Tentamen Wat is Wiskunde (WISB101)
Donderdag 9 november 2017, 9:00 - 12:00

Docenten: *Barbara van den Berg & Gil Cavalcanti & Karma Dajani & Carel Faber & Harry Smit & Guido Terra-Bleeker*

- GEBRUIK EEN APART VEL VOOR IEDERE OPGAVE. Het tentamen bestaat uit zes opgaven die elk even zwaar meetellen.
- Dit tentamen bevat een NEDERLANDSE en een ENGELSE VERSIE. De Engelse versie staat na de Nederlandse versie.
- Schrijf je naam en studentnummer op elk vel.
- Het gebruik van telefoons, computers, rekenmachines, boeken of aantekeningen is niet toegestaan.
- Geef niet alleen antwoorden, maar laat bij elke (deel)opgave duidelijk zien hoe je aan je antwoorden komt en bewijs al je beweringen.
- Ook als je een onderdeel van een opgave niet kunt bewijzen, mag je dat resultaat in het vervolg wel gebruiken.

Opgave 1 (nieuw vel papier)

(a). (*8 punten*) Laat P en Q twee beweringen zijn. Bewijs met behulp van een waarheidstabel dat de volgende bewering een tautologie is:

$$((P \Rightarrow Q) \wedge \sim Q) \Rightarrow \sim P.$$

(b). (*2 punten*) Laat $f\colon X \to Y$ een functie zijn. Geef de definities van injectiviteit en surjectiviteit met behulp van kwantoren en logische symbolen.

Uitwerking.

1. **Te bewijzen:** De samengestelde bewering

$$((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$$

waarin P en Q willekeurige beweringen zijn, is een tautologie.

Bewijs: We beschouwen de vier verschillende gevallen voor het al dan niet waar zijn van de beweringen P en Q in een waarheidstabel:

P	Q	$P \Rightarrow Q$	$\neg Q$	$(P \Rightarrow Q) \wedge \neg Q$	$\neg P$	$((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$
T	T	T	F	F	F	T
T	F	F	T	F	F	T
F	T	T	F	F	T	T
F	F	T	T	T	T	T

Hierin staat T voor het waar en F voor het onwaar zijn van de desbetreffende bewering. De implicatie $P \Rightarrow Q$ is alleen onwaar als P wel waar is, maar Q niet. De kolommen voor $\neg Q$ en $\neg P$ bevatten simpelweg het tegengestelde van de waarheidswaarde van Q resp. P. De conjunctie $(P \Rightarrow Q) \wedge \neg Q$ is alleen waar als beide beweringen $(P \Rightarrow Q)$ en $\neg Q$ waar zijn, dus alleen in het laatste van de vier gevallen. De implicatie in de laatste kolom is weer waar tenzij de premisse $(P \Rightarrow Q) \wedge \neg Q$ waar is terwijl de conclusie $\neg P$ dat niet is. Die combinatie komt nooit voor, dus die implicatie is altijd waar, zoals weergegeven met een T in elke cel van de laatste kolom. We hebben dus laten zien dat de desbetreffende samengestelde bewering $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$ in alle gevallen waar is, hetgeen betekent dat deze een *tautologie* is.

2. **Gegeven:** Twee verzamelingen X en Y en een functie $f : X \to Y$ van X naar Y.

   Definitie: De functie f heet *injectief* als voor elke $a, b \in X$ de volgende implicatie geldt:
$$f(a) = f(b) \Rightarrow a = b.$$
   Oftewel:
$$\forall\, a \in X, \forall\, b \in X: \; f(a) = f(b) \Rightarrow a = b.$$

   Definitie: De functie f heet *surjectief* als er voor elke $y \in Y$ een $x \in X$ bestaat zodanig dat
$$f(x) = y.$$
   Oftewel:
$$\forall\, y \in Y : \exists\, x \in X : \; f(x) = y.$$

Opgave 2 (nieuw vel papier)

(a). (*4 punten*) Laat X en Y twee verzamelingen zijn. Bewijs dat $X \cap Y = X \cup Y$ dan en slechts dan als $X = Y$.

We definiëren een relatie R op $\mathbb{R}$ door: xRy dan en slechts dan als $\lceil x \rceil = \lceil y \rceil$.

(b). (*4 punten*) Bewijs dat R een equivalentierelatie is.

(c). (*2 punten*) Beschrijf de partitie van $\mathbb{R}$ bepaald door R (in termen van intervallen van $\mathbb{R}$). Bewijs je bewering.

Uitwerking.

(a) We bewijzen de twee implicaties:

  (1) als $X \cap Y = X \cup Y$ dan $X = Y$;

  (2) als $X = Y$ dan $X \cap Y = X \cup Y$.

Bewijs van (1): Laat $x \in X$ willekeurig zijn. Dan is $x \in X$ of $x \in Y$, dus $x \in X \cup Y$. Uit de aanname $X \cap Y = X \cup Y$ volgt dat $x \in X \cap Y$. We zien dat $x \in Y$ en concluderen dat $X \subseteq Y$. Net zo bewijzen we dat $Y \subseteq X$, en dus $X = Y$.

Bewijs van (2): Als $X = Y$ dan is $X \cup Y = X \cup X = X$ en $X \cap Y = X \cap X = X$. We concluderen dat $X \cap Y = X \cup Y$.

Uit de twee implicaties volgt dat $X \cap Y = X \cup Y$ dan en slechts dan als $X = Y$.

(b) We bewijzen dat R reflexief, symmetrisch en transitief is.

Laat $a, b, c \in \mathbb{R}$ willekeurig zijn. Ten eerste merken we op dat voor alle $a \in \mathbb{R}$ geldt dat $\lceil a \rceil = \lceil a \rceil$, dus aRa. We zien dat R reflexief is. Ten tweede geldt dat als aRb dan is $\lceil a \rceil = \lceil b \rceil$, en dus $\lceil b \rceil = \lceil a \rceil$, oftewel bRa. We concluderen dat R ook symmetrisch is. Tenslotte geldt dat als aRb en bRc, dan is $\lceil a \rceil = \lceil b \rceil$ en $\lceil b \rceil = \lceil c \rceil$ en dus $\lceil a \rceil = \lceil c \rceil$, oftewel aRc. Dus R is transitief. Omdat R reflexief, symmetrisch en transitief is, is R een equivalentierelatie.

(c) De partitie van $\mathbb{R}$ bepaald door R wordt gegeven door de verzameling equivalentieklassen $\{[x] | x \in \mathbb{R}\}$ van R. Laat $x \in \mathbb{R}$ willekeurig en noem $\lceil x \rceil = n$. Dan is $n \in \mathbb{Z}$ en dus $\lceil n \rceil = n$, en we concluderen dat x gerelateerd is aan n. Dus xRn en dus (stelling uit het boek) $[x] = [n]$. We zien dat:

$$\{[x] | x \in \mathbb{R}\} = \{[n] | n \in \mathbb{Z}\}.$$

Voor iedere $n \in \mathbb{Z}$ geldt: $y \in [n]$ dan en slechts dan als yRn en dus per definitie $\lceil y \rceil = \lceil n \rceil$, wat gelijk is aan $\lceil y \rceil = n$ omdat n geheel is. Dit is equivalent aan $n - 1 < y \leq n$, dat wil zeggen $y \in (n-1, n]$. We concluderen dat:

$$\{[x] | x \in \mathbb{R}\} = \{[n] | n \in \mathbb{Z}\} = \{(n-1, n] | n \in \mathbb{Z}\} = \{\cdots (-2, -1], (-1, 0], (0, 1], (1, 2], \cdots\}.$$

Opgave 3 (nieuw vel papier)

In deze opgave bepalen we de waarde van

$$\sum_{k=1}^{\infty} \frac{k}{2^k}.$$

(a). (*4 punten*) Voor $n \in \mathbb{N}$ definiëren we $t_n = \frac{n}{2^n} + \sum_{k=1}^{n} \frac{k}{2^k}$. Bewijs met volledige inductie dat voor alle $n \in \mathbb{N}$ geldt dat $t_n = 2 - \frac{1}{2^{n-1}}$.

(b). (*4 punten*) Bepaal $\lim_{n \to \infty} t_n$ en geef hiervoor een ϵ-N-bewijs.

(c). (*2 punten*) Bepaal $\sum_{k=1}^{\infty} \frac{k}{2^k}$. Je mag hierbij gebruik maken van het feit dat $\lim_{n \to \infty} \frac{n}{2^n} = 0$ en dat

$$\lim_{n \to \infty} t_n = \lim_{n \to \infty} \frac{n}{2^n} + \lim_{n \to \infty} \sum_{k=1}^{n} \frac{k}{2^k}.$$

Uitwerking. Dit is een uitgebreide uitwerking. Het werd op het tentamen niet bestraft als je beknopter was dan dit.

(a) We bewijzen met inductie dat de formule $t_n = 2 - \frac{1}{2^{n-1}}$ waar is.

Inductiebasis. We substitueren $n = 1$ in de formule van t_n en krijgen $t_1 = \frac{1}{2^1} + \sum_{k=1}^{1} \frac{k}{2^k} = \frac{1}{2} + \frac{1}{2} = 1$. Verder geldt $2 - \frac{1}{2^{1-1}} = 2 - \frac{1}{1} = 1$, dus de formule klopt inderdaad voor $n = 1$.

(1 punt, -0.5 voor als je opschrijft dat $t_1 = 2 - \frac{1}{2^{1-1}}$)

Inductiehypothese. Stel nu dat de formule geldt voor een zekere $m \in \mathbb{N}$, dat wil zeggen, we nemen aan dat $t_m = 2 - \frac{1}{2^{m-1}}$. We gaan in de inductiestap laten zien dat $t_{m+1} = 2 - \frac{1}{2^{(m+1)-1}} = 2 - \frac{1}{2^m}$. Volgens het principe van inductie is de formule vervolgens waar voor elk natuurlijk getal.

(1 punt, -0.5 bij onduidelijkheid wat je inductiehypothese is)

Inductiestap. Er geldt dat

$$\begin{aligned} t_{l+1} &= \frac{m+1}{2^{m+1}} + \sum_{k=1}^{m+1} \frac{k}{2^k} \\ &= 2\frac{m+1}{2^{m+1}} + \sum_{k=1}^{m} \frac{k}{2^k} \\ &= \frac{m+1}{2^m} + \sum_{k=1}^{m} \frac{k}{2^k} \\ &= \frac{1}{2^m} + \frac{m}{2^m} + \sum_{k=1}^{m} \frac{k}{2^k} \\ &= \frac{1}{2^m} + \left[\frac{m}{2^m} + \sum_{k=1}^{m} \frac{k}{2^k} \right] \\ &= \frac{1}{2^m} + t_l. \end{aligned}$$

Volgens de inductiehypothese geldt dat $t_m = 2 - \frac{1}{2^{m-1}}$. We substitueren dit in onze zojuist gevonden formule van t_{m+1}:

$$\begin{aligned} t_{m+1} &= \frac{1}{2^m} + t_m \\ &= \frac{1}{2^m} + 2 - \frac{1}{2^{m-1}} \\ &= 2 - \frac{1}{2^{m-1}} + \frac{1}{2^m} \\ &= 2 - \frac{2}{2^m} + \frac{1}{2^m} \\ &= 2 - \frac{1}{2^m}. \end{aligned}$$

Dit voltooit de inductiestap. Zoals eerder gezegd kunnen we nu concluderen dat $t_n = 2 - \frac{1}{2^{n-1}}$.

(2 punten (1 voor het toepassen van de inductiehypothese en 1 voor het correct verder uitwerken, -1 bij onduidelijkheid over wat je al hebt bewezen en wat je nog moet bewijzen ("de verkeerde kant op werken"), -0.5 bij vergeten conclusie)

(b) Er geldt dat $\lim_{n\to\infty} t_n = 2$, hetgeen we laten zien met een ϵ-N-bewijs. Zij $\epsilon > 0$ en definieer $N = \max(1, \lceil \log_2(\frac{1}{\epsilon}) \rceil + 1)$. Merk op dat $N \in \mathbb{N}$. Voor elke $n \in \mathbb{N}$, $n > N$ geldt nu dat

$$|t_n - 2| = \left| 2 - \frac{1}{2^{n-1}} - 2 \right| = \left| -\frac{1}{2^{n-1}} \right| = \frac{1}{2^{n-1}} < \frac{1}{2^{N-1}}.$$

Verder geldt $N \geq \lceil \log_2(\frac{1}{\epsilon}) \rceil + 1 \geq \log_2(\frac{1}{\epsilon}) + 1$, dus $2^{N-1} \geq 2^{\log_2(\frac{1}{\epsilon})} = \frac{1}{\epsilon}$. Omdat zowel 2^{N-1} en ϵ positief zijn, volgt dat $\frac{1}{2^{N-1}} \leq \epsilon$. Dit heeft tot gevolg dat $|t_n - 2| < \frac{1}{2^{N-1}} \leq \epsilon$. We mogen nu concluderen dat $\lim_{n\to\infty} t_n = 2$.

(4 punten, 1 voor bepaling limiet, 2 voor correcte N, 1 voor juiste uitwerking $|t_n - 2|$. -1 bij slechts geven van een bewijsstrategie, -0.5 (per fout) voor een N die niet altijd geheel/positief is, -0.5 bij vergeten conclusie)

(c) Bij deel (b) hebben we bewezen dat $\lim_{n\to\infty} t_n = 2$. Gegeven is dat $\lim_{n\to\infty} \frac{n}{2^n} = 0$ en dat

$$\lim_{n\to\infty} t_n = \lim_{n\to\infty} \frac{n}{2^n} + \lim_{n\to\infty} \sum_{k=1}^{n} \frac{k}{2^k}.$$

Het combineren van deze drie stukken informatie geeft dat

$$\lim_{n\to\infty} \sum_{k=1}^{n} \frac{k}{2^k} = \lim_{n\to\infty} t_n - \lim_{n\to\infty} \frac{n}{2^n} = 2 - 0 = 2.$$

Omdat per definitie geldt dat $\sum_{k=1}^{\infty} \frac{k}{2^k} = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{k}{2^k}$, concluderen we dat $\sum_{k=1}^{\infty} \frac{k}{2^k} = 2$.

(2 punten, -0.5 indien niet duidelijk aangegeven waar de informatie van $\lim_{n\to\infty} t_n = 2$ en $\lim_{n\to\infty} \frac{n}{2^n} = 0$ vandaan komt (dit kan worden gecompenseerd indien netjes is aangegeven dat $\sum_{k=1}^{\infty} \frac{k}{2^k} = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{k}{2^k}$))

Opgave 4 (nieuw vel papier)

Laat X en Y twee niet-lege verzamelingen zijn. Bewijs de volgende drie beweringen:

(a). (*4 punten*) Laat $g : Y \to X$ een functie zijn. Als er een functie $f : X \to Y$ bestaat zodat voor alle $x \in X$ geldt dat $(g \circ f)(x) = x$, dan is g surjectief.

(b). (*4 punten*) Laat $f : X \to Y$ een functie zijn. Als er een functie $g : Y \to X$ bestaat zodat voor alle $x \in X$ geldt dat $(g \circ f)(x) = x$, dan is f injectief.

(c). (*2 punten*) Laat $f : X \to Y$ een functie zijn. Als f injectief is, dan bestaat er een functie $g : Y \to X$ met de eigenschap dat $(g \circ f)(x) = x$ voor alle $x \in X$.

Solution.

1. We give a direct proof. To show that $g : Y \to X$ is surjective we need to show that for every $x \in X$ there is $y \in Y$ such that $g(y) = x$. Let $x \in X$ and take $y = f(x)$. Then

$$g(y) = g(f(x)) = g \circ f(x) = x.$$

Therefore g satisfies the definition of a surjective function.

2. Again we give a direct proof. To show that $f : X \to Y$ is injective we need to show that if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Let $x_1, x_2 \in X$ be such that $f(x_1) = f(x_2)$, then

$$x_1 = g \circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g \circ f(x_2) = x_2$$

Therefore f satisfies the definition of an injective function.

3. This is an existence statement. We will prove it by producing an example of a function g with the desired property.

Given an injective function $f : X \to Y$, we can consider the function

$$f_1 : X \to \text{range}(f), \qquad f_1(x) = f(x).$$

Since f is injective, so is f_1. By construction it is clear that f_1 is also surjective hence f_1 is a bijection and as such has an inverse $f_1^{-1} : \text{range}(f) \to X$. Since X is nonempty, it has an element. Let $x_0 \in X$. Define a function g as follows

$$g : Y \to X; \qquad g(y) = \begin{cases} f_1^{-1}(y), & \text{if } y \in \text{range}(f) \\ x_0, & \text{if } y \notin \text{range}(f) \end{cases}$$

Then

$$g \circ f(x) = g(f(x)) = f_1^{-1}(f(x)) = f_1^{-1}(f_1(x)) = x,$$

where in the second equality we used $f(x) \in \text{range}(f)$ and in the third that $f_1(x) = f(x)$. Therefore we conclude that the function g has the desired property.

Opgave 5 (nieuw vel papier)

(a). (*3 punten*) Beschouw de functie $f : \{0,1,2,3,4\} \times \mathbb{N} \to \mathbb{N}$ gegeven door $f((i,n)) = i + 5n$. Wat is $f((0,1))$? En wat is $f((1,2))$? Laat zien dat f injectief is.

(b). (*2 punten*) Bewijs dat $\{0,1,2,3,4\} \times \mathbb{N}$ aftelbaar oneindig is.

(c). (*3 punten*) Bewijs dat $|\{-1,1\} \times \mathbb{R}| \leq |\mathbb{R}|$. Je mag hierbij gebruik maken van het feit dat de functie $f \colon \mathbb{R} \to \mathbb{R}^+$ gedefinieerd door $f(x) = e^x$ injectief is.

(d). (*2 punten*) Bewijs dat $|\{-1,1\} \times \mathbb{R}| = |\mathbb{R}|$.

Uitwerking(a): $f((0,1)) = 5$ en $f((1,2)) = 11$. We bewijzen nu dat f injectief is. Stel dat $f(i,n) = f(j,m)$, dan $i + 5n = j + 5m$ ofwel $i - j = 5(m - n)$. Dus $5|(i-j)$ en aangezien dat $i - j \in \{-4,-3,-2,-1,0,1,2,3,4\}$, zien we dat $i - j = 0$. Er volgt dat $i = j$ en $n = m$ en dus f injectief is.

Uitwerking(b): We gaan Schröder-Bernstein gebruiken. Uit onderdeel (a) hebben we een injectieve functie $f : \{0,1,2,3,4\} \times \mathbb{N} \to \mathbb{N}$. Definieer $g : \mathbb{N} \to \{0,1,2,3,4\} \times \mathbb{N}$ door $g(n) = (0,n)$, dan is g injectief (als $(0,n) = (0,m)$ dan is $n = m$). Door de stelling van Schröder-Bernstein zien we dat $|\mathbb{N}| = |\{0,1,2,3,4\} \times \mathbb{N}|$ en $\{0,1,2,3,4\} \times \mathbb{N}$ is dus aftelbaar oneindig.

Uitwerking(c): Definieer $h : \{-1,1\} \times \mathbb{R} \to \mathbb{R}$ door $h(i,x) = ie^x$. We beweren dat h injectief is. Stel dat $h(i,x) = h(j,y)$ dan $ie^x = je^y$. Omdat $e^x, e^y > 0$, dan $i = j$ (anders krijgen we dat een positief getal gelijk is aan een negatief getal). Dan $e^x = e^y$ en dus $x = y$. Er volgt dat $(i,x) = (j,y)$ en h injectief is. Dus $|\{-1,1\} \times \mathbb{R}| \leq |\mathbb{R}|$.

Uitwerking(d): Door Schröder-Bernstein is het voldoende om te bewijzen dat $|\mathbb{R}| \leq |\{-1,1\} \times \mathbb{R}|$. Definieer $g : \mathbb{R} \to \{-1,1\} \times \mathbb{R}$ door $g(x) = (1,x)$ dan g is duidelijk injectief en dus $|\mathbb{R}| \leq |\{-1,1\} \times \mathbb{R}|$. Uit onderdeel (b) en de stelling van Schröder-Bernstein, volgt er dat $|\{-1,1\} \times \mathbb{R}| = |\mathbb{R}|$.

Z.O.Z.

Opgave 6 (nieuw vel papier)

Voor een natuurlijk getal $n \geq 2$ en een geheel getal a schrijven we de congruentieklasse van a modulo n als $[a]_n$. Dit is een element van $\mathbb{Z}_n$.

(a). (*4 punten*) Laat m en n natuurlijke getallen ≥ 2 zijn. Bewijs: als $m|n$, dan bestaat er een welgedefinieerde functie $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ gegeven door $f([a]_n) = [a]_m$.

(b). (*3 punten*) Bewijs ook de omkering: als er een welgedefinieerde functie $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ bestaat die gegeven wordt door $f([a]_n) = [a]_m$, dan geldt $m|n$.

(c). (*3 punten*) Neem nu aan dat $m|n$ en laat $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ de functie zijn gegeven door $f([a]_n) = [a]_m$. Bewijs dat voor alle $a, b \in \mathbb{Z}$ geldt dat

$$f([a]_n + [b]_n) = f([a]_n) + f([b]_n) \qquad \text{en} \qquad f([a]_n \cdot [b]_n) = f([a]_n) \cdot f([b]_n).$$

Merk op: links van het gelijkteken wordt de optelling/vermenigvuldiging in $\mathbb{Z}_n$ gebruikt, rechts die in $\mathbb{Z}_m$.

Uitwerking.

(a) Neem aan dat $m|n$, d.w.z., m deelt n, d.w.z., $\exists k \in \mathbb{Z}$ zodat $n = km$. We moeten bewijzen dat voor $a, b \in \mathbb{Z}$ geldt: indien $[a]_n = [b]_n$ als elementen van $\mathbb{Z}_n$, dan $[a]_m = [b]_m$ als elementen van $\mathbb{Z}_m$. Welnu, $[a]_n = [b]_n$ betekent dat a en b congruent zijn modulo n, d.w.z. dat n een deler is van $a - b$, dus er bestaat een $j \in \mathbb{Z}$ met $a - b = jn$. Aangezien $n = km$, volgt dat $a - b = jn = j(km) = (jk)m$. Volgens de axioma's is $jk \in \mathbb{Z}$, dus m deelt $a - b$, dus a en b zijn congruent modulo m, dus $[a]_m = [b]_m$. Hiermee hebben we bewezen: als $m|n$, dan bestaat er een welgedefinieerde functie $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ gegeven door $f([a]_n) = [a]_m$.

(b) Voor de omkering nemen we aan dat voor $a, b \in \mathbb{Z}$ geldt: indien $[a]_n = [b]_n$ als elementen van $\mathbb{Z}_n$, dan $[a]_m = [b]_m$ als elementen van $\mathbb{Z}_m$. We moeten bewijzen dat hieruit volgt dat m een deler is van n. Welnu, neem $a = n$ en $b = 0$. Dan $n = a - b$ dus $n|(a - b)$ dus $[a]_n = [b]_n$. Er volgt dus dat $[a]_m = [b]_m$, dus $m|(a - b)$ dus $m|n$. Q.E.D.

(c) We weten uit het boek dat de optelling in $\mathbb{Z}_p$ gedefinieerd is d.m.v. $[a]_p + [b]_p = [a+b]_p$ en dat de vermenigvuldiging in $\mathbb{Z}_p$ gedefinieerd is d.m.v. $[a]_p \cdot [b]_p = [ab]_p$. (In het bijzonder hebben we gezien dat de optelling en vermenigvuldiging welgedefinieerd zijn!)

Er geldt dan voor alle $a, b \in \mathbb{Z}$:

$$f([a]_n + [b]_n) = f([a + b]_n) = [a + b]_m = [a]_m + [b]_m = f([a]_n) + f([b]_n)$$

en

$$f([a]_n \cdot [b]_n) = f([ab]_n) = [ab]_m = [a]_m \cdot [b]_m = f([a]_n) \cdot f([b]_n).$$

EINDE TENTAMEN - ENGELSE VERTALING HIERONDER

Exercise 1 (new sheet of paper)

(a). (*8 points*) Let P and Q be statements. Show, by using a truth table, that

$$((P \Rightarrow Q) \wedge \sim Q) \Rightarrow \sim P$$

is a tautology.

(b). (*2 points*) Let $f \colon X \to Y$ be a function. State the definitions of injective (one-to-one) and surjective (onto) using quantifiers and logical connectives.

Exercise 2 (new sheet of paper)

(a). (*4 points*) Let X and Y be sets. Prove that $X \cap Y = X \cup Y$ if and only if $X = Y$.

A relation R is defined on $\mathbb{R}$ by: xRy if and only if $\lceil x \rceil = \lceil y \rceil$.

(b). (*4 points*) Prove that R is an equivalence relation.

(c). (*2 points*) Determine the partition of $\mathbb{R}$ defined by R (in terms of intervals in $\mathbb{R}$). Prove your statement.

Exercise 3 (new sheet of paper)

In this exercise we will compute the value of

$$\sum_{k=1}^{\infty} \frac{k}{2^k}.$$

(a). (*4 points*) For all $n \in \mathbb{N}$ we define $t_n = \frac{n}{2^n} + \sum_{k=1}^{n} \frac{k}{2^k}$. Use mathematical induction to prove that for all $n \in \mathbb{N}$ we have $t_n = 2 - \frac{1}{2^{n-1}}$.

(b). (*4 points*) Determine $\lim_{n\to\infty} t_n$ and prove that this limit is correct with an ϵ-N-proof.

(c). (*2 points*) Determine $\sum_{k=1}^{\infty} \frac{k}{2^k}$. You may use the fact that $\lim_{n\to\infty} \frac{n}{2^n} = 0$ and that

$$\lim_{n\to\infty} t_n = \lim_{n\to\infty} \frac{n}{2^n} + \lim_{n\to\infty} \sum_{k=1}^{n} \frac{k}{2^k}.$$

Exercise 4 (new sheet of paper)

Let X and Y be nonempty sets. Show that the following hold:

(a). (*4 points*) Let $g : Y \to X$ be a function. If there is a function $f : X \to Y$ such that for all $x \in X$ we have $(g \circ f)(x) = x$, then g is surjective (onto).

(b). (*4 points*) Let $f : X \to Y$ be a function. If there is a function $g : Y \to X$ such that for all $x \in X$ we have $(g \circ f)(x) = x$, then f is injective (one-to-one).

(c). (*2 points*) Let $f : X \to Y$ be a function. If f is injective (one-to-one), there is a function $g : Y \to X$ such that $(g \circ f)(x) = x$ for all $x \in X$.

Exercise 5 (new sheet of paper)

(a). (*3 points*) Consider the function $f : \{0, 1, 2, 3, 4\} \times \mathbb{N} \to \mathbb{N}$ given by $f((i, n)) = i + 5n$. What is $f((0, 1))$? And $f((1, 2))$? Show that f is injective (one-to-one).

(b). (*2 points*) Prove that $\{0, 1, 2, 3, 4\} \times \mathbb{N}$ is countably infinite (denumerable).

(c). (*3 points*) Prove that $|\{-1, 1\} \times \mathbb{R}| \leq |\mathbb{R}|$. You may use the fact that the function $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^x$ is injective (one-to-one).

(d). (*2 points*) Prove that $|\{-1, 1\} \times \mathbb{R}| = |\mathbb{R}|$.

Exercise 6 (new sheet of paper)

For every natural number $n \geq 2$ and every integer a we denote the congruence class of a modulo n by $[a]_n$. This is an element of $\mathbb{Z}_n$.

(a). (*4 points*) Let m and n be natural numbers ≥ 2. Prove: if $m|n$, then there exists a well-defined function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ defined by $f([a]_n) = [a]_m$.

(b). (*3 points*) Prove the converse: if there exists a well-defined function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ defined by $f([a]_n) = [a]_m$, then $m|n$.

(c). (*3 points*) We assume that $m|n$ and let $f : \mathbb{Z}_n \to \mathbb{Z}_m$ be the function defined by $f([a]_n) = [a]_m$. Prove that for all $a, b \in \mathbb{Z}$:

$$f([a]_n + [b]_n) = f([a]_n) + f([b]_n) \qquad \text{and} \qquad f([a]_n \cdot [b]_n) = f([a]_n) \cdot f([b]_n).$$

Remark: on the left hand side of the equality we use the addition/multiplication of $\mathbb{Z}_n$, on the right hand side the addition/multiplication of $\mathbb{Z}_m$.

Solution.

(a) Assume that $m|n$, i.e., m divides n, i.e., $\exists k \in \mathbb{Z}$ such that $n = km$. We need to prove that for $a, b \in \mathbb{Z}$ the following holds: if $[a]_n = [b]_n$ as elements of $\mathbb{Z}_n$, then $[a]_m = [b]_m$ as elements of $\mathbb{Z}_m$. Now $[a]_n = [b]_n$ means that a and b are congruent modulo n, i.e., that n divides $a - b$, so there exists $j \in \mathbb{Z}$ with $a - b = jn$. Since $n = km$, it follows that $a - b = jn = j(km) = (jk)m$. According to the axioms, we have that $jk \in \mathbb{Z}$, so m divides $a - b$, so a and b are congruent modulo m, so $[a]_m = [b]_m$. We have proved: if $m|n$, then there exists a well-defined function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ given by $f([a]_n) = [a]_m$.

(b) For the converse, we assume that for $a, b \in \mathbb{Z}$ we have: if $[a]_n = [b]_n$ as elements of $\mathbb{Z}_n$, then $[a]_m = [b]_m$ as elements of $\mathbb{Z}_m$. We need to prove that it follows that m divides n. Take $a = n$ and $b = 0$. Then $n = a - b$ so $n|(a - b)$ so $[a]_n = [b]_n$. It follows that $[a]_m = [b]_m$, so $m|(a - b)$ so $m|n$. Q.E.D.

(c) We know from the book that addition in $\mathbb{Z}_p$ is defined via $[a]_p + [b]_p = [a + b]_p$ and that multiplication in $\mathbb{Z}_p$ is defined via $[a]_p \cdot [b]_p = [ab]_p$. (In particular, we have seen that addition and multiplication are well-defined!)

Then, for all $a,\, b \in \mathbb{Z}$:

$$f([a]_n + [b]_n) = f([a+b]_n) = [a+b]_m = [a]_m + [b]_m = f([a]_n) + f([b]_n)$$

and

$$f([a]_n \cdot [b]_n) = f([ab]_n) = [ab]_m = [a]_m \cdot [b]_m = f([a]_n) \cdot f([b]_n).$$