

Rings Intro I

Def a ring has 1, but it could be that  $1 = 0$ .

- ①  $(R, +, 0)$  is an abelian gr
- ②  $(R, \cdot, 1)$  is a monoid
- ③  $a(b+c) = ab + ac$   
 $(a+b)c = ac + bc$

Example  $\mathbb{Z}$ .

Observation:  $\forall a, b \in R, \quad (1+1)(a+b) = 1(a+b) + 1(a+b) = a+b+a+b$

$$\text{Also, } (1+1)(a+b) = (1+1)a + (1+1)b = a+a+b+b$$

$$\text{so } b+a = a+b.$$

(additive gr must be abelian by dist. laws).

ex:  $\mathbb{Z}_3$ . Can  $2^2 = 0$  or  $2$ ?

ex if  $ab = ba$ ,  $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ .

Note  $R = 0$  iff  $1 = 0$ .

Def  $R$  is a domain (integral domain)  
if  $R^* = R \setminus \{0\}$  is a submonoid of  $(R, \cdot, 1)$ .

(So  $0$  is not a domain).

prop  $R$  is a domain iff  $R \neq 0$  and  $\forall a, b \in R, ab = 0 \Rightarrow a = 0$  or  $b = 0$ .  
[equivalently if  $a, b \in R^*$  then  $ab \neq 0$ ].

Note  $M_n(R)$  is not commutative if  $R \neq 0$  and  $n > 1$ .

Note  $[0, 1]^{\mathbb{R}}$  is not a domain.

prop  $R$  is a domain iff  $R \neq 0$  and the cancellation laws hold:

$$ab = ac, a \neq 0 \Rightarrow b = c$$

$$ac = bc, c \neq 0 \Rightarrow a = b.$$

pf distributive law

Def  $a \in R$  is a <sup>(left)</sup> zero divisor if  $\exists b \neq 0$  s.t.  $ab = 0$ .

Ex  $0$  is a zero divisor, if  $R \neq 0$ .

Def a subring has 1.

Def  $R$  is a division ring if  $R^* = R \setminus \{0\}$  is a subgroup of the monoid  $(R, \cdot, 1)$  (every element  $\neq 0$  is invertible)

Ex a subring of a division ring is a domain

Def a field is a commutative division ring.

Def the group of units  $U = R^*$  in  $R$  is the subset of  $(R, \cdot, 1)$  consisting of invertible elements.