

①

A RING IS A SET  $R$  WITH TWO LAWS OF COMPOSITION, ADDITION & MULTIPLICATION, SATISFYING

1)  $(R, +)$  IS A COMM GRP

2)  $\cdot$  IS ASSOCIATIVE WITH A UNIT

3)  $\forall x, y, z \in R, (x+y)z = xz + yz$  &  $z(x+y) = zx + zy$ .

$\text{id}_{(R,+)} = 0$        $\text{id}_{(R,\cdot)} = 1$

IN FACT, I WILL ASSUME THAT THE RING IS COMMUTATIVE, I.E. THAT  $xy = yx \forall x, y \in R$ .

LET'S PROVE 3 ELEMENTARY FACTS ABOUT RINGS

(1)  $0x = 0 \forall x \in R$

(2)  $\forall x, y, (-x)y = -xy$

(3)  $(-x)(-y) = xy$

Pf;

$$(1) \quad 0x + x = (0+1)x = 1 \cdot x = x$$

$$0x + x = x$$

$$0x = 0$$

$$(2) \quad xy + (-x)y = (x + (-x))y$$

$$= 0y$$

$$= 0$$

$$(-x)y = -(xy)$$

$$(3) \quad \text{~~if } x=1 \text{ in (2), } -(1 \cdot y) = -y = -1 \cdot y~~$$

$$\bullet \quad \text{~~if } x=1 \text{ in (2), } -(1 \cdot y) = -y = -1 \cdot y~~$$

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

$$\text{if } x=1 \text{ in (2), } -(1 \cdot y) = -y = -1 \cdot y$$

$$(-x) \cdot (-1) \cdot y = 0$$

$$0 \cdot y = 0$$

(2)

Examples:  $\circ \mathbb{Z}$  IS A RING UNDER  $(+, \cdot)$ .

- CLEARLY  $(\mathbb{Z}, +)$  IS AN ABELIAN GROUP.

-  $(i \cdot j) \cdot k = i \cdot (j \cdot k) \quad \forall i, j, k$

-  $i(j+k) = i \cdot j + i \cdot k$

$\circ \mathbb{R}$  IS A RING UNDER  $(+, \cdot)$

$\circ \mathbb{Z}_2$  IS A RING UNDER  $(+, \cdot)$

" $\{0, 1\}$ "  $\Rightarrow \left\{ \begin{array}{l} 0+1=1 \\ 1+1=0 \\ 0+0=0 \end{array} \right\}$

(1) THIS IS COMMUTATIVE  $\uparrow$

(2) ASSOC. IS TRIVIAL

(3) DISTRIB IS TRIVIAL

$\circ \{0\}$  IS A RING ( $0_R = 1_R = 0$ )

LET  $R$  BE A RING,  $\mathcal{U} \subset R$  BE THE SUBSET OF ELEMENTS WITH A MULTIPLICATIVE INVERSE;  $\forall r \in \mathcal{U} \exists r^{-1} \in \mathcal{U}$  WITH  $r \cdot r^{-1} = 1_R$ .

NOTE THAT  $\forall r, s \in \mathcal{U}$ ,  $r \cdot s \in \mathcal{U}$ , SINCE  $s^{-1} r^{-1} = (r \cdot s)^{-1}$ .

INDEED,  $\mathcal{U}$  IS IN FACT A MULTIPLICATIVE GROUP, THE GROUP OF UNITS OF THE RING.

$\circ \mathcal{U}_{\mathbb{Z}} = \{1, -1\}$

$\circ \mathcal{U}_{\mathbb{Z}_2} = \{1\}$

$\circ \mathcal{U}_{\mathbb{R}} = \mathbb{R} \setminus \{0\}$

IF  $\bullet$  EVERY NON-ZERO ELEMENT OF A RING IS INVERTIBLE, IT IS CALLED A FIELD;

$\circ \mathbb{R}$

$\circ \mathbb{C}$

$\circ \mathbb{Z}_2$

(3)

NOTE THAT  $\mathbb{Z}_2 = \{0, 1\}$  IS THE MINIMAL FIELD;  $\nexists$  1-ELEM FIELDS.

CONSIDER A SUBSET  $S \subset R$  WHICH IS ~~CLOSED~~  
AN ABELIAN SUBGROUP UNDER ADDITION, ~~FIELD~~ CONTAINS 1,  
& IS CLOSED UNDER MULTIPLICATION. THEN  $S$  IS CALLED  
A SUBRING.

- $\mathbb{Q} \subset \mathbb{R}$  IS A SUBRING (IN FACT, A SUBFIELD)
- $\mathbb{Z} \subset \mathbb{R}$  IS A SUBRING
- $\mathbb{R} \subset \mathbb{C}$  — " —

NOTE THAT  $\mathbb{Z}_2 \subset \mathbb{Z}$  IS NOT A SUBRING, SINCE ADDITION IS DIFFERENT. ALSO,  $2\mathbb{Z} \subset \mathbb{Z}$  IS NOT A SUBRING, SINCE IT DOES NOT CONTAIN 1.

THIS LAST FACT LEADS US TO IDEALS; AN IDEAL  $I \subset R$   
IS A SUBGROUP UNDER ADDITION, &  
 $\forall r \in R \ \& \ i \in I, \ r \cdot i \in I$

THUS  $2\mathbb{Z}$  IS NOT A SUBRING BUT IT IS AN IDEAL: CLEARLY  
THE EVEN INTS IS AN ADDITIVE SUBGROUP, & IF  $j \in \mathbb{Z}$   
&  $2i \in 2\mathbb{Z}$   $j \cdot 2i \in 2\mathbb{Z}$ .

◦ LET  $R$  BE ANY RING. THEN  $\{0\} \subset R$  IS THE ZERO-IDEAL

◦ SUBRINGS ARE NOT NECESSARILY IDEALS;  $\mathbb{Q} \subset \mathbb{R}$  IS A  
SUBRING, BUT  $\pi \cdot \frac{1}{2}$  IS NOT A RAT<sup>l</sup>.

(4)

## RING HOMOMORPHISMS.

LET  $A$  &  $B$  BE RINGS &  $f: A \rightarrow B$  A MAP OF SETS.

IF,  $\forall a \text{ & } a' \in A$ ,

$$f(a+a') = f(a) + f(a')$$

$$f(a)f(a') = f(aa')$$

$$f(1) = 1$$

$$f(0) = 0$$

THEN  $f$  IS CALLED A RING HOMOMORPHISM.

•  $i: \mathbb{Z} \rightarrow \mathbb{R}$  IS A RING HOM<sup>m</sup>

•  $\exp: \mathbb{Z} \rightarrow \mathbb{C}$  IS NOT A RING HOM<sup>m</sup>

$$\exp(2\pi i(j+k)) \neq \exp(2\pi i)j + \exp(2\pi i)k$$

•  $\text{Re}: \mathbb{C} \rightarrow \mathbb{R}$  IS NOT A RING HOM<sup>m</sup>

$$\text{Re}(x+y) = \text{Re } x + \text{Re } y$$

$$\text{Re}(x \cdot y) \neq \text{Re}(x) \text{Re}(y)$$

IF  $f: A \rightarrow B$  IS A RING HOM<sup>m</sup>, ITS KERNEL IS THE KERNEL OF  $f$  AS A ~~Map~~<sup>Hom</sup> OF ABELIAN GROUPS.

NOTE THAT BY FORGETTING " $\cdot$ ", ANY RING IS AN AB. GRP.

•  $\text{ker } i: \mathbb{Z} \rightarrow \mathbb{R} = \{0\}$

INDEED,  $\text{ker } f$  IS AN IDEAL OF  $A$ : IF  $a \text{ & } b \in \text{ker } f$ , &  $c \in A$

$$f(a+b) = f(a) + f(b) = 0$$

$$f(ca) = f(c)f(a) = f(c) \cdot 0 = 0$$

$$f(-a) = f(-1 \cdot a) = f(-1) \cdot f(a) = 0$$

(5)

Let  $f: A \rightarrow B$  be a ring homomorphism. Then  $\text{Im } f$  is a subring of  $B$ .

Let  $R$  be any ring. Then  $\exists!$  ring homomorphism  $\lambda: \mathbb{Z} \rightarrow R$  defined by  $\lambda(n) = n \cdot 1_R \equiv \underbrace{1_R + \dots + 1_R}_{n \text{ times}}$

~~NOTE THAT USE  $\lambda$~~  A ring-homomorphism is an isomorphism if it has a 2-sided inverse; equivalently, if it is bijective.

POLYNOMIAL RINGS ARE A VERY IMPORTANT CLASS OF RINGS. I WON'T GIVE A PRECISE DEFINITION OF A POLYNOMIAL RING, SINCE WE ALL KNOW "HOW" TO USE THEM, & THE DEFINITION PROVIDES NO HUGE INSIGHTS. WE WILL TREAT A POLYNOMIAL WITH COEFFICIENTS IN A RING  $R$  AS FORMAL COMBOS OF THE FORM

$$r x_1^{i_1} \dots x_n^{i_n}$$

WITH  $r \in R$  &  $i_1, \dots, i_n \geq 0$ , & ADDITION & MULT<sup>n</sup> OF TERMS DEFINED AS YOU WOULD EXPECT. THE RING OF ALL SUCH FORMS IS DENOTED

$$R[x_1, x_2, \dots, x_n].$$

NOTE THAT  $R \subset R[x_1, x_2, \dots, x_n]$  IS A SUBRING, AS IS  $R[x_1, x_2, \dots, x_{n-1}]$ .

CONSIDER  $\mathbb{C}[x]$ ,  $\mathbb{C}$  POLYNOMIALS IN 1-VARIABLE. CONSIDER ALL POLYS OF THE FORM  $\kappa f(x)$ . THIS SET SUBSET FORMS AN IDEAL;

$$\kappa g(x) + \kappa f(x) = \kappa (g(x) + f(x))$$
$$\kappa \cdot g(x) \cdot \kappa f(x) = \kappa (\kappa g(x) f(x))$$

(6)

THIS IS THE IDEAL GENERATED BY  $\alpha$ , WRITTEN  $(\alpha)$ . AN IDEAL  $I$  OF A RING  $R$  IS GENERATED BY  $\{r_i\} \in I$  IF ANY ELEMENT  $i \in I$  CAN BE WRITTEN

$$r_1 s_1 + r_2 s_2 + \dots + r_n s_n \quad s_n \in R$$

I CAN ALSO BE WRITTEN AS  $(r_1, r_2, \dots, r_n)$ .

Ex:  $R = \mathbb{C}[x, y]$ ,  $I = (x, y)$ .

I IS THE SET OF POLYS

$$x f(x, y) + y g(x, y), \quad f, g \in R$$

$R = \mathbb{C}[x, y]$ ,  $I = (f(x, y))$   $f(x, y) = x^2 + 1$

I IS THE SET OF POLYS

$$(x^2 + 1) g(x, y) \quad \text{WITH } g \in R$$

$R = \mathbb{Z}$ ,  $I = (n)$

I IS THE SET OF INTEGER MULTIPLES OF  $n$   
 $n \cdot i$

LET'S THINK ABOUT THIS LAST EXAMPLE A BIT MORE, IN THE CASE WHERE  $n$  IS A PRIME NUMBER  $p$ . THEN IF  $i \cdot j \in (p)$  IF  $i, j \in \mathbb{Z}$   $\&$   $i \cdot j \in (p)$ ,  $i \in (p)$  OR  $j \in (p)$

Pf:  $i \cdot j = kp$  FOR SOME  $k \in \mathbb{Z}$ . ASSUME  $i \notin (p)$ ,  
 $\&$  WRITE  $i = \prod_{j \in \mathcal{P}} p_j^{i_j}$   
 $k \in \mathbb{Z}$

DECOMP BY PRIMES IS UNIQUE  $\prod_{j \in \mathcal{P}} p_j^{i_j} \prod_{k \in \mathcal{P}} p_k^{j_k} = \prod_{l \in \mathcal{P}} p_l^{n_l} p$

(7)

THIS LEADS TO THE CONCEPT OF A PRIME IDEAL.  
 $\mathfrak{p} \neq R$

AN IDEAL  $\mathfrak{p} \subset R$  IS PRIME IF  $\forall x, y \in R$  S.T.  
 $x \cdot y \in \mathfrak{p}$ ,  $x \in \mathfrak{p}$  OR  $y \in \mathfrak{p}$

EX;  $(x) \subset \mathbb{C}[x]$  IS PRIME

IF  $f(x) \in (x)$ ,  $f(x) = x g(x)$ ,  $\exists x \in (x)$

$(x^2 - 1) \subset \mathbb{C}[x]$  IS NOT PRIME

$x+1$  &  $x-1$  ARE NOT OF THE FORM

$(x^2 - 1) f(x)$ , BUT  $(x+1)(x-1) = (x^2 - 1) \cdot 1 \in (x^2 - 1)$

$(0) \subset \mathbb{C}[x]$  IS PRIME

~~A MAXIMAL IDEAL~~

$(1)$  IS NOT PRIME, SINCE  $(1) = R \forall R$ .