### Definition: Ring

Let R be a non-empty set and let there be two operations + and · on R with the following

(

R, +) is an abelian group. a, b, c ∈ R

is a semigroup with a neutral element.

3.The following distribution laws apply to all a· b+c = a·b+a·c

Then we call (R, +, ·) a ring.a+b ·c = a·c+b·c and

Condition 1 concerns only the + on R operation. We call this operation the addition of R. Let’s take a closer look at this definition:

The condition is,

that + is associative,

that there is an identity element 0 with respect to R ++,

that each element in is invertible with respect to and

that the operation + is commutative. · R

cation in R. The condition states Condition 2 refers exclusively to the operation on . We call this operation the multipli-

that · is associative and

that there is an identity element 1 with respect to multiplication.

The distribution laws from condition 3 govern the interaction of addition and multiplication.

The identity element in 1, and the

also write inverse element to each a−1. b − a exists, we call itb + (−a) we

As you can see, rings describe a mathematical structure that you know from your daily life. In the following example, we look at the ring of integers, with which you have been calculating intuitively since primary school.

#### Example: Rings

We consider the addition (ℤ, +, ·ℤ ) · : ℤ × ℤ → ℤ( + : ℤ × ℤ → ℤℤ defined by · (a, b) := a · ba ∈ ℤ+(a, b) := a + b+ −a ∈ ℤ(a, b) ∈ ℤ × ℤ(ℤ, ·. It is an oper-)(ℤ, +)

ation on , 0 is the identity element and for each then is the inverse element. The operation is both associative and commutative. This makes an abelian group.

The multiplication , defined by for all , is also an associative operation on with 1 as a neutral element. Thus is a semigroup with a neutral element.

In addition, the above-mentioned distribution laws apply to and ·.

Thus is a ring.

Other obvious examples of rings are (ℚ, +, ·) and (ℝ, +, ·).

On the other hand, ℕ, +, ·) for example, is not a ring, because there is no identity

element in (ℕ, +). 1 −1 · (ℤ, +,

·), for example, only elements and are invertible with respect to . This leads us to the As a rule, not every element is invertible with respect to multiplication. In the ring following definition.

is called invertible if r is invertible in R(R, ·). An . The set of all invertible elements in is called

Theorem and Definition: Unit GroupLet (R, +, ·) be a ring. Then (Rx, ·) is a group. This is called the unit group of R.

Proof: is Let , because is just the inverse element of and is the inverse element is also x. It of · bb−1. Obviously, · a−1 = 1 = b−1 · a−1 · a · ba−1 · b it follows that −1 a · b ∈ R· x. Thus · is a link on R. Because Rx.

1 ∈ R is the identity element of multiplication. Obviously 1 because of . To show that 1 ∈ is an operation on Rx 1R · 1 = x ≠ ∅. 1 is theRa · b For In Definition: Commutative RingThus, it follows overall that (Ra ∈ Rx,·) the associative law applies, because this law is already valid in the ring x it applies also that (Rax, ·)− 1 ∈ R is a group. x, because □ a · a − 1 = a − 1 · a = 1. (R, +, ·).

(R, ·) (ℤ, +, ·

According to the definition of a ring, A ring though therefore always given for the addition. One speaks now of a commutative ring, evenrings. (R, +, · is also commutative. ) is called commutative if (R, (R, ·+)) must be an abelian group. Commutativity is) and is commutative.(ℝ, +, ·) are examples of commutative

Although you can calculate intuitively in rings, we would like to briefly highlight and summarize the most important calculation rules in the following. Let Proof:Theorem: Calculation Rules in Rings1.2.3. (0(−1)(−R, +, · ∙a) · b = −(a · b) = a · (−b a = a · 0 = 0 · a = −a = a · ) be a ring. Then the following calculation rules apply:(−1) ) .

adding the inverse element that To 2:Thus, the overall claim For To 1:Completely analogously, the equation we get because of the distribution laws. By adding the additive inverse to a ∈ R, it applies that 0 = 0 · aa · 0 = a · (0 + 0) = a · 0 + a · 00 · a = (0 + 0) · a = 0 · a + 0 · a. 0 = a · 0 for all 0. a ∈ R is valid. because of and from this it follows by0 · a on both sides of0 = 0 + 0 and

0 · a = 0 = a ·

For a ∈ R it applies with the distributive law and the first calculation rule that:==0=0−·a1+1·a+1·a·a

Thus . Because is commutative, a + (−1) · a = 0a is also valid.+

Thus is the uniquely determined inverse element to with respect to . We had designated this with .

a·

and thus · (−1) = 0= −a a · (−1) + a = 0a · (−1) (R, +) it follows again that + a · (−1)a + a

and thus is the inverse element of a with respect to . Thus and with this the assertion is valid.

For a, b ∈ R it applies with the associative law and with the second calculation rule that:a·b··aa·b·b To 3:

Accordingly it follows that: a·