5.A Group homomorphisms

Homomorphisms between sets with similar structures are maps which are compatible with these structures. Homomorphisms between K-vector spaces are therefore maps which respect the group structures of both vector spaces and also respect the scalar multiplications.

First we consider only the homomorphisms of groups. Unless otherwise specified the binary operations are written multiplicatively.

5.A.1 Definition Let G and H be groups. A map $\varphi: G \to H$ is called a (group)-homomorphism if for all $a, b \in G$ we have: $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

The set of all group homomorphisms from G into H is denoted by

$$\underset{\text{Groups}}{\text{Hom}}(G, H) \text{ or } \text{Hom}(G, H)$$

Bijective homomorphisms are called isomorphisms. Homomorphisms from G into itself ($H = G$) are called endomorphisms; bijective endomorphisms are therefore isomorphisms of G onto itself, these are called automorphisms of G. Two groups G and H are said to be isomorphic if there exists an isomorphism from G onto H. In this we write

$$G \cong H.$$

The identity id_G is an automorphism of the group G. The constant map $G \longrightarrow H$, $a \longmapsto e_H$ from a group G into a group H, which maps every element of G to the neutral element e_H of H, is a homomorphism. It is called the trivial homomorphism from G into H.

5.A.2 Theorem Let $\varphi : G \longrightarrow H$ be a homomorphism of groups with neutral elements e_G resp. e_H. Then:

(1) $\varphi(e_G) = e_H$

(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$.

(3) $\varphi(a^n) = \varphi(a)^n$ for all $a \in G$ and all $n \in \mathbb{Z}$

Proof (1) From $e_G = e_G \cdot e_G$, it follows that $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$ and by cancelling $\varphi(e_G)$ we get the equality $e_H = \varphi(e_G)$.

(2) From $e_H = \varphi(e_G) = \varphi(a\bar{a}^1) = \varphi(a)\varphi(\bar{a}^1)$ and $e_H = \varphi(e_G) = \varphi(\bar{a}^1 a) = \varphi(\bar{a}^1)\varphi(a)$, it follows that $\varphi(\bar{a}^1) = \varphi(a)^{-1}$.

(3) If $n \in \mathbb{N}$, then $\varphi(a^n) = \varphi(a)^n$ by the general rule $\varphi(a_1 \cdots a_m) = \varphi(a_1) \cdots \varphi(a_m)$ for arbitrary elements $a_1, \ldots, a_m \in G$, which is easily proved by induction on n (where in starting of induction at $n=0$ is the assertion (1)). If $n \in \mathbb{Z}$, $n < 0$, then $-n > 0$ and $\varphi(a^n) = \varphi((\bar{a}^n)^{-1}) = \varphi(\bar{a}^n)^{-1} = (\varphi(a)^{-n})^{-1} = \varphi(a)^n$.

5.A.3 Let $\psi : F \longrightarrow G$ and $\varphi : G \longrightarrow H$ be homomorphism of groups. Then

(1) The composition $\varphi \circ \psi : F \longrightarrow H$ is again a homomorphism of groups.

(2) If φ is an isomorphism, then the

inverse map $\varphi^{-1}: H \to G$ is also an isomorphism.

Proof (1) For $a, b \in F$, $(\varphi \circ \psi)(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) = \varphi(\psi(a)) \cdot \varphi(\psi(b)) = (\varphi \circ \psi)(a) \cdot (\varphi \circ \psi)(b)$.

(2) Let $c, d \in H$. Then $\varphi(\varphi^{-1}(c)\,\varphi^{-1}(d)) = \varphi(\varphi^{-1}(c))\,\varphi(\varphi^{-1}(d)) = cd$ and hence it follows that $\varphi^{-1}(cd) = \varphi^{-1}(c) \cdot \varphi^{-1}(d)$.

From 5.A.3 it follows directly that the automorphisms of a group form a subgroup of the permutation group $S(G)$ of G. This group is called the automorphism group of G and is denoted by $\mathrm{Aut}G$.

The set of endomorphisms of G is denoted by $\mathrm{End}G$.

It is a monoid with the composition as binary operation. Further from 5.A.3, it follows that on a set of groups, the isomorphie is an equivalence relation

The equivalence classes with respect to the "isomorphic" are also called the isomorphism classes.

5.A.4 Theorem Let $\varphi: G \to H$ be a homomorphism of groups. Then:

(1) If $G' \subseteq G$ is a subgroup of G, then $\varphi(G') \subseteq H$ is a subgroup of H. In particular, $\operatorname{Im}\varphi := \varphi(G)$ is a subgroup of H

(2) If $H' \subseteq H$ is a subgroup of G, then $\bar{\varphi}^1(H') \subseteq G$ is a subgroup of G. In particular,

$$\operatorname{Ker}\varphi := \bar{\varphi}^1(e_H) = \{a \in G \mid \varphi(a) = e_H\}$$

is a subgroup of G.

Proof (1) Since $e_G \in G'$, $e_H = \varphi(e_G) \in \varphi(G')$. If $c = \varphi(a)$ and $d = \varphi(b)$, $a, b \in G'$, are elements in $\varphi(G')$, then $cd = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(G')$, since $ab \in G$. Further, if $c = \varphi(a)$, $a \in G'$, then $\bar{c}^1 = \varphi(a)^{-1} = \varphi(\bar{a}^1) \in \varphi(G')$, since $\bar{a}^1 \in G'$.

(2) Since $\varphi(e_G) = e_H \in H'$, $e_G \in \bar{\varphi}^1(H')$. If $a, b \in \bar{\varphi}^1(H')$, then $\varphi(ab) = \varphi(a)\varphi(b) \in H'$

and hence $ab \in \bar{\varphi}^{-1}(H')$. Finally, if $a \in \bar{\varphi}^{-1}(H')$, then $\varphi(\bar{a}^{-1}) = \varphi(\bar{a})^{-1} \in H'$ and hence $\bar{a}^{-1} \in \bar{\varphi}^{-1}(H')$.

If the group homomorphism $\varphi: G \to H$ is injective, then the kernel of φ $\operatorname{Ker}\varphi$ (defined in 5.A.4(2)) has only one element, namely the neutral element e_G of G. Moreover, the converse also holds:

5.A.5 Injectivity-Criterion. A

homomorphism $\varphi: G \to H$ of groups is injective if and only if $\operatorname{Ker}\varphi = \{e_G\}$.

Proof Suppose that $\operatorname{Ker}\varphi = \{e_G\}$. Then, from $\varphi(a) = \varphi(b)$, $a, b \in G$, it follows that $\varphi(a\bar{b}^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H$, and hence $a\bar{b}^{-1} \in \operatorname{Ker}\varphi$ and $a\bar{b}^{-1} = e_G$, i.e. $a = b$.

5.A.5 is a special case of the following more general assertion on the fibres of group homomorphisms:

5.A.6 Theorem Let $\varphi: G \to H$ be a group homomorphism. Let $a \in G$ and $b := \varphi(a) \in H$. Then:

$$\bar{\varphi}^{-1}(b) = \bar{\varphi}^{-1}(\varphi(a)) = a(\operatorname{Ker}\varphi) = (\operatorname{Ker}\varphi)a.$$

Therefore all elements of the fibre $\bar{\varphi}^{-1}(b)$ are obtained by multiplying an element a of this fibre with all elements of the kernel $\operatorname{Ker}\varphi$ of φ, on the right (or left).

Proof We only show $\bar{\varphi}^{-1}(b) = a(\operatorname{Ker}\varphi) := \{ah \mid h \in \operatorname{Ker}\varphi\}$. The other equality $\bar{\varphi}^{-1}(b) = (\operatorname{Ker}\varphi)a$ is proved analogously.

Let $x \in \bar{\varphi}^{-1}(b)$, i.e. $\varphi(x) = b$. Then $\varphi(a^{-1}x) = \varphi(a)^{-1}\varphi(x) = \varphi(a)^{-1}b = b^{-1}b = e_H$ and so $y := a^{-1}x \in \operatorname{Ker}\varphi$, i.e. $x = ay \in a(\operatorname{Ker}\varphi)$. This proves the inclusion $\bar{\varphi}^{-1}(b) \subseteq a(\operatorname{Ker}\varphi)$.

Conversely, if $x = ay$ with $y \in \operatorname{Ker}\varphi$, then $\varphi(x) = \varphi(ay) = \varphi(a)\cdot\varphi(y) = \varphi(a)e_H = b$, i.e. $x \in \bar{\varphi}^{-1}(b)$ and hence $a(\operatorname{Ker}\varphi) \subseteq \bar{\varphi}^{-1}(b)$.

5.A.7 Examples (1) Let $a \in \mathbb{R}$, $a > 0$, $a \neq 1$. The exponential map $(\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^{\times}, \cdot)$

$x \mapsto a^x$, is an isomorphism of the additive group $(\mathbb{R}, +)$ of $\mathbb{R}$ onto the multiplicative group $(\mathbb{R}_+^\times, \cdot)$ of positive real numbers. The inverse-isomorphism is the logarithm-function $y \mapsto \log_a y$ with base a of $(\mathbb{R}_+^\times, \cdot)$ onto $(\mathbb{R}, +)$.

(2) For $a \in \mathbb{C} \setminus \mathbb{R}_-$, the map

$$(\mathbb{C}, +) \longrightarrow (\mathbb{C}^\times, \cdot), \quad z \mapsto a^z := e^{z \ln a},$$

is a surjective group homomorphism from the additive group $(\mathbb{C}, +)$ of $\mathbb{C}$ onto the multiplicative group $(\mathbb{C}^\times, \cdot)$.

This homomorphism is not injective, its kernel is the subgroup

$$\{z \in \mathbb{C} \mid e^{z \ln a} = 1\} = \{z \in \mathbb{C} \mid z \ln a \in 2\pi i \mathbb{Z}\}$$
$$= \frac{2\pi i}{\ln a} \mathbb{Z}.$$

of all integer-multiples of $\frac{2\pi i}{\ln a}$ in $(\mathbb{C}, +)$.

In particular, in the case $a = e$, this kernel is equal to $2\pi i \mathbb{Z}$.

(3) Let $U \subseteq \mathbb{C}^\times$ be the circle-group

i.e. the multiplicative group of complex numbers of modulus 1:

$$U := \{z \in \mathbb{C} \mid |z| = 1\}$$

Then the map $\mathbb{R} \times U \longrightarrow (\mathbb{C}^\times, \cdot)$, $(r, u) \longmapsto e^r u$, is an isomorphism of the product group $(\mathbb{R}, +) \times (U, \cdot)$ (with the componentwise operation) onto the multiplicative group $(\mathbb{C}^\times, \cdot)$. The set $\mathbb{R} \times U \subseteq \mathbb{R} \times \mathbb{C} = \mathbb{R}^3$ is a cylinder and hence the group $\mathbb{R} \times U$ is often called the cylinder-group. It is therefore isomorphic to the group $(\mathbb{C}^\times, \cdot)$. The circle-group U is a homomorphic image of the additive group of the surjective homomorphism $t \longmapsto e^{it}$ with the kernel $2\pi\mathbb{Z}$.

5.A.8 Example (Order of an element in a group; Characteristic of a ring). Let $a \in G$ be an element in a group G. The map $\varphi: \mathbb{Z} \longrightarrow G$, $n \longmapsto a^n$, is a homomorphism from the additive group $(\mathbb{Z}, +)$ of $\mathbb{Z}$ into the group G. The image is

the cyclic subgroup $H(a) \subseteq G$ of G generated by a. The kernel is the subgroup $\operatorname{Ker}\varphi = \{n \in \mathbb{Z} \mid a^n = e_G\} \subseteq \mathbb{Z}$. By 1.C.5 this is precisely the integer multiples $\mathbb{Z}\cdot m$ of a unique natural number $m \in \mathbb{N}$.

If $m = 0$, then φ is injective and all powers a^n, $n \in \mathbb{Z}$, of a are pairwise distinct. In this case one says that the order of a is zero[1]. If $m > 0$, then by 5.A.6, $\bar{\varphi}^{-1}(a^n) = n + \mathbb{Z}m$ is the residue class of n modulo m. Therefore: $a^n = a^{n'}$ if and only if $n \equiv n' \pmod m$, i.e. $n - n'$ is divisible by m. Therefore $e_G = a^0, a = a^1, \dots, a^{m-1}$ are all distinct powers of a and so the cyclic subgroup $H(a)$ generated by a has exactly m elements; m is called the order of a and is denoted by $\operatorname{Ord} a$. In this case $\operatorname{Ker}\varphi =$

---

1 In this case often (also) one says that: the order of a is infty (∞), since the subgroup $H(a)$ has infinitely many (distinct) elements.

Z. Ord a. An element $a \in G$ in a group G with $\operatorname{Ord} a \neq 0$ is called a torsion-element of G. If G is abelian, then the torsion-elements of G form a subgroup of G (proof!); this subgroup is called the torsion-subgroup of G.

The order of the unity 1_A of a ring A in the additive group $(A,+)$ of A is very important; it is called the characteristic of A and is denoted by $\operatorname{Char} A$. $\operatorname{Char} A = 0$ means that the multiples $n \cdot 1_A$, $n \in \mathbb{Z} \setminus \{0\}$ are all non-zero in A, i.e. $n \cdot 1_A \neq 0_A$ for all $n \in \mathbb{Z} \setminus \{0\}$. The characteristic of A is positive if and only if there exists a natural number $n \in \mathbb{N}$ such that $n \cdot 1_A = 0$. Since $n \cdot a = (n \cdot 1_A) \cdot a$, we have $n \cdot a = 0$ for all $a \in A$. In this case the $\operatorname{Char} A$ is the smallest positive natural number with this property. For $m \in \mathbb{N}^*$, the residue-class ring $\mathbb{Z}/\mathbb{Z}m$

has characteristic m. The characteristic of a field (or more generally of an integral domain or a division-ring) K is either 0 or a prime number. For, if $m = \mathrm{Char}\, K > 0$, then $m > 1$, since $1_K \neq 0_K$ and from $m = rs$ with $1 < r, s < m$, it follows that $r \cdot 1_K \neq 0$, $s \cdot 1_K \neq 0$ and $0_K = m \cdot 1_K = (r \cdot 1_K)(s \cdot 1_K)$ a contradiction. Examples of fields of characteristic 0 are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The residue-class field $K_p = \mathbb{Z}/\mathbb{Z}p$, $p \in \mathbb{N}^*$ a prime number, has the characteristic p.

If A is a commutative ring of characteristic p, then the map $A \longrightarrow A$, $x \longmapsto x^p$ (and hence the map $x \mapsto x^{p^m}$, for every $m \in \mathbb{N}$) is a ring homomorphism. Since p divides $\binom{k}{k}$ for every $0 < k < p$ (check!), it follows that: for all $x, y \in A$:

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p.$$

5.A.9 Example Let $\varphi: G \to H$ be a homomorphism of groups. Suppose that G is finite. Then by 5.A.6 every non-empty fibre of φ has exactly as many elements as in $\operatorname{Ker}\varphi$, i.e. if $\varphi^{-1}(b) \neq \emptyset$, $b \in H$, then $\#\varphi^{-1}(b) = \#\operatorname{Ker}\varphi$. Since there are exactly $\#\operatorname{Im}\varphi$ non-empty fibres, it follows that

$$\#G = (\#\operatorname{Im}\varphi)(\#\operatorname{Ker}\varphi).$$

5.A.10 Example (Cayley's Representation Theorem) If $\varphi: G \to H$ is an injective group homomorphism, then φ induces an isomorphism of G onto the subgroup $\operatorname{Im}\varphi$ of H. We then say that G can be realised or (faithfully) represented as a subgroup of H via φ. An important representation of a group G is the following simple Theorem of Cayley:

5.A.11 Theorem (Cayley) Let G be

group. Then the map

$$\lambda : G \longrightarrow \mathfrak{S}(G),\ a \longmapsto \lambda_a : G \to G,\ x \mapsto ax$$

which associates every element $a \in G$ the left-multiplication $\lambda_a : G \to G$, $x \mapsto ax$, by a, is an injective group homomorphism from G into the permutation group $\mathfrak{S}(G)$ of G. In particular, every group is isomorphic to a subgroup of a permutation group and every group with n elements, $n \in \mathbb{N}^*$, is a subgroup of the group $\mathfrak{S}_n$.

Proof Since $\lambda_{ab}(x) = (ab)x = a(bx)$ $= \lambda_a(bx) = \lambda_a(\lambda_b(x)) = (\lambda_a \circ \lambda_b)(x)$, we have $\lambda_{ab} = \lambda_a \circ \lambda_b$, i.e. λ is a group homomorphism. (One should first note that λ_a is bijective for every $a \in G$, but this is clear, since $\lambda_{a^{-1}}$ is the inverse-map of λ_a: $\lambda_a \circ \lambda_{a^{-1}} = \lambda_{a \cdot a^{-1}} = \lambda_{e_G} = id_G = \lambda_{a^{-1}} \circ \lambda_a$) Further since $\lambda_a(e_G) = a$ for all $a \in G$, λ is injective.

For groups G and H, $\mathrm{Hom}(G,H)$ is a subset of the product group H^G of all maps from G into H. More generally, for a family H_i, $i \in I$, of groups, the product group $\prod_{i\in I} H_i$ is defined by the componentwise operation

$$(a_i)(b_i) := (a_i b_i).$$

Then (e_{H_i}) is the neutral element of the product group and (a_i^{-1}) is the inverse of (a_i). Further, $\prod_{i\in I} H_i$ is abelian if and only if each H_i, $i \in I$, is abelian.

For abelian groups we have:

5.A.12 Theorem Let G and H be abelian group. Then $\mathrm{Hom}(G,H)$ is a subgroup of the (abelian) group H^G.

Proof We shall write the binary operations in G and H additively. The neutral element in H^G is the zero-map and it belongs to $\mathrm{Hom}(G,H)$ as the trivial homomorphism.

If φ and ψ are homomorphisms from G into H, then $\varphi - \psi$ is also a homomorphism from G into H, since, for $a, b \in G$, we have

$$(\varphi-\psi)(a+b) = \varphi(a+b) - \psi(a+b) =$$

$$\varphi(a) + \varphi(b) - \psi(a) - \psi(b) = \varphi(a) - \psi(a) +$$

$$\varphi(b) - \psi(b) = (\varphi-\psi)(a) + (\varphi-\psi)(b).$$

Therefore by 1.C.2 $\mathrm{Hom}(G,H)$ is a subgroup of H^G.

It is clear that in 5.A.12 it is enough to assume that H is abelian.

Let H be an additively written abelian group. Then the set $\mathrm{End}\,H$ of all endomorphisms of H is an abelian group by 5.A.12, its binary operation is also written additively:

$$(\varphi+\psi)(a) = \varphi(a) + \psi(a)$$

$\varphi, \psi \in \mathrm{End}\,H$, $a \in H$. Other than this addition there is a natural composition on $\mathrm{End}\,H$. With this binary operation we have:

5.A.13 Theorem Let H be an additively written abelian group. Then $\mathrm{End}\,H$ with

the composition of homomorphisms as multiplication, is a ring.

Proof We need only to verify the distributive law. For endomorphisms $\varphi, \psi, \chi \in \mathrm{End}\, H$ and $a \in H$, we have

$$(\varphi+\psi)\chi(a) = \varphi\chi(a) + \psi\chi(a) = (\varphi\chi + \psi\chi)(a)$$ and

$$\chi(\varphi+\psi)(a) = \chi(\varphi(a)+\psi(a)) = \chi\varphi(a) + \chi\psi(a) = (\chi\varphi + \chi\psi)(a).$$

In the situation of 5.A.13, $\mathrm{End}_R H$ is called the endomorphism ring of H.

5.A.14 Example Let A be a ring. For $a \in A$, the left translation $\lambda_a : A \to A$, $x \longmapsto ax$ is an endomorphism of the additive group $(A,+)$ of A. The distributive law in A: $a(x+y) = ax+by$ precisely proves it. Further, $\lambda_{a+b} = \lambda_a + \lambda_b$ by the distributive law: $(a+b)x = ax+bx$. Therefore the map $(A,+) \xrightarrow{\lambda} \mathrm{End}(A,+)$, $a \longmapsto \lambda_a$, is a homomorphism from the additive group of A in the additive group

of the endomorphism ring $\mathrm{End}(A,+)$.
This map is also compatible with the multiplications in A resp. in $\mathrm{End}\,A$.
This follows from the associative law of the multiplication in A, namely

$$\lambda_{ab}(x) = (ab)x = a(bx) = \lambda_a(bx) = (\lambda_a \cdot \lambda_b)(x).$$

Further, the image λ_{1_A} of the identity element 1_A of A is the identity element id_A of the ring $\mathrm{End}(A,+)$.
Therefore λ is (moreover injective) ring homomorphism from A into $\mathrm{End}(A,+)$.

More generally, a map $\varphi : A \longrightarrow B$ from a ring A into another ring B is called a ring homomorphism if φ is a homomorphism ~~from~~ the additive group $(A,+)$ as well as the multiplicative monoid $(A,\cdot)$ into resp. ~~those of~~ B. The last condition is

$$\varphi(ab) = \varphi(a)\,\varphi(b) \text{ for all } a,b \in A$$

and that $\varphi(1_A) = 1_B$. See also the following:

5.A.15 Example (Characters) Let M and N be monoid. A map $\varphi : M \longrightarrow N$ is called

a monoid homomorphism if $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in M$ and $\varphi(e_M) = e_N$.

Let M be a monoid and let K be a field. By a character of M in K we mean a homomorphism of M into the multiplicative monoid $(K, \cdot)$ of K. The following assertion used frequently:

5.A.16 Theorem *Let M be a monoid and let K be a field. The set of characters of M into K is linearly independent in the K-vector space K^M of K-valued functions on M.*

Proof Suppose that $\varphi = a_1\varphi_1 + \cdots + a_r\varphi_r$ with pairwise distinct characters $\varphi, \varphi_1, \cdots, \varphi_r$. Assuming that $\varphi_1, \cdots, \varphi_r$ are linearly independent and $a_1, \cdots, a_r \in K$. We must get a contradiction. For all $x, y \in M$, on one side

$$\varphi(xy) = a_1\varphi_1(xy) + \cdots + a_r\varphi_r(xy)$$
$$= a_1\varphi_1(x)\varphi_1(y) + \cdots + a_r\varphi_r(x)\varphi_r(y)$$

and on the other side

$$\varphi(xy) = \varphi(x)\varphi(y) = a_1\varphi(x)\varphi_1(y) + \cdots + a_r\varphi(x)\varphi_r(y)$$

Now since $\varphi_1, \cdots, \varphi_r$ are linearly independent

it follows that $a_i\varphi_i(x) = a_i\varphi(x)$ for all $i=1,\dots,r$ and all $x \in M$, i.e. $\varphi = \varphi_i$ for all i with $a_i \neq 0$, a contradiction.

Now, let $M = G$ be a group and let K be a field. A character $G \to K$ is then a group homomorphism $G \to K^*$ and the group $\mathrm{Hom}(G, K^*)$ (by 5.A.12) is a subgroup of $(K^*)^G$. If G is finite and $\chi: G \to K^*$ is a non-trivial character, then $\sum_{x \in G} \chi(x) = 0$. For, if $y \in G$ is an element with $\chi(y) \neq 1_K$, then

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \Big(\sum_{x \in G} \chi(x)\Big)\chi(y)$$

and hence $\sum_{x \in G} \chi(x) = 0$, since $\chi(y) \neq 1_K$.

The group $\mathrm{Hom}(G, \mathbb{C}^*)$ of characters of G in $\mathbb{C}^*$ is called the character-group of G and is denoted by $\widehat{G}$. This group plays an important roll in the study of abelian groups.