MATH4302, Algebra II

Jiang-Hua Lu

The University of Hong Kong

Week 1, Thursday January 20, 2022

Outline

Topics for today: §1.2.2 of Lecture notes.

1. Two properties of a PID

Recall from last lecture: Principal Ideal Domains (PID).

Definition. An integral domain R is called a Principal Ideal Domain, or a PID, if every ideal I of R is principal, i.e. $I = aR$ for some $a \in R$.

Examples of PIDs:

- Any field;
- Any Euclidean domain;
- $\mathbb{Z}$;
- $K[x]$ for any field K;
- The ring $\mathbb{Z}[\sqrt{-1}]$ of Gauss integers;

A non-example: The ring $R = \mathbb{Z}[x]$ is an integral domain but not a PID.

Recall from last lecture. Let R be an integral domain.

1. A non-unit $a \in R$ is said to be irreducible if whenever $a = bc$, either b or c is a unit.

2. A non-zero non-unit $a \in R$ is said to be prime if aR is a prime ideal, or, equivalently, if $b, c \in R$ and $a|bc$, then $a|b$ or $a|c$.

$a|b$ means $\exists\ x \in R$ s.t. $b = ax$

Lemma. Every prime element in an integral domain is irreducible.

Example. $\mathbb{Z}(\sqrt{-5})$ is not a PID:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

One then checks that $2 \in \mathbb{Z}(\sqrt{-5})$ is irreducible but not prime.

First property of a PID

Lemma. If R is a PID, then every irreducible element of R is prime.

Proof. Assume that $p \in R$ is irreducible. Want to show that p is prime. Suppose $b, c \in R$ are such that $p \mid bc$. We need to show that either $p \mid b$ or $p \mid c$.

Write $bc = px$, where $x \in R$. Let $I = bR + pR$.

Since R is a PID, $\exists\, a \in R$ st. $I = aR$.

$\Rightarrow bR \subset aR, \quad pR \subset aR$

$\Rightarrow b = ay, \quad p = az$ for some $y, z \in R$

Since p is irreducible, either a is a unit or z is a unit.

① If a is a unit: then $I = R \Rightarrow 1 \in I$

$\Rightarrow 1 = b\alpha + p\beta \quad \Rightarrow c = \underline{bc\alpha} + \underline{pc\beta}$

$\Rightarrow p \mid c.$

(2) z is unit. Then $I = pR$

$\Rightarrow b \in I = pR$

$\Rightarrow p \mid b.$

//

~~A consequence of the first property of a PID:~~

Lemma. A non-zero ideal I in a PID is prime if and only if it is maximal.

Proof. Only need to show that if $I \subset R$ is prime, $I \neq 0$, then R is maximal.

Assume J is an ideal of R st. $J \supseteq I$.

Need to show that $J = I$ or $J = R$. Since R is a PID $\exists\ a \in R$ st. $J = aR$. Let $I = pR$, where p is prime

Since $I \subset J \Rightarrow p \in J = aR \Rightarrow p = ar$ for some $r \in R$

Since p is prime, p is irreducible $\Rightarrow a$ is a unit or r is a unit.

If a is unit, $J = R$

If r is a unit, $aR = pR$ i.e. $J = I$ //

Question: Why do we care so much about irreducible elements in a PID?

Corollary: If R is a PID and $a \in R$ is irreducible, then aR is a maximal ideal so R/aR is a field.

Proof. $a \in R$ irred. $\Rightarrow$ a is prime

$\Rightarrow$ aR is a non-zero prime ideal

$\Rightarrow$ aR is a maximal ideal //

Ex: $R = \mathbb{Z}$

$R = k[x]$, where k is a field

Definition. Let R be an integral domain. An irreducible element in $R[x]$ is called an irreducible polynomial over R.

$f(x) = x^2 + 2x \in \mathbb{Z}[x]$
$\in \mathbb{R}[x]$

Theorem. If $f(x)$ is an irreducible polynomial over a field F, then $F[x]/\langle f(x)\rangle$ is a field containing F as a sub-field.

Proof. A direct consequence of the above corollary.

$F \to F[x]/\langle f(x) \rangle$

$\lambda \longmapsto \lambda + \langle f(x) \rangle$

Remarks:

$\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}\, b : a, b \in \mathbb{Q}\}$
$\subset \mathbb{Q}$

- The Theorem is one of the most important ways of constructing a new field from an old one.
- The theorem raises the problem of classifying/understanding all irreducible polynomials over a field F. The problem is especially interesting if $F = \mathbb{Q}$ or if F is a finite field.

If p is prime number, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \cdots \overline{p-1}\}$