

# MATH 593 - Ring

A Ressegetes Stery

November 21, 2023

## Contents

<b>1</b>	<b>Ring homomorphism, Quotient Ring</b>	<b>2</b>
<b>2</b>	<b>Ring of Fractions</b>	<b>3</b>
2.1	Localization of a Ring . . . . .	4
<b>3</b>	<b>Polynomial Rings</b>	<b>5</b>
<b>4</b>	<b>Ideals</b>	<b>7</b>
<b>5</b>	<b>Noetherian Ring</b>	<b>9</b>
<b>6</b>	<b>Euclidean Domain, PIDs and UFDs</b>	<b>10</b>

# 1 Ring homomorphism, Quotient Ring

**Definition 1.1** (Ring Homomorphism). Let  $X, Y$  be rings. A **Ring Homomorphism** is a map  $f : X \rightarrow Y$  satisfying the following properties:

- $f(1) = 1$ .
- $\forall x_1, x_2 \in X, f(x_1) + f(x_2) = f(x_1 + x_2)$ .
- $\forall x_1, x_2 \in X, f(x_1 x_2) = f(x_1) f(x_2)$

**Definition 1.2** (Quotient Ring). Let  $R$  be a ring and  $I \subseteq R$  a two-sided ideal. The **Quotient Ring**  $(R/I)$  is defined as  $(R/\sim)$  with an equivalence relation  $\sim$  where  $a \sim b$  if and only if  $a - b \in I$ . Elements in  $(R/I)$  are denoted as  $\bar{a}$ , where  $\bar{a} = \bar{b}$  if and only if  $a \sim b$ .

The natural homomorphism  $\pi_I : R \rightarrow (R/I)$  is defined as  $\pi(a) = \bar{a}$ , which satisfies the *universal property of quotient rings*:

**Theorem 1.1** (Fundamental Theorem of Ring Homomorphisms). Let  $\varphi : R \rightarrow S$  be a ring homomorphism,  $I$  a two-sided ideal s.t.  $I \subseteq \ker \varphi$ , and  $\pi$  be the natural ring homomorphism from  $R$  to  $(R/I)$ . Then there exists a unique ring homomorphism  $f : R/I \rightarrow S$  s.t. the following diagram commutes, i.e.  $\varphi = f \circ \pi$ .

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow \pi & \uparrow f \\ & & R/I \end{array}$$

*Proof.* It suffices to prove that  $f$  exists and is unique, and verify that  $f$  is indeed a ring homomorphism.

- **Uniqueness.** By the requirement that  $f$  should make the diagram commute,  $f(\bar{a}) = \varphi(a)$ ,  $\forall a \in R$ . Uniqueness of  $f$  follows from the fact that  $\varphi$  maps every element in  $R$  to a unique element in  $S$ .
- **Existence.** It suffices to verify that  $f$  is well-defined, i.e. does not vary w.r.t. change of representative in  $(R/I)$ . For all  $a, b \in R$  s.t.  $\bar{a} = \bar{b}$ ,  $(a - b) \in I \implies \varphi(a - b) = 0 \implies \varphi(a) = \varphi(b)$  since  $\varphi$  is a ring homomorphism. By the uniqueness of  $f$  it is specified that  $f(\bar{a}) = \varphi(a)$ , which implies that for all  $\bar{a} = \bar{b} \in (R/I)$ ,  $f(\bar{a}) = \varphi(a) = \varphi(b) = f(\bar{b})$ .
- **$f$  is indeed a homomorphism.** This follows from the fact that  $\varphi$  is a ring homomorphism.

□

## 2 Ring of Fractions

**Definition 2.1** (Multiplicative System). A subset  $S \subseteq R$  for a ring  $R$  is a **multiplicative system** if  $1 \in S$ , and  $\forall s_1, s_2 \in S, s_1 \cdot s_2 \in S$ , where  $\cdot$  is the multiplication in  $R$ .

**Definition 2.2** (Ring of Fractions). Let  $R$  be a commutative ring, with  $S \subseteq R$  a multiplicative subset, the **ring of fraction**  $S^{-1}R$  is defined as  $R \times S / \sim$ , where  $(s_1, r_1) \sim (s_2, r_2)$  if and only if there exists  $t \in R$  s.t.  $t(s_1 r_2 - s_2 r_1) = 0$ .  $(s, r) \in S^{-1}R$  is denoted as  $\frac{s}{r}$ . The definition of operations follows directly from analogy of that in  $\mathbb{Q}$ .

The natural homomorphism (inclusion map) from  $R$  to  $S^{-1}R$  is defined as  $r \mapsto \frac{r}{1}$ .

**Remark 2.1.** If  $R$  is an integral domain, then  $(s_1, r_1) \sim (s_2, r_2)$  iff  $s_1 r_2 = s_2 r_1$ , as for  $\mathbb{Q}$ .

**Remark 2.2.** If  $R$  is not an integral domain, and  $S$  contains zero divisors, then the inclusion map ceases to be injective, as choosing  $t$  s.t. it satisfies  $ts_1 = ts_2 = 0$  for some  $s_1, s_2$  that are zero divisors gives  $\varphi(s_1) = \varphi(s_2)$ . Changing  $R$  to an integral domain guarantees that the inclusion map  $\varphi$  is injective.

**Proposition 2.1.**  $\sim$  is an equivalence relation.

*Proof.* It is clear that  $\sim$  is reflexive and symmetric. For transitivity, consider  $(s_1, r_1) \sim (s_2, r_2) \wedge (s_2, r_2) \sim (s_3, r_3)$ . That is, there exists some  $t_1, t_2 \in R$  s.t.

$$\begin{cases} t_1(s_1 r_2 - s_2 r_1) = 0 \\ t_2(s_2 r_3 - s_3 r_2) = 0 \end{cases} \implies t_1 t_2 (s_1 r_2 s_3 - s_2 r_1 s_3) = t_1 t_2 (s_1 s_2 r_3 - s_2 r_1 s_3) = t_1 t_2 s_2 (s_1 r_3 - s_3 r_1) = 0$$

□

**Remark 2.3.** Notice that if  $s \in S$ , then  $\frac{s}{a}$  for  $a \in R$  is invertible. This tends more to a field, with more elements being “reachable” via multiplying an element from one side. A direct consequence is that less ideals exist in  $S^{-1}R$ , with ideals in  $R$  whose generators differ by a factor that divides  $s$  being identified in  $S^{-1}R$ .

**Remark 2.4.** It is required that  $R$  is commutative is to preserve the most structures from  $R$ , i.e. ensure that  $S^{-1}I$  is an ideal for all ideals in  $R$ . This is due to the addition in action:

$$\forall \frac{r_1}{s_1}, \frac{r_2}{s_2} \in S^{-1}R, \quad \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + s_1 r_2}{s_1 s_2}$$

which indicates that  $S^{-1}I$  is a two-sided ideal if and only if  $I \subseteq R$  is a two-sided ideal. For one-sided (left/right) ideal the property is not fully inherited.

**Theorem 2.1** (Universal Property of Ring of Fractions). Suppose  $R$  and  $T$  are commutative rings, with  $\varphi$  the inclusion of  $R$  into  $S^{-1}R$ . Then for  $f : R \rightarrow T$  s.t.  $\forall s \in S, f(s)$  is invertible in  $T$ , there exists a unique ring homomorphism  $g$  s.t.  $f = g \circ \varphi$ , i.e. make the following diagram commute:

*Proof.* Adopt the same strategy as in the previous section:

- **Existence.** For all  $\frac{a}{s} \in S^{-1}R$ ,  $g(\frac{a}{s}) := f(a)(f(s))^{-1}$  which is well-defined since  $f$  is required to map all elements in  $S$  to invertible elements.  $g$  being a ring homomorphism follows from the fact that  $f$  is a ring homomorphism.

$$\begin{array}{ccc}
 R & \xrightarrow{\varphi} & S^{-1}R \\
 & \searrow f & \downarrow g \\
 & & T
 \end{array}$$

- **Uniqueness.** Follows from specifying  $g(\frac{a}{s}) := f(a)(f(s))^{-1}$ .

□

**Remark 2.5.** If  $S := R \setminus \{0\}$ , then  $S^{-1}R$  is the whole field, with localization equivalent to completion of inverse of  $R$ .

## 2.1 Localization of a Ring

**Definition 2.3.** A commutative ring  $R \neq \{0\}$  is **local** if it admits a unique maximal ideal  $M$ . Local rings are denoted by a pair  $(R, M)$ .

**Example 2.1.** Let  $R$  be a commutative ring, with  $\mathfrak{p} \subseteq R$  a prime ideal. Let  $S = R \setminus \mathfrak{p}$  be a multiplicative system. Then the ring  $S^{-1}R$  is local, with the maximal ideal of it being  $S^{-1}\mathfrak{p}$ . This results from the fact that  $S^{-1}I$  is an ideal if and only if  $I$  is an ideal in  $R$ . Further since  $\mathbb{Z}$  is a PID (see next section), all prime ideals are maximal,  $S^{-1}\mathfrak{p}$  is indeed maximal. The fact that there is only one such maximal ideal results from that all other primes are in  $S$ , i.e.  $S^{-1}\mathfrak{p}' = S^{-1}R$  for all  $\mathfrak{p}' \neq \mathfrak{p}$ .

**Proposition 2.2.** Let  $R \neq \{0\}$  be a commutative ring. Then  $R$  being local if and only if for all  $a \in R$ , either  $a$  is invertible or  $(1 - a)$  is invertible. In this case, the maximal ideal  $M$  is the set of all non-invertible elements.

*Proof.* Proceed by showing implication in both directions:

$\Rightarrow$ : Suppose that  $(R, M)$  is the local ring of interest. Proceed by showing a contradiction: suppose that both  $a$  and  $(1 - a)$  are non-invertible. Then since  $R$  is local  $(a) \subseteq M$ ,  $(1 - a) \subseteq M$  indicating that  $1 \in M$  which is a contradiction. In this case for all  $a$  non-invertible,  $(a) \subseteq M$ , which implies that  $M$  is the set of all non-invertible elements.

$\Leftarrow$ : Define set  $M := \{a \in R \mid \forall x \in R, ax \neq 1\}$ . By construction if  $M$  is an ideal then it must be maximal, as including an invertible element expands the ideal to the whole ring. Verify that  $M$  is indeed an ideal:

- *Closed with addition.* Proceed via showing that the contraposition. Suppose that there exists  $a, b \in R$  s.t. both  $a$  and  $b$  are non-invertible, but there exists some  $c \in R$  s.t.  $c(a + b) = 1$ . Then  $ca = 1 - (cb)$  is non-invertible, which implies that  $1 - ca$  is invertible. But notice  $1 - ca = cb$  is also non-invertible, which is a contradiction.
- *Absorption with multiplication.* This simply results from the fact that a non-invertible element multiplied by a unit is still non-invertible.

Further notice that this is indeed the only maximal ideal, as for all  $u \in R \setminus M$ , it is invertible, i.e. for all ideals  $I \subseteq R$ ,  $u \in I \implies 1 \in I \implies I = R$ . Therefore  $(R, M)$  is local.

□

### 3 Polynomial Rings

**Definition 3.1** (R-algebra). Let  $R$  be a ring. Then a ring  $S$  is an  **$R$ -algebra** for the specific  $R$  mentioned if there exists a ring homomorphism  $\varphi : R \rightarrow S$  s.t.  $\forall r \in R, s \in S, \varphi(r)s = s\varphi(r)$ . When the homomorphism needs to be specified, the algebra is often denoted as a pair  $\langle S, \varphi \rangle$

**Remark 3.1.** An  $R$ -algebra is a two-sided  $R$ -module, which can be regarded as a generalization of the structure in  $R$ .  $R$  itself is not necessarily commutative, which implies that the associated homomorphism maps  $R$  to the center of  $S$ .

**Definition 3.2** (Morphism of  $R$ -algebras). Let  $\langle R_1, f_1 \rangle, \langle R_2, f_2 \rangle$  be  $R$ -algebras. A **Morphism of  $R$ -algebras** is a ring homomorphism  $\varphi : R_1 \rightarrow R_2$  s.t. the following diagram commute; i.e.  $f_2 = \varphi \circ f_1$ :

$$\begin{array}{ccc} R & \xrightarrow{f_1} & R_1 \\ & \searrow f_2 & \downarrow \varphi \\ & & R_2 \end{array}$$

**Definition 3.3** ( $R$ -subalgebra). Let  $\langle S, f_s \rangle$  be a  $R$ -algebra for  $R$  a ring.  $\langle T, f_t \rangle$  is a  **$R$ -subalgebra** of  $S$  if  $T$  is a  $R$ -algebra, with  $f_t(R) \subseteq S$ ; and there exists a morphism  $\varphi$  from  $T$  to  $S$ , i.e.  $\varphi$  makes the following diagram commute:

$$\begin{array}{ccc} R & \xrightarrow{f_t} & T \\ & \searrow f_s & \downarrow \varphi \\ & & S \end{array}$$

**Definition 3.4** (Polynomial Ring). Let  $R$  be a commutative ring. The **polynomial ring of  $R$** , denoted  $R[x]$ , is defined as

$$R[x] := \left\{ \sum_{i=0}^n c_i x^i \mid n \in \mathbb{N}, c_i \in R \right\}$$

with the addition and multiplication the same as in polynomials over  $\mathbb{Z}$ . The natural inclusion from  $R$  to  $R[x]$  is defined as  $r \mapsto r$  which is a polynomial of degree 0.

**Remark 3.2.** If  $R$  is a domain, then  $R[x]$  is also a domain (consider the product of terms with highest degree); where  $\deg(fg) \leq \deg(f) + \deg(g)$ .

**Theorem 3.1** (Universal Property of Polynomial Ring). Let  $R$  be a ring and  $\langle S, f \rangle$  an  $R$ -algebra, and  $\varphi$  be the inclusion map from  $R$  to  $R[x]$ . For all  $s \in S$ , there exists a unique morphism of  $R$ -algebra  $g : R[x] \rightarrow S$  s.t.  $g(x) = a$ , and the following diagram commutes, i.e.  $f = g \circ \varphi$ :

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R[x] \\ & \searrow f & \downarrow g \\ & & S \end{array}$$

*Proof.* Proceed similarly by first determining the form that  $g$  takes, and then showing the uniqueness and existence.

- **Uniqueness.** Since it is required that  $g$  is a morphism of  $R$ -algebras, we have

$$g\left(\sum_{i=0}^n a_i x^i\right) = \sum_{i=0}^n g(a_i)g(x^i) = \sum_{i=0}^n f(a_i)g(x^i) = \sum_{i=0}^n f(a_i)a^i$$

by the requirement that  $g(x) = a$ . This is the only form that  $g$  could take, and thus proves its uniqueness.

- **Existence.** For existence it suffices to check that  $g$  is indeed a ring homomorphism. By the uniqueness  $g$  is fixed by sending  $x \in R[x]$  to  $a \in R$ . Notice that  $R$  is commutative, which indicates that both left and right composition is satisfied; with the addition condition verified in the uniqueness part.

□

**Theorem 3.2** (Universal Property of Polynomial Ring of Several Variables). *Let  $A$  be a commutative  $R$ -algebra and  $g$  be the inclusion map from  $R$  to  $R[x_1, \dots, x_n]$  with a fixed  $n$ . For every  $R$ -algebra  $S$  and  $(a_1, \dots, a_n) \in S$ , there exists a unique homomorphism of  $R$ -algebra  $h : R[x_1, \dots, x_n] \rightarrow S$  s.t.  $h(x_i) = a_i$  for all  $i \in \llbracket 1, n \rrbracket$ , and the following diagram commutes, i.e.  $f = h \circ g$ :*

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ & \searrow g & \uparrow h \\ & & R[x_1, \dots, x_n] \end{array}$$

*Sketch of Proof.* The idea is similarly consider substitution  $x_i \mapsto a_i$ , and proceed to verify that this is indeed a ring homomorphism. One step that requires caution is that polynomials of several variables are defined in an inductive manner; therefore here proof should also be done inductively, on the number of variables involved.

□

Using polynomial of several variables, it is clearer to formalize the “generating set” of a ring via specifying which element each variable maps to:

**Definition 3.5** (Finitely Generated  $R$ -algebra). *Let  $R$  be a commutative ring, with  $A$  a commutative  $R$ -algebra. Fix  $(a_1, \dots, a_n) \in A$ . By the universal property of polynomial of several variables, there exists a unique homomorphism  $\varphi : R[x_1, \dots, x_n] \rightarrow A$  s.t.  $\varphi(x_i) = a_i$ . Then the subalgebra  $\text{im } \varphi$  is said to be **generated** by  $\{a_1, \dots, a_n\}$ .*

**Remark 3.3.** Using the same formalization as in the definition above,  $\text{im } \varphi$  is smallest  $R$ -subalgebra of  $A$  that contains  $\{a_1, \dots, a_n\}$ .

*Proof.* It is clear that  $\text{im } \varphi$  contains  $\{a_1, \dots, a_n\}$ . To see that it is smallest, suppose there is a smaller one  $A'$ , then there must be some  $\sum_{i=0}^n a_i x^i \notin A'$ , which contradicts with the fact that a ring should be closed.

□

Notice that in the definition of polynomial ring it is only required that  $x$  could be multiplied with powers of itself. This enables making polynomial a representation of groups:

**Definition 3.6** (Group Ring). Let  $R$  a commutative ring, and  $G$  a group. A **group ring of  $R$  on  $G$**  is defined as

$$R[G] := \left\{ \sum_{g \in G} a_g g \mid a_g \in R \right\}$$

with the addition and multiplication the same as that in the polynomial ring.

**Remark 3.4.** The operation between the ring and the group is not required to be defined and is simply a notation. The polynomial cannot admit any structure that is more complicated (e.g. changing the group to be a ring) as otherwise the addition will not be well-defined.

## 4 Ideals

**Definition 4.1** (Finitely-Generated Ideals). Let  $R$  be a ring. Then

- Let  $(I_\alpha)$  be a family of ideals for  $\alpha \in \Lambda$  the index set, then the **ideal generated by (sum of)  $(I_\alpha)$**  is defined as

$$\sum_{\alpha \in \Lambda' \subseteq \Lambda} I_\alpha := \left\{ \sum_{\alpha \in \Lambda'} a_\alpha \mid a_\alpha \in I_\alpha, |\Lambda'| \text{ finite} \right\}$$

- Alternatively one could consider the **ideal generated by (product of) two ideals** (which can be easily extended to several ideal cases)  $I$  and  $J$  to be

$$I \cdot J := \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{Z}_{>0}, a_i \in I, b_i \in J \forall i \right\}$$

- Suppose further that  $R$  is commutative. Let  $\Lambda := \{\lambda_1, \dots, \lambda_n\}$  be a subset of  $R$ . Then the **ideal generated by  $\Lambda$**  is defined as

$$(\lambda_1, \dots, \lambda_n) := \left\{ \sum_{k=1}^n r_k \lambda_k \mid r_k \in R \right\}$$

**Remark 4.1.** Ideals generated by only one element is principal. For finitely generated ideals, the ideal generated by a set of elements is the same as the ideal generated by the corresponding principal ideals of the elements. This simply results from the fact that  $(a) = \{ra \mid r \in R\}$ .

Specify  $R$  to be a commutative ring, with  $I \subseteq R$  an ideal of  $R$ . Consider the following special cases of ideals:

**Definition 4.2** (Radical Ideal).  $I \subseteq R$  is a **radical ideal** if for all  $a \in R$ ,  $\exists n \in \mathbb{Z}_{>0} a^n \in I \implies a \in I$ .

**Definition 4.3** (Prime Ideal).  $I \subseteq R$  is a **prime ideal** if  $I \neq R$ , and for all  $a, b \in R$ ,  $ab \in I \implies (a \in I) \vee (b \in I)$ .

**Definition 4.4** (Maximal Ideal).  $I \subseteq R$  is a **maximal ideal** if  $I \neq R$ ; and there is no ideal  $J$  in  $R$  s.t.  $I \subsetneq J \subsetneq R$ .

**Remark 4.2.** Recall that  $R$  is a domain if and only if for all  $a, b \in R$ ,  $ab = 0 \implies a = 0 \vee b = 0$ . This implies that for any ring  $R$  with  $\mathfrak{p}$  a prime ideal in it,  $R/\mathfrak{p}$  is a domain.

**Definition 4.5** (Reduced Ring). A  $R$  is a **reduced ring** if and only if it does not have any nilpotent elements, i.e. for all  $u \in R$ ,  $u^n = 0 \implies u = 0$  for all  $n \in \mathbb{Z}_{>0}$ .

**Remark 4.3.** For a commutative ring  $R$ ,  $I$  is a radical ideal if and only if  $R/I$  is a reduced ring.

**Proposition 4.1.**  $I$  is a maximal ideal if and only if  $R/I$  is a field.

*Proof.* This fact follows directly from the following simple lemma. □

**Lemma 4.1.**  $R = K$  is a field if and only if it only has two ideals  $(0)$  and  $(1)$ .

*Proof.* Consider in both directions:

$\Rightarrow$ : If  $K$  is a field, then either there are no invertible elements, which in this case the ideal  $I$  can only contain 0 as this is the only non-invertible element in a field; or 1 and therefore every element is in the ideal, as  $\forall g \in I, \exists g^{-1} \in K, gg^{-1} = 1 \in I$ .

$\Leftarrow$ : If a ring  $R$  has only two ideals  $(0)$  and  $(1)$ , then for all  $0 \neq u \in R$  consider  $(u)$ . By hypothesis  $(u) = (1)$ , i.e. there exists some  $u^{-1} \in R$ , which implies that  $R$  is actually a field. □

**Proposition 4.2.** An ideal being maximal implies that it is prime; and an ideal being prime implies that it is radical.

*Proof. Maximal ideals are prime.* Suppose that  $I \subseteq R$  is maximal but is not prime, i.e. there exists some  $a, b \in R$  s.t.  $ab \in I, a \notin I, b \notin I$ . By hypothesis  $I \cup \{a\} = R$ , i.e. there exists some  $r \in R, t \in I$  s.t.  $a + rt = 1$ . But then  $b = ba + (br)t \in I$  which is a contradiction.

*Prime ideals are radical.* Consider inductively on  $a$  and  $a^{n-1}$ ; apply the definition of prime ideals. □

**Example 4.1.** Consider counterexamples of the converse of the proposition above:

- $\mathbb{Z}_N$  for  $N$  not a power of prime is radical, but not prime.
- A trivial case for an ideal being prime but not maximal is  $(0)$ , where as long as the ring is not a field, it is maximal.
- A more interesting case for an ideal being prime but not maximal is for finitely generated non-PIDs, adding a generator to a prime ideal suffices to create a “larger” ideal. Take the example  $(x) \subseteq R[x]$  where  $R$  is a domain, which is prime as  $R[x]/\langle x \rangle \cong R$  is also a field. But  $(x) \subseteq (2, x)$  which is not the whole ring.



## 5 Noetherian Ring

**Lemma 5.1** (Zorn's Lemma). *Suppose that  $(P, \leq)$  is an ordered set s.t. every totally order subset  $P_0 \subseteq P$  has an upper bound, then  $P$  has a maximal element.*

**Theorem 5.1.** *Let  $I \subseteq R$  be an ideal of a commutative ring  $R$ . Then there exists some maximal ideal  $M$  s.t.  $I \subseteq M$ .*

*Proof.* The proof is simply a re-formalization of Zorn's Lemma (Lemma 5.1).

Consider  $P := \{J \subseteq R \mid J \text{ ideals}, I \subseteq J, J \neq R\}$ , with the order of inclusion. Take  $P_0 := \{I_\alpha \mid \alpha \in \Lambda\} \subseteq P$  to be totally ordered. Then  $J := \bigcup_\alpha I_\alpha$  is also an ideal. Further  $1 \notin J$ , otherwise there will exist some  $\alpha \in \Lambda$  s.t.  $I_\alpha = R$ , which contradicts the hypothesis. Therefore  $J$  is the upper bound for the family  $P_0$ . Applying Zorn's Lemma finishes the proof.  $\square$

**Definition 5.1** (Noetherian Ring). *A ring  $R$  is (left) **Noetherian** if it satisfies the Ascending Chain Condition (ACC), for (left) ideals, i.e. there is no infinite strictly increasing sequence of (left) ideals:*

$$I_1 \subsetneq I_2 \subsetneq \dots$$

**Proposition 5.1.** *Let  $R$  be a ring, then the followings are equivalent:*

1.  $R$  is (left) Noetherian.
2. Let  $P$  be a family of (left) ideals in  $R$ , then  $P$  has a maximal element.
3. Every (left) ideal in  $R$  is finitely generated.

*Proof.* • (i) being equivalent to (ii) is via simply reformatizing the definition.

- (i) implies (iii). Proceed by proving the contraposition. Suppose that there exists an ideal  $I_0 \subseteq R$  that is not finitely generated, then there exists an infinite sequence of generators of  $I_0$   $(a_i), i \in \mathcal{I}$ . Then there exists an infinite ACC  $(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, \dots, a_k), \subsetneq \dots$ .
- (iii) implies (i). Prove by showing a contradiction. Suppose that there exists an infinite ACC  $I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_k \subsetneq \dots$ . Then consider  $I := \bigcup_{n \geq 1} I_n$ . By the hypothesis it is finitely generated, i.e. there exists some  $(a_1, \dots, a_m)$  s.t.  $a_i \in I_{n_i}$  for all  $i \in \llbracket 1, m \rrbracket$ . Define  $n := \max\{n_i \mid i \in \llbracket 1, m \rrbracket\}$ . Then  $I_n = I_{n+1}$  which is a contradiction.

$\square$

**Theorem 5.2** (Hilbert's Basis Theorem). *Let  $R$  be a commutative Noetherian ring. Then  $R[x]$  is a Noetherian ring.*

*Proof.* By proposition 5.1 it suffices to show that every ideal of  $R[x]$  is finitely generated.

In the case that  $I = (0)$ , it is finitely generated as  $R$  is Noetherian. For the case of that  $I \neq (0)$ , consider a family of ideals where  $f_1 \in I \setminus \{0\}$ , with  $f_k \in I \setminus (f_1, \dots, f_k)$  for  $k > 1$  s.t.  $\deg f_k = \min\{\deg f \mid f \in I \setminus (f_1, \dots, f_k)\}$ . If there exists some  $k$  s.t.  $(f_1, \dots, f_k) = I$  then  $R[x]$  is by definition Noetherian. Suppose that it is not. Then there exists an infinite ascending chain.

Denote  $f_n = a_n x^{d_n} + \sum_{k=0}^{d_n-1} a_k x^k$ . From the construction it is clear that  $d_1 \leq d_2 \leq \dots \leq d_n \leq \dots$ .

Define  $I := (a_1, \dots, a_n \mid n \geq 1)$ . By hypothesis  $I \subseteq R$ , which implies that it is finitely generated. Then there exists some  $k$  s.t.  $I = (a_1, \dots, a_k)$ , with  $d_i \geq 1$  (otherwise suppose there exists some  $a_0 \in R \setminus (a_1, \dots, a_k)$ , simply add  $a_0x$  to the generators; and do the similar to ensure that the degree of polynomial associated with the corresponding coefficients is at least one. Since  $R$  is Noetherian, it is finitely generated, i.e. the process above will terminate, which does not interfere with the condition that the ascending chain does not terminate.)

For  $f_{k+1}$ , we know that there exists a family  $(c_j)_{j=1}^k$  s.t.  $a_{k+1} = \sum_{j=1}^k c_j a_j$  since  $(a_1, \dots, a_k)$  are generators. Then consider

$$f = f_{k+1} - \sum_{i=1}^k c_i x^{d_{k+1}-d_i} f_i$$

which is a polynomial that is not in  $I \setminus (f_1, \dots, f_n)$ , which is a contradiction.  $\square$

**Corollary 5.1.** By induction  $R[x_1, \dots, x_n]$  is also Noetherian if  $R$  is Noetherian. Quotient and localization preserves the property that a ring is Noetherian.

## 6 Euclidean Domain, PIDs and UFDs

**Definition 6.1** (Principal Ideal Domain (PID)). *Let  $R$  be a integral domain.  $R$  is a **Principal Ideal Domain (PID)** if every ideal in  $R$  is principal.*

**Remark 6.1.** If  $R$  is a PID, then  $R$  is Noetherian, as principal ideals are by definition finitely generated.

**Proposition 6.1.** *If  $R$  is a PID, then every prime ideal in it is maximal.*

*Proof.* Prove by contradiction. Suppose that  $I = (p)$  is a prime ideal that is not maximal. Then by Theorem 5.1 there exists some maximal ideal  $x \notin I$  s.t.  $I \subseteq (x)$ , i.e. there exists some  $r \in R$  s.t.  $p = xr$ . Since  $x \notin I$ ,  $r \in I$ . Write  $r = pr'$  for  $r' \in R$ . Then  $xr' = 1$ , i.e.  $(x) = (1)$  which is a contradiction.  $\square$

**Definition 6.2** (Euclidean Domain). *A **Euclidean Domain** is an integral domain  $R$ , for which there exists a function (norm)  $N : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ , s.t.  $\forall a, b \in R, b \neq 0$ , there exists some  $q, r \in R$  s.t.  $a = bq + r$ ; and either  $r = 0$ , or  $N(r) < N(b)$ .*

**Proposition 6.2.** *A Euclidean Domain is a PID.*

*Proof.* Let  $R$  be a euclidean domain. Since the domain of the norm is  $\mathbb{Z}_{\geq 0}$ , there exists some element  $b$  s.t.  $N(b)$  is minimal. Claim that  $R = (b)$ .

This is indeed true, as there does not exist any  $r$  s.t.  $N(r) < N(b)$ . Then apply the definition of a Euclidean Domain.  $\square$

**Definition 6.3.** *Let  $a, b \in R \setminus \{0\}$ . Then  $a$  is **associated with**  $b$  (denoted  $a \sim b$ ) if there exists some  $u$  invertible, s.t.  $a = ub$ .*

**Remark 6.2.**  $a \sim b$  if and only if  $(a) = (b)$ .

**Definition 6.4** (Greatest Common Divisor). *Let  $a, b \in R$  that are not both zero. The **Greatest Common Divisor** of  $a$  and  $b$  is an element in  $R \setminus \{0\}$  s.t.  $d \mid a, d \mid b$ ; and for all  $x \in R \setminus \{0\}$ ,  $x \mid a \wedge x \mid b \implies x \mid d$ .*

**Proposition 6.3.** *Let  $R$  be a domain, and  $d$  be the gcd of  $a$  and  $b$ . If  $(a, b) = (d)$ , then  $d = \gcd(a, b)$ .*

*Proof.*  $d$  is a common divisor of  $a$  and  $b$  as  $a, b \in (d)$ . It is the greatest one as since  $d \in (a, b)$ , there exists some  $\lambda, \mu \in R$  s.t.  $\lambda a + \mu b = d$ . Both sides should divide  $d$ , which implies that if there exists some  $d' \mid a, d' \mid b$ , then  $d' \mid d$ .  $\square$

**Definition 6.5** (Prime; Irreducible). *Let  $R$  be a domain, and  $a$  a non-zero element. Then*

- $a$  is a **prime** if  $(a)$  is a prime ideal.
- $a$  is **irreducible** if for all  $b_1, b_2 \in R$  s.t.  $a = b_1 b_2$ , either  $b_1$  is invertible or  $b_2$  is invertible.

**Proposition 6.4.** *Let  $R$  be a PID and  $r \in R$  a non-zero element. Then  $r$  is irreducible if and only if  $(r)$  is a maximal ideal.*

*Proof.* Proceed by showing implication in two directions:

$\Rightarrow$ : Let  $r$  be an irreducible element. Suppose that there exists an ideal  $I$  s.t.  $(r) \subsetneq I \subsetneq R$ . Since  $R$  is a PID, there exists some  $a \in R$  s.t.  $I = (a)$ , which indicates that there exists some  $x \in R$  s.t.  $r = ax$ . But since  $r$  is irreducible, either  $a$  is a unit, i.e.  $I = R$ , or  $x$  is a unit, i.e.  $I = (r)$ . Both of which lead to a contradiction.

$\Leftarrow$ : Proceed by showing the contraposition. Suppose that  $r$  is not irreducible, then there exists  $p, q \in R$  which are not units s.t.  $r = pq$ . Then  $(r) \subsetneq (p) \subsetneq R$  which implies that  $(r)$  is not maximal.  $\square$

**Proposition 6.5.** *If  $a$  is prime, then  $a$  is irreducible.*

*Proof.* Let  $a$  be a prime. Suppose that there exists  $b_1, b_2 \in R$  s.t.  $b_1 b_2 = a$ . Then  $b_1 b_2 \in (a)$ . Without loss of generality assume  $b_1 \in (a)$ , i.e. there exists some  $r \in R$  s.t.  $b_1 = ar$ . This gives  $arb_2 = a$ , i.e.  $b_2$  is invertible.  $\square$

**Remark 6.3.** The converse is generally not true. Consider in  $\mathbb{Z}[\sqrt{5}i]$  which is not a UFD. Then  $(2)$  is not prime (as  $2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$ ) but  $2$  is irreducible.

**Definition 6.6** (Unique Factorization Domain (UFD)). *A domain  $R$  is a **Unique Factorization Domain (UFD)** if for all nonzero  $a \in R$  that is not invertible, there exists a decomposition  $a = p_1 \cdots p_r$  where  $p_1, \dots, p_r$  are irreducible. For all other families of irreducible elements  $q_1, \dots, q_r \in R$  s.t.  $a = q_1 \cdots q_r$ , there exists a permutation  $\varepsilon : [r+1] \rightarrow [r+1]$  s.t.  $p_i \sim q_{\varepsilon(i)} \forall i$ .*

**Proposition 6.6.** *Let  $R$  be a UFD. Then every irreducible element  $p \in R$  is prime.*

*Proof.* Claim that  $(p)$  is a prime ideal given that  $p$  is irreducible. Since  $p$  is irreducible and  $R$  is UFD, for all  $b_1 b_2 \in (p)$ , there exists some irreducible  $q_i$ s for  $i \in I$  s.t.  $b_1 b_2 = p \cdot \prod_{i \in I} q_i$ . Since factorization unique, at least one of  $b_1$  and  $b_2$  admits a divisor  $p$ , which indicates that  $(p)$  is a prime ideal.  $\square$

**Proposition 6.7.** *Let  $R$  be a domain s.t. every irreducible element is prime. Then  $R$  is a UFD.*

*Proof.* It suffices to prove that factorization is unique up to permutation and multiplication by units. Suppose that  $p_i$ s and  $q_i$ s are two irreducible decomposition of  $a$ , i.e.  $a = p_1 \cdots p_r = q_1 \cdots q_s$ . Then either

- $r = 0$ . Then  $a$  is a unit, which indicates that  $s = 0$ .

- $r \neq 0$ . Then  $s \neq 0$ . Since  $p_i$  is prime for all  $i$ , there exists some  $q_j$  s.t.  $p_i \mid q_j$ . this implies that  $r \leq s$ . Then consider  $q_i$ s as prime, which implies  $s \leq r$  and therefore  $s = r$ . Further since  $p_i$ s and  $q_i$ s are irreducible, for  $p_i \mid q_j$  this implies  $q_j = p_i u$  for  $u$  a unit.

This verifies the definition of a UFD. □

**Proposition 6.8.** *Let  $R$  be a Noetherian ring. Then every element  $a \in R$  attains an irreducible decomposition  $a = p_1 \cdots p_r$  with  $p_i$  irreducible for all  $i$ .*

*Proof.* This is simply a re-formalization of the fact that Noetherian rings are finitely generated. Consider the following cases:

- $a$  is irreducible. Then the factorization process is done.
- $a = b_1 b_2$  where  $b_1$  and  $b_2$  are both not units. Then consider separately  $b_1$  and  $b_2$  with this process. This process is sure to terminate at some point as otherwise this gives an ideal of infinite generators.

□

**Remark 6.4.** Noetherian rings are generally not UFDs. A simple example is  $\mathbb{Z}[\sqrt{5}i]$ , the Gaussian Integers.

**Theorem 6.1.** *Every PID is a UFD.*

*Proof.* Since principal ideals are finitely generated, all PIDs are Noetherian. By proposition 6.8 there exists a decomposition; and by proposition 6.4 and 6.1 irreducible elements are prime. By proposition 6.7 it is a UFD. □

**Example 6.1.** An example where a ring is a UFD but not a PID (where prime ideals are not maximal) is  $\mathbb{Z}[x]$ , with the ideal  $(2, x)$  which is not principal.  $(x)$  is prime, but not maximal.

The following proves the theorem:

**Theorem 6.2.** *Let  $R$  be a UFD, then  $R[x]$  is also a UFD.*

**Definition 6.7** (Primitive; Content). *Let  $f \in R[x]$  a nonzero polynomial. Then*

- The **content** of  $f$ , denoted as  $c(f)$  is the greatest common divisor of the coefficient of its terms.
- $f \in R[x]$  is **primitive** if its content is a unit.

**Lemma 6.1.** *Let  $R$  be a UFD. Define  $K := \text{Frac}(R)$ , i.e.  $K = S^{-1}R$  for  $S := R \setminus \{0\}$ . A nonzero element  $f \in R[x]$  is irreducible if and only if either of the following holds:*

- $\deg f = 0$ , and  $f$  is irreducible in  $R$ .
- $\deg f \geq 1$ ,  $f$  is primitive and is irreducible in  $K[x]$ .

*Proof.* Consider the following two cases:

- $\deg f = 0$ . Since  $R \subseteq R[x]$ ,  $f$  irreducible in  $R[x]$  implies that it is irreducible in  $R$ . For the converse, notice that  $R$  is a domain, where the degree of product of two polynomials is at the sum of the degree of the two polynomials, indicating that  $f \in R[x]$  could only attain degree 0 factors. The fact that  $f$  is irreducible in  $R$  finishes the proof.

- $\deg f \geq 1$ . Consider the two directions:

$\Rightarrow$ : Suppose that  $f$  is irreducible in  $R[x]$ . Notice that for all  $g \in K[x]$ ,  $c(g)^{-1}g \in R[x]$ . Proceed by showing a contradiction.

Suppose that there exists  $f_1, f_2 \in K[x]$  of degree at least one s.t.  $f = f_1 f_2$  (i.e.  $f$  is not irreducible in  $K[x]$ ). Then

$$f = (c(f_1)^{-1}f_1)(c(f_2)^{-1}f_2)c(f_1)c(f_2)$$

where the four operands for multiplication are all in  $R$ . Since  $f$  is irreducible in  $R$ , either  $(c(f_1)^{-1}f_1)$  or  $(c(f_2)^{-1}f_2)$  is a unit, which contradicts the hypothesis that  $\deg f_1 \geq 1 \wedge \deg f_2 \geq 1$ .

$\Leftarrow$ : Proceed by showing that the contraposition is true. Suppose that  $f = f_1 f_2$  where  $f_1, f_2$  are both not units, in  $R$ . Then  $f = f_1 f_2 \in K[x]$  which is also not irreducible.

□

**Lemma 6.2.** *Let  $K$  be a field. Then  $K[x]$  is a PID.*

*Proof.* Let  $I$  be an ideal in  $K[x]$ . Define  $k := \{\deg f \mid f \in I\}$ . Such  $k$  indeed exists as the degree has a lower bound 0; and  $k$  could take only finitely many values with some element  $f_0 \in I$  fixed; namely  $\llbracket 0, \deg f_0 \rrbracket$ . Claim that  $I = (x^k)$ .

Either  $k = 0$ , where  $I = (1)$ ; or  $k \neq 0$ , where for all  $f = \sum_{i|d_i \geq d} c_i x^{d_i} \sum_i c_i x^{d_i - d} \in K[x]$ .

□

*Proof of Theorem 6.2.* Define  $K = S^{-1}R$  for  $S = R \setminus \{0\}$ . From lemma 6.2 we know  $K[x]$  is a PID, which is therefore a UFD. The general strategy is to transform the whole problem into  $K[x]$  using lemma 6.1, and use the fact that  $K[x]$  is a UFD, with elements differ only by a factor in  $R$  (which is also a UFD) from those in  $R[x]$ .

It suffices to show that the decomposition exists and is unique:

- *Existence.* Decompose  $f$  in  $R[x]$   $f = c(f)g$  s.t.  $g$  is primitive. Then  $c(g) = u$  where  $u$  is some unit in  $R$ . Applying the inclusion map gives  $g \in K[x]$ , where it could be decomposed into  $g = g_1 \cdots g_n$  where  $g_i$ s are irreducible. Denote  $g_i = c(g_i)h_i$ , which gives  $g = \prod_{i=1}^n c(g_i)h_i = c(g) \prod_{i=1}^n h_i = u \prod_{i=1}^n h_i$ . Since  $c(f) \in R$  which is a UFD, there exists a decomposition  $c(f) = f_1 \cdots f_n$ . This gives an irreducible decomposition  $f = f_1 \cdots f_n h_1 \cdots h_n$ .
- *Uniqueness.* This follows from the fact that both  $f$  and  $K[x]$  are UFDs, i.e. decomposition of  $f \in R$  and  $g \in K[x]$  are unique. (Alternatively one could prove that irreducible elements in  $R[x]$  are also prime, which is essentially the same approach as the content is prime follows from the fact that  $R$  is UFD; and the primitive is prime as  $K[x]$  is a UFD).

□