Groups, rings and fields

Notes by Markus Renoldner
Based on the lecture Lineare Algebra I and II
from Dr. Menny Akka Ginosar at ETH Zürich

March 29, 2023

Contents

1 Groups

Definition 1 (Group). *A group is a set G together with an element $e \in G$, the neutral element, as well as an operation ("Verknüpfung") $G \cdot G \to G$ that satisfies*

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ ... *Associativity*
2. $e \cdot g = g$ ... *neutral element*
3. $g' \cdot g = e$ ... *inverse element*

Its notated by the triple: $(G, e, \cdot)$

Th notation of the operation means, that $\cdot$ takes two elements and ouputs a third element, all from G. An example of a group is $(\mathbb{R}, 0, +)$. The triple $(\mathbb{N}, 0, +)$ is not a group, as its members dont have inverse elements.

Lemma 2 (Group properties).

1. *the neutral elemenet of a group is unique*
2. *the inverse element of g is unique, which allows to write g^{-1}*
3. *for all $a, b \in G$ we have $(a^{-1})^{-1} = a$ and $(ab)^{-1} = a^{-1}b^{-1}$*
4. *for all $a, b, c \in G$ we have $ab = ac$ if and only if $b = c$.*
   Same for $ba = ca$

Proof. TODO □

Definition 3 (Abelian group). *A group is called abelian ("abelsch") if it is commuative: $a \cdot b = b \cdot a$*

Definition 4 (Subgroup). *A subset of G is a subgroup of G if it is a group.*

Definition 5 (Homomorphism). *Let $(G, \cdot)$ and $(H, *)$ be groups. A mapping $\phi : G \to H$ is a homomorphism if*

$$\phi(a \cdot b) = \phi(a) * \phi(b)$$

for all $a, b \in H$

Definition 6 (Isomorphism). *A bijective homomorphism is an isomorphism.*

Lemma 7 (Properties of homomorphisms). *Let ϕ be a homomorphism and e_i be the neutral element of group i.*

1. $\phi(e_G) = e_H$
2. $\phi(a^{-1}) = \phi(a)^{-1}$

Proof.

1. by above definitions:
$$\phi(e_G) = \phi(e_G \cdot e_G) = \phi(e_G) * \phi(e_G)$$
Now apply $\phi(e_G)^{-1}$ from left
$$e_H = \phi(e_G)^{-1} * \phi(e_G) * \phi(e_G) = e_H * \phi(e_G) = \phi(e_G)$$
2. Let $a \in G$. We just showed that
$$\phi(a) * \phi(a^{-1}) = \phi(a \cdot a^{-1}) = \phi(e_G) = e_H$$
But we also know that
$$\phi(a^{-1}) * \phi(a) = \phi(a^{-1} \cdot a) = \phi(e_G) = e_H$$
As the inverse element is unique (see lemma 2), the statement follows.

□

2 Rings and fields

(German: "Ringe" und "Körper")

Definition 8 (Ring). *A ring is a set R with the two operations addition and multiplication:*

$$+ : R \times R \to R \tag{1}$$
$$\cdot : R \times R \to R \tag{2}$$

and the following properties:

- *R is an ablian Group*
- *$\cdot$ is associative*
- *it holds that $a \cdot (b + c) = a \cdot b + a \cdot c$*

A ring is called unitary ring or ring with unity if $\exists 1 \in R$ st. $1 \cdot a = a \cdot 1 = a \forall a \in R$ this element is called unity- or one-element.

Apparently now one can already proof fun statements like this:

Lemma 9 (Good to know lemma). *Seemingly*

$$a \cdot 0 = 0$$

Proof. Take $0 + 0 = 0$ and distributivity:

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

add the inverse of (fancy way of saying subtract) $0 \cdot a$ and use associativity

$$0 = 0 \cdot a - 0 \cdot a(0 \cdot a + 0 \cdot a) - 0 \cdot a = 0 \cdot a + (0 \cdot a - 0 \cdot a) = 0 \cdot a + 0 = 0 \cdot a$$

Beautiful. □

Definition 10 (Definition of fields based on groups)**.** *("Körper") A field is a unitary ring where each nonzero element has a multiplicative invers. More explicit:*
A tuple $(K, +, \cdot, 0, 1)$ *where*

$$+ : K \times K \to K \tag{3}$$
$$\cdot : K \times K \to K \tag{4}$$

and where K *is a set, is called field if*

- K *together with addition is an abelian group with neutral element* 0
- $K\backslash\{0\}$ *together with multiplication is an abelian group with neutral element* 1
- *distributivity:* $a \cdot (b + c) = a \cdot b + a \cdot c$

Definition 11 (Axiomatic definition of fields)**.** *A tuple* $(K, +, \cdot, 0, 1)$ *where*

$$+ : K \times K \to K \tag{5}$$
$$\cdot : K \times K \to K \tag{6}$$

and where K *is a set, is called field if the following axioms hold*

- *associativity, commutativity, existence of neutral element, and existence of inverse element of addition*
- *associativity, commutativity, existence of neutral element, and existence of inverse element of multiplication*
- *distributivity of addition and multiplication*
- $1 \neq 0$

Lemma 12 (Properties of fields)**.** *We have that:*

- *Every field has at least two elements*
- $0 \cdot a = 0$
- *Fields dont have zero divisors, in other words:* $a \cdot b = 0 \implies a = 0 \vee b = 0$
- $a \cdot (-b) = -(a \cdot b)$ *and* $(-a) \cdot (-b) = a \cdot b$
- $x \cdot a = y \cdot a$ *with* $a \neq 0 \implies x = y$

Proof. TODO □