MATH 171: WORKSHEET 1

DAGAN KARP

ABSTRACT. The goal of Class R1 is to gain an introduction to rings: definitions and basic examples.

1. RINGS

Definition 1. *A* ring $(R+, \cdot)$ *is a set together with two binary operations, called addition and multiplication respectively, satisfying the following three axioms.*

(1) *The set* $(R, +)$ *together with addition is an* <u>*Abelian*</u> *group.*
(2) *The binary operation* $\cdot$ *is associative on* R*.*
(3) *The distributive law holds in* R*; for all* $a, b, c \in \mathbb{R}$*,*

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Definition 2. *The ring* R *is* commutative *if multiplication is commutative.*

Definition 3. *The ring* R *has an* identity*, or* unity *or* contains a 1 *if there is an element* $1 \in \mathbb{R}$ *such that for all* $a \in \mathbb{R}$*,*

$$1 \cdot a = a \cdot 1 = a.$$

Remark 4. By abuse of notation, multiplication $\cdot$ may be denoted by simple juxtaposition, e.g. $a \cdot b = ab$.

Remark 5. For a ring with 1, condition (1), commutativity under addition, is redundant. Indeed, note that for any $a, b \in \mathbb{R}$,

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b,$$

and

$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b.$$

Therefore $a + b + a + b = a + a + b + b$ and therefore $a + b = b + a$. Thus R is Abelian.

Definition 6. *A ring with identity is a* division ring *if every non-zero element has a multiplicative inverse.*

Definition 7. *A* field *is a commutative division ring.*

Example 8. *The real numbers* $\mathbb{R}$ *form a ring under addition and multiplication of real numbers. In fact,* $\mathbb{R}$ *is a field.*

Date: March 6, 2018.

Example 9 (The zero ring). *Let* $R = \{0\}$. *Then* R *is a ring and is called the* zero ring. *Indeed, all of the axioms of a ring are trivially satisfied.*

$$0 + 0 = 0 \qquad\qquad 0 \cdot 0 = 0$$

Example 10 (Trivial rings). *For any Abelian group* $G, +$, *consider the ring* $(G, +, \cdot)$, *where multiplication is given by*

$$a \cdot b = 0$$

for any $a, b \in G$.

Example 11. *The integers* $\mathbb{Z}$ *form a ring under usual operations of addition and multiplication. Note that* $\mathbb{Z} - \{0\}$ *is not a group under multiplication! The other number rings are indeed rings as well:* $\mathbb{Q}, \mathbb{C}$.

Example 12. $\mathbb{Z}/n\mathbb{Z}$ *is a ring under addition and multiplication modulo* n:

$$a + b = (a + b) \mod n$$
$$a \cdot b = (ab) \mod n$$

Example 13. *The quaternions are defined by*

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R},\ i^2 = j^2 = k^2 = -1, \\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j\},$$

and they form a ring, where it is assumed that real coefficients commute with the distinguished elements i, j, k.

Example 14. *Let* X *be a set and* A *be a ring. The set*

$$R = \{f : X \to A : f \textit{ is a map of sets }\}$$

is a ring under pointwise addition and multiplication:

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

Proposition 15. *Let* R *be a ring, and* $a, b \in R$.

(1) $0a = a0 = 0$
(2) $(-a)b = a(-b) = -(ab)$, *where* $-(a)$ *is the additive inverse of* a.
(3) $(-a)(-b) = ab$
(4) *If* R *has identity* 1, *then it is unique and* $-a = (-1)a$.

Definition 16. *A nonzero element* a *of a ring* R *is a* zero divisor *if there is a non-zero* $0 \neq b \in R$ *such that* $ab = 0$ *or* $ba = 0$.

Definition 17. *Let* R *be a ring with identity. An element* a *of* R *is an* unit *if it has a multiplicative inverse, i.e. there is some* $b \in R$ *such that*

$$ab = ba = 1.$$

The set of units of R *is denoted* $R^\times$.

Definition 18. *An* integral domain *is a commutative ring with identity which has no zero divisors.*

Proposition 19. *Let* R *be an integral domain, and let* $a, b, c \in R$. *If*

$$ab = ac,$$

then $a = 0$ *or* $b = c$.

Exercises. Answer the questions posed in the following exercises.

Exercise 1. *Which of the following are rings, integral domains, division rings or fields?*

(1) $\mathbb{N}$
(2) $2\mathbb{Z}$
(3) $\mathbb{Z}/3\mathbb{Z}$
(4) $\mathbb{Z}/n\mathbb{Z}$
(5) $\mathbb{Q}$

Exercise 2. *What are the units of* $\mathbb{Z}/n\mathbb{Z}$*?*

Exercise 3. *Prove Proposition 15*