Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on:
  `https://japorized.github.io/TeX_notes`

32 Lecture 32 Jul 18th 2018

32.1 Factorizations in Integral Domains (Continued 2)

32.1.1 Ascending Chain Condition (Continued)

Theorem 95 (Integral Domain that Satisfies ACCP has a Polynomial Ring that Satisfies ACCP)

If R is an integral domain satisfying ACCP, so does $R[x]$.

Proof

Suppose not, i.e. $R[x]$ does not satisfy ACCP. Then there exists a chain of principal ideals such that

$$\langle f_1 \rangle \subsetneq \langle f_2 \rangle \subsetneq \langle f_3 \rangle \subsetneq \dots \quad \text{in } R[x]. \tag{32.1}$$

Let a_i be the leading coefficient of f_i. Note that $a_i \in R$. From Equation (32.1), we have that $f_{i+1} \mid f_i$, and so we must have $a_{i+1} \mid a_i$. Then

$$\langle a_1 \rangle \subseteq lraa_2 \subseteq \langle a_3 \rangle \subseteq \dots .$$

Since R satisfies ACCP, $\exists n \in \mathbb{N}$ such that

$$\langle a_n \rangle = \langle a_{n+1} \rangle = \dots ,$$

i.e. $a_n \sim a_{n+1} \sim \dots$. For $m \geq n$, let $f_m = g f_{m+1}$ for some $g(x) \in R[x]$. If $b \in R$ is the leading coefficient of $g(x)$, then $a_m = b a_{m+1}$. Since $a_m \sim a_{m+1}$. b is a unit in R. However, $g(x)$ is not a unit in $R[x]$ since $\langle f_m \rangle \subsetneq \langle f_{m+1} \rangle$. Thus $g(x) \neq b$, which implies $\deg g \geq 1$. Then by

Proposition 82,

$$\deg f_m > \deg f_{m+1},$$

which is true for $m \geq n$. By the same argument, we have that

$$\deg f_m > \deg f_{m+1} > \deg f_{m+2} > \dots,$$

which leads to a contradiction since $\deg f_i \geq 0$ for all $i \in \mathbb{N}$. Thus $R[x]$ must satisfy ACCP. □

Example 32.1.1

Since $\mathbb{Z}$ satisfies ACCP, by Theorem 95, $\mathbb{Z}[x]$ also satisfies ACCP.

32.1.2 Unique Factorization Domains and Principal Ideal Domains

Definition 57 (Unique Factorization Domain (UFD))

*An integral domain R is called a **unique factorization domain** (UFD) if it satisfies the following conditions:*

1. *If $0 \neq a \in R$ is a non-unit, then a is a product of irreducible elements in R.*
2. *If $p_1 p_2 \dots p_r \sim q_1 q_2 \dots q_s$ where p_i and q_i are irreducibles, then $r = s$ and (possibly after relabelling) $p_i \sim q_i$ for each $1 \leq i \leq r = s$.*

Example 32.1.2

Both $\mathbb{Z}$ and $F[x]$, where F is a field, are UFDs.

Example 32.1.3

Any field is a UFD since all elements in a field are either 0 or units.

Recall Proposition 93: If p is a prime, then p is irreducible. In comparison, we have the following:

Proposition 96 (Irreducibles are Primes in a UFD)

Let R be a UFD and $p \in R$. If p is irreducible, then p is a prime.

This also means that in a UFD, primes and irreducibles are the same.

Proof

Let $p \in R$ be an irreducible. If $p \mid ab \in R$, then $\exists d \in R$ such that $ab = pd$. Since R is a UFD, we can factor a, b, and d into irreducible elements, say

$$a = p_1 p_2 \dots p_k$$
$$b = q_1 q_2 \dots q_l$$
$$d = r_1 r_2 \dots r_m.$$

where $k, l, m \in \mathbb{N} \cup \{0\}$. Then

$$ab = pd \iff p_1 \dots p_k q_1 \dots q_l = p r_1 \dots r_m.$$

Since p is irreducible, by Proposition 92, $p \sim p_i$ or $p \sim q_i$. Therefore $p \mid a$ or $p \mid b$, which is the definition of a prime. □

Example 32.1.4

Consider $R = \mathbb{Z}[\sqrt{-5}]$ and $p = 1 + \sqrt{-5}$. We proved that p is irreducible but p is not prime. Then by Proposition 96, we have that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Definition 58 (Greatest Common Divisor)

Let R be an integral domain, and $a, b \in R$. We say $d \in R$ is the ***greatest common divisor*** *of a, b, denoted as $\gcd(a, b) = d$, if it satisfies the following conditions:*

1. *$d \mid a$ and $d \mid b$;*
2. *$e \in R\ e \mid a \wedge e \mid b \implies e \mid d$.*

Proposition 97

Let R be a UFD and $a, b \in R$. If $p_1, \dots, p_k$ are the non-associated primes dividing a and b, say

Exercise 32.1.1
Prove Proposition 97.

$$a \sim p_1^{a_1} \dots p_k^{a_k}$$
$$b \sim p_1^{b_1} \dots b_k^{b_k}$$

with a_i, $b_i \in \mathbb{N}$, *then*

$$\gcd(a,b) \sim p_1^{\min(a_1,b_1)} \dots p_k^{\min(a_k,b_k)}$$

Proof

Let $d = \gcd(a,b)$. *It suffices to show that*

$$d \mid p_1^{\min(a_1,b_1)} \dots p_k^{\min(a_k,b_k)},$$

since $p_1^{\min(a_q,b_1)} \dots p_k^{\min(a_k,b_k)}$ *divides* a *and* b *and so it must also divide* d.

Suppose that $d \nmid p_1^{\min(a_1,b_1)} \dots p_k^{\min(a_k,b_k)}$. *Then* $d \not\sim p_i^{\min(a_i,b_i)}$ *for* $1 \leq i \leq k$. *But that implies that* $d = 1$, *otherwise* $d \nmid a$ *and* $d \nmid b$. *However,*

$$p_1^{\min(a_1,b_1)} \dots p_k^{\min(a_k,b_k)} \nmid 1$$

which contradicts the choice of d *as the greatest common divisor.* □

Note

If R *is a UFD with* $d, a_1, ..., a_m \in R$, *then*

$$\gcd(da_1, da_2, ..., da_m) \sim d \gcd(a_1, ..., a_m).$$

Theorem 98 (UFD and ACCP)

Let R *be an integral domain. TFAE:*

1. R *is a UFD;*
2. R *satisfies ACCP and* $\forall a, b \in R$, $\exists d = gcd(a,b) \in R$;
3. R *satsifies ACCP and every irreducible element in* R *is a prime.*

Proof

(1) $\implies$ (2): *By Proposition 97,* $\forall a, b \in R \quad \exists d = \gcd(a,b) \in R$. *Suppose there exists*

$$0 \neq \langle\, a_1 \,\rangle \subsetneq \langle\, a_2 \,\rangle \subsetneq \langle\, a_3 \,\rangle \; subsetneq \ldots \; in \; R.$$

Since $\langle\, a_1 \,\rangle \neq R$, a_1 *is not a unit*[1] *Since R is a UFD, let* $a_1 \sim p_1^{k_1} \ldots p_r^{k_r}$, *where the* p_i*'s are non-associated primes and* $k_i \in \mathbb{N}$, *for* $1 \leq i \leq r$. *Since* $a_i \mid a_1$ *for* $2 \leq i \leq r$, *we have that*

[1] Otherwise, $1 \in \langle\, a_1 \,\rangle \implies \langle\, a_1 \,\rangle = R$.

$$a_i \sim p_1^{d_{i,1}} p_2^{d_{i,2}} \ldots p_r^{d_{i,r}}$$

where $0 \leq d_{i,j} \leq k_j$ *for* $1 \leq j \leq r$. *This implies that there are only finitely many non-associated choices for* a_i, *which implies that there exists* $m \neq n$ *such that* $a_m \sim a_n \implies \langle\, a_m \,\rangle = \langle\, a_n \,\rangle$, *a contradiction. Therefore, R must satisfy ACCP.*

(2) $\implies$ (3): *Let* $p \in R$ *be an irreducible, and suppose* $p \mid ab$. *By* (2), *let* $d = \gcd(a,p)$. *Then* $d \mid p$, *and by Proposition 92, we have either* $p \sim 1$ *or* $d \sim p$ *since p is an irreducible. If* $d \sim p$, *since* $d \mid 1$, *we have that* $p \mid 1$. *If* $d \sim 1$, *note that we have that*

$$\gcd(ab, pb) \sim b \gcd(a,p) \sim b.$$

Since $p \mid ab$ *and* $p \mid pb$, *we have* $p \mid \gcd(ab,pb)$ *and so* $p \mid b$.

: (3) $\implies$ (1): *R satisfies ACCP implies, by Proposition 96, every non-unit non-zero* $a \in R$ *is a product of irreducible elements in R. It sufficies to prove that the factorization is unique*[2]. *Suppose we have*

[2] This would ssatisfy the definition of a UFD.

$$p_1 p_2 \ldots p_r \sim q_1 q_2 \ldots q_s$$

where p_i *and* q_j *are irreducibles, for* $1 \leq i \leq r$ *and* $1 \leq j \leq s$. *Now* $p_1 \mid p_1 p_2 \ldots p_r$, *and so* $p_1 \mid q_1 q_2 \ldots q_s$. *By Proposition 92 and since* p_1 *is an irreducible,* $p_1 \sim q_j$ *for some* $1 \leq j \leq s$. *We may relabel this* q_j *to be* q_1. *Now since* $p_1 \sim q_1$ *and* $p_1 p_2 \ldots p_r \sim q_1 q_2 \sim q_s$, $\exists a, b \in R$ *that are units suchthat*

$$\begin{aligned} & ap_1 = q_1 \;\; and \;\; p_1 p_2 \ldots p_r = b q_1 q_2 \ldots q_s = ba p_1 q_2 \ldots q_s \\ & \implies p_2 \ldots p_r = baq_2 \ldots q_s \implies p_2 \ldots p_r \sim q_2 \ldots q_s. \end{aligned}$$

By repeating the same argument, we have that $r = s$ *and* $p_i \sim q_i$ *for* $1 \leq i \leq r$. *Therefore the factorization is unique.* $\square$

Definition 59 (Principal Ideal Domain (PID))

An integral domain R is a ***principal ideal domain*** *(PID) if every ideal is principal.*

Example 32.1.5

A field F is a PID since its only ideals are $\{0\} = \langle\, 0 \,\rangle$ and $F = \langle\, 1 \,\rangle$.

Example 32.1.6

$\mathbb{Z}$ and $F[x]$ are PIDs.