i(a)i(b) = [(a, 1)][(b, 1)] = [(ab, 1)],$$

so $i(ab) = i(a)i(b)$.

It remains for us to show only that i is one-to-one. If $i(a) = i(b)$, then

$$[(a, 1)] = [(b, 1)],$$

so $(a, 1) \sim (b, 1)$ giving $a1 = 1b$; that is,

$$a = b.$$

Thus i is an isomorphism of D with $i[D] = D'$, and, of course, D' is then a subdomain of F. ◆

Explanation of the Isomorphism $i : D \to F$

The function $i : D \to F$ defined by

$$i(a) = [(a, 1)]$$

embeds D into F, identifying each element $a \in D$ with the fraction $\frac{a}{1}$. We need to show that i is a **ring homomorphism** and that its image forms a **subring** of F.

1. **Addition Compatibility**:

$$i(a) + i(c) = [(a, 1)] + [(c, 1)] = [(a \cdot 1 + c \cdot 1, 1 \cdot 1)] = [(a + c, 1)] = i(a + c).$$

   This shows that addition is preserved.

2. **Multiplication Compatibility**:

$$i(a) \cdot i(c) = [(a, 1)] \cdot [(c, 1)] = [(a \cdot c, 1 \cdot 1)] = [(ac, 1)] = i(ac).$$

   Thus, multiplication is preserved.

3. **Injectivity**: If $i(a) = i(b)$, then

$$[(a, 1)] = [(b, 1)] \implies a \cdot 1 = b \cdot 1 \implies a = b.$$

   So i is injective.

Since i is an injective ring homomorphism, $i(D)$ is a subring of F, which we call D'. This subring consists of elements $[(a, 1)]$, which are naturally identified with elements of D within F.

Non-Trivial Examples

Example 1: Rational Numbers as the Field of Quotients of $\mathbb{Z}$

Let $D = \mathbb{Z}$, the ring of integers. The field of quotients is $F = \mathbb{Q}$, the field of rational numbers.

- The embedding $i : \mathbb{Z} \to \mathbb{Q}$ is given by:

$$i(n) = [(n, 1)] = \frac{n}{1} = n.$$

  This maps integers to their usual representation in $\mathbb{Q}$.

- Addition and multiplication are preserved:

$$i(2) + i(3) = [(2, 1)] + [(3, 1)] = [(2 \cdot 1 + 3 \cdot 1, 1 \cdot 1)] = [(5, 1)] = i(5).$$

$$i(2) \cdot i(3) = [(2, 1)] \cdot [(3, 1)] = [(2 \cdot 3, 1 \cdot 1)] = [(6, 1)] = i(6).$$

  Hence, $\mathbb{Z}$ is isomorphic to its image D' in $\mathbb{Q}$.

Example 2: Rational Function Field as the Field of Quotients of $k[x]$

Let $D = k[x]$, the ring of polynomials over a field k. The field of quotients is $F = k(x)$, the field of rational functions.

- The embedding $i : k[x] \to k(x)$ is given by:

$$i(f(x)) = [(f(x), 1)] = \frac{f(x)}{1} = f(x).$$

  This maps polynomials to their natural form within the field of rational functions.

- Addition and multiplication are preserved:

$$i(x^2 + 1) + i(x) = [(x^2 + 1, 1)] + [(x, 1)] = [(x^2 + 1 + x, 1)] = [(x^2 + x + 1, 1)] = i(x^2 + x + 1).$$

$$i(x^2 + 1) \cdot i(x) = [(x^2 + 1, 1)] \cdot [(x, 1)] = [(x^3 + x, 1)] = i(x^3 + x).$$

  Hence, $k[x]$ is isomorphic to its image in $k(x)$.

21.5 Theorem Any integral domain D can be enlarged to (or embedded in) a field F such that every element of F can be expressed as a quotient of two elements of D. (Such a field F is a **field of quotients of** D.)

The process of enlarging an integral domain D to a field F such that every element of F can be expressed as a quotient of two elements of D is called the **field of fractions** (or **field of quotients**) of D. This construction generalizes the way the field of rational numbers $\mathbb{Q}$ is constructed from the integers $\mathbb{Z}$.

Here are two **non-trivial examples** of integral domains and their fields of fractions:

Example 1: $\mathbb{Z}$ and $\mathbb{Q}$

- **Integral domain D:** $\mathbb{Z}$, the ring of integers.
- **Field of fractions F:** $\mathbb{Q}$, the field of rational numbers.
- **Explanation:**
  - $\mathbb{Z}$ is an integral domain because it is a commutative ring with unity and has no zero divisors.
  - The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$, where every element of $\mathbb{Q}$ can be written as a quotient $\frac{a}{b}$, with $a, b \in \mathbb{Z}$ and $b \neq 0$.
  - For example, $\frac{3}{4} \in \mathbb{Q}$ is a quotient of the integers 3 and 4.

Example 2: $\mathbb{Q}[x]$ and $\mathbb{Q}(x)$

- **Integral domain D:** $\mathbb{Q}[x]$, the ring of polynomials with coefficients in $\mathbb{Q}$.
- **Field of fractions F:** $\mathbb{Q}(x)$, the field of rational functions with coefficients in $\mathbb{Q}$.
- **Explanation:**
  - $\mathbb{Q}[x]$ is an integral domain because it is a commutative ring with unity and has no zero divisors (the product of two non-zero polynomials is non-zero).
  - The field of fractions of $\mathbb{Q}[x]$ is $\mathbb{Q}(x)$, where every element of $\mathbb{Q}(x)$ can be written as a quotient $\frac{f(x)}{g(x)}$, with $f(x), g(x) \in \mathbb{Q}[x]$ and $g(x) \neq 0$.
  - For example, $\frac{x^2+1}{x-3} \in \mathbb{Q}(x)$ is a quotient of the polynomials $x^2 + 1$ and $x - 3$.

Section 21: The Field of Quotients of an Integral Domain

Example 3: $\mathbb{Z}[i]$ and $\mathbb{Q}(i)$

- **Integral domain D:** $\mathbb{Z}[i]$, the ring of Gaussian integers (complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$).
- **Field of fractions F:** $\mathbb{Q}(i)$, the field of Gaussian rationals (complex numbers of the form $\frac{a+bi}{c+di}$, where $a, b, c, d \in \mathbb{Z}$ and $c + di \neq 0$).
- **Explanation:**
  - $\mathbb{Z}[i]$ is an integral domain because it is a commutative ring with unity and has no zero divisors.
  - The field of fractions of $\mathbb{Z}[i]$ is $\mathbb{Q}(i)$, where every element of $\mathbb{Q}(i)$ can be written as a quotient $\frac{a+bi}{c+di}$, with $a + bi, c + di \in \mathbb{Z}[i]$ and $c + di \neq 0$.
  - For example, $\frac{1+2i}{3-4i} \in \mathbb{Q}(i)$ is a quotient of the Gaussian integers $1 + 2i$ and $3 - 4i$.

Key Observations:

1. In each case, the field of fractions F is constructed by taking all possible quotients $\frac{a}{b}$, where $a, b \in D$ and $b \neq 0$.
2. The field of fractions is the smallest field containing D, and it generalizes the construction of $\mathbb{Q}$ from $\mathbb{Z}$.
3. These examples demonstrate how integral domains can be embedded into fields, allowing division by non-zero elements.

General Construction of the Field of Fractions

Given an integral domain D, the field of fractions F is constructed as follows:

1. Define the set F as the set of equivalence classes of pairs (a, b), where $a, b \in D$ and $b \neq 0$. Two pairs (a, b) and (c, d) are equivalent if $ad = bc$.
2. Define addition and multiplication on F by:
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$
3. Verify that F satisfies all the field axioms.

This construction ensures that F is a field containing D, and every element of F can be expressed as a quotient of two elements of D.

21.4 Lemma The map $i : D \to F$ given by $i(a) = [(a, 1)]$ is an isomorphism of D with a subring of F.

Yes, the function $i : D \to F$ in the construction of the **field of quotients** is **always** given by:

$$i(a) = [(a, 1)] = \frac{a}{1}.$$

Why is this the Standard Definition?

1. **Natural Inclusion**:
   - The field of quotients F consists of elements of the form $[(a, b)] = \frac{a}{b}$ for $a, b \in D, b \neq 0$.
   - To embed D inside F, we identify each element $a \in D$ with the fraction $\frac{a}{1}$, which belongs to F.
2. **Ring Homomorphism Properties**:
   - **Addition**:

     $$i(a) + i(c) = [(a, 1)] + [(c, 1)] = [(a \cdot 1 + c \cdot 1, 1 \cdot 1)] = [(a + c, 1)] = i(a + c).$$

   - **Multiplication**:

     $$i(a) \cdot i(c) = [(a, 1)] \cdot [(c, 1)] = [(a \cdot c, 1 \cdot 1)] = [(ac, 1)] = i(ac).$$

   - **Injectivity**: If $i(a) = i(b)$, then:

     $$[(a, 1)] = [(b, 1)] \Rightarrow a \cdot 1 = b \cdot 1 \Rightarrow a = b.$$

     This proves i is injective.
3. **Subring Formation**:
   - The image $i(D)$ is a subring of F, consisting of elements of the form $[(a, 1)] = a/1$, which behave just like the elements of D under addition and multiplication.

Alternative Definitions?

In some contexts, the map i could be written differently (e.g., using a different notation for equivalence classes), but it always represents the same concept: identifying elements of D with their natural form in F.

Thus, the definition:

$$i(a) = [(a, 1)] = \frac{a}{1}$$

is the **canonical choice** in the construction of the field of quotients.

Section 21: The Field of Quotients of an Integral Domain

21.5 Theorem Any integral domain D can be enlarged to (or embedded in) a field F such that every element of F can be expressed as a quotient of two elements of D. (Such a field F is a **field of quotients of** D.)

Statement Explanation

Any integral domain D can be **embedded** into a field F such that every element of F is a quotient of two elements of D. This means that F consists of elements of the form:

$$\frac{a}{b}, \quad \text{where } a, b \in D,\ b \neq 0.$$

This construction ensures that division is well-defined, allowing us to create a field from any integral domain.

Example 1: The Rational Numbers $\mathbb{Q}$ as the Field of Quotients of $\mathbb{Z}$

Step 1: Integral Domain D

Consider $D = \mathbb{Z}$, the ring of integers. It is an integral domain since it has no zero divisors.

Step 2: Constructing the Field of Quotients F

The field of quotients of $\mathbb{Z}$ is $\mathbb{Q}$, the field of rational numbers. Every rational number can be written as:

$$\frac{a}{b}, \quad \text{where } a, b \in \mathbb{Z},\ b \neq 0.$$

This satisfies the definition of a field of quotients.

Step 3: Verification

- The map $i : \mathbb{Z} \to \mathbb{Q}$ given by $i(a) = \frac{a}{1}$ embeds $\mathbb{Z}$ into $\mathbb{Q}$.
- Addition and multiplication in $\mathbb{Q}$ follow naturally from integer operations.
- Every element in $\mathbb{Q}$ is a fraction of two integers, proving that $\mathbb{Q}$ is the field of quotients of $\mathbb{Z}$.

Example 2: The Rational Function Field $k(x)$ as the Field of Quotients of $k[x]$

Step 1: Integral Domain D

Consider $D = k[x]$, the ring of polynomials in one variable x over a field k. It is an integral domain because it has no zero divisors.

Step 2: Constructing the Field of Quotients F

The field of quotients of $k[x]$ is the field of rational functions:

$$k(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x],\, g(x) \neq 0 \right\}.$$

This field consists of fractions of polynomials, analogous to how $\mathbb{Q}$ consists of fractions of integers.

Step 3: Verification

- The embedding $i : k[x] \to k(x)$ is given by $i(f(x)) = \frac{f(x)}{1}$, which preserves structure.
- Addition and multiplication follow the usual fraction rules:

$$\frac{f(x)}{g(x)} + \frac{h(x)}{k(x)} = \frac{f(x)k(x) + h(x)g(x)}{g(x)k(x)}$$

$$\frac{f(x)}{g(x)} \cdot \frac{h(x)}{k(x)} = \frac{f(x)h(x)}{g(x)k(x)}$$

- Every element in $k(x)$ is a quotient of two elements from $k[x]$, confirming that $k(x)$ is the field of quotients of $k[x]$.

Conclusion

In both examples:

1. The integral domain D is embedded in a field F.
2. Every element of F can be written as a quotient of elements from D.
3. F satisfies the field properties while preserving the structure of D.

Thus, these illustrate how any integral domain can be extended to a field of quotients.

Section 21: The Field of Quotients of an Integral Domain

21.6 Theorem Let F be a field of quotients of D and let L be any field containing D. Then there exists a map $\psi : F \to L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for $a \in D$.

Explanation of the Claims

Let F be a **field of quotients** of an integral domain D, and let L be any field containing D. The claim states that:

1. There exists a **map** $\psi : F \to L$ that is an **isomorphism** onto a subfield of L.
2. The map satisfies $\psi(a) = a$ for all $a \in D$.
3. Any field that contains D necessarily contains a **subfield** isomorphic to F.
4. Any two fields of quotients of D are **isomorphic**, meaning the field of quotients of D is unique up to isomorphism.

Proof Sketch of the Claims

- Since F is a field of quotients, every element of F is of the form $\frac{a}{b}$ with $a, b \in D, b \neq 0$.
- Define a function $\psi : F \to L$ by:

$$\psi\left(\frac{a}{b}\right) = \frac{a}{b} \quad \text{(interpreting the fraction in } L)$$

- This function is well-defined because L contains D and allows division by nonzero elements of D.
- ψ preserves **addition** and **multiplication**:

$$\psi\left(\frac{a}{b} + \frac{c}{d}\right) = \psi\left(\frac{ad + bc}{bd}\right) = \frac{ad + bc}{bd} = \psi\left(\frac{a}{b}\right) + \psi\left(\frac{c}{d}\right).$$

$$\psi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \psi\left(\frac{ac}{bd}\right) = \frac{ac}{bd} = \psi\left(\frac{a}{b}\right) \cdot \psi\left(\frac{c}{d}\right).$$

- ψ is injective because if $\psi(a/b) = \psi(c/d)$, then $a/b = c/d$ in F, meaning a/b and c/d were already the same element.
- ψ is an **isomorphism onto its image**, making $\psi(F)$ a **subfield of** L.
- This shows that every field L containing D must also contain a **subfield isomorphic to** F.
- Since F is unique up to isomorphism, any two fields of quotients of D must be isomorphic.

Three Non-Trivial Examples

Example 1: The Field of Rational Numbers in $\mathbb{R}$

- Let $D = \mathbb{Z}$, whose field of quotients is $F = \mathbb{Q}$.
- The real numbers $L = \mathbb{R}$ contain $\mathbb{Q}$.
- The identity function $\psi : \mathbb{Q} \to \mathbb{R}$ given by $\psi(q) = q$ is an **isomorphism** of $\mathbb{Q}$ onto a subfield of $\mathbb{R}$.
- This shows that any field (like $\mathbb{R}$) that contains $\mathbb{Z}$ also contains a subfield isomorphic to $\mathbb{Q}$.

Example 2: The Field of Rational Functions in $\mathbb{C}(x)$

- Let $D = \mathbb{C}[x]$, the ring of polynomials over $\mathbb{C}$.
- The field of quotients of $\mathbb{C}[x]$ is $F = \mathbb{C}(x)$, the field of rational functions.
- The field $L = \mathbb{C}((x))$, the field of **formal Laurent series**, contains $\mathbb{C}(x)$.
- The function $\psi : \mathbb{C}(x) \to \mathbb{C}((x))$ defined by $\psi(f(x)/g(x)) = f(x)/g(x)$ is an **isomorphism** of $\mathbb{C}(x)$ onto a subfield of $\mathbb{C}((x))$.

Example 3: The p-adic Numbers in $\mathbb{Q}_p$

- Let $D = \mathbb{Z}_{(p)}$, the **localization** of $\mathbb{Z}$ at a prime p (elements are fractions with denominators not divisible by p).
- The field of quotients of $\mathbb{Z}_{(p)}$ is $F = \mathbb{Q}$.
- The **p-adic numbers** $\mathbb{Q}_p$ contain $\mathbb{Q}$.
- The identity map $\psi : \mathbb{Q} \to \mathbb{Q}_p$ is an **isomorphism** onto a subfield of $\mathbb{Q}_p$.

Conclusion

1. Every field containing an integral domain D contains a **subfield isomorphic to its field of quotients**.
2. The field of quotients F is **unique up to isomorphism**, meaning any two fields of quotients of D are isomorphic.
3. The examples illustrate this for rational numbers, rational functions, and p-adic numbers, showing the generality of this result.

Section 21: The Field of Quotients of an Integral Domain

Explanation of Example 2: Rational Function Field in the Field of Formal Laurent Series

Step 1: Define the Integral Domain D

Let $D = \mathbb{C}[x]$, the ring of polynomials in one variable x over the complex numbers $\mathbb{C}$. This ring is an **integral domain** because it has no zero divisors.

Step 2: Define the Field of Quotients F

The **field of quotients** of $\mathbb{C}[x]$ is the field of **rational functions**:

$$F = \mathbb{C}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{C}[x],\ g(x) \neq 0 \right\}.$$

This field consists of ratios of polynomials, analogous to how $\mathbb{Q}$ consists of ratios of integers.

Step 3: Define the Larger Field L

The field $L = \mathbb{C}((x))$ is the field of **formal Laurent series**, which consists of infinite series of the form:

$$\sum_{n=-N}^{\infty} a_n x^n, \quad \text{where } a_n \in \mathbb{C} \text{ and } N \in \mathbb{Z}.$$

This field allows terms with negative exponents (unlike power series $\mathbb{C}[[x]]$, which only allow nonnegative exponents).

Step 4: Show the Isomorphism

There is an obvious embedding $\psi : \mathbb{C}(x) \to \mathbb{C}((x))$ given by:

$$\psi\left(\frac{f(x)}{g(x)}\right) = f(x)g(x)^{-1},$$

where $g(x)^{-1}$ is expanded as a Laurent series if necessary.

For example, consider:

$$\frac{1}{1-x} \in \mathbb{C}(x).$$

In $\mathbb{C}((x))$, we recognize that:

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n.$$

Thus, ψ preserves addition and multiplication, and it is injective because distinct rational functions remain distinct in $\mathbb{C}((x))$. This shows $\mathbb{C}(x)$ embeds as a **subfield** of $\mathbb{C}((x))$.

Explanation of Example 3: Localization of $\mathbb{Z}$ at a Prime p and p-adic Numbers

Step 1: Define the Integral Domain D

The **localization of $\mathbb{Z}$ at a prime p** is the ring:

$$D = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \text{ is not divisible by } p \right\}.$$

This ring consists of rational numbers with denominators **coprime to** p.

Step 2: Define the Field of Quotients F

The **field of quotients** of $\mathbb{Z}_{(p)}$ is simply the **field of rational numbers**:

$$F = \mathbb{Q}.$$

Every rational number $\frac{a}{b}$ with $a, b \in \mathbb{Z}, b \neq 0$ can be written as a fraction where the denominator is not divisible by p, making $\mathbb{Q}$ the field of quotients.

Step 3: Define the Larger Field L

The **p-adic numbers** $\mathbb{Q}_p$ are a completion of $\mathbb{Q}$ with respect to the p-adic valuation.

- The **p-adic norm** $|\cdot|_p$ is defined by:

$$|p^k a/b|_p = p^{-k}, \quad \text{where } p \nmid a, b.$$

- The field $\mathbb{Q}_p$ is obtained as the **completion** of $\mathbb{Q}$ with respect to this norm, analogous to how $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value norm.

Step 4: Show the Isomorphism

There is a natural embedding $\psi : \mathbb{Q} \to \mathbb{Q}_p$ given by:

$$\psi(q) = q.$$

This map preserves arithmetic structure and is injective since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Therefore, ψ is an **isomorphism onto its image**, meaning $\mathbb{Q}$ embeds as a subfield of $\mathbb{Q}_p$.

Conclusion

1. **Example 2:** $\mathbb{C}(x) \subseteq \mathbb{C}((x))$
   - $\mathbb{C}(x)$ (rational functions) embeds in $\mathbb{C}((x))$ (formal Laurent series) because rational functions can be expanded as Laurent series.
2. **Example 3:** $\mathbb{Q} \subseteq \mathbb{Q}_p$
   - $\mathbb{Q}$ embeds in $\mathbb{Q}_p$ (the field of p-adic numbers) via the identity map since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Both cases demonstrate how any field containing an integral domain also contains a **subfield isomorphic to its field of quotients**, supporting the claim that all fields of quotients of D are **unique up to isomorphism**.

21.8 Corollary Every field L containing an integral domain D contains a field of quotients of D.

Three Non-Trivial Examples

Example 1: The Rational Numbers $\mathbb{Q}$ as the Field of Quotients of $\mathbb{Z}$, Embedded in $\mathbb{R}$

- **Integral domain:** $D = \mathbb{Z}$ (the ring of integers).
- **Field of quotients:** $F = \mathbb{Q}$ (the field of rational numbers).
- **Larger field:** $L = \mathbb{R}$ (the field of real numbers).

Verification:

- Every rational number $\frac{a}{b}$ (with $a, b \in \mathbb{Z}, b \neq 0$) belongs to $\mathbb{R}$.
- The map $\psi : \mathbb{Q} \to \mathbb{R}$ given by $\psi(q) = q$ is an **injective homomorphism**.
- This shows that $\mathbb{Q}$ is a **subfield** of $\mathbb{R}$, and any field containing $\mathbb{Z}$ (like $\mathbb{R}$ or $\mathbb{C}$) also contains a subfield **isomorphic to** $\mathbb{Q}$.

Uniqueness:

- Any field of quotients of $\mathbb{Z}$ must be isomorphic to $\mathbb{Q}$, so the construction of $\mathbb{Q}$ is unique up to isomorphism.

Example 2: The Rational Function Field $k(x)$ as the Field of Quotients of $k[x]$, Embedded in $k((x))$

- **Integral domain:** $D = k[x]$ (the ring of polynomials over a field k).
- **Field of quotients:** $F = k(x)$ (the field of rational functions, i.e., quotients of polynomials).
- **Larger field:** $L = k((x))$ (the field of formal Laurent series, which allows negative powers of x).

Verification:

- Every rational function $f(x)/g(x)$ belongs to $k((x))$ because Laurent series can express rational functions.
- The **map** $\psi : k(x) \to k((x))$ given by:

$$\psi\left(\frac{f(x)}{g(x)}\right) = f(x)g(x)^{-1}$$

  is **injective**, meaning $k(x)$ is embedded as a **subfield** of $k((x))$.
- Since any field containing $k[x]$ must also contain all fractions $f(x)/g(x)$, any such field contains a **subfield isomorphic to** $k(x)$.

Uniqueness:

- Any field of quotients of $k[x]$ must be isomorphic to $k(x)$, confirming the uniqueness.

Section 21: The Field of Quotients of an Integral Domain

21.8 Corollary Every field L containing an integral domain D contains a field of quotients of D.

Example 3: The Field of p-adic Numbers $\mathbb{Q}_p$ as an Extension of the Field of Quotients of $\mathbb{Z}_{(p)}$

- **Integral domain:** $D = \mathbb{Z}_{(p)}$, the **localization of** $\mathbb{Z}$ **at** p, meaning it consists of fractions $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ and b is **not divisible by** p.
- **Field of quotients:** $F = \mathbb{Q}$, since every rational number can be written as a fraction with denominator coprime to p.
- **Larger field:** $L = \mathbb{Q}_p$, the p**-adic numbers**, which is a completion of $\mathbb{Q}$ with respect to the p-adic norm.

Verification:

- Every element of $\mathbb{Q}$ is naturally in $\mathbb{Q}_p$ because the p-adic numbers extend the rational numbers.
- The **map** $\psi : \mathbb{Q} \to \mathbb{Q}_p$ given by $\psi(q) = q$ is **injective**, showing $\mathbb{Q}$ is a **subfield** of $\mathbb{Q}_p$.
- Since any field containing $\mathbb{Z}_{(p)}$ must contain all fractions a/b, it contains a **subfield isomorphic to** $\mathbb{Q}$.

Uniqueness:

- Any field of quotients of $\mathbb{Z}_{(p)}$ must be isomorphic to $\mathbb{Q}$, confirming that $\mathbb{Q}$ is the unique fraction field.

Conclusion

1. **Every field L that contains D necessarily contains a subfield isomorphic to the field of quotients F.**
2. **Any two fields of quotients of D are isomorphic.**
3. **Examples demonstrate this general principle:**
   - $\mathbb{Q} \subseteq \mathbb{R}$ (Rational numbers inside real numbers).
   - $k(x) \subseteq k((x))$ (Rational functions inside Laurent series).
   - $\mathbb{Q} \subseteq \mathbb{Q}_p$ (Rationals inside p-adic numbers).

This confirms that the field of quotients of D is **always uniquely determined up to isomorphism** and embeds naturally in any larger field containing D.