Christian-Albrechts-Universität zu Kiel
Technische Fakultät

Dependable Systems Group
D. Nowotka, P. Fleischmann

Example solution for Series #1

Exercise 1 — 10 Points

You get for each correct answer 1 point, but you will lose 1 point for an incorrect answer.

a) Equivalence relations are reflexive, antisymmetric, and transitiv. ○ true ⊗ false

b) In a group $(G, \cdot, e)$ where a^{-1} denotes the inverse element of $a \in G$, the inverse element of $a \cdot b$ is $b^{-1} \cdot a^{-1}$. ⊗ true ○ false

c) Define the complement as $A^C = U \backslash A$ for a set U and $A \subseteq U$. The complement operation is idempotent. ⊗ true ○ false

d) The intersection on sets is commutative. ⊗ true ○ false

e) The usual substraction $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is associative. ○ true ⊗ false

f) The natural numbers $\mathbb{N}$ are not closed under division. ⊗ true ○ false

g) Functions are left-total and right-unique relations. ⊗ true ○ false

h) Each group is abelian w.r.t. its operation. ○ true ⊗ false

i) $(\mathbb{Z}, +, \cdot, 0, 1)$ is a field with the usual addition and multiplication. ○ true ⊗ false

j) Two sets A and B are equal iff $A \subseteq B$ and $B \subseteq A$. ⊗ true ○ false

Exercise 2 — 7 Points

Give the following definitions and notations:

a) $R \subseteq G \times G$ over a group $(G, \cdot, e)$ is a congruence relation. (1P)
b) $R \subseteq M \times M$ for a set M be a well-ordering relation. (1P)
   a) Find R and M such that R is a well-ordering on M. (0.5P)
   b) Find R' and M' such that R' is not a well-ordering on M'. (0.5P)
c) Symmetric group $\mathcal{S}_n$ on the set $[n]$ for $n \in \mathbb{N}$. (1P)
d) $(M, \cdot, e)$ monoid. (1.5P)
e) Let $f, g : \mathbb{N} \to \mathbb{R}$ be functions, define the Landau sets
   i) $f \in \mathcal{O}(g)$ (0.5P)
   ii) $f \in \Omega(g)$ (0.5P)
   iii) $f \in \Theta(g)$ (0.5P)

Solution:

a) R is an equivalence relation and for all $(g_1, g_2), (g_1', g_2') \in R$ we have $(g_1 \cdot g_1', g_2 \cdot g_2') \in R$.
b) A relation is a well-order iff it is a total order and each subset has a minimum.
   i) $<$ on $\mathbb{N}$ is a well-ordering.
   ii) $<$ on $\mathbb{Z}$ is not a well-ordering.
c) For $n \in \mathbb{N}$ the symmetric group $\mathcal{S}_n$ is defined as set of all permutations on $[n]$.
d) $(M, \cdot, e)$ is a monoid if M is closed under $\cdot$, $\cdot$ is associative and e is the neutral element w.r.t. $\cdot$.
e) i) $f \in \mathcal{O}(g)$ iff $\exists c > 0 \exists n_0 \in \mathbb{N} \forall n \in \mathbb{N}_{\geq n_0} : f(n) \leq cg(n)$
   ii) $f \in \Omega(g)$ iff $g \in \mathcal{O}(f)$

iii) $f \in \Theta(g)$ iff $g \in \mathcal{O}(f)$ and $f \in \mathcal{O}(g)$

Exercise 3

17 Points

a) Define $f : \mathbb{N} \to \mathbb{R}; n \mapsto 4n^2 + 7n + 3$ and $g : \mathbb{N} \to \mathbb{R}; n \mapsto n^2$. Prove $f \in \mathcal{O}(g)$. (2P)

b) Let $(G, \cdot, e)$ be a group. Prove that the right-neutrality of e follows by the left-neutrality of e. (2P)

c) Define $\equiv_c \subseteq \mathbb{Z} \times \mathbb{Z}$ for $c \in \mathbb{N}$ by $(a, b) \in \equiv_c$ iff $c|a - b$. For convenience we write $a \equiv_c b$ instead of $(a, b) \in \equiv_c$. Prove that $\equiv_c$ is a congruence relation. (4P)

d) i) Prove that the symmetric group $\mathcal{S}_n$ for $n \in \mathbb{N}$ is indeed a group with composition $\circ : \mathcal{S}_n \times \mathcal{S}_n \to \mathcal{S}_n$ as operation. (8P)

ii) Decide whether $\mathcal{S}_n$ is abelian or not. Justify your answer. (1P)

Solution:

a) For $c = 14$ and $n_0 = 1$ we have by $n^2 \geq n$ for all $n \in \mathbb{N}$

$$f(n) = 4n^2 + 7n + 3 \leq 4n^2 + 7n^2 + 3n^2 = 14n^2 = c \cdot g(n). \quad \square$$

b) Let $a \in G$. Since e is right-neutral we have $a \cdot e = a$. Since e is neutral we have $a^{-1} \cdot a = e$ for the inverse element a^{-1} of a. By the associativity of $\cdot$ on G we get

$$a = a \cdot e = a \cdot (a^{-1} \cdot a) = (a \cdot a^{-1}) \cdot a = e \cdot a. \quad \square$$

c) We prove firstly that $\equiv_c$ is an equivalence relation. By $c|0$ we have $c|a - a$ for all $a \in \mathbb{Z}$ and thus $a \equiv_c a$, which proves the reflexivity of $\equiv_c$. Let $a, b \in \mathbb{Z}$ with $a \equiv_c b$. For the symmetry we have to prove $b \equiv_c a$, i.e. $c|b - a$. By $c|a - b$ and the implication that if a number n divides a number m then n divides also pm for all integers p, we have $c|(-1)(a - b) = -a + b = b - a$. For the transitivity let $a, b, d \in \mathbb{Z}$ with $a \equiv_c b$ and $b \equiv_c d$. By the implication that if a number n divides m_1 and m_2 then n divides also $m_1 + m_2$ we get

$$c|(a - b) + (b - d) = a - b + b - d = a - d.$$

Now we prove the congruence property. Assume $a_1 \equiv_c b_1$ and $a_2 \equiv_c b_2$. Again by the *addition-argument* we get

$$c|(a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2). \quad \square$$

d) i) We have to prove that the composition $\circ : \mathcal{S}_n \times \mathcal{S}_n \to \mathcal{S}_n$ is closed and associative. Moreover we have to find a neutral element and to show that for each element $\pi \in \mathcal{S}_n$ exists the inverse element in $\mathcal{S}_n$. Let $\pi_1, \pi_2 \in \mathcal{S}_n$. Permutations are defined as bijective mappings and thus we have to prove that $\pi_1 \circ \pi_2$ is bijective on $[n]$. Let $m \in [n]$. Since π_2 is surjective there exists an $m_1 \in [n]$ with $\pi_2(m_1) = m$. Since π_1 is surjective there exists an $m_2 \in [n]$ with $\pi_1(m_2) = m_1$. This implies $\pi_2(\pi_1(m_2)) = \pi_2(m_1) = m$, i.e. $\pi_1 \circ \pi_2$ is surjective. For the injectivity consider $m_1, m_2 \in [n]$ with $\pi_2(\pi_1(m_1)) = \pi_2(\pi_1(m_2))$. Since π_2 is injective we get $\pi_1(m_1) = \pi_1(m_2)$. Since π_1 is injective we get $m_1 = m_2$, i.e. the injectivity of $\pi_1 \circ \pi_2$. This proves that $\mathcal{S}_n$ is closed under $\circ$. We are going to prove now the associativity of $\circ$. Let $\pi_1, \pi_2, \pi_3 \in \mathcal{S}_n$ and $m \in [n]$. By the definition of the composition we get

$$((\pi_1 \circ \pi_2) \circ \pi_3)(n) = (\pi_3(\pi_1 \circ \pi_2))(n) = \pi_3(\pi_2(\pi_1(n))) = (\pi_2 \circ \pi_3)(\pi_1(n)) = (\pi_1 \circ (\pi_2 \circ \pi_3))(n).$$

Define $\mathrm{id}_n : [n] \to [n]; n \mapsto n$. Let $\pi \in \mathcal{S}_n$ and $m \in [n]$. Then we get $(\pi \circ \mathrm{id}_n)(m) = \mathrm{id}_n(\pi(m)) = \pi(m)$ and thus id_n is the neutral element of $\mathcal{S}_n$. For $\pi \in \mathcal{S}_n$ define $\psi : [n] \to [n]$ by $\psi(m) = m'$ iff $\pi(m') = m$. ψ is well-defined since π is a permutation. For $m \in [n]$ we get

$$(\psi \circ \pi)(m) = \pi(\psi(m)) = \pi(m') = m = \mathrm{id}_n(m).$$

This proves that there exists an inverse element for each permutation; this concludes the prove that $\mathcal{S}_n$ is a group.

ii) The symmetric group is not abelian, witnessed by the permutations $\pi_1 = (1234)$ and $\pi_2 = (143)(2)$:

$$\pi_1 \circ \pi_2 = (12)(3)(4) \quad \text{and} \quad \pi_2 \circ \pi_1 = (1)(23)(4). \quad \square$$