2.D HOMOMORPHISMS

In algebra the question of (fundamental importance is the structure) of binary operations. One can make it abstract by taking the advantage of the special properties of the elements in the underlying sets. The equality of the structure of binary operations will therefore be described more precisely by the concept of (isomorphism).

Definition 2.D.1 Let $(M, \top)$ and $(M', \top')$ be two binary-operation structures

(1) A map $\varphi: M \longrightarrow M'$ is called a homomorphism from M into M' (with respect to $\top$ and $\top'$) if for all $a, b \in M$, we have $\varphi(a \top b) = \varphi(a) \top' \varphi(b)$

(2) A bijective homomorphism $\varphi: M \longrightarrow M'$ is called an isomorphism from M onto M'.

If there exists an isomorphism from M onto M' then we say that M is isomorphic to M' and write $M \xrightarrow{\sim} M'$.

For example, for any $n \in \mathbb{N}$ (resp. $n \in \mathbb{Z}$) the (usual) left-multiplication by n, $\lambda_n: \mathbb{N} \longrightarrow \mathbb{N}$ (resp. $\lambda_n: \mathbb{Z} \longrightarrow \mathbb{Z}$), $a \mapsto na$ is a homomorphism[1] of $(\mathbb{N}, +)$ (resp. $(\mathbb{Z}, +)$); but λ_n is not an isomorphism unless $n = 1$ (resp. $n = \pm 1$).

---

[1] Remember the binding (distributive law) between the usual $+$ and usual multiplication: for all $a, b, c \in \mathbb{Z}$, $a(b+c) = (ab) + (ac)$ and $(b+c)a = (ba) + (ca)$

For any set X, the complement (w.r.to X)
$C_X : (\mathcal{P}(X), \cup) \longrightarrow (\mathcal{P}(X), \cap)$, $A \longmapsto C_X A := X \setminus A$
is a homomorphism. In fact an isomorphism, since $C_X \circ C_X = id_{\mathcal{P}(X)}$.

2.D.2 Lemma Let $(M,\top)$, $(M',\top')$ and $(M'',\top'')$ be binary operation structures. Then:
(1) If $\varphi : M \longrightarrow M'$ and $\varphi' : M' \longrightarrow M''$ are homomorphisms, then the composition $\varphi' \circ \varphi : M \to M''$ is also a homomorphism. Moreover, if both φ and φ' are isomorphisms, then $\varphi' \circ \varphi$ is also an isomorphism. The identity map $id_M : (M,\top) \longrightarrow (M,\top)$ is an isomorphism.
(2) If $\varphi : (M,\top) \longrightarrow (M',\top')$ is an isomorphism, then the inverse map $\bar{\varphi}^1 : (M',\top') \longrightarrow (M,\top)$ is also an isomorphism.

Proof (1) For all $a, b \in M$, we have $(\varphi' \circ \varphi)(a \top b) = \varphi'(\varphi(a \top b)) = \varphi'(\varphi(a) \top' \varphi(b)) = \varphi'(\varphi(a)) \top'' \varphi'(\varphi(b)) = (\varphi' \circ \varphi)(a) \top'' (\varphi' \circ \varphi)(b)$, i.e. $\varphi' \circ \varphi$ is a homomorphism. Moreover, if φ and φ' are bijective, then $\varphi' \circ \varphi$ is also bijective.
(2) Since isomorphisms are bijective, for $a', b' \in M'$, there exist unique $a, b \in M$ such that $a' = \varphi(a)$, $b' := \varphi(b)$, i.e. $\bar{\varphi}^1(a') = a$ and $\bar{\varphi}^1(b') = b$. Since φ is a homomorphism, $\bar{\varphi}^1(a' \top' b') = \bar{\varphi}^1(\varphi(a) \top' \varphi(b)) = \bar{\varphi}^1(\varphi(a \top b)) = (\bar{\varphi}^1 \circ \varphi)(a \top b) = a \top b = \bar{\varphi}^1(a') \top \bar{\varphi}^1(b')$, i.e. $\bar{\varphi}^1$ is a homomorphism, and naturally $\bar{\varphi}^1$ is bijective.

2.D.3 Remark On a set of binary operation structures the isomorphism $\xrightarrow{\simeq}$ is an equivalence relation. Namely, in 2.D.2 we have proved:
(1) $M \underset{id_M}{\xrightarrow{\simeq}} M$ (2) If $M \xrightarrow[\varphi]{\simeq} M'$ and $M' \xrightarrow[\varphi']{\simeq} M''$, then $M \xrightarrow[\varphi'\varphi]{\simeq} M''$ (3) If $M \xrightarrow[\varphi]{\simeq} M'$, then $M' \xrightarrow[\varphi^{-1}]{\simeq} M$.
The equivalence classes are called isomorphism classes or also isomorphism-type.

We shall show that some (but not all) properties of binary operation structures are carried over under homomorphisms. However, under isomorphisms all assertions and concepts which are formulated by the binary operation are carried over and hence isomorphism is a permission to rename structures. Therefore in algebra isomorphism of binary operation structure is considered "essentially equal". For example, if $\varphi: M \to M'$ is an injective homomorphism of binary-operation structure, then M (via φ) is isomorphic to the sub-binary operation structure $\varphi(M)$ (= the image of φ) of M'. With this we can then identify the elements a in M with their images $\varphi(a)$ in M' and M is considered as a sub-binary operation structure of M'. This is used before the construction of the usual number systems $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$.

2.D.4 Example Let X and Y be sets with the same cardinality, i.e. there is a bijective map $f: X \longrightarrow Y$. Then the monoids $(X^X, \circ)$ and $(Y^Y, \circ)$ are isomorphic. In fact, the map $\Phi_f: X^X \longrightarrow Y^Y$ defined by $\varphi \longmapsto f \varphi f^{-1}$ is an isomorphism, since Φ_f is bijective with the inverse $\Phi_f^{-1}: Y^Y \longrightarrow X^X$, $\psi \longmapsto f^{-1} \psi f$ and for arbitrary $\varphi_1, \varphi_2 \in X^X$, we have

$\Phi_f(\varphi_1 \circ \varphi_2) = f \circ (\varphi_1 \circ \varphi_2) f^{-1} = (f \circ \varphi_1 f^{-1}) \circ (f \circ \varphi_2 \circ f^{-1}) = \Phi_f(\varphi_1) \circ \Phi_f(\varphi_2)$. Moreover, Φ_f maps the permutation group $\mathfrak{S}(X)$ into $\mathfrak{S}(Y)$ and Φ_f^{-1} maps $\mathfrak{S}(Y)$ into $\mathfrak{S}(X)$. Therefore Φ_f is an isomorphism of $\mathfrak{S}(X)$ onto $\mathfrak{S}(Y)$. In particular, permutation groups on equipotent sets are isomorphic.

2.D.5 Example Let $a \in \mathbb{R}$, $a > 0$ and $a \neq 1$. Then the well-known (real) exponential map $\mathbb{R} \longrightarrow \mathbb{R}_+$, $x \longmapsto a^x$, from the set of all real numbers in the set $\mathbb{R}_+^*$ of all positive real numbers is bijective. Further, $a^{x+y} = a^x \cdot a^y$ for arbitrary $x, y \in \mathbb{R}$. Therefore $(\mathbb{R}, +) \longrightarrow (\mathbb{R}_+^*, \cdot)$, $x \longmapsto a^x$ is an isomorphism from the additive group of real numbers $(\mathbb{R}, +)$ onto the multiplicative group of positive real numbers $(\mathbb{R}_+^*, \cdot)$. The inverse

isomorphism $(\mathbb{R}_+^\times, \cdot) \longrightarrow (\mathbb{R}, +)$ is the well-known logarithm-function $y \longmapsto \log_a x$ (with respect to the base a)

Further using this isomorphism the structure of the multiplicative group $(\mathbb{R}_+^\times, \cdot)$ can be completely described by using the structure of the additive group $(\mathbb{R}, +)$. This makes computation easier to handle. It took about hundred years to get used to this practical use of calculation. Because of the preference of the decimal system one can choose in general the base $a = 10$ (Briggs' logarithm). The calculation with logarithm goes back to J. Neper (Napier; 1550-1617) and J. Burgi (1552-1632) (both agree on the natural logarithm) and above them to H. Briggs (1561-1630). The first comprehensive table-form of the function $\log_{10}$ (logarithm-table) is computed by Briggs and is published in 1617.

2.D.6 Example (Transference of binary operation)

Let M be a set with binary operation $\top$ and let $\varphi : M \longrightarrow M'$ be a bijective map from M onto the set M'. Then we can define a binary-operation $\top' : M' \times M' \longrightarrow M'$ by $(a', b') \longmapsto a' \top' b' := \varphi(\varphi^{-1}(a') \top \varphi^{-1}(b'))$ for $a', b' \in M'$. This binary operation $\top'$ (on M') is said to have obtained by transferring the binary operation $\top$ on M by using the bijection $\varphi : M \longrightarrow M'$. With this $\varphi : (M, \top) \longrightarrow (M', \top')$ is an isomorphism.

If $(M, \top)$ and $(M', \top')$ are binary-operation structures, then a bijective map $\varphi: M \to M'$ is an isomorphism if and only if the binary operation $\top'$ on M' is obtained from the binary operation $\top$ on M by transferring to M' by using φ. Moreover, in this case, the binary operation $\top'$ on M' satisfies exactly the same properties as the binary operation $\top$ on M satisfies. For example, M' is a semigroup (resp. monoid, group) if and only if M has the corresponding property. Therefore the transfer of binary operation mean only the interchanging (renaming) elements without changing the structure of binary operation.

2.D.7 Example Let G be a group and let G^{op} denote the set G with the opposite binary operation $*$ obtained from the binary operation of G, i.e. $a * b = ba$ for $a, b \in G$. The map $G \to G$, $a \mapsto \bar{a}^1$ is bijective and $(ab)^{-1} = \bar{b}^1\bar{a}^1 = \bar{a}^1 * \bar{b}^1$. Therefore: The inverse map in a group G is an isomorphism from G onto G^{op}. If G is abelian, then $G^{op} = G$ and the inverse map in an abelian group is an isomorphism of the group onto itself.

In the case of semigroup or monoid M, in general M and M^{op} need not be isomorphic, See Exercise 2D.

2.D.8 Example Let $\mathbb{P}$ denote the set of prime numbers (in $\mathbb{N}$). The fundamental theorem of elementary number theory (FTN) says that the map

$$\varphi : (\mathbb{N}^{(\mathbb{P})}, +) \longrightarrow (\mathbb{N}^*, \cdot), \quad (\alpha_p)_{p\in\mathbb{P}} \longmapsto \prod_{p\in\mathbb{P}} p^{\alpha_p},$$

is bijective from the $\mathbb{P}$-fold direct sum $(\mathbb{N}^{(\mathbb{P})}, +)$ of the additive monoid $(\mathbb{N}, +)$ onto the multiplicative monoid $(\mathbb{N}^*, \cdot)$. The existence-assertion in FTN is equivalent to the surjectivity of φ and the uniqueness assertion in FTN is equivalent to the injectivity of φ. Moreover, φ is an isomorphism of monoids. For $(\alpha_p)_{p\in\mathbb{P}}$ and $(\beta_p)_{p\in\mathbb{P}} \in \mathbb{N}^{(\mathbb{P})}$, we have $\varphi\left((\alpha_p)_{p\in\mathbb{P}} + (\beta_p)_{p\in\mathbb{P}}\right) =$

$$\varphi\left((\alpha_p+\beta_p)_{p\in\mathbb{P}}\right) = \prod_{p\in\mathbb{P}} p^{\alpha_p+\beta_p} = \left(\prod_{p\in\mathbb{P}} p^{\alpha_p}\right)\left(\prod_{p\in\mathbb{P}} p^{\beta_p}\right) =$$

$\varphi\left((\alpha_p)_{\alpha\in\mathbb{P}}\right) \cdot \varphi\left((\beta_p)_{p\in\mathbb{P}}\right)$. With this isomorphism the structure of the multiplicative monoid $(\mathbb{N}^*, \cdot)$ is transfered back onto the (lucid) structure of the additive monoid $(\mathbb{N}^{(\mathbb{P})}, +)$. The inverse isomorphism of φ is the map $n \longmapsto \left(\nu_p(n)\right)_{p\in\mathbb{P}}$, where $\nu_p : \mathbb{N}^* \longrightarrow \mathbb{Z}$ denote the p-exponent map. Similarly, the map

$\mathbb{Z}^\times \times \mathbb{N}^{(\mathbb{P})} \longrightarrow (\mathbb{Z}\setminus\{0\}, \cdot)$ defined by:

$$(\varepsilon, (\alpha_p)_{p\in\mathbb{P}}) \longmapsto \varepsilon \prod_{p\in\mathbb{P}} p^{\alpha_p}$$

is an isomorphism of the (product) monoid $\mathbb{Z}^\times \times \mathbb{N}^{(\mathbb{P})}$ onto the multiplicative monoid $(\mathbb{Z}\setminus\{0\}, \cdot)$ and also the (same) map $\mathbb{Z}^\times \times \mathbb{Z}^{(\mathbb{P})} \longrightarrow (\mathbb{Q}^\times, \cdot)$ $(\varepsilon, (\alpha_p)_{p\in\mathbb{P}}) \longmapsto \varepsilon \prod_{p\in\mathbb{P}} p^{\alpha_p}$ is an isomorphism of groups, where $\mathbb{Z}^\times = (\{1,-1\}, \cdot)$ is the unit group of $(\mathbb{Z}, \cdot)$ and $\mathbb{Q}^\times = (\mathbb{Q}\setminus\{0\}, \cdot)$ is the unit group of $(\mathbb{Q}, \cdot)$.

Let M and M' be sets with multiplicatively written binary operations. The set of all homomorphisms from M into M' is denoted by

$$\mathrm{Hom}(M, M') \ (\subseteq M^{M'})$$

A homomorphism of M into itself is also called an endomorphism of M and the set of all endomorphisms from M into itself is denoted by $\mathrm{End}\, M$, i.e. $\mathrm{End}\, M = \mathrm{Hom}(M, M). \ (\subseteq M^M)$

An isomorphism of M onto itself M is also called an automorphism of M and the set of all automorphisms from M onto M is denoted by $\mathrm{Aut}\, M$ $(\subseteq \mathfrak{S}(M))$. Since the identity map id_M of M is an automorphism of M and since the composition $\varphi\circ\psi$ of two automorphisms φ, ψ of M is again an automorphism of M, further the inverse map φ^{-1} of φ is also an automorphism of M, it follows from the subgroup criterion that :

2.D.9 Lemma The automorphisms $\mathrm{Aut}\, M$ of a set M with binary operation form a subgroup of the permutation group $(\mathfrak{S}(M), \circ)$ of M.

→ 2.D.10 and 2.D.11 on pages 2D|9-a and 2D|9-b

2.D.12 Example (Monoid of Endomorphisms)

Let M be a set with binary operation. Then by 2.D.2 $\mathrm{End}\, M$ is a sub-semigroup of $(M^M, \circ)$ and since $\mathrm{id}_M \in \mathrm{End}\, M$, it is a submonoid. In particular, $\mathrm{End}\, M$ has the structure of a monoid. This canonical monoid is called the monoid of endomorphisms of M. It is clear that $\mathrm{Aut}\, M = \mathfrak{S}(M) \cap \mathrm{End}\, M$. Further, $\mathrm{Aut}\, M$ is even the group of the invertible elements of the monoid $\mathrm{End}\, M$, i.e. $\mathrm{Aut}\, M = (\mathrm{End}\, M)^\times$. Proof If $\varphi \in \mathrm{Aut}\, M$, then $\varphi^{-1} \in \mathrm{Aut}\, M$ and so $\varphi \in (\mathrm{End}\, M)^\times$. On the other hand the elements of $(\mathrm{End}\, M)^\times$ are necessarily bijective and hence are automorphisms.

2.D.13 Example (Homomorphisms into direct products) Let M_i', $i \in I$ be a family of sets with binary operations and let $M' := \prod_{i \in I} M_i'$ with the product of the binary operations of M_i', $i \in I$. Then for every $i \in I$, the i-th projection map $\pi_i : M' \longrightarrow M_i'$, $(a_i)_{i \in I} \longmapsto a_i$ is clearly a homomorphism. Further, let M be a set with

2.D.10 Example Let M, M' be sets with binary operations. If M and M' are isomorphic, then $\mathrm{Aut}\,M$ and $\mathrm{Aut}\,M'$ are also isomorphic. Namely, if $f: M \longrightarrow M'$ is an isomorphism, then the map $\Phi_f: G(M) \longrightarrow G(M')$ defined by $\varphi \longmapsto f\varphi f^{-1}$ maps $\mathrm{Aut}\,M$ onto $\mathrm{Aut}\,M'$ and hence Φ_f restricts to an isomorphism from $\mathrm{Aut}\,M$ onto $\mathrm{Aut}\,M'$.

2.D.11 Example First we compute the automorphism group of $(\mathbb{N}, +)$. Let $h \in \mathrm{Aut}(\mathbb{N}, +)$. Then $h(a+b) = h(a) + h(b)$ for all $a, b \in \mathbb{N}$ and hence $h(a) = a\,h(1)$ for all $a \in \mathbb{N}$. Since h is surjective, it follows that $h(1) = 1$ and then $h = id_{\mathbb{N}}$. This proves that $\mathrm{Aut}(\mathbb{N}, +) = \{id_{\mathbb{N}}\}$ is the trivial group.

For the computation of the automorphism group of the multiplicative monoid $(\mathbb{N}^*, \cdot)$, let $\mathbb{P}$ denote the set of all prime numbers. Note that every automorphism h of $(\mathbb{N}^*, \cdot)$ maps the divisor of an arbitrary $a \in \mathbb{N}^*$ onto the divisor of $h(a)$. For $p \in \mathbb{P}$, $h(p)$ has therefore exactly two divisors, i.e. $h(p) \in \mathbb{P}$. Therefore the restriction $h|_{\mathbb{P}}$ of h to $\mathbb{P}$ is bijective with the inverse $(h|_{\mathbb{P}})^{-1} = h^{-1}|_{\mathbb{P}}$. Therefore we have the map

$$\Phi: \mathrm{Aut}(\mathbb{N}^*, \cdot) \longrightarrow G(\mathbb{P}), \quad h \longmapsto h|_{\mathbb{P}}$$

Since h is an automorphism, h is uniquely determined by its values on the prime factors of the elements of

$\mathbb{N}^*$, this means that the map Φ is injective. Further, Φ is also surjective. For, if $\sigma \in \mathfrak{S}(\mathbb{P})$, the map $\mathbb{N}^* \xrightarrow{h} \mathbb{N}^*$, $\prod_{p\in\mathbb{P}} p^{\alpha_p} \longmapsto \prod_{p\in\mathbb{P}} \sigma(p)^{\alpha_p}$, is the automorphism of $(\mathbb{N}^*, \cdot)$ with $\Phi(h) = h|_{\mathbb{P}} = \sigma$. Altogether, Φ is an isomorphism $\mathrm{Aut}(\mathbb{N}^*, \cdot) \xrightarrow{\sim} \mathfrak{S}(\mathbb{P})$.

a binary operation. For every homomorphism $\varphi: M \longrightarrow M'$, put $\varphi_i := \pi_i \circ \varphi$, $i \in I$, a family of homomorphisms. Conversely, if $\psi_i: M \longrightarrow M_i$, $i \in I$, is a family of homomorphisms, then $\psi: M \longrightarrow M' = \prod_{i \in I} M_i'$ defined by $x \longmapsto (\psi_i(x))_{i \in I}$ is a homomorphism with $\pi_i \circ \psi = \psi_i$; moreover, it is unique! This result can be written as follows: The map

$$\mathrm{Hom}\left(M, \prod_{i \in I} M_i'\right) \longrightarrow \prod_{i \in I} \mathrm{Hom}(M, M_i'),$$

defined by $\varphi \longmapsto (\pi_i \circ \varphi)_{i \in I}$ is bijective.

In the following we continue to denote binary operations multiplicatively.

2.D.14 Proposition Let $\varphi: M \longrightarrow N$ be a homomorphism of sets with binary operations. Then:

(1) If $M' \subseteq M$ is closed with respect to the binary operation of M, then the image $\varphi(M')$ of M' is closed with respect to the binary operation of N.

(2) If $N' \subseteq N$ is closed with respect to the binary operation of N, then the inverse image $\bar{\varphi}^1(N')$ of N' is closed with respect to the binary operation of M.

Proof (1) Let $x, y \in \varphi(M')$ be given, say $x = \varphi(a)$, $y = \varphi(b)$ with $a, b \in M'$. Then $xy = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(M')$, since with $a, b \in M'$, also $ab \in M'$.

(2) Let $a, b \in \varphi^{-1}(N')$ be given, then $\varphi(ab) = \varphi(a) \cdot \varphi(b) \in N'$, since $\varphi(a), \varphi(b) \in N'$ and hence $ab \in \varphi^{-1}(N')$.

A special case of 2.D.12 (1): The image $\varphi(M)$ is closed in N and therefore is provided with a binary operation, namely defined by the restriction of the binary operation of N.
In particular, if $\varphi: M \longrightarrow N$ is injective, then the map induced by φ from M onto $\operatorname{Im}\varphi$, $M \xrightarrow{\varphi} \operatorname{Im}\varphi$, $a \longmapsto \varphi(a)$ is an isomorphism.

2.D.15 Remark (Identification) Let $\varphi: M \to N$ be an injective homomorphism of sets with binary operations. It is often useful to consider the isomorphic image $N' := \varphi(M) \subseteq N$ of M instead of M, the elements $x \in M$ and $\varphi(x) \in N$ are therefore identified with x. Then M appears as substructure N' of N and φ is the canonical injection $N' \longrightarrow N$. In this case we say that M is identified with $N' \subseteq N$ via the injective map φ. With such an identification we always keep in mind the homomorphism φ
Since there are different injective homomorphisms $M \to N$, M is also identified with different sub-structures of N.
An another possibility for the identification is that for every $x \in M$, the element x is replaced by $\varphi(x)$. On $\overline{N} := M \cup (N \setminus \varphi(M))$ define a binary

operation on $\overline{N}$ in a natural way such that M is a (proper) sub-structure of $\overline{N}$ and $\overline{N}$ is isomorphic to N. This is possible only in the case when M and $N \setminus \varphi(M)$ are disjoint; in this given case we can transfer the given structure on N onto the structure on $\overline{N}$.
Both types of identifications serve the simplification. Often injective homomorphisms are also called embeddings.

2.D.16 Example (Cayley's representation)
Let G be a group. For every $a \in G$, the left-translation $\lambda_a : G \longrightarrow G$, $x \longmapsto ax$, is a permutation on the set G; the inverse map of λ_a is $\lambda_{a^{-1}}$. The map $\lambda : G \longrightarrow \mathfrak{S}(G)$ defined by $a \longmapsto \lambda_a$ is a homomorphism, since for $a, b \in G$, we have $\lambda(ab) = \lambda_{ab} = \lambda_a \circ \lambda_b = \lambda(a) \circ \lambda(b)$. Moreover, λ is injective, namely, if e is the neutral element of G, then $\lambda_a(e) = a$. It follows that λ is an isomorphism of G onto the image $\operatorname{Im}\lambda \subseteq \mathfrak{S}(G)$, which is a group and as sub-structure of $\mathfrak{S}(G)$ also a subgroup of $\mathfrak{S}(G)$. The homomorphism λ is called the Cayley's representation of G.

2.D.17 Theorem (Cayley) *Every group is isomorphic to a subgroup of a permutation group.*

Note that if $\# G = n$, then $\mathfrak{S}(G)$ is isomorphic to $\mathfrak{S}_n = \mathfrak{S}(\{1, \dots, n\})$, see Example 2.D.4 and

it follows that:

2.D.18 Corollary *Every finite group of order n is isomorphic to a subgroup of the permutation group $\mathfrak{S}_n = \mathfrak{S}(\{1, \cdots, n\})$.*

2.D.19 Remark (Transformation groups) Groups were originated (always) as subgroups of permutation groups $\mathfrak{S}(X)$. Such subgroups are also known as transformation groups; they arise in a natural way as automorphism groups of mathematical structures; for this 2.D.9 is trivial. The abstract concept of a group, like we have defined in 2A were introduced much later, in the late 19th century, for instance by Dyck (1882) and Weber (1882, 1885). However, as Theorem 2.D.15 shows that every abstract group is a subgroup of a permutation group.

2.D.20 Remark (Anti-homomorphisms) Let M, N be sets with (multiplicative) binary operations. A map $\varphi : M \longrightarrow N$ is called an anti-homomorphism if for all $a, b \in M$, we have $\varphi(ab) = \varphi(b)\varphi(a)$. This is exactly the case if the map φ as a map from M into N^{op} is a homomorphism and in any case, if and only if, as a map from M^{op} into N is a homomorphism. Therefore it is not necessary to anti-homomorphisms systematically.

The composition of two anti-homomorphisms is a homomorphism. The inverse map $x \longmapsto x^{-1}$ of a group is an anti-homomorphism, see Example 2.D.7. From anti-homomorphisms of groups one can sooner or later produce the inverse-map homomorphism. This is an unwritten assertion given in many constructions in group theory.

Finally we make remarks on the properties of binary operations which are often transferred on the images of homomorphisms. For this by Proposition 2.D.12-(1) it is enough to consider surjective homomorphisms.

2.D.21 Proposition *Let $\varphi : M \longrightarrow N$ be a surjective homomorphism of sets with binary operations. Then:*
(1) *If M is a semigroup, then N is also a semigroup.*
(2) *If $e \in M$ is a neutral element in M, then $\varphi(e)$ is a neutral element in N.*
(3) *If M is a monoid, then N is also a monoid.*
(4) *If M is a group, then N is also a group.*

2.D Exercises

1 Give an example of a monoid M with three elements which is not isomorphic to the opposite monoid M^{op}. For a set X with $\#X > 1$, the monoids $(X^X, \circ)$ and $(X^X, \circ)^{op}$ are not isomorphic.

2 Let I be a set and $M := (\mathbb{N}^{(I)}, +)$. Then $\mathrm{Aut}\, M \cong \mathfrak{S}(I)$. (Hint: For $i \in I$, let e_i denote the function $I \to \mathbb{N}$, $j \mapsto \delta_{ij} :=$ the Kroneckers delta. The elements of the form e_i are all elements of M determined by the following property: if $f, g \in M$ are non-zero functions, then $f + g \neq e_i$.)

3 For a group G the following statements are equivalent:

(i) G is commutative

(ii) The map $G \to G$, $x \mapsto x^{-1}$, is an endomorphism of G.

(iii) The map $G \to G$, $x \mapsto x^2$ is an endomorphism of G.

4 An automorphism of a group G is said to be fixed point free if other than the neutral element it has no other fixed point. An automorphism $\varphi : G \to G$ of a group is fixed point free if and only if the map $G \to G$, $y \mapsto y^{-1}\varphi(y)$

is injective. Let $\varphi : G \to G$ be a fixed point free automorphism of a finite group G with $\varphi^2 = id_G$. Then φ is the inverse-map $x \mapsto x^{-1}$ of G and G is abelian of odd-order.