DEFINITION 7 (BINARY OPERATION). *A binary operation f on a set S is a mapping from the Cartesian product $S \times S$ to S:*

$$f : S \times S \longrightarrow S.$$

DEFINITION 8 (GROUP). *A group G is a set with a binary operation $*$, (called the "law of composition") which satisfies the group axioms:*

ASSOCIATIVITY: $(a * b) * c = a * (b * c)$ *for all* $a, b, c \in G$.
IDENTITY: *There exists an element* $i_G \in G$ *such that* $a * i_G = a$ *for all* $a \in G$.
INVERSE: *For every* $a \in G$, *there exists and element* b *such that* $a * b = b * a = i_G$.

The sets with a binary operation which only partially fulfill the group axioms, have differnt names:

DEFINITION 9 (SEMIGROUP AND MONOID). *If* $(G, *)$ *only satisfies the* ASSOCIATIVITY *axiom, we call* G *a semigroup. If a semigroup* G *has an* IDENTITY *element, we call* G *a monoid.*

DEFINITION 10 (ABELIAN GROUP). *A group G with a commutative law of composition $*$ (i.e. which satisfies the following axiom) is called a commutative or abelian* group:*

COMMUTATIVITY: $a * b = b * a$ *for all* $a, b \in G$.

DEFINITION 11 (RING). *A ring is a set R equipped with two binary operations $+$ and $*$, called "addition" and "multiplication", such that $(R, +)$ is an abelian group, $(R, *)$ is a monoid and the operation $*$ is ditributive with respect to $+$:*

DISTRIBUTIVITY: $a * (b + c) = a * b + b * c$ *and* $(b + c) * a = b * a + c * a$ *for all* $a, b, c \in G$.

By 0_R and 1_R, we denote the additive and the multipplicative identities of R, respectively. If $*$ is commutative, then we call R a commutative ring.

DEFINITION 12 (FIELD). *A field is a commutative ring F such that $F^* := F \setminus \{0\}$ is also an abelian group under multiplication.*