Randolf Chung

A Compendium on Basic Commutative Ring Structures

Incomplete

January 22, 2019

Preface

It seems that a majority of my undergraduate algebra career was spent trying to prove inclusions, mutual intersections, and reformulations of different commutative ring structures. In this short story, I will attempt to provide a compendium of equivalency theorems, properties, and other elements of commutative algebra. The pedagogy here is purposefully unmotivating; you can probably find some motivation on Wikipedia or among other sources, however I contend these are not the best sources and encourage looking at them for finding references only.

I complete this as I feel. All proofs are internal to this document implying any accessory lemmas are placed in the Appendix. The level of accessory is kind of arbitrary, but reading the current version will give a good hint of the standard I use.

If you would like to give corrections or provide proofs, please email me at `university@jeongjh.com`. Do not reference books or webpages; if I did this, there would be no point in writing this. The proofs should solely be yours and I will only take TeXed documents. Creative and short solutions are given priority over long and pedagogical ones.

Bonn, Germany
January 2019

Contents

1

Introduction

Our object of study will be the following:

Definition 1.1. *A **commutative ring** $(R, +, \cdot)$ is an abelian group R with a compatible commutative monoid structure.*

We write $+$ for the abelian group structure and call it *additive* and write $\cdot$ for the (commutative) monoid structure and call it *multiplicative*.

1.1 Notation

- $\mathbb{N}$ contains 0.
- $R := (R, +, \cdot)$ denotes a commutative ring, unless otherwise stated.
- $R^+ := (R, +)$ denotes the underlying additive group of a ring R.
- $R^\times := (R, \cdot)$ denotes the underlying multiplicative monoid of a ring R.
- R^* denote the group of units in R.
- $R_{\setminus\{0\}}$ denotes the multiplicative set $R \setminus \{0\}$.
- Ideals R denotes the set of ideal of R.
- Spec R denotes the set of prime ideals of R.
- mSpec R denotes the set of maximal ideals of R.
- Frac R denotes the field of fractions of R.
- $\mathrm{R}_\mathfrak{p}$ denotes the localization of R at a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$.

1.2 Definitions

In this section, we will provide the definitions we will consider. We use the most intuitive ones.

1.2.1 Non-commutative Definitions

These definitions do not require commutativity, so we list them here.

Definition 1.2. *A ring is **division** (or **skew**) if the monoid structure restricted to $R_{\setminus\{0\}}$ can be given a compatible group structure.*

Definition 1.3. *A ring is (left) **local** if*

$(*)$ *R has a unique (left) maximal ideal* $\mathfrak{m}$.

Definition 1.4. *A ring is (left) **Noetherian** if*

$(*)$ *For any ascending chain of (left) ideals*

$$I_1 \subseteq I_2 \subseteq \dots$$

there exists $N \geq 1$ such that $I_N = I_n$ for all $n \geq N$.

The condition $(*)$ is called the ascending chain condition (or a.c.c.). If only principal ideals are considered, then $(*)$ is called a.c.c.p. for ascending chain condition for principal ideals.

Definition 1.5. *A ring is (left) **Artinian** if*

$(*)$ *For any descending chain of (left) ideals*

$$I_1 \supseteq I_2 \supseteq \dots$$

there exists $N \geq 1$ such that $I_N = I_n$ for all $n \geq N$.

The condition $(*)$ is called the descending chain condition (or d.c.c.).

Definition 1.6. *A ring is (left) **hereditary** if*

$(*)$ *for any projective (left) R-module P, every submodule is projective.*

*If we only consider finitely-generated submodules, R is (left) **semihereditary**.*

Definition 1.7. *A ring is **simple** if*

$(*)$ *the only two-sided ideal is (0) and itself.*

Definition 1.8. *A ring is **indecomposable** if*

$(*)$ *the only subrings $S, T \subseteq R$ such that $S \oplus T = R$ is (0) and itself.*

Definition 1.9. *A ring is **completely reducible** if*

$(*)$ *R is a direct sum of simple subrings.*

Definition 1.10. *A ring is **completely decomposable** if*

$(*)$ *R is a direct sum of indecomposable subrings.*

Since left and right ideals are identified in commutative rings, we can just say ideal. The division ring definition reduces to an abelian group structure since the monoid structure is commutative; thus commutative division rings are the same as **fields**.

1.2.2 Main Definitions

We will assume *all* the remaining definitions will also include the following:

Definition 1.11. *A ring is an **integral domain** (or **entire**) if the monoid structure restricted to $R_{\setminus\{0\}}$ is a submonoid of R.*

We will see later if entirety is not included, definitions begin to breakdown, in the sense, the other conditions will break.

Common Definitions

Definition 1.12. *A ring is a **unique factorization domain** or **UFD** (or **factorial**) if*

$(*)$ *every $x \in R_{\setminus\{0\}}$ can be written as a unique (up to unit) finite product of irreducible elements x_i.*

The condition $(*)$ is called unique factorization.

Definition 1.13. *A ring is a **principal ideal domain** or **PID** if*

$(*)$ *every ideal is principal.*

The condition $(*)$ is called principality.

Definition 1.14. *A ring is a **Euclidean domain** (or **Euclidean**) if*

$(*)$ *there exists a function*

$$\mathrm{rem} : R \setminus \{0\} \to \mathbb{N}$$

such that for any $x \in R$, $y \in R \setminus \{0\}$, there exists $q, r \in R$ such that $r = 0$ or $\mathrm{rem}(r) < \mathrm{rem}(b)$.

The function rem *is called a Euclidean function.*

Definition 1.15. *A ring is **integrally closed domain** (or **integrally closed**) if*

$(*)$ *it is integrally closed in its field of fraction* $\mathrm{Frac}\, R$.

Definition 1.16. *A ring is **valuation** if*

$(*)$ *there exists a surjective group homomorphism*

$$v : \mathrm{Frac}(R)^\times \to \Gamma$$

such that Γ is abelian and totally ordered, and R can be identified with the set

$$\{x \in \mathrm{Frac}(R)^\times : v(x) \geq 0\} \cup \{0\}.$$

The group Γ is called the valuation group of R and v is called a valuation. If R is a field, then v is also called a place.

Definition 1.17. *A ring is **discrete valuation** (or a **DVR**) if*

$(*_1)$ *it is a valuation ring,*

$(*_2)$ *Γ is isomorphic to* $(\mathbb{Z},+)$.

Definition 1.18. *A ring is* ***Dedekind*** *if*

$(*_1)$ *R is Noetherian,*
$(*_2)$ *$R_{\mathfrak{m}}$ is a DVR for every* $\mathfrak{p} \in \operatorname{mSpec} R$.

Definition 1.19. *A ring is* ***Krull*** *if*

$(*_1)$ *$R_{\mathfrak{p}}$ is a DVR for every height one* $\mathfrak{p} \in \operatorname{Spec} R$.
$(*_2)$

$$R = \cap_{\mathfrak{p} \in \operatorname{Spec} R} R_{\mathfrak{p}} \subseteq \operatorname{Frac} R$$

$(*_3)$ *If $x \in R_{\setminus\{0\}}$, x is contained in finitely many height one prime ideals.*

Less Common Definitions

Definition 1.20. *A ring is a* ***factorization domain*** *if*

$(*)$ *every $x \in R_{\setminus\{0\}}$ can be written as a finite product of irreducible elements p_i.*

The condition $(*)$ is called factorization.

Definition 1.21. *A ring is a* ***GCD domain*** *(or* ***LCD domain****) if*

$(*)$ *for $x,y \in R$, there exists $d \in R$ such that $d \mid x, d \mid y$ and for all $s \in R$,*

$$s \mid x, s \mid y \implies s \mid d.$$

Such a d is called the greatest common denominator (or gcd) and written $\gcd(x,y)$.

Definition 1.22. *A ring R is a* ***Bézout domain*** *(or* ***Bézout****) if*

$(*)$ *for any two principal ideals* $(x),(y) \in \operatorname{Ideals} R$,

$$(x)+(y) = (z) \in \operatorname{Ideals}$$

for some $z \in R$

Definition 1.23. *A ring R is a* ***Prüfer domain*** *(or* ***Prüfer****) if*

$(*)$ *for any non-zero ideal* $I \in \operatorname{Ideals} R$,

$$II^{-1} = R$$

where $I^{-1} = \{x \in \operatorname{Frac} R : xI \subseteq R\}$.

The multiplication takes place in $\operatorname{Frac} R$.

2

Equivalency Propositions

2.1 Statements

In this chapter, we will list and prove equivalencies of the definitions in each proposition.

2.1.1 Non-commutative Equivalences

2.1.2 Commutative Equivalences

Proposition 2.1 (Integral domains).

(∗) *R is an integral domain.*
(1) *R has no non-zero zero divisors.*
(2) *For $x, y \in R$ and a non-zero $r \in R$, $rx = ry$ implies $x = y$.*
(3) *The endomorphism $L_r : x \mapsto rx$ is injective for $r \neq 0$.*
(4) $(0) \in \operatorname{Spec} R$.
(5) *R is isomorphic to a subring of* $\operatorname{Frac} R$.

The endomorphism in (3) is called the (left) principal homomorphism of L_r. *Such an element is called* (left) regular *if its (left) principal homomorphism is injective.*

Proposition 2.2 (Unique factorization domains).

(∗) *R is UFD.*
(1) *Every $x \in R_{\setminus\{0\}}$ can be written as a finite product of prime elements p_i.*
(2) *Every non-zero prime ideal contains a prime element.*
(3) $(*_1)$ *R is a factorization domain,* $(*_2)$ *every irreducible element is prime.*
(4) $(*_1)$ *R satisfies a.c.c.p.,* $(*_2)$ *every irreducible element is prime.*
(5) $(*_1)$ *R satisfies a.c.c.p.,* $(*_2)$ *is a GCD domain.*
(6) $(*_1)$ *R is Krull,* $(*_2)$ *every prime ideal of height one is principal.*
(7)$(*_1)$ *R is Krull,*

$(*_2)$ *for any non-zero fractional ideal I such that*

$$I = \cap_{\text{principal}} J$$

where the intersection runs over all principal fractional ideals of R containing I, I is principal.

The ideal in the last condition is called divisorial *(excluding the principality conclusion).*

Proposition 2.3 (Principal ideal domains).

$(*)$ *R is PID.*
(1) $(*_1)$ *R is Dedekind,* $(*_2)$ *is UFD.*
(2) $(*_1)$ *R is Bézout,* $(*_2)$ *satisfies a.c.c.p.*

Proposition 2.4 (Integrally closed domains).

$(*)$ *R is integrally closed.*
(1) *$R_{\mathfrak{p}}$ is integrally closed for all $\mathfrak{p} \in \operatorname{Spec} R$.*
(2) *$R_{\mathfrak{m}}$ is integrally closed for all $\mathfrak{m} \in \operatorname{mSpec} R$.*

Proposition 2.5 (Valuation rings).

$(*)$ *R is valuation.*
(1) *For every non-zero $x \in \operatorname{Frac} K$, x or x^{-1} lies in R.*
(2) $\operatorname{Ideals} R$ *is totally ordered by inclusion.*
(3) *The principal ideals are totally ordered by inclusion.*

Proposition 2.6 (Discrete valuation rings).

$(*)$ *R is DVR.*
(1) $(*_1)$ *R is PID,* $(*_2)$ *local,* $(*_3)$ *not a field.*
(2) $(*_1)$ *R is PID,* $(*_2)$ $|\operatorname{Spec} R| = 2$, $(*_3)$ *not a field.*
(3) $(*_1)$ *R is UFD,* $(*_2)$ *there exists a unique (up to unit) irreducible element.*
(4) $(*_1)$ *R is Dedekind,* $(*_2)$ *local,* $(*_3)$ *not a field.*
(5) $(*_1)$ *R is Noetherian,* $(*_2)$ *local,* $(*_3)$ *has a principal maximal ideal.*
(6) $(*_1)$ *R is Noetherian,*
$(*_2)$ *every non-zero fractional ideal I is cannot be written as a finite intersection of fractional ideals containing it,*
$(*_3)$ *not a field.*

Proposition 2.7 (Dedekind rings).

$(*)$ *R is Dedekind.*
(1) *every non-zero proper ideal is a product of prime ideals.*
(2) $(*_1)$ *R is Noetherian,* $(*_2)$ *is integrally closed,* $(*_3)$ *every non-zero prime ideal is maximal.*
(3) $(*_1)$ *R is Noetherian,*
$(*_2)$ *for any $I, J \in \operatorname{Ideals} R$, $I \subseteq J$ if and only if there is an ideal K such that $I = JK$.*
(4) *The set of fractional ideals is a group.*

(5) *R is hereditary.*
(6) $(*_1)$ *R is Prüfer,* $(*_2)$ *is Noetherian*

Proposition 2.8 (GCD domains).

$(*)$ *R is a GCD domain.*
(1) *Every finite intersection of principal ideals is principal.*

Proposition 2.9 (Prüfer domains).

$(*)$ *R is Prüfer.*
(1) $R_{\mathfrak{p}}$ *is a valuation ring for all* $\mathfrak{p} \in \operatorname{Spec} R$.
(2) $R_{\mathfrak{m}}$ *is a valuation ring for all* $\mathfrak{m} \in \operatorname{mSpec} R$.
(3) *For any finitely-generated non-zero ideals* $I, J, K \in \operatorname{Ideals} R$,

$$I \cap (J + K) = (I \cap J) + (I \cap K)$$

(4) *For any finitely-generated non-zero ideals* $I, J, K \in \operatorname{Ideals} R$,

$$I(J \cap K) = IJ \cap IK$$

(5) *For any finitely-generated non-zero ideals* $I, J \in \operatorname{Ideals} R$,

$$(I + J)(I \cap J) = IJ$$

(6) *For any finitely-generated non-zero ideals* $I, J, K \in \operatorname{Ideals} R$,

$$IJ = IK \implies J = K \vee I = (0)$$

2.2 Proofs

In each proof, the direction of the proof will be written (left to right) as a transposition $(i\ j) \in S_n$ where S_n is some symmetric group and i, j are integers or a $*$.

In general, I attempt to prove in a cyclic order, but sometimes it is futile to do such and better to end a cycle and use the full force of the equivalencies proven to prove the remaining equivalencies. In this spirit, I will write the cycle I will be proving beforehand and reserve the symbol $*'$ to denote "$(*)$ and all other proven equivalencies".

I may reference some proposition before having proven it. Rest assured, their proof will be independent of the one at hand, but I recommend the reader to follow the rabbit themselves to fully grasp the proofs from grassroots.

2.2.1 Proof of Proposition 2.1

$(* \ 1)$ Let $x, y \in R_{\setminus\{0\}}$. Then $xy \in R_{\setminus\{0\}}$ since $R_{\setminus\{0\}}$ is closed under multiplication. By definition, $xy \neq 0$, that is, $xy = 0$ implies $x = 0$ or $y = 0$.
$(1\ 2)$ If $rx = ry$ for $r \neq 0$, then $r(x - y) = 0$, so either $r = 0$ or $x = y$ implying $x = y$.
$(2\ 3)$ This is by definition.

(3 4) If $0 \mid ab$, then $ab = 0$. If both are not zero, then the injectivity of L_a implies $b = 0$, a contradiction. So either a or b is zero, that is, lies in (0).
(4 5) Let $i : R \to \operatorname{Frac} R$ be the canonical ring homomorphism. It suffices to show i is injective, i.e. R is isomorphic to $i(R) \subseteq \operatorname{Frac} R$. Let $x \in \ker i$. Then $x/1 = 0$, or equivalently by definition, $sx = 0$ for some $s \in R_{\setminus\{0\}}$. Since (0) is prime, $x \in (0)$, that is, $\ker i \subseteq (0)$. Trivially $(0) \subseteq \ker i$, so i is injective.
$(4 *)$ Let $x, y \in R_{\setminus\{0\}}$ such that $xy = 0$. Let i denote the isomorphism between R and the subring $A \subseteq \operatorname{Frac} R$. If $j : A \hookrightarrow \operatorname{Frac} R$ denotes the canonical inclusion, then $f := j \circ i$ is injective, so $f(x), f(y) \neq 0$. Since $0 = f(xy) = f(x)f(y)$, we have

$$f(x) = 0 f(y)^{-1} = 0$$

since $\operatorname{Frac} R$ is a field. But $i(x) \neq 0$ so we have a contradiction.

2.2.2 Proof of Proposition 2.2

We remark the simple fact that a prime element is also irreducible will be used without mention except for defining moments. Also the simple equivalence that an element is prime if and only if it generates a prime principal ideal.

Proof of $(* 1 2 3 4)$

$(* 1)$ Let $x \in R_{\setminus\{0\}}$ be written as

$$x = x_1 \cdots x_n$$

where x_i are irreducible. Suppose $x_i \mid ab$ for some $a, b \in R$. By definition, if $a = a_1 \cdots a_j$ and $b = b_1 \cdots b_k$ where a_i, b_i are irreducible, then by uniqueness and irreducibility of x_i, $x_i = a_i$ or $x_i = b_i$ for some i. But this implies $x_i \mid a$ or $x_i \mid b$, so x_i is prime. Thus $x_1 \cdots x_n$ is a finite product of prime elements.
(1 2) Consider a non-zero prime ideal $\mathfrak{p} \in \operatorname{Spec} R$. Let $x \in \mathfrak{p}$ be non-zero. Then $x = x_1 \cdots x_n$ where x_i are prime elements. By definition, (x_1) is prime, and since $x_1 \mid x$, $(x_1) \subseteq (x) \subseteq \mathfrak{p}$, so $x_1 \in \mathfrak{p}$.
(2 3) $(*_1)$ If $x = 0$ or $x \in R^*$, then there is nothing to show. Assume $x \notin\notin R^* \cup \{0\}$. Let S be the set of all finite[1] products of non-zero prime elements in R. Clearly S is multiplicative and $0 \notin S$. Suppose $(x) \cap S = \emptyset$. Then by Proposition 4.5 there is a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ containing (x) but missing S. By assumption, this prime ideal contains a prime element, but this cannot be since S at least contains all prime elements. So $(x) \cap S$ must be non-empty implying $rx \in S$ for some $r \in R$. Thus

$$rx = x_1 \cdots x_n$$

where each x_i is prime. By primality, $x_i \mid r$ or $x_i \mid x$. If all $x_i \mid x$, then $x = cx_1 \cdots x_n$, so $rc = 1$ (equivalently $r \in R^*$) since R is entire and $x \in S$. If $x_i \mid r$, say, for the first m x_i's, then $r = cx_1 \cdots x_m$ where $x_i \mid c$ for any i. Thus $cx = x_{m+1} \cdots x_n$ since again R is entire and all $x_i \mid x$. This reduces to the previous argument and we are done by definition of S and primality implies irreducibility.

[1] Empty products not considered

$(*_2)$ Let $x = ab$ be irreducible. Write $a = a_1 \cdots a_n$ and $b = b_1 \cdots b_m$ where a_i, b_i are prime using the previous $(*_1)$'s construction. Then a_i, b_i are irreducible and

$$x = a_1 \cdots a_n b_1 \cdots b_m$$

Since x is irreducible, $a_i, b_i \in R^*$ except for a single one. Thus x must be prime since it equals this single factor up to unit.
$(3\,4)$ $(*_1)$ Let $(x_1) \subseteq (x_2) \subseteq \ldots$ be an ascending chain of principal ideals. Suppose the chain does not stabilize. Then for brevity, assume each inclusion is proper. Consider x_1. We have

$$x_1 = p_1 \ldots p_n \text{ and } x_1 = r x_2$$

where p_i are prime. Each p_i must divide r or x_2. If they all divide x_2, then by the argument given in $(2\,3)$, $r \in R^*$ implying $(x_1) = (x_2)$, a contradiction. If some $p_i \mid x_2$, say, for the first m p_i's, then $x_2 = c p_1 \cdots p_m$ where m is *strictly* less than n and $c \in R^*$. Repeating this argument for x_2, x_3, and onward, $x_i = c' p_1, c' \in R^*$ after at most $n-1$ repetitions. Repeating the argument once more thus shows $(x_{i+1}) = R$ or $(x_i) = (x_{i+1})$. Both cases are absurd by our supposition, so the chain must stabilize.
$(*_2)$ By assumption.
$(4\,*)$ Let $x \in R$. Let $x_0 := x$. Write $x_i = ab$ where $a, b \in R$. If x_i is irreducible, then a or b is a unit and we let x_{i+1} be the non-unit. If not, then a and b do not lie in R^* and we let x_{i+1} be either. This construction provides an ascending chain

$$(x) \subseteq (x_1) \subseteq \ldots$$

which must stabilize at x_N for some large N. By construction, the x_N is irreducible, so write $p_1 := x_n$ and $x = c_1 p_1$ for some $c_1 \in R$. If c_1 is irreducible or a unit, then we are done. Otherwise, repeating this construction on c_i, we have an ascending chain

$$(x) \subseteq (p_1) \subseteq (p_1 p_2) \subseteq \ldots$$

which must stabilize at $p_1 \cdots p_m$ for some large m. Thus $x = c p_1 \cdots p_m$ for some $c \in R^*$ where each p_i is irreducible. Since irreducible elements are prime by assumption, the representation must be unique.

Proof of $(*'\,5)$

$(*'\,5)$ $(*_1)$ Using $(4)(*_1)$.
$(*_2)$ If $x, y \in R$, then x and y can be written uniquely as a product of irreducible elements. Let d be the product of common irreducible elements of x and y. Then if $s \mid x$ and $s \mid y$ and $s \nmid d$, then s contains an irreducible element as a factor which d does not contain. But $s \mid x$ and $s \mid y$ implies that irreducible element is a common irreducible element of x and y, so d must contain it. Hence $s \mid d$ and the gcd exists.
$(5\,*')$ We will use (4) to prove this.
$(*_1)$ By assumption.
$(*_2)$ Let x be irreducible and $x \mid ab$ where $a, b \in R$. Let $d = \gcd(xa, ab)$. Trivially and by hypothesis, $a \mid ab, a \mid xa, x \mid xa, x \mid ab$, so $d = au = xv$ for some $u, v \in R$. Since $d \mid xa$, $xa = auw$ for some $w \in R$ implying $x = uw$ by Proposition 2.1(2). Since x

is irreducible, $u \in R^*$ or $w \in R^*$. For the former, $xvu^{-1} = a$, so $x \mid a$. For the latter, $xw^{-1} = u$ and since $d \mid ab$, $rd = ab$ for some $r \in R$ so

$$ab = rd = rau = raxw^{-1}$$

Cancelling a shows $x \mid b$. Thus x is prime.

Proof of $(*'\ 6\ 7)$

$(*'\ 6)$ $(*_1)$ Note using (1), every $x \in R$ can be written as a finite product of prime elements, that is, x is contained in finitely many principal prime ideals. Let $\mathfrak{p} \in \operatorname{Spec} R$ with height one.

- $(*_1.*_1)$ We use Proposition 2.6(3). By Corollary 4.3 and Proposition 3.2(Localization, i), $R_\mathfrak{p}$ is local and UFD. Since $\mathfrak{p}$ has height one, the proof of Proposition 3.1(Localization, iii) shows the unique maximal ideal is principal. This ideal is prime, so the generating element p must be prime, that is, irreducible. Any other irreducible element must lie in the maximal ideal, hence is a multiple of p or p up to a unit. The former is ridiculous, so it must be the latter.
- $(*_1.*_2)$ If $x/s \in R_\mathfrak{p}$, then s does not lie in any prime ideal, or in particular, any maximal ideals, so s must be a unit, that is, $xs^{-1} \in R$. Since R injects into every $R_\mathfrak{p}$ by Proposition *(ii)*, we have the result.
- $(*_1.*_3)$ The prime principal ideals containing $x \in R$ must be of height one for any height larger would imply the other prime ideals are also principal, distinct, and a multiple of the original prime ideal; the latter reasoning gives the absurdity.

$(*_2)$ Using (2), every non-zero $\mathfrak{p} \in \operatorname{Spec} R$ contains a non-zero prime element. This element generates a principal prime ideal. If $\mathfrak{p}$ is of height one, then the ideals must coincide, implying $\mathfrak{p}$ is principal.

$(6\ 7)$ $(*_1)$ By assumption.

$(*_2)$ UNFINISHED

2.2.3 Proof of Proposition 2.3

$(*\ 1)$ $(*_1)$

- $(*_1.*_1)$ Let $I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals.
- $(*_1.*_2)$

$(*_2)$

3

Property Propositions

3.1 Statements

3.1.1 Commutative Equivalences

Let S denote a multiplicative set without (0).

Proposition 3.1 (Integral domains).

Sub-objects. Every subring is an integral domain.
Localization.

- (i) *Every localization with respect to S is an integral domain.*
- (ii) *R injects into* $S^{-1}R$.
- (iii) *If* $R_{\mathfrak{p}}$ *is a field, then* $\mathfrak{p} = (0)$ *and* $R_{\mathfrak{p}} = \operatorname{Frac} R$.
- (iv) *If I is a principal fractional ideal, then rI is a principal ideal for some* $r \in R$.

Proposition 3.2 (Unique factorization domains).

Localization.

- (i) *Every localization with respect to S is UFD.*

3.1.2 Non-commutative Equivalences

3.2 Proofs

When referencing a type of ring in a proof, I will use *all* equivalent definitions (and in particular, the integral domain ones without mention).

3.2.1 Proof of Proposition 3.1

Sub-objects. If S is a subring of R, then $S_{\setminus\{0\}}$ is a submonoid of $R_{\setminus\{0\}}$.
Localization.

(*i*) If $(x/s)(y/t) = 0 \in S^{-1}R$, then $rxy = 0$. Since $r \neq 0$, $xy = 0$. Either x or y must be 0, but in either case, x/s or y/t is 0, so $S^{-1}R$ contains no non-zero zero divisors.

(*ii*) If $q : R \to S^{-1}R$ is the canonical homomorphism, let $x \in \ker q$. Then $xs/s = 0$, i.e. $s'xs = 0$ for some $s' \in S$. $0 \notin S$, so xs must be 0. By the same reason, x must be 0.

(*iii*) If $R_\mathfrak{p}$ is a field, then the unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$ is (0). Clearly $q^{-1}(\mathfrak{p}R_\mathfrak{p}) = \mathfrak{p}$ Let $q : R \to R_\mathfrak{p}$ be the canonical homomorphism. By (*ii*), q is injective, thus

$$(0) = q^{-1}((0)) = q^{-1}(\mathfrak{p}R_\mathfrak{p}) = \mathfrak{p}.$$

The last statement follows by definition.

(*iv*) If $I = \langle x/s \rangle$ is a principal fractional ideal, let $r \in R$ such that $r\langle x/s \rangle \subseteq R$. We show $(z) = rI$ for some $z \in R$. If $ux/s \in I, u \in R$. Then $x_u/1 = rux/s \in rI \subseteq R$ for some $x_u \in R$, so

$$t(rux - sx_u) = 0$$

By integrality, $rux = sx_u$. Evaluating at $u = 1$ gives $rx = sx_1$, so $sx_1u = rxu = sx_u$. Cancelling s gives $x_1u = x_u$. So $x_u \in (x_1)$ implying $rI \subseteq (x_1)$. Let $z = x_1$. Then $uz \in (z)$ implies $uz/1 = uzs/s = urx/s = r(ux/s) \in rI$, so $(z) = rI$.

3.2.2 Proof of Proposition 3.2

Localization.

(*i*) If $\mathfrak{p} \in \operatorname{Spec} S^{-1}R$ is non-zero, the ideal $\mathfrak{p} \cap R$ is a prime not intersecting S by Corollary 4.2, so contains a principal prime ideal (x) by Proposition 2.2(2). A priori, this ideal does not intersect S, so $S^{-1}(x) \in \operatorname{Spec} S^{-1}R$ by the same corollary. Clearly $S^{-1}(x) = (x/1)$, so $x/1$ is prime. By Proposition 4.6(a), $\mathfrak{p}$ must contain $S^{-1}(x)$, i.e. contain the prime element $x/1$. We can conclude using Proposition 2.2(2) on $S^{-1}R$.

4

Appendix

4.1 Set Theory

Proposition 4.1. *Let A, B, C be sets, and let $f : A \to B$ and $g : B \to C$ be injective and surjective respectively. If every ascending sequence in B stabilizes, this is also true for A and C.*

Proof. If $C_1 \subseteq C_2 \subseteq \dots$ is an ascending sequences in C, then $g^{-1}(C_1) \subseteq g^{-1}(C_2) \subseteq \dots$ is an ascending sequence in B which stabilizes, so the sequence in C must stabilize. Similarly, if $A_1 \subseteq A_2 \subseteq \dots$ is an ascending sequence in A, then $f(A_1) \subseteq f(A_2) \subseteq \dots$ is an ascending sequence in B which stabilizes, so $A_n = A_{n+1}$ for some n.

4.2 Non-commutative ring theory

Proposition 4.2. *Every chain of (left) ideals ordered by inclusion is bounded above and below.*

Proof. Consider a chain

$$\dots \subseteq \mathfrak{a}_{-1} \subseteq \mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots$$

Let $\mathfrak{a}_L = \cap_i \mathfrak{a}_i$ and $\mathfrak{a}_U = \cup_i \mathfrak{a}_i$.

If $x, y \in \mathfrak{a}_L$, then $x, y \in \mathfrak{a}_i$ for all i, so $x - y \in \mathfrak{a}_i$ for all i. Thus $x - y \in \mathfrak{a}_L$. Similarly, $ax \in \mathfrak{a}_L$ for all $a \in R$, so $\mathfrak{a}_L$ is a (left) ideal. By definition, $\mathfrak{a}_L \subseteq \mathfrak{a}_i$ for all i, so $\mathfrak{a}_L$ is a lower bound for the chain.

If $x, y \in \mathfrak{a}_U$, then for sufficiently large n, $x, y \in \mathfrak{a}_n$, so $x - y \in \mathfrak{a}_n \subseteq \mathfrak{a}$. If $r \in R$, then $rx \in \mathfrak{a}_n \subseteq \mathfrak{a}$, so $\mathfrak{a}$ is an ideal. By definition, $\mathfrak{a}_i \subseteq \mathfrak{a}$ for all i, so $\mathfrak{a}_U$ is a upper bound for the chain.

We call $\mathfrak{a}_U$ (resp. $\mathfrak{a}_L$) the **canonical upper** (resp. **lower**) **bound** of $\{\mathfrak{a}_i\}$.

Proposition 4.3. *If $f : A \to B$ is a surjective ring homomorphism, then there is a bijection between prime ideals in B and prime ideals in A containing* $\ker f$ *given by*

$$\mathfrak{b} \mapsto f^{-1}(\mathfrak{b}) \text{ and } \mathfrak{a} \mapsto f(\mathfrak{a})$$

Proof. Clearly the maps are inverses, so it suffices to show they are well-defined.

$f^{-1}(\mathfrak{b})$: $xy \in f^{-1}(\mathfrak{b}), x \notin f^{-1}(\mathfrak{b}) \implies f(x) \notin \mathfrak{b}, f(xy) \in f^{-1}(\mathfrak{b}) \implies y \in f^{-1}(\mathfrak{b})$.

$f(\mathfrak{a})$: $xy \in f(\mathfrak{a}), x \notin f(\mathfrak{a}) \implies f^{-1}(xy) \in \mathfrak{a}, f^{-1}(x) \notin \mathfrak{a}$; $f^{-1}(x)f^{-1}(y) - f^{-1}(xy) \in \ker f \subseteq \mathfrak{a}$ (not necessarily zero), so $[f^{-1}(x)f^{-1}(y) - f^{-1}(xy)] + f^{-1}(xy) = f^{-1}(x)f^{-1}(y) \in \mathfrak{a} \implies y \in f(\mathfrak{a})$ since $\mathfrak{a}$ is prime.

4.3 Commutative ring theory

Proposition 4.4. *Let $\mathfrak{a}, \mathfrak{b} \in \operatorname{Ideals} R$. Then the following hold:*

(a) If $\mathfrak{m} \in \operatorname{mSpec} R$ with $\mathfrak{m} \cap \mathfrak{a} = (0)$, then for all $i, j \geq 0$,

$$\mathfrak{m}^i + \mathfrak{a}^j = R$$

(b) If $\mathfrak{a} + \mathfrak{b} = A$, then

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$$

Proof. (a) We have

$$\begin{aligned} R^{i+j-1} = (\mathfrak{m} + \mathfrak{a})^{i+j-1} &\subseteq \sum_{k=0}^{i+j-1} \mathfrak{m}^k \mathfrak{a}^{i+j-k} \\ &= \mathfrak{a}^j \left(\sum_{k=0}^{i-1} \mathfrak{m}^k \mathfrak{a}^{i-k} \right) + \mathfrak{m}^i \left(\sum_{k=0}^{j-1} \mathfrak{m}^k \mathfrak{a}^{j-k} \right) \subseteq \mathfrak{m}^i + \mathfrak{a}^j \end{aligned}$$

The right side must be in R, so since $R^{i+j-1} = R$, the conclusion must follow.
(b) Clearly $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$. On the other hand, if $x \in \mathfrak{a} \cap \mathfrak{b}$, then $xa + xb = x$ for some $a \in \mathfrak{a}, b \in \mathfrak{b}$. By assumption, xa and xb are elements in $\mathfrak{a}\mathfrak{b}$.

Proposition 4.5. *Let S be a multiplicative set and I be an ideal not intersecting S. Then there is a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ such that $I \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap S = \emptyset$.*

Proof. The set of ideals containing I and missing S is non-empty since I itself belongs in it. The canonical upper bound lies in the set as well, so by Zorn's lemma, there is a maximal element $\mathfrak{p}$. Let $ab \in \mathfrak{p}$. Then the ideals $(\mathfrak{p}, a)$ and $(\mathfrak{p}, b)$ intersect S if $a, b \notin \mathfrak{p}$ by maximality. Since S is multiplicative, $(\mathfrak{p}, a)(\mathfrak{p}, b)$ contains an element of S. But

$$(\mathfrak{p}, a)(\mathfrak{p}, b) = (\mathfrak{p}, ab) \subseteq \mathfrak{p}$$

This contradicts the definition of $\mathfrak{p}$, so a or b must lie in $\mathfrak{p}$ and $\mathfrak{p} \in \operatorname{Spec} R$.

Corollary 4.1. *Let S be a multiplicative set not containing 0. Then there is a prime ideal $\mathfrak{p} \in \operatorname{Spec} R$ such that $\mathfrak{p} \cap S = \emptyset$.*

Proof. Let $I = (0)$ and apply the previous proposition.

4.3.1 Properties of localization

Let $q : R \to S^{-1}R$, and

$$(\cdot)_S : \operatorname{Ideals} R \to \operatorname{Ideals} S^{-1}R$$

$$\cdot \cap R : \operatorname{Ideals} S^{-1}R \to \operatorname{Ideals} R$$

be defined by $\mathfrak{x} \mapsto S^{-1}\mathfrak{x}$ and $\mathfrak{x} \mapsto q^{-1}(\mathfrak{x})$ respectively. The reader should check the first map is well-defined. It's clear the second one is (why?).

Proposition 4.6. *Let $\mathfrak{a} \neq S^{-1}R$ be an ideal in $S^{-1}R$, and let $\mathfrak{b}$ be an ideal in R. Then*

(a) $(\mathfrak{a} \cap R)_S = \mathfrak{a}$
(b) $\mathfrak{b}_S \cap R \supseteq \mathfrak{b}$
(c) $(\mathfrak{a} \cap R) \cap S = \emptyset$

Proof. (a) Let $\mathfrak{a}$ be an ideal of $S^{-1}R$. Let $\mathfrak{b} = \varphi^{-1}(\mathfrak{a})$. If $x/t \in S^{-1}\mathfrak{b}$, then $x \in \varphi^{-1}(\mathfrak{a})$, so $x/1 \in \mathfrak{a}$ implying $(x/1)(1/t) = x/t \in \mathfrak{a}$. If $x/t \in \mathfrak{a}$, then $(x/t)(t/1) = x/1 \in \mathfrak{a}$, so $x \in \mathfrak{b}$, implying $x/t \in S^{-1}\mathfrak{b}$.
(b) If $x \in \mathfrak{b}$, then $x/t \in \mathfrak{b}$, so $(x/t)(t/1) = x/1 \in \mathfrak{b}$, thus $x \in \mathfrak{b} \cap R$.
(c) If $s \in (\mathfrak{a} \cap R) \cap S$, then $s/1 \in \mathfrak{a}$ implying $(s/1)(1/s) = 1 \in \mathfrak{a}$, so $\mathfrak{a} = S^{-1}R$, a contradiction.

Corollary 4.2. *There is a bijection between* $\operatorname{Spec} S^{-1}R$ *and ideals in* $\operatorname{Spec} R$ *not intersecting S given by $(\cdot)_S$ and $\cdot \cap R$.*

Proof. Let $\mathfrak{p}$ and $\mathfrak{q}$ be primes in R and $S^{-1}R$ respectively. By Proposition 4.6, it suffices to show the maps restricted to Spec are well-defined and $\mathfrak{p} \supseteq \mathfrak{p}_S \cap A$.

Maps are well-defined: If $(a/s)(b/t) \in \mathfrak{p}_S, a/s \notin \mathfrak{p}_S$, then $ab \in \mathfrak{p}$ and $a \notin \mathfrak{p}$, so $b \in \mathfrak{p}$. Thus $b/t \in \mathfrak{p}_S$ and $\mathfrak{p}_S$ is prime. If $ab \in \mathfrak{q} \cap R, a \notin \mathfrak{q} \cap R$, then $ab/1 = (a/1)(b/1) \in \mathfrak{q}$ and $a/1 \notin \mathfrak{q}$, so $b/1 \in \mathfrak{q}$. Thus $b \in \mathfrak{q} \cap R$ and $\mathfrak{q} \cap R$ is prime. By Proposition 4.6(c), $(\mathfrak{q} \cap R) \cap S = \emptyset$.

$\mathfrak{p} \supseteq \mathfrak{p}_S \cap R$: If $x \in \mathfrak{p}_S \cap R$, then $x/1 \in \mathfrak{p}_S$, so $xt \in \mathfrak{p}$ for any $t \in S$. Since $\mathfrak{p}$ does not intersect S and is prime, $x \in \mathfrak{p}$.

Corollary 4.3. *$R_\mathfrak{p}$ is a local ring with maximal ideal given by $\mathfrak{p}_\mathfrak{p}$*

Proof. The only prime ideal not intersecting $R \setminus \mathfrak{p}$ is $\mathfrak{p}$ itself and any prime ideal contained in $\mathfrak{p}$. Trivially, $\mathfrak{p}$ is maximal among the ideals contained in it, so $\mathfrak{p}_\mathfrak{p}$ contains all prime ideals by Corollary 4.2. The maximal ideal in $R_\mathfrak{p}$ is prime, so $\mathfrak{p}_\mathfrak{p}$ must contain it, so by maximality, must be equal to it.