Lecture 12

01 March 2024 16:07

Last time:

- We defined zero-divisors:

  If $a, b \neq 0$ but $a \cdot b = 0$ then a, b are zero-divisors

- Integral domains are commutative rings with identity without zero-divisors.

- An element u is a unit if it is invertible.

  The inverse of u is unique, denoted u^{-1}.

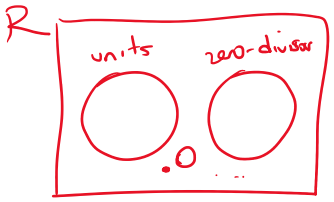
Proposition: Let R a ring with identity.

(a) • If u is a unit then u^{-1} is also a unit.

(b) • If u and v are units, then $u \cdot v$ is also a unit, and $(u \cdot v)^{-1} = v^{-1} \cdot u^{-1}$.

(c) • If u is a unit then u is not a zero-divisor:

Picture



Proof:

(a) If u is a unit, $u \cdot u^{-1} = 1 = u^{-1} \cdot u$.

This equation also shows that u^{-1} is a

This equation also shows that u^{-1} is a unit and $(u^{-1})^{-1} = u$.

(b) To show that $(uv)^{-1} = v^{-1}u^{-1}$, let's compute

$$(u \cdot v)(v^{-1}u^{-1}) = u \cdot (v \cdot v^{-1}) \cdot u^{-1}$$
$$= u \cdot 1 \cdot u^{-1}$$
$$= u \cdot u^{-1}$$
$$= 1.$$

$$(v^{-1}u^{-1}) \cdot (uv) = v^{-1}(u^{-1} \cdot u)v$$
$$= v^{-1} \cdot 1 \cdot v$$
$$= v^{-1}v$$
$$= 1$$

(c) Suppose u is a unit.

To show that u is not a zero-divisor,

Suppose $u \cdot b = 0$

Multiplying by u^{-1} on both sides we get

$$u^{-1} \cdot u \cdot b = u^{-1} \cdot 0$$

$$1 \cdot b = 0$$

$$b = 0$$

so 0 is not a zero-divisor.

Corollary: Any nonzero element in a field is a unit and therefore not a zero-divisor.

So every field is an integral domain.

Ex: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Question: What are the units and the zero-divisors of $\mathbb{Z}_m$?

Proposition: Suppose $[x]_m$ is a nonzero elemt of $\mathbb{Z}_m$.

- If $g.c.d(x, m) = 1$ then $[x]_m$ is a unit.
- If $g.c.d(x, m) > 1$ then $[x]_m$ is a zero-divisor.

Proof: Suppose $g.c.d(x, m) = 1$. By the Euclid's Algorithm, we can write

Extended Euclid's Algorithm, we can write

$$p \cdot x + q \cdot m = 1 \quad \text{with} \quad p, q \in \mathbb{Z}$$

Taking this equation modulo m, we get

$$[1]_m = [px + qm]_m = [px]_m = [p]_m \cdot [x]_m$$

so $[x]_m$ is a unit and $[x]_m^{-1} = [p]_m$.

If $\text{g.c.d.}(x, m) = d > 1$, consider $\frac{m}{d}$.

↓ integer less than m.

We have

$$[x]_m \cdot \underbrace{\left[\frac{m}{d}\right]_m}_{\text{not } [0]_m \text{ because } \frac{m}{d} < m.}$$

$$= \left[x \cdot \frac{m}{d}\right]_m = \left[\underbrace{\frac{x}{d}}_{\text{integer as } d \mid x.} \cdot m\right]_m = [0]_m$$

so $[x]_m$ is a zero-divisor.

Corollary: If p is a prime number then $\mathbb{Z}_p$ is a field (because any $0 < x < p$ satisfies $\text{g.c.d}(x, p) = 1$ so $[x]_p$ is a unit).

Associates

Suppose R is a commutative ring with identity (R is a domain).

Two elements $a, b \in R$ are called <u>associates</u> if $b = u \cdot a$ for u a unit of R.

We denote this as $b \sim a$.

<u>Proposition:</u> This relation is an equivalence relation.

<u>Proof</u>:

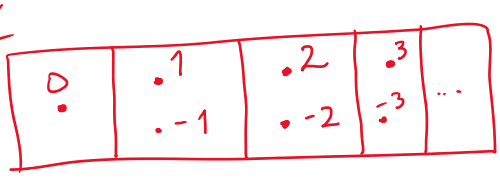
- <u>Reflexive</u>: $a \sim a$ since $a = 1 \cdot a$ (1 is a unit).
- <u>Symmetric</u>: If $a \sim b$ then $b \sim a$ because if $a = u \cdot b$ (u unit) and so $u^{-1} \cdot a = b$ (u^{-1} unit), thus $b \sim a$.
- <u>Transitive</u>: If $a \sim b$ and $b \sim c$, this means that $a = u \cdot b$ (u unit) $b = v \cdot c$ (v unit), so $a = u \cdot (v \cdot c) = (u \cdot v) \cdot c$, so

unit

$a \sim c$.

Def. The equivalence classes of $\sim$ are called **associate classes**. They form a partition of R.

Ex: For $R = \mathbb{Z}$, the partition into associate classes is



Exercises:

- Consider $R = \mathbb{Z}_{56}$ ← integers modulo 56.
  - Is $[15]_{56}$ a unit in R? If so, compute $[15]_{56}^{-1}$.
  - Is $[24]_{56}$ a zero-divisor? If so, find some $x \in R$ nonzero such that $[24]_{56} \cdot x = 0$.
- Draw the partition of $\mathbb{Z}_{18}$ into associate classes.

Previous topic:

[Previous topic]

- Use the 1st Iso. Thm to prove

$$\mathbb{R}[x] \Big/ \{f \mid f \text{ is divisible by } x-2\} \cong \mathbb{R}.$$

Answers: • Euclid's Extended Algorithm

$$15 \cdot 15 + (-4) \cdot 56 = 1$$

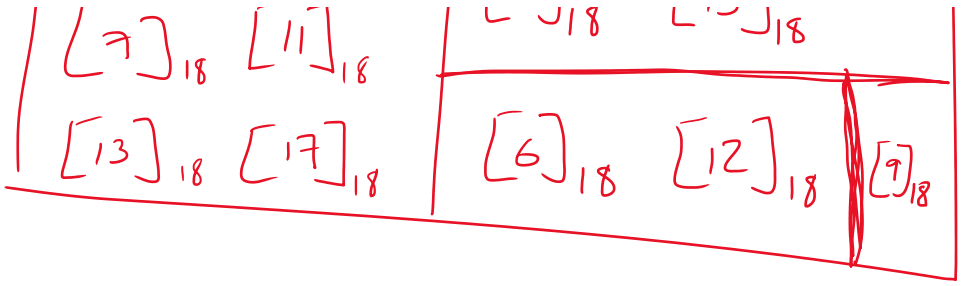
$$[15]_{56}^{-1} = [15]_{56}$$

- $[24]_{56} \cdot [\ \ ]_{56} = [0]_{56}$

multiple of 7

- $\mathbb{Z}_{18}$

$[0]_{18}$	$[2]_{18}$	$[16]_{18}$	$[10]_{18}$	$[14]_{18}$
			$[4]_{18}$	$[8]_{18}$
$[1]_{18}$	$[5]_{18}$			
$[7]_{18}$	$[11]_{18}$		$[3]_{18}$	$[15]_{18}$


[7]18 [11]18
[13]18 [17]18
[6]18 [12]18
[9]18