Chapter 10.2 part 2

Section 10.2

PID - Principal Ideal Domain

Def A PID is an integral domain in which every ideal is principal

Recall $(a) = \{ar \mid r \in R\}$ for $a \in R$

a principal ideal (generated by $a \in R$)

Not a principal ideal

$(2, x) \subset \mathbb{Z}[x]$

$(2,x) = \{2f + xg \mid f, g \in \mathbb{Z}[x]\}$

Th10.8 Every Euclidean domain is a PID.

Idea of the proof $I \subset R$ - Euclidean domain

Consider $\{\delta(i) \mid i \in I, i \neq 0_R\}$ - a set of non-negative integers, therefore has its minimal element b, meaning $\delta(b) \leq \delta(i)$ for all $i \in I, i \neq 0_R$.

Claim $I = (b)$ - with the help of Euclid's Lemma, one proves that $b \mid i$ for every $i \in I$.

Th10.12 The Fundamental Theorem of Arithmetic holds true in every PID.

A translation of divisibilities into the language of principal ideals

Recall $(a) = \{ra \mid r \in R\}$ $(b) = \{sb \mid s \in R\}$

$a \mid b$ means $b = ra$ means $b \in (a)$ implies (by the absorbtion property) $sb \in (a)$

for any $c \in R$
means $(b) \subseteq (a)$

Th 10.9 Let $a, b \in R$

(1) $(a) \subseteq (b)$ iff $b \mid a$

(2) $(a) = (b)$ iff $b \mid a$ and $a \mid b$

(3) $(a) \subsetneq (b)$ iff $b \mid a$ but $a \nmid b$

For the existence clause of The Fundamental Theorem of Arithmetic we need to avoid the following situation:

$$p_1 \mid a_1 \qquad a_1 = p_1 a_2$$
$$p_2 \mid a_2 \qquad a_1 = p_1 p_2 a_3$$
$$p_3 \mid a_3 \qquad a_1 = p_1 p_2 p_3 a_4$$
$$\dots$$

– We want that to stop at a moment

Example 1 – an example of a situation when that does not stop, and in the integral domain $\mathbb{Q}_{\mathbb{Z}}[x]$ no decomposition into a product of irreducibles exists.
In $\mathbb{Q}_{\mathbb{Z}}[x]$ The Fundamental Theorem of Arithmetic fails for this reason – existence fails

<u>Def</u> An integral domain satisfies Ascending Chain Condition - ACC on principal ideals if for any chain of ideals

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \dots$$

there exists n such that

$$\left.(a_n) = (a_{n+1}) = (a_{n+2}) = \quad\right\} \quad (a_n) = (a_i) \text{ for } i \geq n$$

Lemma 10.10 Every PID satisfies the ACC.

<u>Pf</u> Consider $A = \bigcup_i (a_i)$

Easy to check: $A \subset R$ is an ideal.

Since R is a PID, A must be a principal ideal. $A = (a)$, $a \in R$.

But $a \in A$, therefore $a \in \bigcup_i (a_i)$, thus $a \in (a_n)$ for some n.

It follows that $(a_n) = (a_{n+1}) = (a_{n+2}) \dots$

Existence of a factorization into a product of irreducibles in Th 10.12 follows from Lemma 10.10

Key for the uniqueness in 10.12 - The Fundamental Theorem of Arith for PID's.

Lemma 10.11

Let R be a PID; let $p \in R$ be irreducible.

$p | bc$ implies $p | b$ or $p | c$ (or both)

Th 1.5 for $\mathbb{Z}$

Th 4.12 (2) for $F[x]$

Cor 10.4 Euclidean domains

Pf

$p | bc$ means $bc \in (p)$ | Wanted: $b \in (p)$ or $c \in (p)$

That is, want to claim that the ideal (p) is prime.

(p) is prime will follow from (p) is maximal

Cor 6.16 - every maximal ideal is prime

Assume $(p) \subseteq I \subseteq R$, I - an ideal

Since R is a PID, thus I must be principal: $I = (d)$

$(p) \subseteq (d)$ means $d | p$, but p is irreducible

Thus d may be

either a unit — $(d) = R$

or an associate of p — $(d) = (p)$

Uniqueness in 10.12 follows from Lemma 10.11 in a standard way.

An example of a PID which is not an Euclidean domain.

$\{ a + b \frac{1+\sqrt{-19}}{2} \mid a, b \in \mathbb{Z} \}$ - subring of $\mathbb{C}$

UFD - Unique Factorization Domain - an integral domain where the Fundamental Theorem of Arithmetic holds true.

-def-

- every non-zero non-unit element has a factorization into a product of irreducibles, and this factorization is unique up to permutations and associates

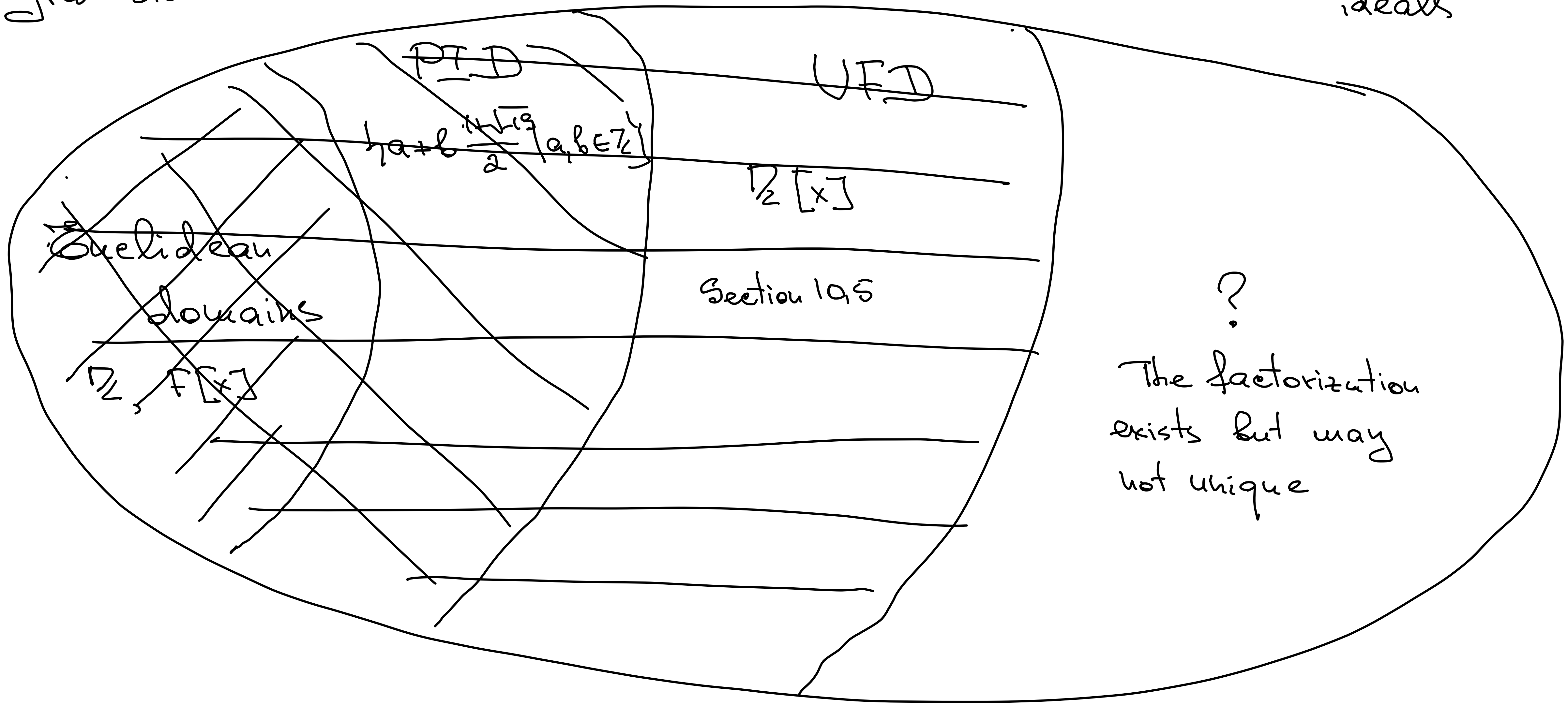
Th 10.16 An integral domain is a UFD iff:

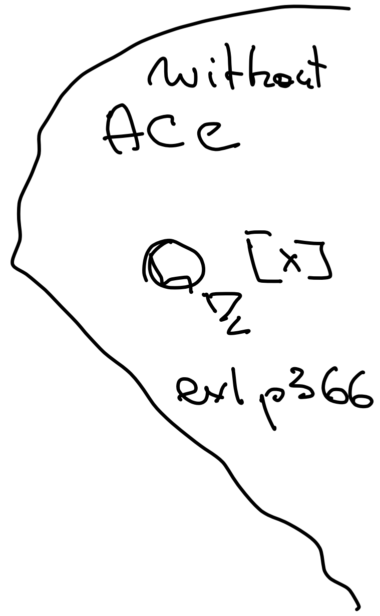
(a) The integral domain has the ACC on principal ideals } existence

(b) wherever p is irreducible, $p|cd$ implies $p|c$ or $p|d$ (or both). } uniqueness

Summarizing diagram
- integral domains

Integral domains with ACC on principal ideals





$\mathbb{Z}[x] \supset (2,x)$ - not a principal ideal

$\mathbb{Q}[x]$ is a UFD

$\mathbb{Z}$ is a UFD