Review of 561/562

(3) Structure of Rings...

A ring is an abstraction of
(1) Integers } commutative
(2) Polynomials }
(3) Matrices } NOT comm.

! In 561/562 all rings are comm. !

DEF: A (comm.) ring with 1 is a tuple $(R, +, \times, 0, 1, =)$ where

- $(R, +, 0, =)$ is abelian group
- $(R, \times, 1, =)$ is abelian semigroup
- $\forall a, b, c \in R$.

$$a \times (b + c) = a \times b + a \times c$$

A map $\varphi : R \to S$ is a ring hom if

- $\forall a, b \in R, \quad \varphi(a+b) = \varphi(a) + \varphi(b)$
- $\forall a, b \in R, \quad \varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$

Ex: Chinese Remainder Theorem.

$\forall a, n \in \mathbb{Z}$ write $[a]_n = a + n\mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ is a ring with $[a]_n$ "$+$" $[b]_n := [a+b]_n$

$[a]_n$ "$\times$" $[b]_n := [ab]_n$

Thm: If $\gcd(m,n) = 1$, then we have

$$\mathbb{Z}/mn\mathbb{Z} \approx \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$[a]_{mn} \longmapsto ([a]_m, [a]_n)$$

ring isomorphism.

Proof: Exercise.

Hint: Since $\gcd(m,n) = 1$ $\exists\, x, y \in \mathbb{Z}$ with $xm + yn = 1$. Show that

$$[bxm + ayn]_{mn} \longmapsto ([a]_m, [b]_n)$$

$\boxtimes$

Cor: Consider groups of units to get

$$(\mathbb{Z}/mn\mathbb{Z})^\times \approx (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

Cor: For m, n coprime, $\varphi(mn) = \varphi(m)\varphi(n)$.

$=$

DEF: Say $I \subseteq R$ is *ideal* if
- $\forall a, b \in I$, $a+b \in I$
- $\forall a \in I, r \in R$, $ar \in I$.

Exercise: $I \subseteq R$ is ideal $\Leftrightarrow$ $\exists$ ring hom $\varphi : R \to R'$ with $\ker \varphi = I$.

Hint: Given ideal $I \subseteq R$ consider the additive group $R/I = \{a + I : a \in R\}$ with projection hom.

$$\begin{aligned} \varphi : R &\longrightarrow R/I \\ a &\longmapsto a + I \end{aligned}$$

Think: Maybe φ is a ring hom?

$$\varphi(ab) = (ab) + I \overset{?}{=:} (a+I)(b+I)$$

Yes. Since I is ideal this is well-defined. ///

DEF: $\forall a \in R$ $\exists$ *principal ideal* $(a) \subseteq R$.

Thm: $\mathbb{Z}$ is PID

Proof: Exercise.

Lattice Isom Thm: Given ideal $I \leq R$ with projection $\varphi : R \to R/I$, get an isomorphism of lattices of ideals

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, dash] & R/I \arrow[d, dash] \\
J \arrow[r, "\varphi"] \arrow[d, dash] & J/I \arrow[d, dash] \\
I \arrow[r, "\varphi"] & I/I = (0)
\end{tikzcd}$$

<u>DEF</u>: Say R is a <u>domain</u> if $\forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ OR $b = 0$.

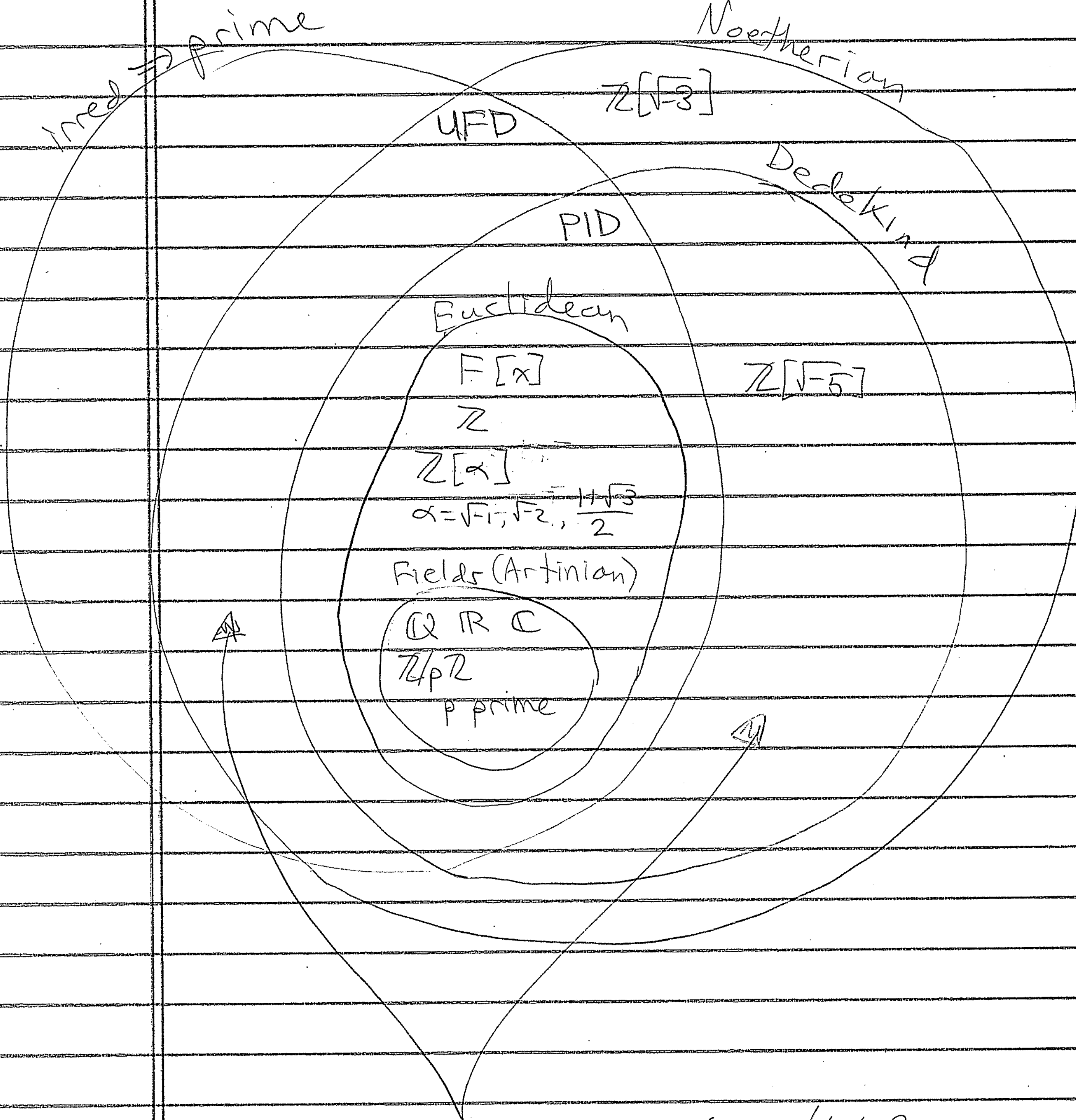
Exercise: Given ideal $I \leq R$, prove:

R/I domain $\iff$ I prime
R/I field $\iff$ I maximal.

Exercise: "domain" = "subring of field"

Exercise: Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD
(See 562 Exam 1 Review).

Domain of Domains



for more see 661/662

Appendix: $F[x]$ (F field)

- Euclidean with norm = deg $\Longrightarrow$ PID. (long division)

- Given fields $F \subseteq K$, $\alpha \in K$, $\exists !$ ring hom $\varphi_\alpha : F[x] \to K$ defined by $\varphi_\alpha(x) := \alpha$.

Notation:
- $\varphi_\alpha(f(x)) =$ "$f(\alpha)$" (evaluation)
- $\ker \varphi_\alpha = (0)$ means α transcendental $/F$
- $\ker \varphi_\alpha \neq (0)$ means α algebraic $/F$.

α alg. $\overset{\text{PID}}{\Longrightarrow} \ker \varphi_\alpha = (m_\alpha(x))$ for monic $m_\alpha(x) \in F[x]$ called minpoly of α / F.

Exercise: $m_\alpha(x)$ irred/prime over F.

- α trans. $\Longrightarrow F[x] \cong \operatorname{im} \varphi_\alpha = F[\alpha]$
- α alg $\Longrightarrow F[x]/(m_\alpha(x)) \cong \operatorname{im} \varphi_\alpha = F(\alpha)$

- if $\deg(m_\alpha(x)) = n$ then $F(\alpha)$ is vector space over F with basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$

$\Longrightarrow [F(\alpha) : F] = \dim_F F(\alpha) = \deg(m_\alpha(x))$.

//