21-237: Math Studies Algebra I	November 2, 2022

Lecture 24 : Integral domains and fields

Lecturer: James Cummings
Scribe: Rajeev Godse

1 Commutative shift

Until further notice, **ring** means unital commutative ring. Then, the distinction etween left, right, and 2-sided ideals and modules disappears, and the definition of subring and ring homomorphism changes to require containment of 1 and mapping of 1 to 1.

2 Quotients redux

If I is an ideal of R, then we can form quotient ring R/I and homomorphism $\phi_I : R \to R_I$. First IM theorem holds: if $\phi : R \to S$, then $R/\ker(\phi) \simeq \mathrm{im}(\phi)$ via $r + \ker(\phi) \leftrightarrow \phi(r)$.

There is a bijection between ideals of R/I and ideals of R containing I (easy: the subgroups of $(R/I, +)$ which are ideals correspond to subgroups of $(R, +)$ which are ideals).

3 Integral domains and fields

R is a **zero ring** $\iff R = \{0_R\} \iff 1_R = 0_R$.

For any ring R, $a \in R$ is a **unit** if and only if a has a multiplicative inverse. (If the inverse exists, it's unique and is written a^{-1}.) The units of R form a group under multiplication, called $U(R)$. We can view U as a functor from the category of rings to the category of abelian groups.

For a ring R and any $a \in R$, the least ideal containing a is denoted (a) and computed by $(a) = Ra = \{ra : r \in R\}$. $(0) = 0 \iff a = 0$. $(a) = R \iff a$ is a unit.

A ring R is an **integral domain** if and only if $1 \neq 0$ and for all $a, b \in R$, $ab = 0 \implies a = 0$ or $b = 0$. An example is $\mathbb{Z}$, while a non-example is $\mathbb{Z}/6\mathbb{Z}$ since $(2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 6\mathbb{Z} = 0$.

We say R is a **field** if $1 \neq 0$ and every nonzero element is a unit. Examples include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Non-examples (which are still integral domains) include $\mathbb{Z}$, $\mathbb{R}[x]$.

Note: If R is a field, then the ideals of R are 0 or R (and conversely, if R has exactly 2 ideals, 0 and R, then R is a field).

Let R be a ring and consider the poset $(\{I : I \text{ ideal of R }, I \neq R\}, \subseteq)$. We say an ideal I of R is **maximal** if it is maximal in this poset, i.e. $I \neq R$ and if ideal $J \neq\supseteq I$, $J = R$ or $J = I$. Examples include $2\mathbb{Z}$.

Theorem: Let I be an ideal of R. The following are equivalent:

(1) R is maximal

(2) R/I is a field

Proof: R/I is a field $\iff R/I$ has exactly 2 ideals (0 and R/I) $\iff$ the only ideals containing I are I and $R \iff I$ is maximal. □

Note: As $2\mathbb{Z}$ is maximal in $\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ is a field.

Fact: Any subring of a field is an ID (integral domain).

An ideal I or R is **prime** if and only if $I \neq R$ and for all $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

Theorem: R/I is an ID $\iff$ I is a prime ideal of R.

Fact: If I is an ideal, $I \neq R$, there is an ideal $J \supseteq I$, J is maximal via Zorn's Lemma.