

Let  $S \subset T$  such that  $S \neq \emptyset$  ( $S$  is non-empty).

**Binary Relations** Let  $* : S \times S \rightarrow S$  be a map denoted by  $a * b$  for all  $a, b \in S$ . Such a map  $*$  is called a *binary relation* on  $S$ . Notice that part of the definition of a binary relation is that the range of  $*$  is contained in  $S$ . Thus if we have  $* : S \times S \rightarrow T$ , then to check that  $*$  is a binary relation we must verify that  $a * b \in S$  for all  $a, b \in S$  (this is called checking *closure*).

Let  $S$  be a non-empty set with a binary relation  $*$ .

**Associativity** If  $a * (b * c) = (a * b) * c$  for all  $a, b, c \in S$ , then we say  $*$  is an *associative* operation on  $S$ .

**Identity** Suppose we have an element  $e \in S$  such that  $a * e = a = e * a$  for all  $a \in S$ . Then  $e$  is called an *identity* element for the operation  $*$  on  $S$ .

**Inverses** Suppose that  $e \in S$  is an identity element. Then  $S$  has *inverses* if for each  $a \in S$  there exists some  $b \in S$  such that  $a * b = e = b * a$  ( $b$  is the *inverse* of  $a$ ).

**Commutativity** If  $a * b = b * a$  for all  $a, b \in S$ , then  $*$  is a *commutative* operation on  $S$ .

Some basic algebraic objects...

**Semigroup** A set  $S$  with an associative binary operation  $*$  is called a *semigroup*.

**Monoid** A semigroup  $S$  with an identity element  $e \in S$  is called a *monoid*.

**Group** A monoid  $S$  such that each element has an inverse is called a *group*.

**Abelian Group** A group  $S$  with a commutative binary operation is called an *Abelian group* (or sometimes a commutative group).

**Ring** Let  $R$  be a non-empty set equipped with two binary operations:

- $+$  :  $R \times R \rightarrow R$  called *addition* denoted  $a + b$  for all  $a, b \in R$ .
- $\cdot$  :  $R \times R \rightarrow R$  called *multiplication* denoted  $ab$  for all  $a, b \in R$ .

Then  $R$  is a *ring* if the following axioms hold:

- (i)  $R$  paired with the operation  $+$  is an Abelian group – denote the identity element by  $0$ . That is:
  - (a) Addition is associative: for all  $a, b, c \in R$  we have  $a + (b + c) = (a + b) + c$ .
  - (b) There is an additive identity  $0 \in R$ : for all  $a \in R$  we have  $a + 0 = a = 0 + a$ .
  - (c) Additive inverses exist: for all  $a \in R$  there exists  $-a \in R$  such that  $a + (-a) = 0 = (-a) + a$ .
  - (d) Addition is commutative: for all  $a, b \in R$  we have  $a + b = b + a$ .
- (ii) The multiplication on  $R$  is associative: for all  $a, b, c \in R$  we have  $a(bc) = (ab)c$  (that is  $R$  paired with the multiplicative operation is a semigroup).
- (iii) The multiplication on  $R$  distributes across the addition on  $R$ . That is for all  $a, b, c \in R$ :

**Left-Distributive**  $a(b + c) = ab + ac$

**Right-Distributive**  $(a + b)c = ac + bc$

Let  $R$  be a ring.

**Zero Divisors** Let  $a, b \in R$  be two non-zero elements ( $a \neq 0$  and  $b \neq 0$ ). Then if  $ab = 0$ , we call both  $a$  and  $b$  *zero divisors*.

**Units** Let  $a \in R$ . If there exists  $b \in R$  such that  $ab = 1 = ba$ , then  $a$  is called a *unit* in  $R$ . The collection of all units of  $R$  is called the *group of units* and is denoted  $U(R)$ .

---

Again, let  $R$  be a ring. Special types of rings...

**Ring with Identity** If there exists some element  $1 \in R$  such that  $a1 = a = 1a$  for all  $a \in R$ , then  $R$  is called a *ring with identity* (or ring with 1).

**Commutative Ring** If the multiplication on  $R$  is commutative (that is  $ab = ba$  for all  $a, b \in R$ ), then  $R$  is called a *commutative ring*.

**Integral Domains** Let  $R$  be a commutative ring with identity such that  $1 \neq 0$ . If  $R$  has no zero divisors, then  $R$  is an *integral domain*. This means that for all  $a, b \in R$  if  $ab = 0$ , then either  $a = 0$  or  $b = 0$ .

**Fields** Let  $R$  be a commutative ring with identity such that  $1 \neq 0$ . If every non-zero element of  $R$  is a unit, then  $R$  is a *field*. That means that for all  $a \in R$  there exists  $a^{-1} \in R$  such that  $aa^{-1} = 1 = a^{-1}a$ .

**Domains** If we remove the assumption of commutativity from the definition of an integral domain, we get the definition of a *domain*.

**Division Rings** If we remove the assumption of commutativity from the definition of a field, we get the definition of a *division ring* (or *skew field*).

---

Some notation...

**Additive Notation** Typically the “+” symbol is only used for commutative operations, and the identity element is denoted by “0”. Let’s say that  $(R, +)$  forms an Abelian group (this is true for any ring  $R$ ). Then each element  $a \in R$  has a *unique* additive inverse which we denote by  $-a$ . Let  $n \in \mathbb{Z}_{>0}$  then by  $na$  we mean:  $na = \underbrace{a + a + \dots + a}_{n \text{ times}}$ . Also,  $0a$  is defined to be  $0a = 0$ . Notice that the zero on

the left hand side is the integer zero whereas the zero on the right hand side is the zero of the group (or ring). Since  $-a$  exists, we define:  $(-n)a = \underbrace{(-a) + (-a) + \dots + (-a)}_{n \text{ times}}$ .

**Multiplicative Notation** Typically the multiplication in a ring is denoted by juxtaposition (putting symbols next to each other). If a ring has a multiplicative element, it is usually denoted by “1”. If  $R$  is a ring with 1 and  $a \in R$ , then  $a$  may or may not have a (multiplicative) inverse. However, if  $a$  does have an inverse, this inverse is *unique* and is denoted by  $a^{-1}$ . Let  $n \in \mathbb{Z}_{>0}$  and  $a \in R$  (a ring), then by  $a^n$  we mean:  $a^n = \underbrace{aa \dots a}_{n \text{ times}}$ . If  $R$  is a ring with 1, we define  $a^0 = 1$  where the zero in

the exponent is the integer zero and the 1 on the right hand side is the multiplicative identity of  $R$ . Finally, if  $R$  is a ring with 1 and  $a$  is a unit of  $R$  ( $a$  has a multiplicative inverse), then by  $a^{-n}$  we mean:  $\underbrace{a^{-1}a^{-1} \dots a^{-1}}_{n \text{ times}}$ .

**WARNING:** Some (in fact many) authors require that **all** rings have multiplicative identities. In fact, what we call a ring they call a *rng* (the i has been deleted). Also, some authors require in addition that  $1 \neq 0$ . To explore more definitions try visiting the online encyclopedia “Wikipedia”

<http://en.wikipedia.org/>