

Lecture 9 (The Ideals of \mathbb{Z} and Divisibility)

Last time we defined ideals.

A subring I of a ring S such that $rx, xr \in I$ for all $x \in I, r \in R$ is called an *ideal*.

Note if I closed under multiplication on the left and right by elements of R then it is certainly closed under multiplication. So a non-empty subset of \mathbb{R} is an ideal if and only if for all $a, b \in I$ and $r \in R$ the following hold.

$$(1) \quad a + b \in I.$$

$$(2) \quad -a \in I.$$

$$(3) \quad ra, ar \in I.$$

Note if R is a ring with identity 1, then (2) is redundant as it follows from (1) and (3), using $-a = (-1)a$.

For any ring $I = R$ and $I = \{0\}$ are ideals of R .

We now consider the ring \mathbb{Z} and in particular find all its ideals and more.

Definition 9.1 (Division) For $b \neq 0$ we write $b|a$ if b divides a , i.e. if a is an integer multiple of b : $a = bm$ for some $m \in \mathbb{Z}$.

Elementary Properties 9.2

$$(1) \quad a|1 \text{ if and only if } a = \pm 1.$$

$$(2) \quad a|b \text{ implies } a|bm \text{ for all } m \in \mathbb{Z}.$$

$$(3) \quad a|b \text{ and } b|c \text{ implies } a|c.$$

$$(4) \quad a|b \text{ and } b|c \text{ if and only if } a|bm + cn \text{ for all } m, n \in \mathbb{Z}.$$

Exercise Verify these properties.

9.3 (Division with Remainder – Euclid) For $a, b \in \mathbb{Z}, b \neq 0$ there are unique integers q (quotient) and r , (remainder) such that

$$a = bq + r, \quad 0 \leq r < |b|.$$

Modular Arithmetic Review of modular arithmetic ring theoretic terms. Recall for a positive integer m , we write for integers x and y , $x \equiv y \pmod{m}$ if m divides $x - y$.

Exercise: Verify this is an equivalence relation on \mathbb{Z} .

Set $\mathbb{Z}_m = \mathbb{Z}/\equiv$ and let $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_m$ be the canonical map $x \mapsto \bar{x}$. Note this is a surjection.

The equivalence class \bar{x} of $x \in \mathbb{Z}$ is all integers which leave the same remainder on division by m as x . Hence \mathbb{Z}_m has m elements $\bar{0}, \bar{1}, \dots, \overline{m-1} \in \mathbb{Z}_m$.

Suppose $\bar{x} = \bar{x}'$ and $\bar{y} = \bar{y}'$, i.e. $x - x'$ and $y - y'$ are divisible by m .

Then

$$(x + y) - (x' + y') = (x - x') + (y - y')$$

is divisible by m as is

$$(xy - x'y') = (x - x')y + x'(y - y').$$

Hence we can define addition and multiplication in \mathbb{Z}_m by

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x}\bar{y} = \overline{xy}.$$

Because the canonical map θ , which maps \mathbb{Z} onto \mathbb{Z}_m preserves addition and multiplication, ring properties involving addition and multiplication hold in \mathbb{Z}_m whenever they hold in \mathbb{Z} , c.f. **Tutorial 2, Q1**. For example, from the left distributive law $x(y + z) = xy + xz$ in \mathbb{Z} we have $\bar{x}(\bar{y} + \bar{z}) = \bar{x}\bar{y} + \bar{x}\bar{z}$ in \mathbb{Z}_m . Hence the distributive law holds in \mathbb{Z}_m . Similarly you show the other ring axioms hold in \mathbb{Z}_m , that multiplication is commutative and that \mathbb{Z}_m has identity element $\bar{1}$.

So \mathbb{Z}_m into a commutative ring with identity $\bar{1}$. Further the canonical map from \mathbb{Z} to \mathbb{Z}_m is a homomorphism of rings.

What is the kernel of this homomorphism?

Answer: The kernel is $\{x \in \mathbb{Z} \mid \bar{x} = 0 (= \bar{0})\}$, the set of all x divisible by m . Hence all such sets are ideals of \mathbb{Z} .

Notation: For any $m \in \mathbb{Z}$, $m\mathbb{Z} = \{mx \mid m \in \mathbb{Z}\}$.

Note $m\mathbb{Z} = m'\mathbb{Z}$ if and only if $m = \pm m'$, and $0\mathbb{Z} = \{0\}$ is an ideal.

Proposition 9.4 (The Ideals of \mathbb{Z}) The ideals of \mathbb{Z} are $m\mathbb{Z}$, $m = 0, 1, \dots$

Proof From above all these subsets are ideals of \mathbb{Z} . It remains to show these are the only ideals.

If $I = \{0\}$, done. Suppose $I \neq \{0\}$. Then I has a non-zero element x . Because I is an ideal $\pm x \in I$, and one of these is positive. Hence $I^+ = \{x \in I \mid x > 0\}$ is non-empty. Let m be the least element of I^+ .

[Recall any non-empty subset of \mathbb{N} has a least element.]

Claim: $I = m\mathbb{Z}$.

First $m \in I$ implies all multiples of m lie in I , because ideals of a ring are closed under multiplication by elements of the ring. So $m\mathbb{Z} \subseteq I$.

It is sufficient now to show $I \subseteq m\mathbb{Z}$.

Let $a \in I$. Then division by m gives $a = mq + r$, $0 \leq r < m$. From above $(-m)q \in I$. Ideals are closed under multiplication. Hence $r = a + (-m)q \in I$. But m is the least positive integer in I . Hence $r = 0$. Thus $a = mq \in m\mathbb{Z}$. \square

An integer $d > 0$ is called a *greatest common divisor*, (g.c.d.) of integers a and b if

- (1) $d|a$ and $d|b$. (i.e. d is a common divisor.)
- (2) $e|a$ and $e|b$, $e|d$. (no common divisor can have $e > d$.)

Proposition 9.5 If integers a and b are not both 0 they have a greatest common divisor d and there are integers m and n such that $am + bn = d$.

Proof Set $I = \{am + bn \mid m, n \in \mathbb{Z}\}$. Then I is an ideal of \mathbb{Z} containing a and b . By the assumption a and b not both 0, $I \neq \{0\}$ and hence $I = d\mathbb{Z}$ for some positive integer d . This $d \in I$. So for some integers m and n , $am + bn = d$.

Claim d is the g.c.d of a and b .

- (1) Because $a, b \in I = d\mathbb{Z}$, $d|a$ and $d|b$.
- (2) If $e|a$ and $e|b$ then $e|ax + by$ for all $x, y \in \mathbb{Z}$. Hence $e|d = am + bn$. \square

Notation For a, b in \mathbb{Z} , not both 0, their g.c.d is denoted (a, b) .

Definition 9.6 Integers a and b such that $(a, b) = 1$ are called relatively prime.