



# *Rings and Fields*

PMATH 334



Tomáš Vávra

# Preface

---

**Disclaimer** Much of the information on this set of notes is transcribed directly/indirectly from the lectures of PMATH 334 during Winter 2022 as well as other related resources. I do not make any warranties about the completeness, reliability and accuracy of this set of notes. Use at your own risk.

References:

- Dummit, Foote: *Abstract algebra*.
- <http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf>
- <https://notes.sibeliusp.com/pmath347>

The list of theorems is almost following Dummit, Foote.

For any questions, send me an email via <https://notes.sibeliusp.com/contact>.

You can find my notes for other courses on <https://notes.sibeliusp.com/>.

---

Sibeliusp Peng

# Contents

---

<b>Preface</b>	<b>1</b>
<b>1 Introduction &amp; Motivation</b>	<b>4</b>
1.1 Fermat's Last Theorem . . . . .	4
1.2 Straightedge and compass construction . . . . .	4
<b>2 An introduction to Rings</b>	<b>6</b>
2.1 Definitions and basic properties . . . . .	6
2.2 Zero divisor and integral domain . . . . .	7
2.3 Field . . . . .	8
2.4 Subring . . . . .	9
2.5 Unit . . . . .	9
<b>3 Ring Homomorphisms</b>	<b>11</b>
3.1 Ideals & Quotient rings . . . . .	12
3.2 Isomorphism theorems . . . . .	14
<b>4 More on Ideals</b>	<b>16</b>
4.1 Maximal ideals . . . . .	18
4.2 Maximal ideals and Zorn's Lemma . . . . .	19
<b>5 Polynomial Rings &amp; Rings of Fractions</b>	<b>21</b>
5.1 How to make new rings from old rings? . . . . .	21
5.2 Basic Definitions and Examples . . . . .	21
5.3 Rings of fractions . . . . .	22
<b>6 Chinese Remainder Theorem</b>	<b>25</b>
<b>7 Domains</b>	<b>27</b>
7.1 Euclidean Domains . . . . .	27
7.2 GCD & Bézout domains . . . . .	28
7.3 Euclidean Algorithm . . . . .	29
7.4 Principal Ideal Domain . . . . .	30
7.5 Unique Factorization Domain . . . . .	32
<b>8 Polynomial Rings</b>	<b>36</b>
8.1 Polynomial rings over fields . . . . .	36
8.2 Polynomial rings that are UFDs . . . . .	37
8.3 Irreducibility Criteria . . . . .	39
<b>9 Field Theory</b>	<b>42</b>

9.1	Basic Theory of Field Extensions . . . . .	42
-----	--	----

# Introduction & Motivation

---

## 1.1 Fermat's Last Theorem

### Fermat's Last Theorem

The equation  $x^m + y^m = z^m$  has no non-trivial solutions in integers for  $m \geq 3$ .

For example,  $(1, 0, 1)$ ,  $(-1, 0, 1)$  for  $m$  even, are trivial solutions.

In 1897, Gabriel Lamé announced that he has a proof. First he assumed that  $m$  is a prime. He writes

$$z^p = x^p + y^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y)$$

where  $\zeta_p = \cos(\frac{2\pi}{p}) + i \sin(\frac{2\pi}{p})$ . Consider the ring

$$\mathbb{Z}[\zeta_p] = \{a_1 + a_2 \zeta_p + a_3 \zeta_p^2 + \cdots + a_{p-2} \zeta_p^{p-2} : a_i \in \mathbb{Z}\}$$

which is the smallest ring containing  $\mathbb{Z}$  and  $\zeta_p$ .

Then the next step is to show that  $(x + \zeta_p^j y)$ 's are coprime in  $\mathbb{Z}[\zeta_p]$ . Let  $q_i$ 's be primes.

$$\prod_i q_i^{p\alpha_i} = z^p = (x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y)$$

If  $(x + \zeta_p^j y)$ 's are coprime in  $\mathbb{Z}[\zeta_p]$ , then  $(x + \zeta_p^j y) = (\cdots)^p$  is of  $p$ -th power (\*). But this is wrong if the factorization is non-unique. However, we have  $\mathbb{Z}[\zeta_p]$  can be a unique factorization domain (UFD). This means (\*) works. Kummer salvages the argument for approximately (conjecturally) 60% of prime exponents. And these primes are called **regular primes**.

## 1.2 Straightedge and compass construction

We are given a length 1 straightedge ruler, and a compass. With these, we can

- connect two points with a straightedge,
- draw a circle, centered at  $A$ , and going through  $B$ ,
- draw intersections of two line segments, circle & line, two circles.

What lengths are constructible? where length means distance between two points. We can do  $+, -, \times, \div, \sqrt{\phantom{x}}$ . Then we can do field extensions:

$$\mathbb{Q} \rightarrow \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}) \rightarrow \dots$$

Is trisection of an angle doable? No, **not possible**.

Possible to **double the cube**, **square the circle** of the same area?

What regular  $m$ -gons are constructible? This is equivalent to the question: is  $\cos(\frac{2\pi}{m}) + i \sin(\frac{2\pi}{m})$  constructible?

These can be answered via field extensions.

Other applications including **coding theory**.

# An introduction to Rings

## 2.1 Definitions and basic properties

### ring

A ring is a set with two binary operations  $+$ ,  $\times$ , such that

1.  $(R, +)$  is an abelian group.
  - $+$  is commutative and associative.
  - $\exists 0 \in R, 0 + a = a + 0 = a$  for all  $a \in R$ .
  - $\forall a \in R, \exists (-a) \in R, a + (-a) = (-a) + a = 0$ .
2.  $\times$  is associative  $(a \times b) \times c = a \times (b \times c)$ .
3. distributive laws hold:  $(a + b) \times c = (a \times c) + (b \times c)$ .

The ring is called commutative if  $\times$  is commutative. The ring is said to have an identity if  $\exists 1 \in R, 1 \times a = a \times 1 = a$ , for all  $a \in R$ , and this does not require the existence of inverse.

For simplicity, we write

$$ab := a \times b, \quad b - a = b + (-a)$$

**Example:**

$\mathbb{Z}$  is a commutative ring with identity.

Trivial rings: Let  $(R, +)$  be an abelian group. We define  $a \times b = 0$  for all  $a, b \in R$ . The result is a commutative ring with “trivial structure”.

$R = \{0\}$  is a zero ring.  $0 = 1$  in this case, and it is the only such ring. It leads to assumption  $0 \neq 1$ , saying  $R \neq \{0\}$ .

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$  are commutative rings with identity.

$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$  with  $+, \times \bmod m$  is a ring with identity, and commutative.

The real quaternions:  $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ . Addition is “component-wise”. And the multiplication follows

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

And this is non-commutative ring, with identity 1.

Let  $X$  be a set,  $A$  be a ring. Consider the set  $F = \{f : X \rightarrow A\}$ . Define

$$(f + g)(x) = f(x) + g(x), \quad (f \times g)(x) = f(x) \times g(x)$$

$F$  commutative & having identity is inherited from the ring  $A$ .

$M_m(\mathbb{Z})$  is the ring of square  $m \times m$  matrices with coefficients in  $\mathbb{Z}$ . It is non-commutative ring with identity.

A function  $f : \mathbb{R} \rightarrow \mathbb{R}$  is said to have compact support, if  $\exists a, b \in \mathbb{R}$ ,  $f(x) = 0$  for  $x \notin [a, b]$ .  
 $R = \{f : \mathbb{R} \rightarrow \mathbb{R} : f \text{ has compact support}\}$  is a commutative ring, without identity.

### Proposition 2.1

Let  $R$  be a ring. Then

1.  $0a = a0$  for all  $a \in R$ .
2.  $(-a)b = a(-b) = -(ab)$  for all  $a, b \in R$ .
3.  $(-a)(-b) = ab$  for all  $a, b \in R$ .
4. If  $R$  has an identity 1, then it is unique, and  $(-a) = (-1)a$ .

**Proof:**

We see that

$$\begin{aligned} 0a &= (0 + 0)a = 0a + 0a \\ 0a - 0a &= (0a + 0a) - 0a = 0a + (0a - 0a) \\ 0a &= 0 \end{aligned}$$

We also see that

$$(-a)b + ab = ((-a) + a)b = 0b = 0$$

□

We would like to be able to cancel with respect to  $x$ :  $ab = ac$  then  $b = c$ . However, this is not true in general.

**Example:**

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

However,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

## 2.2 Zero divisor and integral domain

### zero divisor

A nonzero element  $a \in R$  is called a zero divisor, if there exists  $b \in R$  and  $b \neq 0$ , such that  $ab = 0$  or  $ba = 0$ .



**integral domain**

A commutative ring with identity,  $1 \neq 0$ , is called an integral domain, if it contains no zero divisor.

**Proposition 2.2**

Let  $R$  be a ring. Assume that  $a, b, c \in R$ , and  $a$  is not a zero divisor. If  $ab = ac$ , then either  $a = 0$  or  $b = c$  (i.e., we can multiplicatively cancel).

**Proof:**

Observe that

$$ab = ac$$

$$ab - ac = 0$$

$$a(b - c) = 0$$

As  $a$  is not zero divisor, then either  $a = 0$  or  $b - c = 0$ . □

If zero divisors exist, then cancellation does not hold:

$$ab = 0 = a \cdot 0 \not\Rightarrow b = 0$$

**Remark:**

In integral domains,  $ab = 0 \implies a = 0$  or  $b = 0$ .

## 2.3 Field

**division ring**

A ring with identity  $1$ ,  $1 \neq 0$ , is called a division ring, if every nonzero element has a multiplicative inverse, i.e., for all  $a \in R, a \neq 0$ , there exists  $b \in R$ , such that  $ab = ba = 1$ .

Consider an example  $ab = 1$  existing and  $ba = 1$  not existing.

**Example:**

Real sequences  $(x_1, x_2, \dots)$ . Ring of operators on the sequences,  $\times$  is composition. Take

$$D : (x_1, x_2, x_3, \dots) \mapsto (x_2, x_3, x_4, \dots)$$

$$S : (x_1, x_2, x_3, \dots) \mapsto (0, x_1, x_2, x_3, \dots)$$

Then

$$D(S(x_1, x_2, \dots)) = Id(x_1, x_2, \dots)$$

but  $S \circ D \neq Id$ .

**field**

A commutative division ring is called a field.

**Example:**

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$  are fields. Quaternions are “only” a division ring because non-commutative.  $\mathbb{Z}_p$  is a field for  $p$  prime.

**Proposition 2.3**

Any finite integral domain is a field.

$\mathbb{Z}$  is an integral domain, but far from a field.

**Proof:**

Check Corollary 10.13 of PMATH 347. □

## 2.4 Subring

### subring

Let  $R$  be a ring. A nonzero subset  $S \subseteq R$  is called a subring of  $R$ , if it is a ring with the operations from  $(R, +, \times)$  restricted to  $S$ .

That means:  $S \neq \emptyset$ .  $x + (-y) \in S, \forall x, y \in S$ .  $xy \in S, \forall x, y \in S$ .

**Example:**

$\mathbb{Z}_2 \subseteq \mathbb{Z}$ , but  $\mathbb{Z}_2$  is not a subring of  $\mathbb{Z}$ .

$2\mathbb{Z} = \{2 \cdot z : z \in \mathbb{Z}\}$  (ring has no identity) is a subring of  $\mathbb{Z}$  (ring has identity).

Ring of matrices  $M_2(\mathbb{R})$  (1 is identity matrix) has a subring  $S = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \right\}$  and

$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$  is the identity in  $S$ .

## 2.5 Unit

### unit

Assume that  $R$  is a ring with an identity  $1 \neq 0$ . A  $a \in R$  is called a unit, if there exists  $b \in R$  such that  $ab = ba = 1$ . Set of units of  $R$  is denoted by  $R^\times$ .

**Example:**

$$\mathbb{Z}^\times = \{\pm 1\}$$

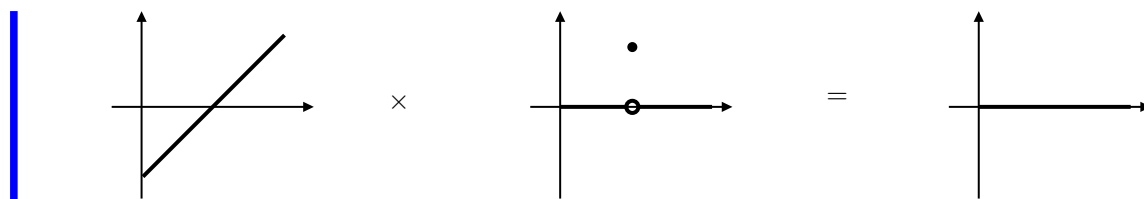
$$\mathbb{Z}_m^\times = \{a \in \mathbb{Z}_m : \gcd(a, m) = 1\}, \mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\} \text{ for } p \text{ prime.}$$

Consider ring  $R$  of  $[0, 1] \rightarrow \mathbb{R}$ , where  $(f \times g)(x) = f(x) \cdot g(x)$ ,  $1_R = 1(x)$ . Units are the functions such that  $f(x) \neq 0$  for  $\forall x \in [0, 1]$ . Then  $f(x)^{-1} = \frac{1}{f(x)}$ . All non-units are zero divisors. If  $g(y) = 0$ ,

$$\text{then } h(x) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} \text{ gives } (g \times h) = 0(x) = 0_R.$$

Ring of all continuous functions  $[0, 1] \rightarrow \mathbb{R}$  is a subring of the previous ring. Units as before, because  $1/f$  exists and is continuous.

Consider  $f(x) = x - 1/2$ .



## Ring Homomorphisms

### ring homomorphism

Let  $R, S$  be rings.

1. A ring homomorphism is  $\phi : R \rightarrow S$ , such that
  - (a)  $\phi(a + b) = \phi(a) + \phi(b)$ , for all  $a, b \in R$ .
  - (b)  $\phi(ab) = \phi(a)\phi(b)$ , for all  $a, b \in R$ .
2. The kernel of  $\phi$ ,  $\ker \phi = \{a \in R : \phi(a) = 0_S\}$ .
3. A bijective homomorphism is called isomorphism.

#### Remark:

Isomorphism means “same ring”, denote  $R \cong S$ .

#### Example:

$\{0, 1\} = \mathbb{Z}_2 = R, S = \{a, b\}$  with  $a + a = a, a + b = b, \dots$ . Then  $R \cong S$ .

#### Example:

$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$  with cancellation  $\frac{a}{b} = \frac{ca}{cb}$

Can we say  $\mathbb{Z} \subseteq \mathbb{Q}$ ? not in the purest sense.  $\mathbb{Z}$  corresponds to  $\{\frac{a}{1} : a \in \mathbb{Z}\}$ .

$\mathbb{Q}$  contains an isomorphic copy of  $\mathbb{Z}$ .  $S \subseteq \mathbb{Q}$  such that  $S \cong \mathbb{Z}$ .

#### Example:

$\phi : \mathbb{Z} \rightarrow \mathbb{Z}_2$ .  $\phi(2k) = 0, \phi(2k + 1) = 1$ . Then

$$\begin{aligned}
 \ker \phi &= 2\mathbb{Z} \\
 \phi^{-1}(0) &= 2\mathbb{Z} = \ker \phi \\
 \phi^{-1}(1) &= 1 + 2\mathbb{Z} \\
 &= 1 + \ker \phi \\
 &= 3 + \ker \phi
 \end{aligned}$$

**Example:**

$\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z} : p(x) \mapsto p(0)$ . Then

$$\begin{aligned}\ker \phi &= \phi^{-1}(0) = \{a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + 0 : a_i \in \mathbb{Z}\} \\ &= x\mathbb{Z}[x] = \{x \cdot p(x) : p(x) \in \mathbb{Z}[x]\}\end{aligned}$$

and

$$\phi^{-1}(a) = x\mathbb{Z}[x] + ax^0 = \ker \phi + ax^0$$

**Example:**

$\phi : \mathbb{Z}[x] \rightarrow \mathbb{Z}_2 : p(x) \mapsto p(0) \bmod 2$ . Then

$$\ker \phi = \phi^{-1}(0) = x\mathbb{Z}[x] + 2\mathbb{Z}$$

$$\phi^{-1}(1) = 1 + \ker \phi$$

**Example:**

$\phi : \mathbb{Z} \rightarrow \mathbb{R} : a \mapsto a$ , then  $\ker \phi = \{0_{\mathbb{R}}\}$ .

### Proposition 3.1

Let  $R, S$  be rings,  $\phi : R \rightarrow S$  be homomorphism.

1. The image of  $\phi$ ,  $(\text{Im}(\phi))$ , or  $\phi(R)$  is a subring of  $S$ .
2.  $\ker \phi$  is a subring of  $R$ . Moreover,  $\forall r \in R, \forall \alpha \in \ker \phi, r\alpha \in \ker \phi, \alpha \in \ker \phi$ . (That is  $\ker \phi$  is closed under multiplication by the elements from  $R$ )

**Proof:**

1. If  $a, b \in \phi(R)$ , then

$$a - b = \phi(x_a) - \phi(x_b) = \phi(x_a - x_b) = \phi(x_{a-b}) \in \phi(R)$$

2.  $\phi(r\alpha) = \phi(r) \cdot \phi(\alpha) = \phi(r) \cdot 0 = 0$

□

Can we get a ring structure on  $a + \ker \phi$ ? There is a factor ring  $R / \ker \phi$ . For example,  $\mathbb{Z} / 2\mathbb{Z} \cong \mathbb{Z}_2$ .

## 3.1 Ideals & Quotient rings

### ideal

Let  $R$  be a ring, let  $I \subseteq R$  be a subring, let  $r \in R$ .

1.  $I$  is called a left ideal, if  $rI \subseteq I$  where  $rI = \{ri : i \in I\}$ .
2.  $I$  is called a right ideal, if  $Ir \subseteq I$ .
3.  $I$  is an ideal, if it is left & right ideal (two sided ideal).

**Ideal Test**

Check  $K$  is an ideal of  $R$ :

- $k - j \in K$  for all  $j, k \in K$ ; and
- $rk, kr \in K$  for all  $k \in K, r \in R$ .

It is a quick generalization of previous definition. Reference: [Laurent W. Marcoux's 334 notes](#).

**additive quotient**

Let  $I \subseteq R$  be an ideal. The additive quotient is defined as  $R/I = \{a + I : a \in R\}$ .

**Example:**

$\mathbb{Z}/3\mathbb{Z} = \left\{ \{\dots, -6, 3, 0, 3, 6, \dots\}, \{\dots, -5, -2, 1, 4, \dots\}, \{\dots, -4, -1, 2, 5, 8, \dots\} \right\}$ . Additive group.

Let  $I = 3\mathbb{Z}$ . Then  $a + I$  are called (additive) cosets.

**Proposition 3.2**

Let  $R$  be a ring,  $I$  an ideal of  $R$ , then  $R/I$  is a ring with the operations

$$(a + I) +_{R/I} (b + I) =: (a +_R b) + I$$

$$(a + I) \times_{R/I} (b + I) = (a \times_R b) + I$$

The ring properties  $R/I$  follow from  $R$  being a ring.

**quotient ring**

$R/I$  is called the quotient ring of  $R$  by  $I$ .

**Remark:**

If  $I$  is not an ideal, then the definition of the operations on  $R/I$  is not well defined.

**Example:**

Let  $R$  be commutative ring with identity  $1 \neq 0$ ,  $m \geq 2$ . Let  $M_m(R)$  be ring of square matrices with coefficients in  $R$ .

Denote

$$L_j(R) = \{A \in M_m(R) \mid A_{ik} = 0, \forall i \in [n], k \in [m] \setminus \{j\}\}$$

which means only the  $j$ -th column can have non-zero entries. Then  $L_j(R)$  is a left ideal in  $M_m(R)$ . This can be verified by the matrix multiplication.  $L_j(R)$  is not a right ideal, i.e.,  $L_j(R) \cdot M \not\subseteq L_j(R)$  for some  $M \in M_m(R)$ .

Analogously, a right ideal can be obtained by taking

$$T_i(R) = \left\{ A \in M_m(R) \mid A_{kj} = 0, \forall k \in [n] \setminus \{i\}, j \in [m] \right\}$$

**Example:**

Let  $R = \mathbb{Z}[x]$  and  $I = x^2\mathbb{Z}[x]$ .

Then  $R/I = \{a + bx + p(x) : a, b \in \mathbb{Z}, p(x) \in I\}$ .

For  $a \in R/I$ ,  $\bar{a}$  denotes  $a + I$ .

## 3.2 Isomorphism theorems

### Lemma 3.3

Let  $I$  be an ideal in  $R$ , then  $a + I = b + I$  ( $\bar{a} = \bar{b}$ ) if and only if  $b - a \in I$ . Namely, every member of the coset can be the representative.

### Theorem 3.4: First isomorphism theorem

If  $\phi : R \rightarrow S$  is a ring homomorphism, then  $\ker \phi$  is an ideal in  $R$ ,  $\text{Im } \phi$  is a subring of  $S$ , and  $R / \ker \phi \cong \text{Im } \phi$ .

**Proof:**

Theorem 4.2 of <http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf>

Consider  $\tau : R / \ker \phi \rightarrow \phi(R) : r + \ker \phi \mapsto \phi(r)$ . □

**Example:**

$\mathbb{Z}[x] / 2\mathbb{Z}[x] \cong \mathbb{Z}_2[x]$ . We can define  $\phi : p(x) \mapsto p(x) \pmod{2}$ .

### Theorem 3.5

For any ideal  $I \subseteq R$ , the map  $R \rightarrow R/I$  defined by  $\pi : r \mapsto r + I$  is a surjective ring homomorphism with kernel  $I$ . It is called the natural projection of  $R$  onto  $R/I$ . Thus every ideal is a kernel of some homomorphism.

**Proof:**

Prove surjectivity is as before in first iso theorem. To prove homomorphism, both  $\times$  and  $+$ . Now prove  $\ker \pi$ .

- Let  $i \in I$ , then  $\pi(i) = i + I = I = 0_{R/I}$ .
- Let  $a \in R/I$ , then  $\pi(a) = a + I$ , but  $a \notin I$ . Thus by lemma,  $a + I \neq I = 0 + I$ . □

### Theorem 3.6: Second isomorphism theorem

Let  $A$  be a subring of  $R$ ,  $B$  an ideal of  $R$ . Then  $A + B = \{a + b : a \in A, b \in B\}$  is a subring of  $R$ .  $A \cap B$  is an ideal of  $R$  and  $(A + B)/B \cong A / A \cap B$ .

**Proof:**

Consider the map  $\phi : A \rightarrow (A + B)/B : a \mapsto a + B$ . Then apply first isomorphism theorem.

Or check Theorem 4.3 of <http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf>. □

**Remark:**

$$(A + B)/B = \{a + b + B : a \in A, b \in B\} = \{a + B : a \in A\} \stackrel{?}{=} A/B$$

This reduction can't happen because  $B$  is not necessarily an ideal of  $A$ .

**Example:**

Let  $R = \mathbb{Z}$ , then  $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b) \cdot \mathbb{Z}$ .  $a\mathbb{Z} \cap b\mathbb{Z} = \text{lcm}(a, b) \cdot \mathbb{Z}$ . Then by second iso thm

$$\frac{\gcd(a, b)\mathbb{Z}}{b\mathbb{Z}} \cong \frac{a\mathbb{Z}}{\text{lcm}(a, b)\mathbb{Z}}$$

**Lemma 3.7**

If  $m \mid n$ , then  $n\mathbb{Z}$  is an ideal of  $m\mathbb{Z}$ , and  $|m\mathbb{Z}/n\mathbb{Z}| = \frac{n}{m}$ .

The coset representative in  $(m\mathbb{Z}/n\mathbb{Z})$  are  $\{0, m, 2m, \dots, (\frac{n}{m} - 1)m\}$ . Applying to  $A + B/B \cong A/A \cap B$ , we have

$$\frac{b}{\gcd(a, b)} = \frac{\text{lcm}(a, b)}{a} \implies ab = \text{lcm}(a, b) \cdot \gcd(a, b)$$

**Theorem 3.8: Third isomorphism theorem**

Let  $I \subseteq J$  be ideals in  $R$ . Then  $J/I$  is an ideal in  $R/I$  and  $(R/I)/(J/I) \cong R/J$ .

**Proof:**

Define  $\phi : R/I \rightarrow R/J : a + I \mapsto a + J$ . Then show that  $\ker \phi = J/I$  and then use first isomorphism theorem.

Or check Theorem 4.4 of <http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf> □

**Example:**

$$(\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3.$$

**Theorem 3.9: Fourth isomorphism theorem/correspondence theorem**

Let  $R$  be ring,  $I$  ideal in  $R$ . The correspondence  $A \leftrightarrow A/I$  is an inclusion preserving bijection between the set of subrings ( $A$ ) of  $R$ ,  $I \subseteq A \subseteq R$ , and the set of subrings of  $R/I$ . Furthermore,  $A/I$  is an ideal in  $R/I$  if and only if  $A$  is an ideal in  $R$  ( $I \subseteq A$ ).

**Proof:**

No first isomorphism theorem. Expand and verify the definitions. □

The interesting part is: subring of  $R/I$  gives subring of  $R$ .



## More on Ideals

Let  $A \subseteq R$  with identity.

$(A)$

1.  $(A)$  = the smallest ideal containing  $A$  (in  $R$ )

2. Let

$$RA = \left\{ \sum r_i a_i : r_i \in R, a_i \in A \right\}$$

$$AR = \left\{ \sum a_i r_i : r_i \in R, a_i \in A \right\}$$

$$RAR = \left\{ \sum r_i a_i r'_i : r_i, r'_i \in R, a_i \in A \right\}$$

where these are all finite sums.

3. If  $A = \{a\}$ , then  $(A) =: (a)$  is called a principal ideal.

4. If an ideal  $I = (A)$  for  $A$  finite, we call  $I$  finitely generated.

**Remark:**

$$(A) = \bigcap_{\substack{I \text{ ideal of } R \\ A \subseteq I}} I$$

The intersection is indeed an ideal.

$(A) \subseteq \cap I$  because  $(A)$  is the smallest.  $\cap I \subseteq (A)$  because it contains  $I = (A)$ .

Note that  $\cup I_\alpha$  is not an ideal in general.

What is  $(A)$ ?

Assume  $R$  is commutative. Then  $(A)$  contains  $a \in R$ , and also  $ra, r \in R, a \in R$ , and their sums. This is precisely the definition of  $RA$ . Thus  $RA \subseteq (A)$ .

Note that  $1 \in R$ . Then  $A \subseteq RA$ , and  $RA$  is an ideal itself. By minimality,  $(A) \subseteq RA$ .

To conclude,  $(A) = RA = AR = RAR$  in the commutative case.

In particular, the principal ideal  $(A) = a \cdot R = \{ar : r \in R\}$ , because let  $A = \{a\}$ , we have

$$AR = \left\{ \sum ar_i : r_i \in R \right\} = \left\{ a \left( \sum r_i \right) : r_i \in R \right\}$$

works in commutative rings.

**Warning** In non-commutative rings, we have  $(A) = RAR$ , so

$$(a) = RaR \neq \{r_i a r'_i : r_i, r'_i \in R\}$$

**Example:**

$R = \mathbb{Z}$ , the principal ideal  $(m)$  is  $m\mathbb{Z}$ .

**Example:**

Let  $R = \{f : [0, 1] \rightarrow \mathbb{R}\}$ . Then  $I = \{f \in R : f(1/2) = 0\}$  is an ideal. And  $I = (g)$  where

$$g(x) = \begin{cases} 0 & \text{if } x = 1/2 \\ 1 & \text{otherwise} \end{cases}$$

For  $h \in I$ ,  $h = g \cdot h \in (g)$ . Note that  $g$  is an identity element of  $I$ , but not of  $R$ .

**Example:**

$C = \{f : [0, 1] \rightarrow \mathbb{R} \mid f \text{ is continuous}\}$  is a subring of  $R$ .  $I = \{f \in C : f(1/2) = 0\}$  is again an ideal. BUT!  $I$  is not a principal ideal,  $I$  is not even finitely generated (not easily proven).

Note that  $I$  here is different from last example, where the instructor made a mistake at first.

**Example:**

Let  $R = \mathbb{Q}[x]$ . Consider subring  $S = x\mathbb{Q}[x] + \mathbb{Z}$ . An ideal  $I = x\mathbb{Q}[x]$ .

1.  $I = (x)$  in  $R$
2.  $I$  is an ideal in  $S$  where  $I$  is not finitely generated

If  $I$  is finitely generated in  $S$ , then there exists  $p_1, \dots, p_k \in I$

$$I = (p_1, \dots, p_k) = \left\{ \sum_{i=1}^k p_i(x) q_i(x) : q_i \in S \right\}$$

As  $p_i$  are in ideal  $I = x\mathbb{Q}[x]$ ,  $p_i$  don't have constant term. However, this is not possible. Take an element  $\frac{a}{b}x \in I$ , then

$$\frac{a}{b}x = \sum_{i=1}^k p_i(x) q_i(x)$$

As  $p_i$ 's are fixed, one need to find proper  $q_i$ 's to make this equation hold. Now consider  $b$  to be a prime such that  $b$  does not divide the product of denominators of  $p_i$ 's, then it's impossible to find any  $q_i$ 's to make this equation holds. Therefore  $I$  is not a finite generated ideal in  $S$ .

#### Proposition 4.1

Let  $I$  be an ideal in  $R$  with identity  $1 \neq 0$ .

1.  $I = R$  if and only if  $I$  contains a unit.
2. Let  $R$  be commutative. Then  $R$  is a field if and only if the only ideals in  $R$  are  $0$  and  $R$ .

**Proof:****Statement 1**

( $\Rightarrow$ ) Because  $1 \in R = I$ , and 1 is a unit.

( $\Leftarrow$ ) Let  $u \in I$  be a unit. Then  $u \cdot u^{-1} = 1 \in I$ . Let  $r \in I$ , as  $1 \in I$ , then  $1 \cdot r \in I$ , hence  $I = R$ .

**Statement 2**

( $\Rightarrow$ ) Let  $0 \neq I \subseteq R$  be an ideal. Then it contains a unit. Then by (1),  $I = R$ .

( $\Leftarrow$ ) Take arbitrary  $0 \neq r \in R$ . The ring  $(r)$  can't be zero ideal, hence  $(r) = R$ . Thus  $1 \in (r)$ . That means there exists  $s \in R$ , such that  $1 = r \cdot s$ . Then  $s = r^{-1}$ . Hence  $r$  is a unit.  $\square$

**Corollary 4.2**

A nonzero homomorphism from a field to a ring is an injection.

**Proof:**

Let  $\phi$  be such a homomorphism.  $\ker \phi$  is an ideal of the field. This implies  $\ker \phi = 0$  (injective homomorphism) or  $R$ , the whole field. And the second possibility tells us  $\phi$  is a zero map, which is eliminated by the assumption.  $\square$

## 4.1 Maximal ideals

**maximal ideal**

An ideal  $M$  in an arbitrary ring  $R$  is called a maximal ideal if  $M \neq R$  and there is no proper ( $\neq R$ ) ideal  $I$ ,  $M \subseteq I \subseteq R$ .

Alternatively, ideal  $I$  of a ring  $R$  is maximal if the only ideals containing  $I$  are  $I$  and  $R$ .

**Theorem 4.3**

Assume that  $R$  ring is commutative. The ideal  $M$  is maximal if and only if  $R/M$  is a field.

**Proof:**

By 4th iso thm, or correspondence theorem,  $R/M$  is a field  $\Leftrightarrow$  ideals of  $R/M$  are zero ideals and  $R/M \Leftrightarrow$  only ideals of  $R$  containing  $M$  are  $M$  and  $R \Leftrightarrow M$  is maximal.  $\square$

**Example:**

$p\mathbb{Z}$  is maximal ideal for any  $p$  prime.

**Theorem 4.4**

$p\mathbb{Z}$  is maximal if and only if  $\mathbb{Z}/p\mathbb{Z}$  is a field.

**Example:**

$(2, x)$  in  $\mathbb{Z}[x]$  is maximal.  $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$  because  $(2, x)$  is a kernel of  $\phi : p(x) \mapsto p(0) \bmod 2$ .

**Example:**

Let  $R = \{f : [0, 1] \rightarrow \mathbb{R}\}$  and  $M_c = \{f \in R : f(c) = 0\}$ . Consider  $\phi : R \rightarrow \mathbb{R} : f \mapsto f(c)$ . Then  $\ker \phi = M_c$ . As  $\mathbb{R} = \phi(R)$ , then  $R/M_c \cong \mathbb{R}$  is a field. Hence  $M_c$  maximal.

## 4.2 Maximal ideals and Zorn's Lemma

Consult Section 10.3 of **PMATH 347** if needed.

Is every ideal (proper) contained in some maximal ideal? No. Consider  $\mathbb{Q}$  with standard  $+$  and  $a \times b = 0_+$  for all  $a, b \in \mathbb{Q}$ . We have ideals

$$\left\{ \frac{a}{2} : a \in \mathbb{Z} \right\} \subseteq \left\{ \frac{a}{4} : a \in \mathbb{Z} \right\} \subseteq \cdots \subseteq \left\{ \frac{a}{2^k} : a \in \mathbb{Z} \right\} \subseteq \cdots$$

These ideals are not contained in a maximal ideal. This happens because there's no identity.

### Theorem 4.5

In a ring with an identity, every proper ideal is contained in some maximal ideal.

**Wrong idea** Given  $I$ , then  $I \subseteq \bigcup_{\substack{I \subsetneq A \\ A \neq R}} A$ . But this is not an ideal. For example,  $\mathbb{Z}_6 \subseteq \mathbb{Z}_2 \cup \mathbb{Z}_3$  is not an ideal.

**Right idea**  $I \subseteq \bigcup_{A \in C} A$  for  $C$  being a “chain”

$$I \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_m \subseteq \cdots$$

### partial order

A partial order on a set  $S$  is a relation on  $X$  such that

1.  $a \leq a$  for all  $a \in S$ ,
2. If  $a \leq b$  and  $b \leq a$  then  $a = b$  for all  $a, b \in S$ ,
3. If  $a \leq b$  and  $b \leq c$ , then  $a \leq c$  for all  $a, b, c \in S$ .

So set inclusion  $\subseteq$  is a partial order.

The ordering does not have to be “linear”:  $\text{sth} \leq \text{sth} \leq \text{sth} \leq \cdots$ . For sets, we can have

$$\begin{array}{ccccc} & \{a, b\} & \subseteq & \{a, b, d\} & \\ & \swarrow & & \searrow & \\ \{a\} & & & & \{a, b, c, d, e\} \\ & \nwarrow & & \nearrow & \\ & \{a, c\} & \subseteq & \{a, c, e\} & \end{array}$$

A chain  $C$  in a partially ordered set  $(S, \leq)$  is a subset such that for all  $x, y \in C$ ,  $x \leq y$  or  $y \leq x$  (i.e., all elements are comparable).

### Zorn's Lemma

Let  $(S, \leq)$  be a partially ordered set with the property that each chain has an upper bound in  $S$ . Then  $S$  contains a maximal element.

### Theorem 4.6

Let  $R$  be a ring with 1. Then every proper ideal  $I$  is contained in some maximal ideal.

**Proof:**

Let  $F = \{J : J \text{ is a proper ideal of } R, M \subseteq J\}$ . Notice  $(F, \subseteq)$  is a poset (partially ordered set). Recall some notations/definitions:

- Chain: subset  $G \subseteq F$ , s.t.  $\forall x, y \in G, x \subseteq y \text{ or } y \subseteq x$  (comparable)
- Upper bound of  $G \in F$ ,  $m \in F$ , s.t.  $\forall g \in G, g \subseteq m$ .
- Maximal in  $F$ :  $m \in F$ , s.t.  $\forall a \in F, (m \subseteq a) \implies (a = m)$ .

Let  $C \subseteq F$  be a chain. Put  $M := \bigcup_{A \in C} A$ .  $M$  is an ideal because

1. nonempty:  $A \in C, I \subseteq A$ , then  $I \in M$ .
2. Let  $a \in A, b \in B$ , and  $A, B \in C$ . WLOG, assume  $A \subseteq B$ . Then  $a, b \in B$ , then  $a - b \in B$ , then  $a - b \in M$ .
3.  $\forall r \in R, a \in M$ , we have  $a \in A \in C$ , then  $ra \in A, ra \in M$ .

We claim that  $M$  is an upper bound of  $C$  in  $F$ . If  $M = R$ , then  $1 \in A \in C$ . But then by proposition,  $A = R$ . Contradiction.

Then apply Zorn lemma.

Or check proposition 10.8 of **PMATH** 347.

□

## Polynomial Rings & Rings of Fractions

---

### 5.1 How to make new rings from old rings?

I don't want to put this section to the previous chapter. So here it is.

#### Direct products

Let  $(R_i, +_i, \times_i)$  be rings.  $R_1 \times R_2$  is a ring with

$$\begin{aligned}(r_1, r_2) \oplus (s_1, s_2) &= (r_1 +_1 s_1, r_2 +_2 s_2) \\ (r_1, r_2) \otimes (s_1, s_2) &= (r_1 \times_1 s_1, r_2 \times_2 s_2)\end{aligned}$$

Then this applies to  $\prod_i R_i$  (works for at most countable  $R_i$ 's).

#### Direct sum

For finitely many  $R_i$ 's, it is just direct product. For infinitely many  $R_i$ 's

$$\bigoplus_{i \in I} R_i = \{(r_1, r_2, r_3, \dots) : r_i \in R_i, \text{ only finitely many } r_i \neq 0\}$$

### 5.2 Basic Definitions and Examples

Let  $R$  be a commutative ring with identity. A polynomial with coefficients in  $R$  with undeterminate/-variable  $x$  is a **formal** expression

$$p(x) = a^n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

with  $a_i \in R, \forall i \in 0, \dots, n$ . If  $a_m \neq 0$ , then  $\deg p = n$ . If  $a_n = 1$ , we call  $p(x)$  monic.

$R[x] = \{a^n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 : n \in \mathbb{N}, a_i \in R\}$  with operations

$$\begin{aligned}\sum_{i=0}^n a_i x^i + \sum_{i=0}^m b_i x^i &= \sum_{i=0}^{n+m} (a_i + b_i) x^i \\ \left(\sum_{i=0}^n a_i x^i\right) \times \left(\sum_{i=0}^m b_i x^i\right) &= \sum_{k=0}^{n+m} \left(\sum_{i=0}^k a_i b_{k-i}\right) x^k\end{aligned}$$

Observe that  $R$  appears in  $R[x]$  as constant polynomials.  $R[x]$  is commutative ring with identity.

**Proposition 5.1**

Let  $R$  be an integral domain, let  $p, q \in R[x]$  be nonzero elements. Then

1.  $\deg pq = \deg p + \deg q$
2. the units of  $R[x]$  are precisely the units of  $R$ .
3.  $R[x]$  is an integral domain.

**Proof:**

$$p(x)q(x) = \underbrace{a_n b_m}_{\neq 0} x^{n+m} + \dots$$

Let  $p(x) \in R[x]$  be invertible, then there exists  $q$  such that  $pq = 1$ . By (1),  $\deg p = 0$ . Thus  $\deg q = 0$ .  $p, q$  are constant polynomials.

$pq = 0$ , then  $\deg p + \deg q = 0$ . Then  $\deg p = \deg q = 0$ . Then they are all constant polynomials. As  $R$  is integral domain, we have  $p = q = 0$ .  $\square$

**Formal power series**

Ring of all power series  $R[[x]] = \{\sum_{i=0}^{\infty} a_i x^i : a_i \in R\}$  with the same operations defined as polynomial rings.

1.  $R[[x]]$  is a commutative ring with identity.
2. Units of  $R[[x]]$  are  $\sum_{i=0}^{\infty} a_i x^i$  with  $a_0$  unit in  $R$ .

**Laurent series**

$$R((x)) = \left\{ \sum_{i=N}^{\infty} a_i x^i : a_i \in R, N \in \mathbb{Z} \right\}$$

**5.3 Rings of fractions**

Construct  $\mathbb{Q}$  from  $R = \mathbb{Z}$ . Define

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}$$

$\frac{p}{q}$  is a “formal” fraction. ( $p \cdot q^{-1}$  does not work). However,  $\frac{1}{1}, \frac{2}{2}, \frac{3}{3}$  are distinct formal fractions. We want to have them be in equivalent classes.

We define  $\frac{a}{b} \sim \frac{c}{d}$  iff  $ad = bc$  (use only the ring operations). Then define  $\mathbb{Q}$  be the equivalence classes of  $\sim$ . For that, we need to show that  $\sim$  is equivalence: reflexive, symmetric, transitive.

We define addition as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

is well-defined on equivalence classes. We can obtain  $+$  on the equivalence classes through definition of  $+$ .

We define multiplication as

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

is well-defined on equivalence classes.

Then we obtain  $\mathbb{Q}$ . Note that the well-definednesses need a proof. See Section 11.1 of [PMATH 347](#).

$\frac{2}{1}, \frac{1}{2} \in \mathbb{Q}$ , then  $\frac{2}{1} \cdot \frac{1}{2} = \frac{2}{2} \sim \frac{1}{1}$  is an identity. Thus 2 is invertible in  $\mathbb{Q}$ . Every integer is a unit in  $\mathbb{Q}$ .

If  $R$  have zero divisors,  $ab = 0$  and  $a, b \neq 0$ . Then if  $a$  invertible:  $1 = a^{-1} \cdot a$ , then  $b = a^{-1}(a \cdot b) = 0$ . Contradiction. Thus **zero divisors do not have inverses in any ring**. Now consider

$$a = \frac{a}{1} = \frac{ab}{b} = \frac{0}{b} = 0$$

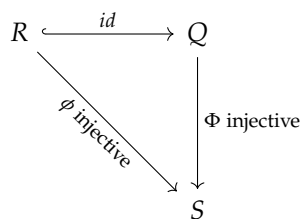
contradiction to  $a \neq 0$ . Thus we will avoid zero divisors.

### Theorem 5.2

Let  $R$  be a commutative ring. Let  $D$  be any subset of  $R$  closed under multiplication and not containing zero divisors and 0. Then there exists a commutative ring  $Q$  with identity such that  $Q$  contains  $R$  as a subring and every element of  $D$  is a unit of  $Q$ . Moreover,

1. every element of  $Q$  is of the form  $\frac{r}{d}$  for some  $r \in R, d \in D$ . If  $D = R \setminus \{0\}$ , then  $Q$  is a field.
2. The ring  $Q$  is the smallest ring containing  $R$  in which all elements of  $D$  are units.

Here we formalize the definition of “smallest”: Let  $S$  be any commutative ring with identity and let  $\phi : R \rightarrow S$  be any injective homomorphism such that  $\phi(d)$  is a unit of  $S$  for each  $d \in D$ . Then there is an injective homomorphism  $\Phi : Q \rightarrow S$  such that  $\Phi|_R = \phi$ . In other words, any ring containing an isomorphic copy of  $R$  in which elements of  $D$  become units must contain  $Q$ .



Thus  $R'' \subseteq S$ .

### Proof:

Almost the same as the proof of Theorem 11.3 of pmath347. Below are some main points.

$F := \{(r, s) : r \in R, d \in D\}$ . Then  $\sim$  is an equivalence relation:  $(r, s) \sim (g, h)$  iff  $rh = sg$ . Then denote by  $\frac{r}{d}$  the equivalence class of  $(r, d)$ . As above, we define  $+$  and  $\times$ .

Let  $Q/\sim$  be the set of equivalence classes of  $\sim$ . We verify it is a ring.

$Q$  contains an isomorphic image of  $R$ : consider a homomorphism  $\sigma : R \rightarrow Q, r \mapsto \frac{rd}{d}$  for any  $d \in D$  (does not depend on choice of  $d$ ). We need to prove injectivity here.

Every  $d \in D$  (i.e.,  $\sigma(d)$ ) is invertible in  $Q$ .

Now let's prove (1) and (2). (1) is trivial. Now prove (2). We claim that there exists  $\psi : Q \rightarrow S$  injective such that  $\psi|_R = \phi$ . Note that  $\phi(d)$  invertible for all  $d \in D$ , thus we can define  $\psi(\frac{r}{d}) = \phi(r)\phi(d)^{-1}$  for all  $r \in R, d \in D$ .  $\psi$  is well defined.  $\psi$  is a homomorphism because  $\phi$  is. Not hard to see  $\psi$  is injective. Finally, we see that  $\psi|_R = \phi$ .  $\square$

### Example:

$R = \mathbb{Z}$ , then  $Q = \mathbb{Q}$ .

If  $R$  is a field, then  $Q = R$ .

$R = 2\mathbb{Z}$  is a ring without identity, then  $Q = \mathbb{Q}$ .  $1_Q = \frac{2}{2}$  for example.



$R := R[x]$ , then  $Q$  is a ring of  $\frac{p(x)}{q(x)}$ ,  $q(x) \neq 0$ . This is rational functions. If we start with  $\mathbb{Z}[x]$ , then  $Q = \{\frac{p(x)}{q(x)} : q(x) \neq 0\}$ . If we start with  $\mathbb{Q}[x]$ , then its  $Q$  is the same.

$R := R[[x]]$ , then  $Q = R((x))$ .

# Chinese Remainder Theorem

## comaximal

The ideals  $A, B \subseteq R$  are said to be comaximal if  $A + B = R$ .

$m, n$  coprime iff  $\exists a, b \in \mathbb{Z}, an + bm = 1$ .

## $A + B$

$A + B := \{a + b : a \in A, b \in B\}$ .

## Example:

$5\mathbb{Z}, 3\mathbb{Z} \subseteq \mathbb{Z}$ . As  $10 + (-9) \in 5\mathbb{Z} + 3\mathbb{Z}$ , hence  $5\mathbb{Z}, 3\mathbb{Z}$  are comaximal.

## $AB$

$AB := \{\sum_{\text{finite sums}} a_i b_i : a_i \in A, b_i \in B\}$ . Similarly we have  $A_1 \cdots A_k := \{\sum a_{i1} \cdots a_{ik} : a_{ij} \in A_j\}$ .

## Theorem 6.1

Let  $R$  be a commutative ring with an identity. Let  $I_1, I_2, \dots, I_k$  be ideals in  $R$ , such that  $I_n, I_m$  are comaximal for  $n \neq m$ . Then

$$R/I_1 I_2 \cdots I_k = R/I_1 \cap I_2 \cap \cdots \cap I_k \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k$$

In particular,  $I_1 I_2 \cdots I_k = I_1 \cap I_2 \cap \cdots \cap I_k$ .

## Proof:

By induction. The proof here is the same as Theorem 11.24 of pmath 347. □

## Remark:

Consider the units of  $R/I_1 \cdots I_k$  and  $R/I_1 \times \cdots \times R/I_k$ . The units are the same (under isomorphism). That means that

$$(R/I_1 \cdots I_k)^\times \cong (R/I_1)^\times (R/I_2)^\times \times \cdots \times (R/I_k)^\times$$

Because units in the product of rings are units in each component.

■ An element of a product ring is a unit iff each component is a unit in its respective ring.

Then apply this remark to integers:  $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ .

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$$

Euler's totient function:  $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ . Thus from the relation above, we have

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$$

which means  $\varphi(\cdot)$  is multiplicative arithmetic function.

# Domains

## 7.1 Euclidean Domains

### norm

A norm on a ring  $R$  is a function  $N : R \rightarrow \mathbb{Z}^+ \cup \{0\}$ , s.t.  $N(0) = 0$ .

### Euclidean domain

An integral domain (identity, commutative, no zero divisors) for which there exists a Norm, such that:  $\forall a, b \in R, b \neq 0$ , there exists  $q, r \in R$  s.t.  $a = qb + r$  with  $N(r) < N(b)$  or  $r = 0$ . This is called a Euclidean domain.

#### Example:

$R = \mathbb{Z}, N(x) = |x|$ . Then  $a = qb + r$  follows from division with remainder. We don't have to keep  $r$  positive/negative.

#### Example:

Fields with  $N(x) = 0$ . We have  $a = (ab^{-1})b = 0$

#### Example:

$F$  a field. Then  $F[x]$  is a Euclidean domain with  $N(p(x)) = \deg(p(x))$ . Then we can have polynomial long division.

#### Example:

Consider Gaussian integers.

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

is ED with  $N(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$ .

### Theorem 7.1

Every ideal in a Euclidean domain is principal.

**Proof:**

Let  $I \subseteq R$  an ideal. Take a nonzero element  $d$  in  $I$  of the smallest norm. Let  $x \in I$ , then  $x = qd + r$  where  $N(r) = 0$  or  $N(r) < N(d)$ . But  $N(r) < N(d)$  is not possible. So  $N(r) = 0$ . Since  $r = x - qd \in I$ , then we must have  $r = 0$ . Then  $x = qd$ . This holds for any  $x \in I$ . Thus  $I = (d)$ .  $\square$

**Remark:**

Every ideal is principal: principal ideal domain (PID). We have  $ED \subseteq \text{PID}$ , not other way around.

## 7.2 GCD & Bézout domains

### greatest common divisor

Let  $R$  be commutative.

1. We say that  $b \mid a$  ( $b$  divides  $a$ ), if there exists  $x \in R$ ,  $a = bx$ .
2.  $d \in R$  is called a  $\gcd(a, b)$  if
  - $\ast$ )  $d \mid a, d \mid b$
  - $\triangle$ ) if  $d' \mid a$  and  $d' \mid b$ , then  $d' \mid d$ .

We can rephrase two conditions:

$$\ast) (a, b) \subseteq (d) \subseteq R$$

$$\triangle) \text{ If } (a, b) \subseteq (d'), \text{ then } (a, b) \subseteq (d) \subseteq (d').$$

### Bézout domain

Bézout domain is a form of a Prüfer domain. It is an integral domain in which the sum of two principal ideals is again a principal ideal.

### Proposition 7.2

In Bezout domains (every  $(a, b)$  is principal),  $(a, b) = (d)$  where  $d = \gcd(a, b)$ .

**Proof:**

Assume  $(a, b) = (\alpha)$ . We know that  $(a, b) = (\alpha) \subseteq (d)$  because  $(d)$  is the smallest ideal containing  $(a, b)$ . Then by definition of  $\gcd$ , we conclude that  $(\alpha) = (d)$ .  $\square$

Bezout domain is not necessary for existence of  $\gcd$ .

**Example:**

$R = \mathbb{Z}[x]$ , what is  $\gcd(2, x)$ ?  $(2, x)$  is not principal. It is a maximal ideal, because  $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$ .

We see that  $(2, x) \subseteq (1)$ . Because  $(2, x)$  is maximal, there are no ideals in between. Hence  $\gcd(2, x^2) = 1$ .

### Theorem 7.3

Let  $R$  be an integral domain (commutative ring with identity), then  $(d) = (d')$  if and only if  $d = d'u$  for a unit  $u \in R$ .

**Example:**

In  $\mathbb{Z}[i]$ , units are  $\{\pm 1, \pm i\}$ , then  $(2) = (-2i)$ .

**Proof:**

We know that  $d \in (d')$  and  $d' \in (d)$ . Thus we can find  $x, y \in R$  such that  $d = d'x$  and  $d' = dy$ . Hence  $d(1 - xy) = 0$ . If  $d = 0$ , then it's a trivial ring. If  $d \neq 0$ , then  $xy = 1$ .  $\square$

**Corollary 7.4**

If  $\gcd(a, b) = d$ , then all gcd's are  $ud$ , for  $u$  a unit.

## 7.3 Euclidean Algorithm

It unfolds as follows

$$\begin{aligned}
 a &= q_0b + r_0, & N(r_0) < N(b) \\
 b &= q_1r_0 + r_1 \\
 r_0 &= q_2r_1 + r_2 \\
 &\vdots \\
 r_{m-2} &= q_mr_{m-1} + r_m \\
 r_{m-1} &= q_{m+1}r_m + 0
 \end{aligned}$$

**Theorem 7.5**

Let  $R$  be a Euclidean domain,  $a, b \neq 0, a, b \in R$ .

1. The last nonzero remainder,  $r_m$ , in Euclidean algorithm is  $\gcd(a, b)$ .
2. Moreover,  $r_m = ax + by$  for  $x, y \in R$ . And  $x, y$  can be obtained from Euclidean algorithm.

**Proof:**

By going backwards in Euclidean algorithm, we obtain inductively that  $r_m \mid r_{m-1}, r_{m-2}, \dots, r_1, r_0$ ,  $r_m \mid a, b$ . This shows that  $(a, b) \subseteq (r_m)$ , which means  $r_m$  is a common divisor. It remains to show that  $(r_m) \subseteq (a, b)$ . We see that

$$\begin{aligned}
 r_0 &= a - q_0b \in (a, b) \\
 r_1 &= b - q_1r_0 \in (a, b) \\
 &\vdots \\
 &\quad \quad \quad \uparrow \\
 &\quad \quad \quad \in (a, b) \\
 r_m &= r_{m-2} - q_mr_{m-1} \in (a, b)
 \end{aligned}$$

Thus  $(r_m) \subseteq (a, b)$ .

Therefore  $(r_m) = (a, b)$ .  $\square$

## 7.4 Principal Ideal Domain

**Example:**

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\right\}$  is PID, but not Euclidean domain. To prove it is not ED, we follow the definition:  $\forall a, b \in R, a = qb + r, N(r) < N(b)$  or  $b = 0$ . Take  $b$  a non-unit, non-zero with minimal norm. Then every  $x$  can be written as  $x = qb + r, r = 0$  or  $r$  is a unit. If  $b$  is defined above, and we know units are  $\{\pm 1\}$ , then  $x = qb \pm 1$  or  $x = qb + 0$ .

Take  $2 = qb + r, r \in \{0, \pm 1\}$ . This gives us three possibilities:  $b \mid 2, b \mid 1, b \mid 3$ .

For the rest, check <https://math.stackexchange.com/a/23872> or page 282 of Dummit & Foote.

### Principal Ideal Domain

An integral domain in which every ideal is principal is called a Principal Ideal Domain (PID).

**Example:**

$\mathbb{Z}, F[x]$  for  $F$  a field.  $\mathbb{Z}[x]$  is not PID.

### Proposition 7.6

Let  $R$  be a PID,  $a, b \neq 0, a, b \in R$ . Then if  $(d) = (a, b)$ , then

1.  $d = \gcd(a, b)$ .
2.  $d = ax + by$  for  $x, y \in R$ .
3.  $d$  is unique up to a multiplication by a unit in  $R$ .

### prime ideal

An ideal  $I \subsetneq R$  is called a prime ideal if  $ab \in I \implies a \in I$  or  $b \in I$ .

**Example:**

$6\mathbb{Z}$  is not prime ideal as  $2 \times 3 \in 6\mathbb{Z}$  and  $2, 3 \notin 6\mathbb{Z}$ .

$7\mathbb{Z}$  is prime ideal.

**Remark:**

A prime  $p$  satisfies  $p \mid ab \implies p \mid a$  or  $p \mid b$ .

### Proposition 7.7

Every maximal ideal is prime.

**Proof:**

Maximal  $\Leftrightarrow R/I$  field  $\Rightarrow R/I$  integral domain  $\Leftrightarrow I$  prime. □

### Theorem 7.8

Every nonzero prime ideal in PID is a maximal ideal.

**Proof:**

Suppose there exists a maximal ideal  $(m)$  where  $m \in R$  such that a prime ideal  $(p) \subseteq (m) \subseteq R$ . Then  $p = rm$ . Then  $rm \in (p)$ . As  $(p)$  is prime ideal, thus either  $r \in (p)$  or  $m \in (p)$ .

If  $m \in (p)$ , then  $(m) \subseteq (p)$ , then  $(m) = (p)$ .

If  $r \in (p)$ , then  $r = sp$  for some  $s \in R$ . Sub it back,  $p = rm = spm$ . Then  $p(1 - sm) = 0$ . As  $p \neq 0$ , then  $sm = 1$ , thus  $s, m$  are units. Thus  $(m) = R$ .  $\square$

**Corollary 7.9**

$\mathbb{Q}[x]/(p(x))$  for  $p(x)$  irreducible (thus  $(p)$  is primal).  $\mathbb{Q}[x]/(p) \cong \mathbb{Q}(\alpha)$ , where  $\alpha$  is a root of  $p$ .

**Corollary 7.10**

If  $F[x]$  is a PID (ED), then  $F$  is a field.

**Proof:**

$(x)$  is an ideal. We know that  $F \cong F[x]/(x)$  is an integral domain. We also know that  $F$  is integral domain iff  $(x)$  is a prime ideal. As  $F[x]$  is PID, then  $(x)$  is also maximal. Thus we conclude that  $F[x]/(x) \cong F$  is a field.  $\heartsuit$

 $\square$ **Remark:**

In ED,  $\forall a, b \neq 0, a = qb - r, N(r) < N(b)$  or  $b \mid a$ .

The norm above generalizes to **Dedekind-Hasse norm**:  $N(0) = 0, N(a) > 0$  if  $a \neq 0$ . Such that  $\forall a, b \in R, a, b \neq 0, \exists s, t \in R : 0 < N(sa - tb) < N(b)$  or  $b \mid a$ .

**Proposition 7.11**

$R$  is PID iff  $R$  has a Dedekind-Hasse norm.

**Corollary 7.12**

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$  is PID.



## 7.5 Unique Factorization Domain

### irreducible/prime

Let  $R$  be an integral domain.

1. Let  $r \in R$ ,  $r \neq 0$ ,  $r$  not a unit. We say that  $r$  is irreducible, if  $r = ab \Rightarrow a$  or  $b$  is a unit of  $R$ .
2.  $p \in R$ , non-unit is called a prime, if  $p \mid ab \Rightarrow p \mid a$  or  $p \mid b$ .
- 2'. (alternatively)  $p$  is prime if  $(p)$  is a prime ideal.
3.  $a, b \in R$  are associated ( $a \sim b$ ) if  $a = ub$  for  $u$  a unit.

### Proposition 7.13

A prime is irreducible.

**Proof:**

Let  $p$  be prime  
and  $p = a \cdot b$ . Then  $p \mid ab$ ,  
then  $p \mid a$  or  $p \mid b$ . WLOG,  
assume  $p \mid a$ . Then  $a = px$ .  
Hence  $p = pxb$ . This  
implies  $xb = 1$ , then  
 $x, b$  are units.  
♡

□

**Example:**

$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ . We found that

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

are two factorizations into irreducibles, and

$$2 \nmid (1 + \sqrt{-5}) \quad \text{and} \quad 2 \nmid (1 - \sqrt{-5})$$

Note that  $N(a + b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z}$ . Then we observe

$$4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$$

Even better, we have

$$(6) = P_2^2 P_3 P'_3,$$

where  $P_2 = (2, 1 + \sqrt{-5})$ ,  $P_3 = (3, 2 + \sqrt{-5})$ ,  $P'_3 = (3, 2 - \sqrt{-5})$  are all prime ideals. In particular,

$$\begin{aligned} (2) &= P_2^2 \\ (3) &= P_3 P'_3 \\ (1 + \sqrt{-5}) &= P_2 P_3 \\ (1 - \sqrt{-5}) &= P_2 P'_3 \end{aligned}$$

**Theorem 7.14**

In PID, primes are precisely irreducibles. In other words, irreducible in PID is prime.

**Proof:**

Let  $r$  be an irreducible. We want to show if  $(r)$  is prime ideal. Let  $(r) \subseteq M = (m)$  for some ideal  $M$ . Then  $r = mx$ . Because  $r$  is irreducible, then either  $m$  or  $x$  is a unit. If  $m$  is a unit, then  $M = R$ . If  $x$  is a unit, then  $r \sim m$ , then  $(r) = (m)$ . This proves  $(r)$  is maximal. As this is PID, then  $(r)$  is prime ideal. Hence  $r$  is prime.

♡

□

**Unique Factorization Domain**

An integral domain  $R$  is called a UFD if every non-zero non-unit  $r \in R$  satisfies

1.  $p_1 p_2 \cdots p_k$  where  $p_i$ 's are irreducibles of  $R$ .
2. if  $r = q_1 q_2 \cdots q_m$ , with  $q_i$ 's irreducibles, then  $m = k$ , and there exists a permutation  $\pi$  of  $\{1, 2, \dots, k\}$ , such that  $p_i \sim q_{\pi(i)}$ .

**Example:**

A field is a UFD.

$\mathbb{Z}[x]$  is a UFD (if  $R$  is UFD, then  $R[x]$  is UFD)

PID is UFD.

$\mathbb{Z}[\sqrt{-5}]$  is NOT a UFD.

**Proposition 7.15**

In UFD, every irreducible is a prime.

**Proof:**

Let  $p$  be irreducible, let  $p \mid ab$ . I.e.,  $ab = px$ . Then we can write

$$(a_1 \cdots a_n)(b_1 \cdots b_m) = p(x_1 \cdots x_{m+n-1})$$

where  $a_i, b_i, p, x_i$  are irreducibles. By UFD property, WLOG assume  $p \sim a_i$ , then  $pu = a_i$  for  $u$  a unit, i.e.,  $p \mid a_i$ . Then

$$p(ua_1 \cdots a_{i-1}a_{i+1} \cdots a_m) = a$$

Hence  $p \mid a$ .

□

**Proposition 7.16**

Let  $a, b \neq 0$  in UFD. If

$$a = up_1^{e_1}p_2^{e_2}\cdots p_n^{e_n} \quad (7.1)$$

$$b = vp_1^{f_1}p_2^{f_2}\cdots p_n^{f_n} \quad (7.2)$$

with  $u, v$  units,  $e_i, f_i \geq 0$  integers,  $p_i$  primes. Then

$$d = p_1^{\min\{e_1, f_1\}} \cdots p_n^{\min\{e_n, f_n\}}$$

is a  $\gcd(a, b)$ .

**Proof:**

Obviously,  $d \mid a, d \mid b$ . In  $d, p_i^{\min\{e_i, f_i\}+1}$  if for some  $i$ , then it is not a divisor for both  $a, b$ . Thus the exponents have to be  $\leq \min\{e_i, f_i\}$ . If all  $\leq$  are  $=$ , then we obtain  $d$ . If not all  $\leq$  are strict, then we get something that divides  $d$ .  $\square$

**Example:**

$\mathbb{Z}[i]$  is UFD, but  $\mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$  is not UFD.

$$4 = 2 \cdot 2 = (-2i)(2i)$$

but  $i \notin \mathbb{Z}[2i]$ , so  $2 \sim (2i)$  or  $(-2i)$ .

Also  $2i$  is not a prime, because  $(2i)$  is not a prime ideal:

$$\mathbb{Z}[2i]/(2i) \cong \mathbb{Z}/4\mathbb{Z}$$

in which  $2 \times 2 = 0$ , which is not an integral domain. This isomorphism is obtained by

$$\phi(a + 2bi) = a \pmod{4}$$

**Theorem 7.17**

Every PID is UFD.

**Proof:**

Two steps:

1. Every nonzero non-unit element is a finite product of irreducibles.
2. Uniqueness.

Let  $r \neq 0$ , non-unit. Either  $r$  is irreducible, or  $r = r_1 \cdot r_2$ ,  $r_1, r_2$  non-units. Then  $r$  is irreducible or  $r = r_1 r_2$  ( $r_1, r_2$  are non-units). Then either  $r_1$  is irreducible or  $r_1 = r_{11} r_{12}$ ;  $r_2$  is irreducible or  $r_2 = r_{21} r_{22}$ . We continue this process, iteratively factor  $r$ . We want to show the factorization is finite.

Assume factorization does not end. Then we obtain an infinite chain  $C$ :

$$(r) \subseteq (r_1) \subseteq (r_{11}) \subseteq (r_{112}) \subseteq \cdots \subseteq R$$

which corresponds to an infinite chain of factorization. Then  $(m) = \bigcup_{(r_\alpha) \in C} (r_\alpha)$  is an ideal in PID. Since  $m \in (r_\alpha)$ , for some  $r_\alpha$  in chain, then  $(r_\alpha) = (m)$ . Then

$$(r) \subseteq (r_1) \subseteq \cdots \subseteq (r_\alpha) = (m) \subseteq (m) \subseteq \cdots \subseteq R$$

The chain stabilizes (Noether Domain). Contradicts infinite factorization.

Let  $r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$  for  $p_i, q_i$  irreducibles. WLOG, assume  $q_1 \mid p_1$  then  $p_1 = u q_1$  for  $u$  a unit. Then  $p_1 \sim q_1$ . Then

$$u q_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \implies (u p_2) \cdots p_n = q_2 \cdots q_m$$

Finish by induction on  $\min\{m, n\}$ . □

### Corollary 7.18

If  $R$  is a PID, then there exists a Dedekind-Hasse norm on  $R$ .

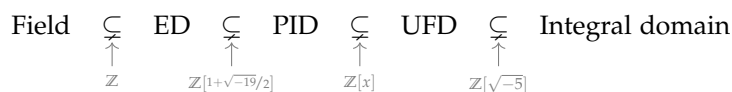
**Proof:**

Define the norm:  $N(0) = 0$  and  $N(p_1 p_2 \cdots p_k) = 2^k$  where  $p_1 p_2 \cdots p_k$  is unique factorization to irreducibles and  $p_i$ 's do not need to be distinct. We observe that  $N(ab) = N(a)N(b)$ , and  $N(a) > 0$  iff  $a \neq 0$ .

Let  $a, b \in R$ , then  $(a, b) = (r)$  for some  $r \in R$ , and we know  $r = \gcd(a, b)$ . Then there exist  $s, t \in R$  such that  $sa - tb = r$ . Taking norms  $N(sa - tb) = N(r)$ . Here  $r$  has less factors than  $a, b$ , thus  $N(r) < N(b)$  because  $r \mid b$ . □

**Remark:**

$\gcd$  in UFD always exist, but consider an example. In  $\mathbb{Z}[x]$ ,  $\gcd(2, x) = 1$ , but  $(2, x) \subseteq (1) = \mathbb{Z}[x]$ . And there don't exist  $\alpha, \beta$  s.t.  $1 = \alpha \cdot 2 + \beta \cdot x$ , namely  $\gcd$  is not a combination of  $a, b$  in this case.



# Polynomial Rings

Previously: If  $R[x]$  is PID (or ED), then  $R$  is a field.

Remember: If  $R$  is ID, then  $R[x]$  is ID.

$$R[x_1, x_2, \dots, x_n]$$

For commutative ring  $R$  with identity,  $x_1, \dots, x_n$  commuting variables, we have

$$R[x_1, x_2, \dots, x_n] = (R[x_1, x_2, \dots, x_{n-1}])[x_n]$$

## Proposition 8.1

Let  $I$  be an ideal in commutative ring  $R$ , with identity. Then  $(R/I)[x] \cong R[x]/(I)$ , where  $(I) = I[x]$  is in  $R[x]$ . Moreover, if  $I$  is a prime ideal in  $R$ , then  $(I) = I[x]$  is a prime ideal in  $R[x]$ .

**Example:**

$$(\mathbb{Z}_5)[x] \cong \mathbb{Z}[x]/5\mathbb{Z}[x]$$

**Proof:**

Consider a homomorphism  $\phi : R[x] \rightarrow (R/I)[x]$  where  $\phi$  is a coefficient reduction mod  $I$ . To check  $\phi$  is a homomorphism, we want to check if  $\phi(pq) = \phi(p)\phi(q)$ . At  $x^k$  of  $p(x)q(x)$ , after  $\phi$  applied to  $\sum_{i=0}^k p_i q_{k-i}$ , we get  $(\sum p_i q_{k-i}) \bmod I = \sum_{i=0}^k (p_i \bmod I)(q_{k-i} \bmod I)$ . We observe that  $\ker \phi = I[x]$ . We also see that  $\phi(R[x]) = (R/I)[x]$ , which is just operations.

$I$  prime ideal, then  $R/I$  ID, then  $(R/I)[x]$  ID, then  $R[x]/I[x]$  ID, thus  $I[x]$  is prime ideal.  $\square$

## 8.1 Polynomial rings over fields

Recall norm on  $R[x]$ :  $N(p(x)) = \deg(p)$ .

### Theorem 8.2

Let  $F$  be a field, then  $F[x]$  is a ED. Namely, if  $a(x), b(x) \in F[x]$ , then there exists unique  $q, r \in F[x]$  such that  $a(x) = b(x)q(x) + r(x)$  with  $\deg(r) < \deg(b)$  or  $r = 0$ . (if  $F \subseteq E$ , then  $F[x] \subseteq E[x]$ ), where  $E$  is a ED.

**Proof:**

By induction for existence.

1. If  $\deg(a) < \deg(b)$ , then  $r = a, q = 0$ .
2. If  $\deg(a) \geq \deg(b)$ , we can write

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \\ b(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0 \end{aligned}$$

where  $m \leq n$ .

Then the polynomial  $\tilde{a}(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$  and  $\deg(\tilde{a}) < \deg(b)$ . Then there exists  $\tilde{q}, \tilde{r}$  such that  $\tilde{a}(x) = \tilde{q}(x)b(x) + \tilde{r}(x)$  with  $\deg(b) > \deg(\tilde{r})$ . Sub in  $a(x)$ , we get

$$a(x) = \left( \tilde{q}(x) + \frac{a_n}{b_m} x^{n-m} \right) b(x) + \tilde{r}(x)$$

Note that  $\frac{a_n}{b_m} = a_n b_m^{-1}$  is well-defined because  $F$  is a field.

As for the uniqueness, assume that  $a = qb + r = q'b + r'$ . Subtracting these two, we have

$$0 = b(x)(q(x) - q'(x)) + (r(x) - r'(x))$$

where  $\deg(r - r') < \deg(b)$ . Then

$$b(x)(q(x) - q'(x)) = (r(x) - r'(x)) = 0$$

Because integral domain,

$$q(x) - q'(x) = r(x) - r'(x) = 0$$

Thus  $q(x) = q'(x)$  and  $r(x) = r'(x)$ . □

### Corollary 8.3

If  $F$  is a field, then  $F[x]$  is a UFD and a PID.

**Example:**

$\mathbb{Z}[x]$  is not a PID because  $(2, x)$  is not principal.

$\mathbb{Q}[x]$  is a PID as  $\mathbb{Q}$  is a field, then  $(2, x) = (1) = \mathbb{Q}[x]$ .

$\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x] \cong \mathbb{Z}_p[x]$ . What happens to  $(2, x)$  in  $(\mathbb{Z}/p\mathbb{Z})[x]$ . If  $p = 2$ , then  $(2, x) = (x)$  in  $\mathbb{Z}_2[x]$ . If  $p > 2$ , then 2 is invertible, then  $(2, x) = (1)$  in  $\mathbb{Z}_p[x]$ .

## 8.2 Polynomial rings that are UFDs

### Proposition 8.4: Gauss' Lemma

Let  $R$  be a UFD with a field of fraction  $F$ , and let  $p(x) \in R[x]$ . If  $p(x)$  is irreducible in  $R[x]$ , then  $p(x)$  is also irreducible in  $F[x]$ . (i.e., if  $p(x)$  is reducible in  $F[x]$ , it is also reducible in  $R[x]$ )

More precisely, if  $p(x) = a(x)b(x)$  in  $F[x]$ , then  $\exists r, s \in F$  such that  $p(x) = \underbrace{(ra(x))}_{\in R[x]} \underbrace{(sb(x))}_{\in R[x]}$ , and

nothing more, with respect to  $a(x), b(x)$ .

**Proof:**

Prove by contrapositive. Let  $p(x) = a(x)b(x)$  in  $F[x]$ . We can multiply the denominator, then

$$dp(x) = A(x)B(x) \quad \text{in } R[x] \quad (*)$$

If  $d$  is a unit of  $R$ , then  $p(x) = d^{-1}A(x)B(x)$  in  $R[x]$ .

If  $d$  is not a unit, then  $d = p_1 p_2 \cdots p_k$  is a unique factorization into irreducible primes. Note that  $(p_1)$  is a prime ideal of  $R$ , then  $(R/(p_1))[x]$  is ID. We then take  $(\text{mod } p_1)$  on both sides of  $(*)$ , then  $0 = \overline{A(x)} \overline{B(x)}$ , where  $\overline{A(x)}, \overline{B(x)} \in (R/(p_1))[x]$ . Then  $\overline{A(x)} = 0$  or  $\overline{B(x)} = 0$  as in ID. I.e., either  $A(x)$  and  $B(x)$  are in  $(p_1)$ . I.e., either  $A(x)$  and  $B(x)$  are multiples of  $p_1$ . Then WLOG  $dp(x) = p_1 \cdots p_k p(x) = (p_1 A'(x))B(x)$ , then  $p_2 \cdots p_k p(x) = A'(x)B(x)$  in  $R[x]$ .

Inductively, we'll have  $p(x) = \tilde{A}(x)\tilde{B}(x)$  in  $R[x]$ . I.e.,  $p(x)$  is reducible in  $R[x]$ . By contrapositive, the first part holds.

If we write  $\tilde{A}(x) = sa(x)$ ,  $\tilde{B}(x) = tb(x)$ , then  $p(x) = (sa(x))(tb(x))$ . Note 1 exists in an UFD.  $\square$

**Example:**

In  $\mathbb{Q}[x]$ ,  $x^2 = 2x \cdot \frac{1}{2}x$ . We cannot get a factorization in  $\mathbb{Z}[x]$  by integer multiples. We can only have  $x^2 = x \cdot x = (-x)(-x)$ .

Does reducibility in  $R[x]$  implies reducibility in  $F[x]$ ? No. In  $\mathbb{R}[x]$ ,  $p(x) = 2 \cdot x$  has two irreducibles. In  $\mathbb{Q}[x]$ ,  $p(x) = 2 \cdot x$  only has one irreducible as 2 is a unit. Reducibility needs (at least) two irreducible factors.

**Corollary 8.5**

Let  $R$  be UFD,  $F$  be its field of fractions and  $p(x) \in R[x]$ . Let gcd of the coefficients of  $p(x)$  be 1. Then  $p(x)$  is irreducible if and only if it is irreducible in  $F[x]$ .

**Proof:**

$\Rightarrow$  is from Gauss' lemma. For  $\Leftarrow$ , suppose  $p(x)$  is reducible in  $R[x]$ . Let  $p(x) = a(x)b(x)$ , then neither of  $a(x), b(x)$  are constants, otherwise gcd of the coefficients of  $p(x)$  would be this constant. So neither  $a(x)$  and  $b(x)$  is a unit. Then  $p(x)$  is reducible in  $F[x]$ .  $\square$

**Theorem 8.6**

$R$  is a UFD if and only if  $R[x]$  is a UFD.

**Proof:**

Suppose  $R[x]$  is a UFD, then constant polynomials has a unique factorization.

Now suppose  $R$  is a UFD. Assume  $p(x) \in R[x]$ , we want to factorize  $p(x)$  into irreducibles. Let  $p(x) = dp'(x)$ , where  $d \in R$  and gcd of coefficients of  $p'(x)$  is 1.

Since  $d \in R$ , which is a UFD, then  $d$  has a unique factorization. It remains to show that  $p(x)$  can be factored uniquely. Factor  $p'(x) = g_1(x)g_2(x) \cdots g_r(x)$  in  $F[x]$ , where  $F[x]$  is the field of fractions of  $R[x]$ . By multiplying  $c_1, c_2, \dots, c_r \in F$ , we get a factorization in  $R[x]$ , which is the same trick in the proof of Gauss' lemma. Then

$$p'(x) = (c_1 g_1(x))(c_2 g_2(x)) \cdots (c_r g_r(x)),$$

and  $c_i g_i(x)$ 's are irreducibles in  $F[x]$ . We want to show  $c_i g_i(x)$ 's are irreducibles in  $R[x]$ . Since  $\gcd(\text{coeff. of } p'(x)) = 1$ , then  $\gcd(c_1, c_2, \dots, c_r) = 1$ , otherwise, we can still factor out a constant from  $p'(x)$  and move it to  $d$ . This shows that  $p(x)$  can be written as a finite product of irreducibles

in  $R[x]$ .

Now suppose in  $R[x]$ ,

$$p(x) = q_1(x) \cdots q_k(x) = q'_1(x) = \cdots q'_r(x)$$

Since  $\gcd(\text{coeffs}) = 1$ , then irreducibility in  $R[x]$  implies irreducibility in  $F[x]$ . This implies  $k = r$  and  $q_i(x) \sim q'_{\pi(i)}(x)$  in  $F[x]$ . Then  $\exists \frac{a}{b} \in F[x]$  such that  $b \cdot q_i(x) = a \cdot q'_{\pi(i)}(x)$ . The gcd of LHS coefficients is  $b$  and RHS coefficients is  $a$ . Thus we must have  $a = ub$  for  $u$  a unit in  $R$ . Then  $q_i(x) = \frac{ub}{b} q'_{\pi(i)}(x)$  and  $\frac{ub}{b}$  is a unit of  $R$ . This proves that  $R[x]$  is a UFD.  $\square$

### Corollary 8.7

$\mathbb{Z}[x]$  is a UFD that is not a PID.

### Example:

What about Gauss' lemma for non UFD?

$R = \mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$  is an ID.

$F = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$  is an ID.

$x^2 + 1 = (x + i)(x - i)$  in  $F[x]$ , but  $x^2 + 1$  is irreducible in  $R[x]$ .

## 8.3 Irreducibility Criteria

### root

$\alpha \in F$  is a root of  $p(x)$  if  $p(\alpha) = 0$ .

### Proposition 8.8

Let  $F$  be a field and  $p(x) \in F[x]$ , then  $p(x)$  has a factor of degree one if and only if  $p(x)$  has a root in  $F$ .

### Proof:

If  $p(x)$  has a factor of degree one, we can assume that the factor is  $(x - \alpha)$ . Then  $p(x) = \underbrace{(1 \cdot x - \alpha)}_{\in F[x]} q(x)$ , so  $p(\alpha) = 0 \cdot q(\alpha) = 0$ .

On the other hand, if  $p(\alpha) = 0$ , then  $p(x) = q(x)(x - \alpha) + r(x)$  where  $\deg(r) = 0$  ( $r$  constant polynomial) or  $r(x) = 0$ . As  $0 = p(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha)$ , thus  $r(\alpha) = 0$ . Hence we conclude  $p(x) = q(x)(x - \alpha)$ .  $\square$

### Corollary 8.9

Suppose  $p(x) \in F[x]$  is of degree 2 or 3.  $p(x)$  is irreducible if and only if  $p(x)$  does not have a root in  $F$ .

### Proof:

If  $p(x) = a(x) \cdot b(x)$ , nonconstant  $a(x), b(x)$ , then  $\deg(a), \deg(b) < \deg(p)$ .  $\square$

### Example:

In  $\mathbb{R}[x]$ ,  $(x^2 + 1)(x^2 + 1)$  is reducible, but does not have a root in  $\mathbb{R}$ .



**Proposition 8.10**

Let  $p(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ . If  $\frac{r}{s} \in \mathbb{Q}$  is a root of  $p$ , with  $\gcd(r, s) = 1$ , then  $r \mid a_0$  and  $s \mid a_n$ .

**Proof:**

We just plug in, and get

$$\begin{aligned} 0 &= a_n \left(\frac{r}{s}\right)^n + \cdots + a_1 \frac{r}{s} + a_0 \\ 0 &= a_n r^n + \cdots + a_1 r s^{n-1} + a_0 s^n \\ a_n r^n &= -s(\cdots) \end{aligned}$$

then  $s \mid a_n r^n$ , then  $s \mid a_n$  from  $\gcd(s, r) = 1$ .

Analogously for  $r \mid a_0$ . □

**Example:**

$p = x^3 - 3x - 1 \in \mathbb{Z}[x]$  is reducible if and only if it has root in  $\mathbb{Z}$ . A root  $r \in \mathbb{Z}$  of  $p$  divides  $-1$ , then  $r = \pm 1$ . Then we can check if  $r$  is a root.

**Example:**

Similarly we can check reducibility for  $x^2 - p, x^3 - p$  for  $p$  prime.

Consider an obvious fact:  $f$  reducible in  $\mathbb{Z}[x]$ , then reducible in  $(\mathbb{Z}/m\mathbb{Z})[x]$ . Now the following proposition generalizes this fact.

**Proposition 8.11**

Let  $I$  be a proper ideal in an integral domain  $R$ . Let  $p(x)$  be a nonconstant, monic polynomial in  $R[x]$ . Then if  $\overline{p(x)} \in (R/I)[x]$  cannot be factored into two polynomials of smaller degree, then  $p(x)$  is irreducible in  $R[x]$ .

**Proof:**

Suppose  $p(x) = a(x)b(x) \in R[x]$ . Then we know that  $a(x)$  and  $b(x)$  are monic, and nonconstant. Reducing the coefficients modulo  $I$  gives a factorization in  $(R/I)[x]$  with nonconstant factors by Proposition 8.1. □

**Example:**

$x^2 + x + 1$  in  $\mathbb{Z}_2[x]$  is irreducible because it has no root in  $\mathbb{Z}_2$ . Thus irreducible in  $\mathbb{Z}[x]$ .

$x^2 + 1 = (x + 1)(x + 1)$  is reducible in  $\mathbb{Z}_2[x]$ .  $x^2 + 1$  is irreducible in  $\mathbb{Z}_3[x]$ , thus  $x^2 + 1$  is irreducible in  $\mathbb{Z}[x]$ .

**Example:**

$x^4 + 1$  is reducible in  $\mathbb{Z}_p[x]$  for any prime  $p$ .

$x^4 - 72x^2 + 4$  is reducible in  $\mathbb{Z}_m[x]$  for any  $m \in \mathbb{N}$ .

But they are irreducible in  $\mathbb{Z}[x]$ .

**Theorem 8.12: Eisenstein's criterion**

Let  $P$  be a prime ideal of an integral domain  $R$ . Let  $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$  such that  $a_{n-1}, \dots, a_0 \in P$ , and  $a_0 \notin P^2 = P \cdot P$ . Then  $p(x)$  is irreducible.

**Proof:**

Assume we have a factorization  $p(x) = a(x)b(x)$  in  $R[x]$ . Then in  $(R/P)[x]$ , we reduce the coefficients mod  $P$ :  $x^n = \overline{a(x)}\overline{b(x)}$ . Then the constant terms of  $\overline{a(x)}$  and  $\overline{b(x)}$  are zero, i.e., the constant terms of  $a(x)$  and  $b(x)$  are elements of  $P$ . But then  $a_0$  would be the product of these two would be an element of  $P^2$ . Contradiction.  $\square$

**Example:**

$x^4 + 10x + 5$  in  $\mathbb{Z}[x]$  is irreducible. Consider prime ideal  $P = (5)$ .

**Example:**

$x^n - a \in \mathbb{Z}[x]$  is irreducible for any  $a \in \mathbb{Z}$  such that for some prime  $p$  with  $p \mid a$  and  $p^2 \nmid a$ .

**Example:**

For  $p$  prime,

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is called  $p$ -th cyclotomic polynomial.

If  $f(x) = g(x)h(x)$ , then  $f(x+1) = g(x+1)h(x+1)$ . We then can investigate reducibility of  $\Phi_p(x+1)$ :

$$\Phi_p(x+1) = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p$$

Since all the coefficients except the first are divisible by  $p$  by the Binomial Theorem. As before, this shows  $\Phi_p(x)$  is irreducible in  $\mathbb{Z}[x]$ .

# Field Theory

## 9.1 Basic Theory of Field Extensions

### field extension

Let  $F$  be a field. A field  $K$  is called an extension of  $F$ , if  $K$  contains an isomorphic copy of  $F$ . We will denote by  $K/F$ .

This is not a quotient.

**Fact**  $x^2 + 1 \in \mathbb{R}[x]$ , but no root in  $\mathbb{R}$ . Make an extension of  $\mathbb{R}$  so that  $\mathbb{C}$  has a field:  $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ .

### Theorem 9.1

Let  $F$  be a field,  $p(x) \in F[x]$  and irreducible polynomial. Then there exists a field  $K$  containing an isomorphic copy of  $F$  in which  $p(x)$  has a root.

Identifying  $F$  with this isomorphic copy shows that there exists an extension of  $F$  in which  $p(x)$  has a root.

### Proof:

Consider the quotient  $K = F[x]/(p(x))$ . As  $p$  is irreducible in PID  $F[x]$ ,  $(p)$  is maximal. Hence  $K$  is a field. Thus  $K$  contains an isomorphic copy of  $F$ . Then we have the canonical projection  $\pi$  of  $F[x]$  to the quotient  $F[x]/(p(x))$  restricted to  $F \subseteq F[x]$  gives a homomorphism:

$$\phi = \pi|_F: F \rightarrow K$$

Then we note that it is a zero map because it maps identity 1 of  $F$  to the identity 1 of  $K$ . Thus  $\phi$  is injective. (or apply Corollary 4.2) Thus  $\phi(F) \cong F$  is an isomorphic copy of  $F$  contained in  $K$ . We identify  $F$  with its isomorphic image in  $K$  and view  $F$  as a subfield of  $K$ . Denote  $\bar{x} = \pi(x)$  the image of  $x$  in the quotient  $K$ , then

$$\begin{aligned} p(\bar{x}) &= \overline{p(x)} && \text{(since } \pi \text{ is a homomorphism)} \\ &= p(x)(\text{mod } p(x)) && \text{in } F[x]/(p(x)) \\ &= 0 && \text{in } F[x]/(p(x)) \end{aligned}$$

so that  $K$  does indeed contain a root of  $p$ . Then  $K$  is an extension of  $F$  in which  $p$  has a root.  $\square$

**degree/index of a field extension**

The degree (or relative degree or index) of a field extension  $K/F$ , denoted  $[K : F]$ , is the dimension of  $K$  as a vector space over  $F$  (i.e.,  $[K : F] = \dim_F K$ ). The extension is said to be finite if  $[K : F]$  is finite and is said to be infinite otherwise.

**Theorem 9.2**

Let  $p(x) \in F[x]$  be an irreducible polynomial of degree  $n \geq 1$  and let  $K$  be the field  $F[x]/(p(x))$ . Let  $\theta = x \bmod (p(x)) \in K$ . Then the elements

$$1, \theta, \theta^2, \dots, \theta^{n-1}$$

are a basis for  $K$  over  $F$ , so the degree of extension is  $n$ , i.e.,  $[K : F] = n$ . Hence

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}$$

consists of all polynomials of degree  $< n$  in  $\theta$ .

From linear algebra,  $\mathbb{C}$  is a vector space over  $\mathbb{R}$ . If we multiply a  $\mathbb{C}$  by  $\mathbb{R}$ , it is still  $\mathbb{C}$ , so it's well defined. Basis in this case is  $1, i$ .  $\dim(\mathbb{C}) = 2$ . Thus  $[\mathbb{C} : \mathbb{R}] = 2$ .

**Example:**

$\mathbb{R}$  is a vector space over  $\mathbb{Q}$ .  $\mathbb{R}$  are the vectors,  $\mathbb{Q}$  are scalars. It is infinite dimensional vector space as it has no finite basis. This is because  $\mathbb{R}$  is uncountable.

# Index

---

## A

additive quotient ..... 13

## B

Bézout domain ..... 28

## C

comaximal ..... 25

## D

degree/index of a field extension ..... 43  
division ring ..... 8

## E

Euclidean domain ..... 27

## F

field ..... 8  
field extension ..... 42

## G

greatest common divisor ..... 28

## I

ideal ..... 12

integral domain ..... 8  
irreducible/prime ..... 32

## M

maximal ideal ..... 18

## N

norm ..... 27

## P

partial order ..... 19  
prime ideal ..... 30  
Principal Ideal Domain ..... 30

## Q

quotient ring ..... 13

## R

ring ..... 6  
ring homomorphism ..... 11  
root ..... 39

## S

subring ..... 9

## U

Unique Factorization Domain ..... 33

unit ..... 9

Z

zero divisor ..... 7