①

Recall: $\mathbb{Z}_n$ is a ring, $n \in \mathbb{N}$

$\mathbb{Z}_5$ $U(5)$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbb{Z}_6$

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

$U(6) = \{1, 5\}$

<u>Def</u> Let R be a ring, elements $a \neq 0$ and $b \neq 0$ are called zero-divisors if $ab = 0$.

<u>Ex:</u> In $\mathbb{Z}_6$ the elements 2 and 3 are zero divisors.

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

<u>Thm</u> An elt. $x \in \mathbb{Z}_n$ is a zero-divisor if and only if $\gcd(x, n) > 1$. I.e. x and n are not coprime.

(2) Pf Let $\overset{x\neq 0}{a\neq 0}$ in $\mathbb{Z}_n$.

If $xa = 0$ in $\mathbb{Z}_n$, then

$m \mid xa$

$a \neq 0$: $m \nmid a$

$x \neq 0$: $m \nmid x$

$m = p_1 \cdots p_k$

some p_i divides x.

If $\gcd(x, n) = d > 0$

$x(n/d) = (x/d)n = 0$ in $\mathbb{Z}_n$

$(n/d)x = n(x/d) = 0$ □

$m = n$

Ex $2^2 = 0$ in $\mathbb{Z}_4$.

Corollary $\mathbb{Z}_p$ has no zero-divisors if and only if p is a prime.

Cancellation

In a group G: $ga = gb$
$$\Downarrow$$
$$g^{-1}(ga) = g^{-1}(gb)$$
$$\Downarrow$$
$$a = b$$

In $\mathbb{Z}_6$: $3 \cdot 2 = 3 \cdot 4 \not\Rightarrow 2 = 4$

In a ring R the Cancellation Law holds if $ax = ay$ implies $x = y$, for $a \neq 0$.

Thm The cancellation Law holds in R if and only if R has no zero-divisors.

Pf "Only if". Let $a \neq 0$ and assume $ab = 0$. With $ab = 0 = a0$ the cancellation law gives $b = 0$.

"If": $\underset{a \neq 0}{ax} = ay \Rightarrow ax - ay = 0$

$\Rightarrow a(x-y) = 0$

$\Rightarrow x - y = 0$ as a not a zero-div

$\Rightarrow x = y$. $\square$

(4)

<u>Def</u> A ring R is called an integral domain if

(1) R commutative

(2) R has unity 1

(3) R has no zero-divisors.

<u>Ex</u> $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

— x —

$$(A+B)^2 = A^2 + AB + BA + B^2 \neq A^2 + 2AB + B^2$$

$x^2 - x = 0$ has 3 solutions in $\mathbb{Z}_6$:

$x(x-1) = 0$

$x = 0$

$x = 1$

$x = 3$

— x —

<u>Defn</u> Let R be a ring with 1.
An element $u \in R$ is called a
<u>unit</u> if there exist $a \in R$
with $au = 1 = ua$. We write $a = u^{-1}$.

(Uniqueness: $au = 1 = ua$, $bu = 1 = ub$:
$a = a1 = a(ub) = (au)b = 1b = b$)

⑤ **Thm** Let R be a ring with 1.
If u is a unit in R, ~~then~~ u
is <u>not</u> a zero-divisor.

Pf Let u be a unit and
$ub = 0$.

$$0 = u^{-1}(ub) = (u^{-1}u)b = 1b = b$$

Corollary $x \in \mathbb{Z}_n$ is $\begin{cases} \text{a unit if } \gcd(x,n) = 1 \\ \text{a zero-div if } \gcd(x,n) > 1 \end{cases}$

Recall that the units in $\mathbb{Z}_n$ form
the group $U(n)$.

Thm. Let R be commutative with 1.
The collection $U(R)$ of all units
in R form a group under mult.

Pf (closure) Let $a, b \in U(R)$

$$(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$$

(associativity) ✓
(identity) $1 \cdot 1 = 1$, so $1 \in U(R)$
(inverse) $aa^{-1} = 1 = a^{-1}a$

$$(a^{-1})^{-1} = a.$$