ETH Zürich, D-INFK
HS 2023, 17. November 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Solution 8

8.1 Algebras

a) $\langle \mathbb{Z}; \star \rangle$ is neither a group nor a monoid, because $\star$ is not associative. The counterexample is the following:

$$2 \star (0 \star 0) = 2 \star 0 = 4 \neq 16 = 4 \star 0 = (2 \star 0) \star 0$$

b) $\langle \mathcal{P}(X); \cup \rangle$ is a commutative monoid but not a group.

Associativity and commutativity of $\cup$ follow directly from Theorem 3.4. The neutral element is $\varnothing$, because (1) $A \cup \varnothing = \varnothing \cup A = A$ for all A and (2) $\varnothing \in \mathcal{P}(X)$, since $\varnothing \subseteq X$ for any X.

To prove that it is not a group, we give a counterexample to **G3**. Since $X \neq \varnothing$, there exists an $x \in X$. Therefore, $\{x\} \in \mathcal{P}(X)$. Assume for contradiction that there exists an inverse element of $\{x\}$, that is, assume that there exists an $A \in \mathcal{P}(X)$ such that $\{x\} \cup A = \varnothing$. But since $x \in \{x\} \cup A$, this is a contradiction.

c) It is a group. zWe prove the three properties separately.

- **G1** (associativity). Let $(a, b), (c, d), (e, f) \in S$ be arbitrary. We have

$$\begin{aligned}((a, b) * (c, d)) * (e, f) &= (ac, ad + b) * (e, f)\\ &= (ace, acf + ad + b).\end{aligned}$$

  Moreover, we have

$$\begin{aligned}(a, b) * ((c, d) * (e, f)) &= (a, b) * (ce, cf + d)\\ &= (ace, a(cf + d) + b)\\ &= (ace, acf + ad + b).\end{aligned}$$

- **G2** (neutral element). The neutral element is $e = (1, 0)$. This is because for any $(a, b) \in S$ we have

$$(a, b) * e = (a, b) * (1, 0) = (a \cdot 1, a \cdot 0 + b) = (a, b)$$

  and

$$e * (a, b) = (1, 0) * (a, b) = (1 \cdot a, 1 \cdot b + 0) = (a, b).$$

- **G3** (inverse). Let $(a, b) \in S$ be arbitrary. Using that $a \neq 0$, let $(x, y) = (\frac{1}{a}, \frac{-b}{a})$. Observe that

$$\begin{aligned}(a, b) * (x, y) &= (a, b) * \left(\frac{1}{a}, \frac{-b}{a}\right) \\ &= \left(a \cdot \frac{1}{a}, a \cdot \frac{-b}{a} + b\right) \\ &= (1, 0) \\ &= e.\end{aligned}$$

Thus, $(x, y) \in S$ is a right inverse of (a, b). As shown in the lecture notes (see Section 5.2.4), this implies that (x, y) is also a left inverse of (a, b).

8.2 Facts About Groups

a) We have to show that e is also a left neutral element. For any $a \in G$, we have

$$e * a \overset{\textbf{G3}}{=} (a * \widehat{a}) * a \overset{\textbf{G1}}{=} a * (\widehat{a} * a) \overset{\textbf{G3}}{=} a * e \overset{\textbf{G2}'}{=} a$$

b) We have to show that $\widehat{b} * \widehat{a}$ is the right inverse of $a * b$, that is, that $(a * b) * (\widehat{b} * \widehat{a}) = e$ (as proved in the lecture notes, this implies that $(\widehat{b} * \widehat{a}) * (a * b) = e$).

$$(a * b) * (\widehat{b} * \widehat{a}) \overset{\textbf{G1}}{=} a * \left(b * (\widehat{b} * \widehat{a})\right) \overset{\textbf{G1}}{=} a * \left((b * \widehat{b}) * \widehat{a}\right) \overset{\textbf{G3}}{=} a * (e * \widehat{a}) \overset{\textbf{G2}}{=} a * \widehat{a} \overset{\textbf{G3}}{=} e$$

c) For any $a, b, c \in G$, we have

$$\begin{aligned}a * b = a * c &\overset{\textbf{G3}}{\Longrightarrow} \widehat{a} * (a * b) = \widehat{a} * (a * c) \\ &\overset{\textbf{G1}}{\Longrightarrow} (\widehat{a} * a) * b = (\widehat{a} * a) * c \\ &\overset{\textbf{G3}}{\Longrightarrow} e * b = e * c \\ &\overset{\textbf{G2}}{\Longrightarrow} b = c\end{aligned}$$

8.3 Group Structure induced by Bijections

a) We prove that associativity axiom **G1** is satisfied (for $\langle S, \star \rangle$). Let $x, y, z, \in S$.

$$\begin{aligned}(x \star y) \star z &= f\left(f^{-1}(x) * f^{-1}(y)\right) \star z && \text{(Definition of} \star \text{)} \\ &= f\big(f^{-1}\left(f\left(f^{-1}(x) * f^{-1}(y)\right)\right) * f^{-1}(z)\big) && \text{(Definition of} \star \text{)} \\ &= f\left(\left(f^{-1}(x) * f^{-1}(y)\right) * f^{-1}(z)\right) && (f^{-1} \circ f = \mathrm{id}_G) \\ &= f\left(f^{-1}(x) * \left(f^{-1}(y) * f^{-1}(z)\right)\right) && (\textbf{G1} \text{ for } G) \\ &= f\left(f^{-1}(x) * f^{-1}\left(f\left(f^{-1}(y) * f^{-1}(z)\right)\right)\right) && (f^{-1} \circ f = \mathrm{id}_G) \\ &= f\left(f^{-1}(x) * f^{-1}(y \star z)\right) && \text{(Definition of} \star \text{)} \\ &= x \star (y \star z). && \text{(Definition of} \star \text{)}\end{aligned}$$

b) Now, we prove that the neutral element axiom **G2′** is satisfied (for $\langle S, \star \rangle$). Let $x \in S$.

$$\begin{aligned} x \star f(e) &= f\left(f^{-1}(x) * f^{-1}\left(f(e)\right)\right) && \text{(Definition of} \star \text{)} \\ &= f(f^{-1}(x) * e) && (f^{-1} \circ f = \mathrm{id}_G) \\ &= f(f^{-1}(x)) && (\textbf{G2} \text{ for } G) \\ &= x && (f \circ f^{-1} = \mathrm{id}_H) \end{aligned}$$

Finally, we prove that the inverse axiom **G3′** is satisfied (for $\langle S, \star \rangle$). Let $x \in S$.

$$\begin{aligned} x \star \widetilde{x} &= x \star f\left(\widetilde{f^{-1}(x)}\right) && \text{(Definition of} \;\widetilde{}\;\text{)} \\ &= f\left(f^{-1}(x) * f^{-1}\left(f\left(\widetilde{f^{-1}(x)}\right)\right)\right) && \text{(Definition of} \star \text{)} \\ &= f\left(f^{-1}(x) * \widetilde{f^{-1}(x)}\right) && (f^{-1} \circ f = \mathrm{id}_G) \\ &= f(e) && (\textbf{G3} \text{ for } G) \end{aligned}$$

From the lecture notes and Task 8.2 we know that axioms **G1**, **G2′**, and **G3′** imply **G2** and **G3**.

c) We prove that f is a group homomorphism. Let $a, b \in G$.

$$\begin{aligned} f(a * b) &= f\left(f^{-1}(f(a)) * b\right) && (f^{-1} \circ f = \mathrm{id}_G) \\ &= f\left(f^{-1}(f(a)) * f^{-1}(f(b))\right) && (f^{-1} \circ f = \mathrm{id}_G) \\ &= f(a) \star f(b) && \text{(Definition of } \star \text{)} \end{aligned}$$

Since f is bijective by assumption, then f is a group isomorphism.

d) Let A be a non-empty countable set. By Theorem 3.17 we know that either A is finite, or $A \sim \mathbb{N}$. We treat these two cases separately.

- **(A is finite)** Then there is a finite $M \subseteq \mathbb{N}$ and a bijection $g : M \to A$. Let $k = |M|$. Since $\mathbb{N}$ is well-ordered, we can order the elements of M as

  $$m_1 < m_2 < \ldots m_k.$$

  Now, consider the function $h : \mathbb{Z}_k \to M$ defined as $i \mapsto m_i$. This map is easily verified to be a bijection, so that $g \circ h$ is a bijection from $\mathbb{Z}_k$ to A. The claim follows from subtask a), by observing that $\langle \mathbb{Z}_k, \oplus \rangle$ is a group.
- **($A \sim \mathbb{N}$)** Then there exists a bijection $g : \mathbb{N} \to A$. Since $\mathbb{Z}$ is countable, there exists a bijection $h : \mathbb{Z} \to \mathbb{N}$. Therefore, the composition $g \circ h$ is a bijection $\mathbb{Z} \to A$, and the claim follows from subtask a), by observing that $\langle \mathbb{Z}, + \rangle$ is a group.

8.4 Structure of Groups

a) There are 6 subgroups:

$$\{(0,0)\}, \quad \{0,2\} \times \{0\}, \quad \mathbb{Z}_4 \times \{0\}, \quad \{0\} \times \mathbb{Z}_5, \quad \{0,2\} \times \mathbb{Z}_5, \quad \mathbb{Z}_4 \times \mathbb{Z}_5$$

You are not required to formally justify why these are all subgroups.

b) Take arbitrary $a, b \in G$. Since $a * a = e$ and $b * b = e$, we have $a = \widehat{a}$, $b = \widehat{b}$ and $a * b = \widehat{a * b}$. Hence, $a * b = \widehat{a * b} \overset{\text{Lemma 5.3}}{=} \widehat{b} * \widehat{a} = b * a$.

c) Let $\langle G; *, \widehat{\ }, e\rangle$ be an abelian group. Let $a, b \in G$ and define $n = \operatorname{ord}(a)$ and $m = \operatorname{ord}(b)$. We show that if $nm = |G|$ and $\langle a\rangle \cap \langle b\rangle = \{e\}$ then $G \simeq \mathbb{Z}_n \times \mathbb{Z}_m$.

Consider the subset $S \subseteq G$ defined as $S = \{a^x * b^y \mid x \in \mathbb{Z}_n \text{ and } y \in \mathbb{Z}_m\}$. Clearly S is a subgroup of G. Since $\langle a\rangle \cap \langle b\rangle = \{e\}$ we have $|S| \geq nm = |G|$ so that $S = G$. Now, consider the map

$$\begin{aligned} \varphi : G &\to \mathbb{Z}_n \times \mathbb{Z}_m, \\ a^x * b^y &\mapsto (x, y). \end{aligned}$$

The map φ is a group homomorphism:

$$\begin{aligned}
\varphi(g * h) &= \varphi\left((a^x * b^y) * \left(a^{x'} * b^{y'}\right)\right) && (S = G)\\
&= \varphi\left(a^{x+x'} * b^{y+y'}\right) && (\text{Commutativity of } *)\\
&= \left(x \oplus x', y \oplus y'\right) && (\text{Definition of } \varphi)\\
&= (x, y) \oplus \left(x', y'\right) && (\text{Definition of direct product})\\
&= \varphi(a^x * b^y) \oplus \varphi\left(a^{x'} * b^{y'}\right) && (\text{Definition of } \varphi)\\
&= \varphi(g) \oplus \varphi(h) && (S = G).
\end{aligned}$$

Furthermore, the map φ is surjective, and since $|\mathbb{Z}_n \times \mathbb{Z}_m| = nm = |G|$ then we conclude it is bijective, and a group isomorphism.

Now, consider

$$\langle \mathbb{Z}_{15}^*, \odot_{15}\rangle = \langle \{1, 2, 4, 7, 8, 11, 13, 14\}, \odot_{15}\rangle,$$

Direct computation shows $\operatorname{ord}(2) = 4$ and $\operatorname{ord}(11) = 2$. Since $|\mathbb{Z}_{15}^*| = \varphi(15) = 8$, we have $\operatorname{ord}(2)\operatorname{ord}(11) = |\mathbb{Z}_{15}^*|$. Again, direct computation shows that $\langle 2\rangle \cap \langle 11\rangle = \{1\}$. Therefore, by the argument above, we have $\mathbb{Z}_{15}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.

Consider

$$\langle \mathbb{Z}_{16}^*, \odot 16\rangle = \langle \{1, 3, 5, 7, 9, 11, 13, 15\}, \odot_{16}\rangle.$$

Direct computation shows $\operatorname{ord}(3) = 4$ and $\operatorname{ord}(7) = 2$. Since $|\mathbb{Z}_{16}^*| = \varphi(16) = 8$, we have $\operatorname{ord}(3)\operatorname{ord}(7) = |\mathbb{Z}_{16}^*|$. Again, direct computation shows that $\langle 3\rangle \cap \langle 7\rangle = \{1\}$. Therefore, by the argument above, we have $\mathbb{Z}_{16}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.

This shows $\mathbb{Z}_{16}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \simeq \mathbb{Z}_{15}^*$.

8.5 A Binary Operation From a Group Homomorphism

First, observe that for any $x, y, z \in G$ we have:

$$\begin{aligned} x \cdot (y \cdot z) &= \psi(x) * \psi(y \cdot z) && \text{(def. }\cdot\text{)} \\ &= \psi(x) * \psi(\psi(y) * \psi(z)) && \text{(def. }\cdot\text{)} \\ &= \psi(x) * (\psi(\psi(y)) * \psi(\psi(z))) && (\psi \text{ homomorphism}) \end{aligned}$$

Moreover, we have

$$\begin{aligned} (x \cdot y) \cdot z &= \psi(x \cdot y) * \psi(z) && \text{(def. }\cdot\text{)} \\ &= \psi(\psi(x) * \psi(y)) * \psi(z) && \text{(def. }\cdot\text{)} \\ &= (\psi(\psi(x)) * \psi(\psi(y))) * \psi(z) && (\psi \text{ homomorphism}) \end{aligned}$$

We prove each direction ($\Longrightarrow$ and $\Longleftarrow$) of the claim separately.

- $\Longrightarrow$: Assume that $\cdot$ is associative. Let $x \in G$ be arbitrary. We have

$$\begin{aligned} x \cdot (e \cdot e) &= \psi(x) * (\psi(\psi(e)) * \psi(\psi(e))) && \text{(above)} \\ &= \psi(x) * (\psi(e) * \psi(e)) && \text{(L5.5 (i))} \\ &= \psi(x) * (e * e) && \text{(L5.5 (i))} \\ &= \psi(x) * e && \text{(G2)} \\ &= \psi(x) && \text{(G2)} \end{aligned}$$

Analogously, we have

$$\begin{aligned} (x \cdot e) \cdot e &= (\psi(\psi(x)) * \psi(\psi(e))) * \psi(e) && \text{(above)} \\ &= (\psi(\psi(x)) * \psi(e)) * e && \text{(L5.5 (i))} \\ &= (\psi(\psi(x)) * e) * e && \text{(L5.5 (i))} \\ &= \psi(\psi(x)) * e && \text{(G2)} \\ &= \psi(\psi(x)) && \text{(G2)} \end{aligned}$$

Since $\cdot$ is associative, we must have

$$x \cdot (e \cdot e) = (x \cdot e) \cdot e.$$

Hence, $\psi(x) = \psi(\psi(x))$.

- $\Longleftarrow$: Assume that ψ is idempotent. Then, we have for any $x, y, z \in G$:

$$\begin{aligned} x \cdot (y \cdot z) &= \psi(x) * (\psi(\psi(y)) * \psi(\psi(z))) && \text{(above)} \\ &= \psi(x) * (\psi(\psi(y)) * \psi(z)) && (\psi \text{ idemp.}) \\ &= \psi(\psi(x)) * (\psi(\psi(y)) * \psi(z)) && (\psi \text{ idemp.}) \\ &= (\psi(\psi(x)) * \psi(\psi(y))) * \psi(z) && \text{(G1)} \\ &= (x \cdot y) \cdot z && \text{(above)} \end{aligned}$$

8.6 Isomorphisms Map Generators to Generators

Take an arbitrary $h \in H$ and let $a = \psi^{-1}(h)$ (the inverse of ψ exists, because ψ is bijective). Since g is a generator, there exists an $m \in \mathbb{Z}$ such that $a = g^m$.

- If $m = 0$, then by Lemma 5.5 (i), $h = \psi(g^0) = \psi(e) = e' = \psi(g)^0$, where e and e' are the neutral elements of G and H, respectively.
- If $m > 0$, then $h = \psi(g^m) = \psi(g)^m$, where the last step is trivial for $m = 1$ and otherwise follows from applying the definition of a homomorphism $m - 1$ times.
- If $m < 0$, then $h = \psi(g^m) = \psi((\widehat{g})^{|m|}) = \psi(\widehat{g})^{|m|} = (\widetilde{\psi(g)})^{|m|} = \psi(g)^m$, where the third step is justified as above, and the fourth step follows from Lemma 5.5 (ii).

8.7 Rotations of a Cube

a) First of all, one has to decide which corner of the sofa coincides with the corner of the room. For this, there are 8 possibilities. Once this corner is set, there are 3 edges coming out of this corner (one of them going up) and, hence, 3 possibilities to place the sofa. Once the corner and the edge going up are fixed, the position of the sofa is fully defined. Hence, there are $3 \cdot 8 = 24$ possibilities overall.

b) Let us first determine $|R|$. Assume that the sofa stands in the corner in a certain (arbitrary) position. After a rotation b, it may end up in one of the 24 possible positions (this follows from Subtask a)). Therefore, we can distinguish 24 different rotations and $|R| = 24$.

It is possible to describe each element of R as a rotation around single axis. To see this, consider all possible different rotations of a cube around an axis:

- Identity.
- Rotation around the centers of two opposite faces. There are 3 pairs of opposite faces and for each pair there are 3 possible rotations: by 90, 180 and 270 degrees. Together, this gives 9 rotations.
- Rotation around two opposite vertices. There are 4 pairs of opposite vertices and for each pair there are 2 possible rotations: by 120 and 240 degrees. Together, this gives 8 rotations
- Rotation around the centers of two opposite edges. There are 6 pairs of opposite edges and for each pair there is only one possible rotation: by 180 degrees. Together, this gives 6 rotations.

One can see (for example by drawing the cube after each rotation) that no two of the above rotations end up with the cube being in the same position. Since together we described 24 rotations and $|R| = 24$, each element of R corresponds to *exactly one* rotation.

c) $\langle R; \circ \rangle$ is a group. Since function composition is associative, $\circ$ is associative as well (this is because every rotation corresponds to a permutation of vertices). The neutral element is the identity. Furthermore, every element has an inverse, namely a rotation around the same axis by 360 degrees minus the original angle.

d) The operation $\circ$ is not commutative. Figure 1 illustrates that there exist rotations, which do not commute.

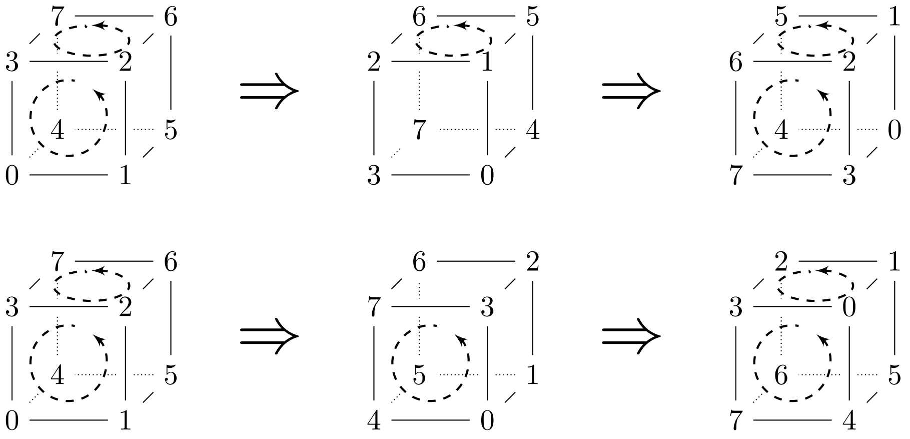

Figure 1: $\langle R; \circ \rangle$ is not commutative.