Definitions Related to Groups and Rings

Definition 1 (Group)**.** A *group* is a set G with a binary operation $*$ such that

1. G is closed under $*$: $a * b \in G$ for all $a, b \in G$.
2. $*$ is associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
3. There is an identity element: There exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
4. Every element has an inverse: For all $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

We denote a group by $(G, *)$ or simply G for short.

Definition 2 (Abelian Group)**.** An *abelian group* is a group $(G, *)$ such that $*$ is commutative: $a * b = b * a$ for all $a, b \in G$.

Definition 3 (Subgroup)**.** A subset H of a group $(G, *)$ that also forms a group under $*$ is called a *subgroup*. To determine whether a given subset H is a subgroup we only need to check that

1. H is closed under $*$: For all $a, b \in H$, $a * b$ is also in H.
2. H is closed under inverses: For all $a \in H$, a^{-1} is also in H.

Definition 4 (Ring)**.** A *ring* is a set R with two binary operations $\boxplus$ and $\boxdot$ such that

0. R is closed under $\boxplus$ and $\boxdot$, i.e., $a \boxplus b \in R$ and $a \boxdot b \in R$ for all $a, b \in R$.
1. $(R, \boxplus)$ is an abelian group.
2. $\boxdot$ is associative, i.e., $(a \boxdot b) \boxdot c = a \boxdot (b \boxdot c)$ for all $a, b, c \in R$.
3. The distributive laws hold, i.e.,
$$a \boxdot (b \boxplus c) = (a \boxdot b) \boxplus (a \boxdot c)$$
and
$$(b \boxplus c) \boxdot a = (b \boxdot a) \boxplus (c \boxdot a)$$
for all $a, b, c \in R$.

We denote a ring by $(R, \boxplus, \boxdot)$ or simply R for short. The identity element for $\boxplus$ is called the *additive identity element* and denoted by 0 or 0_R.

Definition 5 (Commutative Ring)**.** A *commutative ring* is a ring such that $\boxdot$ is commutative, i.e., $a \boxdot b = b \boxdot a$ for all $a, b \in R$.

Definition 6 (Unity)**.** A *ring with unity* is a ring that has a multiplicative identity element (called the *unity* and denoted by 1 or 1_R), i.e., $1_R \boxdot a = a \boxdot 1_R = a$ for all $a \in R$.

Our book assumes that all rings have unity.

Definition 7 (Zero Divisor)**.** $a \in R - \{0_R\}$ is called a *zero divisor* of a ring R iff there exists $b \in R - \{0_R\}$ such that $a \boxdot b = 0_R$ or $b \boxdot a = 0_R$. (So, neither a nor b is equal to 0 but their product is 0, i.e., you can multiply two non-zero things together and get zero.)

Definition 8 (Integral Domain)**.** An *integral domain* (or simply domain) is a commutative ring (with unity) that has no zero divisors.

Definition 9 (Unit)**.** $a \in R - \{0_R\}$ is called a *unit* of a ring R iff there exists $b \in R$ such that $a \boxdot b = b \boxdot a = 1_R$. (So, the units are the elements which have multiplicative inverses.)

Definition 10 (Division Ring)**.** A *division ring* is a ring (with unity) such that every element except 0_R is a unit (i.e., every non-zero element has an inverse).

To show that a ring is a division ring, it is sufficient to show that $(R - \{0_R\}, \boxdot)$ is a group.

Definition 11 (Field - short definition)**.** A *field* is a commutative division ring.

To show that a ring is a field, it is sufficient to show that $(R - \{0_R\}, \boxdot)$ is an abelian group.

Definition 12 (Field - long definition)**.** A *field* is a set R with two binary operations $\boxplus$ and $\boxdot$ such that

0. R is closed under $\boxplus$ and $\boxdot$,
1. $(R, \boxplus)$ is an abelian group,
2. $\boxdot$ is associative,
3. the distributive laws hold,
4. there is a unity,
5. $\boxdot$ is commutative,
6. and every non-zero element is a unit.