Lecture 25

What's Next?

I Different types of Integral Domains

II Polynomial Rings

III Fields

IV Galois Theory

Algebraic Structure (more ↑)

- Fields $\mathbb{C}$
- Division Rings $\mathbb{H}$
- Integral Domains $\mathbb{Z}$
- With Identity $M_2(\mathbb{Z})$ Commutative $n\mathbb{Z}$
- Rings $M_2(n\mathbb{Z})$ $n>1$

(less)

I Different types of Integral Domains

Properties of $(\mathbb{Z}, +, \cdot)$

- It has no zero divisors.
- It has the Division Algorithm.
- It has the concept of gcd & gcd can be computed algorithmically.
- It has the Bézout's identity.
- It has the concept of prime.
- It has the Fundamental Theorem of Arithmetic (FTOA).
- $\mathbb{Z} \subseteq \mathbb{Q}$ where $\mathbb{Q}$ is the smallest field where every element of $\mathbb{Z}$ becomes a unit.

Motivation

Q: Do all integral domains satisfy the properties of $(\mathbb{Z}, +, \cdot)$? No, they don't.

Q: What does a ring need to behave like $(\mathbb{Z}, +, \cdot)$? It must be an ED.

Integral Domains (ID):

- No zero divisor.
- If D is an ID, there exists a field F_D such that $D \subseteq F_D$ and every element of D is a unit in F_D (the field of fractions).
- Concept of divisibility.

Unique Factorization Domain (UFD):

- Concept of irreducible (= prime).
- Concept of decomposition into irreducibles.
- Unique factorization into irreducibles (i.e. FTOA).

Principal Ideal Domain (PID): An ID where every ideal is principal.

- Concept of gcd (but there is no an algorithm to compute it).
- Bézout's identity.

Euclidean Domain (ED): An ID that posses a Division Algorithm, i.e. there is a map $N: R \longrightarrow \mathbb{N}$ s.t. $N(0_R) = 0$ and $\forall a, b \in R$ s.t. $b \neq 0_R$ $\exists q, r$ s.t.

$$a = bq + r, \quad r = 0_R \quad \text{or} \quad N(r) < N(b)$$

N is called a norm (it's a measure of size).

- Concept of gcd that is algorithmically computable.

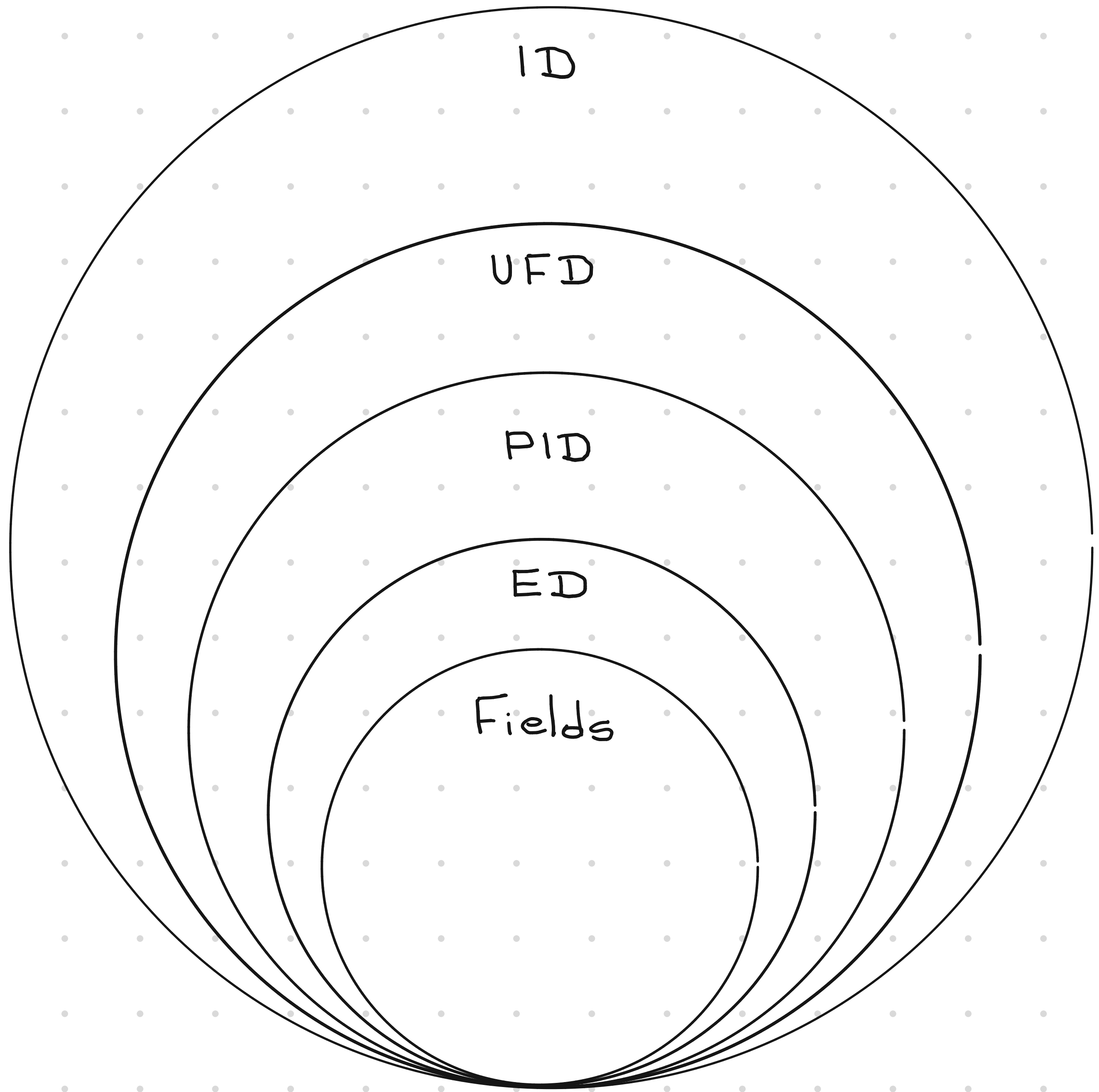
Ex:

$$N: \mathbb{Z} \longrightarrow \mathbb{N}$$
$$a \longmapsto |a|$$

$$N: F \longrightarrow \mathbb{N}, \quad F \text{ a field}$$
$$a \longmapsto 0$$

$$N: F[x] \longrightarrow \mathbb{N}$$
$$p(x) \longmapsto \deg(p(x))$$

Field: An ID where every nonzero element has an inverse.


ID
UFD
PID
ED
Fields

II Polynomial Rings

MOTIVATION

Q: What is the structure of $R[x]$ according to the one of R?

- If F is a field, then $F[x]$ is an ED. Yay! ☺ It satisfies everything $\mathbb{Z}$ does!
- R is an UFD $\iff$ $R[x]$ is an UFD
- Roots: $p(x) \in R[x]$ has a root in R if $\exists\, \alpha \in R$ s.t. $p(\alpha) = 0_R$
- Irreducibility Criteria: Find the irreducible polynomials in $R[x]$.

  Ex: x^2+1 is irreducible in $\mathbb{Z}[x]$ but it is not irreducible in $\mathbb{C}[x]$.

III Fields

MOTIVATION

Consider $p(x) = x^2 + 2$. $p(x)$ is irreducible in $\mathbb{R}[x]$ BUT $p(x) = (x - \sqrt{2}i)(x + \sqrt{2}i)$ in $\mathbb{C}[x]$

$p(x)$ has no roots in $\mathbb{R}$ $p(x)$ has two roots in $\mathbb{C}$

Let F be a field and let $p(x) \in F[x]$.

Q: If $p(x)$ is irreducible in $F[x]$, is there another field K s.t. $F \subseteq K$ and $p(x)$ is reducible in $K[x]$?

Q: If $p(x)$ has no roots in F, is there another field K s.t. $F \subseteq K$ and $p(x)$ has some or all its roots in K?

These are some questions studied in field theory.

Concepts

- Field extensions
- Algebraic extensions
- Splitting fields
- Algebraic closure

IV Galois Theory

Motivation

$ax^2 + bx + c = 0$ can be solved with the formula $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Q: Can we solve any equation $a_n x^n + \cdots + a_1 x + a_0 = 0$ with a formula that only combines $+, -, \times, \div, \sqrt{\ }$?

A: If $n \leq 4$, YES! If $n \geq 5$, NO! ← By Évariste Galois.

Beautiful connection between the structure of groups and the structure of fields.

The Fundamental Theorem of Galois

FIELDS

the roots of $f(x)$ live here!

$f(x) \in F[x]$

$\longrightarrow$

$\longleftarrow$

dictionary between theories

GROUPS

the roots of $f(x)$ are permuted here!

Studying the groups that permute roots is the key to answer the question above.