Workouts

for Part IA CST 2014/15

Discrete Mathematics

<cl.cam.ac.uk/teaching/1415/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

Workout 1
from page 47

Prove or disprove the following statements.

1. The product of two even natural numbers is even.
2. The product of an even and an odd natural number is odd.
3. If $x > 3$ and $y < 2$ then $x^2 - 2 \cdot y > 5$.

Workout 2
from page 54

Prove or disprove the following statements.

1. Suppose n is a natural number larger than 2, and n is not a prime number. Then $2 \cdot n + 13$ is not a prime number.

2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Workout 3
from page 65

1. Characterise those integers d and n such that:

   (a) $0 \mid n$,

   (b) $d \mid 0$.

2. Write an ML function

   ```
   divides: int * int -> bool
   ```

   such that, for all integers m and n, $\texttt{divides}(m, n) = \texttt{true}$ iff $m \mid n$ holds.

You may use `div`, but note that you cannot just define `divides` as

```
fn (m,n) => ( n div m ) = 0 .
```

3. Let n be a natural number. Show that $n \mid n$.

Workout 4
from page 68

1. Let i, j be integers and let m be a positive integer. Show that:

   (a) $i \equiv i \pmod{m}$

   (b) $i \equiv j \pmod{m} \implies j \equiv i \pmod{m}$

   (c) $i \equiv j \pmod{m} \implies i^2 \equiv j^2 \pmod{m}$

2. Find integers i, j, natural numbers k, l, and a positive integer m for which both $i \equiv j \pmod{m}$ and $k \equiv l \pmod{m}$ hold while $i^k \equiv j^l \pmod{m}$ does not.

3. Find an integer i, natural numbers k, l, and a positive integer m for which $k \equiv l \pmod{m}$ holds while $i^k \equiv i^l \pmod{m}$ does not.

4. Formalise and prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. Find analogous criteria for multiples of 9 and for multiples of 11.

Workout 5
from page 70

1. Prove or disprove that: For an integer n, n^2 is even if and only if n is even.

2. Show that for all integers d and n the following statements are equivalent:

   (a) $d \mid n$.

   (b) $-d \mid n$.

   (c) $d \mid -n$.

   (d) $-d \mid -n$.

3. Let k, m, n be integers with k positive. Show that:

$$(k \cdot m) \mid (k \cdot n) \iff m \mid n \quad .$$

Workout 6
from page 79

1. Prove or disprove the following statements.
   (a) For real numbers a and b, if $0 < a < b$ then $a^2 < b^2$.
   (b) For real numbers a, b, and c with $a > b$, if $a \cdot c \leq b \cdot c$ then $c \geq 0$.
2. Prove or disprove that: For all natural numbers n, $2 \mid 2^n$.

3. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the derived statement

$$P^{\#}(m) \;=\; \forall \text{ natural } k.\; 0 \leq k \leq m \implies P(k)$$

again for m ranging over the natural numbers.

Prove the following equivalences:

- $P^{\#}(0) \iff P(0)$
- $\big(P^{\#}(n) \implies P^{\#}(n+1) \big) \iff \big(P^{\#}(n) \implies P(n+1) \big)$
- $$\forall \text{ natural number } m.\, P^{\#}(m)$$
  $$\iff$$
  $$\forall \text{ natural number } m.\, P(m)$$

Workout 7
from page 89

1. Taking inspiration from the proof of Theorem 20 (on page 87), or otherwise, prove that for all integers n,

$$30 \mid n \iff (2 \mid n \wedge 3 \mid n \wedge 5 \mid n) \quad .$$

Can you spot a pattern here? Can you formalise it, test it, and prove it?

2. Find a counterexample to the statement: For all positive integers k, m, n, if $m \mid k \wedge n \mid k$ then $(m \cdot n) \mid k$.

3. Show that for all integers l, m, n,

$$l \mid m \wedge m \mid n \implies l \mid n \;.$$

4. Prove that for all integers d, k, l, m, n,

   (a) $d \mid m \wedge d \mid n \implies d \mid (m+n)$,

   (b) $d \mid m \implies d \mid k \cdot m$,

   (c) $d \mid m \wedge d \mid n \implies d \mid (k \cdot m + l \cdot n)$.

5. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,

   (a) $i \equiv j \pmod{m} \wedge j \equiv k \pmod{m} \implies i \equiv k \pmod{m}$

   (b) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \implies i + k \equiv j + l \pmod{m}$

   (c) $i \equiv j \pmod{m} \wedge k \equiv l \pmod{m} \implies i \cdot k \equiv j \cdot l \pmod{m}$

   (d) $i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}$

Workout 8
from page 104

Prove or disprove the following statements.

1. For every real number x, if $x > 0$ then there is a real number y such that $y(y+1) = x$.

2. For all real numbers x and y there is a real number z such that $x + z = y - z$.

3. For all integers x and y there is an integer z such that $x + z = y - z$.

4. For every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y+1) = x$.

5. The addition of two rational numbers is a rational number.

6. Prove that for all natural numbers p, p_1, p_2,

   (a) $\min(p, p_1 + p_2) = \min\left(p, \min(p, p_1) + \min(p, p_2)\right)$, and

   (b) $\min(p, p_1 + p_2) = \min(p, p_1) + \min\left(p - \min(p, p_1), p_2\right)$.

7. Let $P(x)$ be a predicate on a variable x and let Q be a statement not mentioning x.[a]

   Show that the equivalence

$$\left((\exists x.\, P(x)) \implies Q\right) \iff \left(\forall x.\, (P(x) \implies Q)\right)$$

   holds.

[a] For instance, $P(x)$ could be the predicate "programmer x found a software bug" and Q could be the statement "all the code has to be rewritten".

Workout 9
from page 106

1. Prove that for every real number x there is a unique real number y such that $x^2 \cdot y = x - y$.

2. Prove that there is a unique real number x such that for every real number y, $x \cdot y + x - 4 = 4y$.

3. Prove that for every real number x, if $x \neq 0$ and $x \neq 1$ then there is a unique real number y such that $y/x = y - x$.

4. Prove that for every real number x, if $x \neq 0$ then there is a unique real number y such that for every real number z, $z \cdot y = z/x$.

Workout 10
from page 113

1. Prove or disprove that: For all integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

2. If every pair of people in a group has met, then we will call the group a *club*. If every pair of people in a group has not met, then we will call it a group of *strangers*.

   Prove that every collection of 6 people includes a club of 3 people or a group of 3 strangers.

3. Show that for all integers m and n,

$$m \mid n \wedge n \mid m \implies m = n \vee m = -n \ .$$

4. Prove or disprove that: For all positive integers k, m, n,

   if $k \mid (m \cdot n)$ then $k \mid m$ or $k \mid n$.

5. Prove that for all integers n, there exist natural numbers i and j such that $n = i^2 - j^2$ iff either $n \equiv 0 \pmod 4$, or $n \equiv 1 \pmod 4$, or $n \equiv 3 \pmod 4$. [Hint: Recall Proposition 22 (on page 96).]

6. Prove that $n^3 \equiv n \pmod 6$ for all integers n.

Workout 11
from page 134

1. Search for “Fermat’s Little Theorem” in YouTube and watch a video or two about it.

2. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 \pmod{p-1}$ then $i^n \equiv i \pmod{p}$ for all i not multiple of p.

3. (a) Taking inspiration from the proof of Theorem 20 on page 87, or otherwise, prove that for all integers n,

$$42 \mid n \iff (2 \mid n \wedge 3 \mid n \wedge 7 \mid n) \quad .$$

Can you spot a pattern here? Can you formalise it, test it, and prove it?

(b) Prove that $n^7 \equiv n \pmod{42}$ for all integers n.

4. Show that 66013 is not prime.

Workout 12
from page 137

Justify the boolean equivalences:

$$\neg(P \Longrightarrow Q) \iff P \wedge \neg Q$$

$$\neg(P \iff Q) \iff P \iff \neg Q$$

$$\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$$

$$\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$$

$$\neg(\neg P) \iff P$$

$$\neg P \iff (P \Rightarrow \mathbf{false})$$

$$(P \Longrightarrow Q) \iff (\neg Q \Longrightarrow \neg P)$$

$$(\mathbf{false} \Longrightarrow P) \iff \mathbf{true}$$

$$\big(P_1 \implies (P_2 \implies Q)\big) \iff \big((P_1 \land P_2) \implies Q\big)$$
$$(P \iff Q) \iff \big((P \implies Q) \land (Q \implies P)\big)$$

by means of truth tables, where the truth tables for the boolean statements are:

P	Q	$P \implies Q$	$P \iff Q$	$P \land Q$	$P \lor Q$	$\neg P$
true	**true**	**true**	**true**	**true**	**true**	**false**
false	**true**	**true**	**false**	**false**	**true**	**true**
true	**false**	**false**	**false**	**false**	**true**	
false	**false**	**true**	**true**	**false**	**false**	

Workout 13
from page 150

Give three justifications for the following scratch work:

Before using the strategy

Assumptions	Goal
	$P \Longrightarrow Q$
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$P \quad , \quad \neg Q$	

Workout 14
from page 178

1. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.
2. Write the division algorithm in imperative code.
3. What is $\mathrm{rem}\left(24^{78}, 79\right)$?
4. Prove that for all natural numbers k, l, and positive integer m,
   (a) $\mathrm{rem}(k + l, m) = \mathrm{rem}\big(k + \mathrm{rem}(l, m), m\big)$, and
   (b) $\mathrm{rem}(k \cdot l, m) = \mathrm{rem}\big(k \cdot \mathrm{rem}(l, m), m\big)$.

5. Prove the following Remainder-Linearity Property of the Division Algorithm: for all positive integers k, m, n,

$$\mathtt{divalg}(k \cdot m, k \cdot n) = \big(\mathrm{quo}(m, n), k \cdot \mathrm{rem}(m, n)\big) \quad .$$

6. Prove the General Division Theorem for integers:

   For every integer m and non-zero integer n, there exists a unique pair of integers q and r such that $0 \leq r < |n|$, and $m = q \cdot n + r$.

7. Prove that for all positive integers m and n,

   (a) $n < m \implies \mathrm{quo}(n, m) = 0 \wedge \mathrm{rem}(n, m) = n$, and

   (b) $n \leq m \implies \mathrm{rem}(m, n) < m/2$.

Workout 15
from page 185

1. Calculate that $2^{153} \equiv 53 \pmod{153}$.

   Btw, at first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though?

2. Let m be a positive integer.

   (a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is, that for all i, j, k in $\mathbb{Z}_m$,

   $(i +_m j) +_m k = i +_m (j +_m k)$, and

   $(i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$.

   [Hint: Use Workout 14.4 on page 493.]

   (b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.

3. Calculate the addition and multiplication tables, and the additive and multiplicative inverses tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$, and $\mathbb{Z}_7$. Can you spot any patterns?

Workout 16
from page 222

1. Write Euclid's Algorithm in imperative code.
2. Calculate the set $\mathrm{CD}(666, 330)$ of common divisors of 666 and 330.
3. Find the gcd of 21212121 and 12121212.

4. Show that for all integers k, the conjunction of the two statements

   - $k \mid m \ \wedge \ k \mid n$, and
   - for all positive integers d, $d \mid m \ \wedge \ d \mid n \implies d \mid k$

   is equivalent to the single statement

   for all positive integers d, $d \mid m \ \wedge \ d \mid n \iff d \mid k$.

5. Prove that for all positive integers m and n,

$$\gcd(m, n) = m \iff m \mid n \ .$$

6. Prove that, for all positive integers m and n, and integers k and l,

$$\gcd(m, n) \mid (k \cdot m + l \cdot n) \ .$$

7. Prove that, for all positive integers m and n, there exist integers k and l such that $k \cdot m + l \cdot n = 1$ iff $\gcd(m, n) = 1$.

8. For all positive integers m and n, define

$$m' = \frac{m}{\gcd(m,n)} \quad \text{and } n' = \frac{n}{\gcd(m,n)} \quad .$$

Prove that

(a) m' and n' are positive integers, and that

(b) $\gcd(m', n') = 1$.

Conclude that the representation in lowest terms of the fraction m/n is m'/n'.

9. Use the Key Lemma 56 (on page 196) to show the correctness of the following algorithm

```
fun gcd0( m , n )
  = if m = n then m
    else
      let
        val p = min(m,n) ; val q = max(m,n)
      in
        gcd0( p , q - p )
      end
```

for computing the gcd of two positive integers. Give an analysis of the time complexity.

10. Prove that for all positive integers a and b,

$$\gcd\left(13 \cdot a + 8 \cdot b\,,\, 5 \cdot a + 3 \cdot b\right) \;=\; \gcd(a, b) \quad .$$

Workout 17
from page 230

1. Revisit Theorem 20 (on page 87), Workout 7.1 (on page 481), and Workout 11.3a (on page 489) using Euclid's Theorem (Corollary 64 on page 64) to give new proofs for them. Can you now state and prove a general result from which these follow?

2. (a) Prove that if an integer n is not divisible by 3, then $n^2 \equiv 1 \pmod{3}$.

   (b) Show that if an integer n is odd, then $n^2 \equiv 1 \pmod{8}$

   (c) Conclude that if p is a prime greater than 3, then $p^2 - 1$ is divisible by 24.

3. Prove that $n^{13} \equiv n \pmod{10}$ for all integers n.

4. Write an ML function to calculate the multiplicative inverse of a number in $\mathbb{Z}_p$ to a given prime modular base p.

Workout 18
from page 244

1. Write the Extended Euclid's Algorithm in imperative code.
2. Find integers x and y such that $x \cdot 30 + y \cdot 22 = \gcd(30, 22)$. Now find integers x' and y' with $0 \leq y' < 30$ such that $x' \cdot 30 + y' \cdot 22 = \gcd(30, 22)$.
3. Prove Theorem 69 (on page 235).
4. Let m and n be positive integers with $\gcd(m, n) = 1$. Prove that for every natural number k,

$$m \mid k \wedge n \mid k \implies (m \cdot n) \mid k \quad .$$

5. Prove that for all positive integers l, m, and n, if $\gcd(l, m \cdot n) = 1$ then $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.

6. Prove that for all integers n and primes p, if $n^2 \equiv 1 \pmod{p}$ then either $n \equiv 1 \pmod{p}$ or $n \equiv -1 \pmod{p}$.

7. Solve the following congruences:

   (a) $77 \cdot x \equiv 11 \pmod{40}$

   (b) $12 \cdot y \equiv 30 \pmod{54}$

   (c) $\begin{cases} z \equiv 13 \pmod{21} \\ 3 \cdot z \equiv 2 \pmod{17} \end{cases}$

8. What is the multiplicative inverse of: 2 in $\mathbb{Z}_7$, 7 in $\mathbb{Z}_{40}$, and 13 in $\mathbb{Z}_{23}$?

9. Write an ML function to calculate the multiplicative inverse, whenever it exists, of a number in $\mathbb{Z}_m$ to a given modular base m. Test your answers to the previous item.

10. Prove that 22^{12001} has a multiplicative inverse in $\mathbb{Z}_{175}$.

11. (a) Show that the $\gcd$ of two linear combinations of positive integers m and n is itself a linear combination of m and n.

    (b) Argue that the output $((s,t),r)$ of calling `egcditer` with input

$$\Big(\big((s_1,t_1) , s_1 \cdot m + t_1 \cdot n \big) , \big((s_2,t_2) , s_2 \cdot m + t_2 \cdot n \big) \Big)$$

    is such that

$$\gcd\big(s_1 \cdot m + t_1 \cdot n , s_2 \cdot m + t_2 \cdot n \big) = r = s \cdot m + t \cdot n \quad .$$

Workout 19
from page 249

1. Search for “Diffie-Hellman Key Exchange” in YouTube and watch a video or two about it.

Workout 20
from page 268

1. State the Principle of Induction for the ML

```
datatype
  N = zero | succ of N
```

2. Establish the following:

   (a) For all positive integers m and n,

   $$(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1 \quad .$$

   (b) Suppose k is a positive integer that is not prime. Then $2^k - 1$ is not prime.

3. Prove that

$$\forall n \in \mathbb{N}.\ \forall x \in \mathbb{R}.\ x \geq -1 \implies (1+x)^n \geq 1 + n \cdot x \quad .$$

4. Recall that the Fibonacci numbers F_n for n ranging over the natural numbers are defined by $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

   (a) Prove that for all natural numbers n,

   $$F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^n \quad .$$

   (b) Prove that for all natural numbers k and n,

   $$F_{n+k+1} = F_{k+1} \cdot F_{n+1} + F_k \cdot F_n \quad .$$

   (c) Deduce that $F_n \mid F_{\ell \cdot n}$ for all positive integers ℓ.

   (d) Prove that $\mathtt{gcd}(F_{n+1}, F_n)$ terminates with output 1 in $n+1$ steps for all natural numbers n.

(e) Deduce also that, for natural numbers $n \leq m$,

$$\gcd(F_m, F_n) = \gcd(F_{m-n}, F_n)$$

and hence that, for all positive integers m and n,

$$\gcd(F_m, F_n) = F_{\gcd(m,n)} \quad .$$

(f) Show that for all positive integers m and n, $F_m \cdot F_n \mid F_{m \cdot n}$ if $\gcd(m, n) = 1$.

(g) Conjecture and prove a theorem concerning the sum $\sum_{i=0}^{n} F_{2 \cdot i}$ for n any natural number.

(h) Conjecture and prove a theorem concerning the sum $\sum_{i=0}^{n} F_{2 \cdot i+1}$ for n any natural number.

Workout 21
from page 292

1. Equation $(\star)$ on page 291 gives a *Transfer Principle* of additive properties of $\min$ as multiplicative properties of $\gcd$. To see this, prove that for all positive integers m, m_1, m_2,

   (a) $\gcd(m, m_1 \cdot m_2) = \gcd\big(\, m\,,\ \gcd(m, m_1) \cdot \gcd(m, m_2)\,\big)$, and

   (b) $\gcd(m, m_1 \cdot m_2) = \gcd(m, m_1) \cdot \gcd\Big(\frac{m}{\gcd(m,m_1)}, m_2\Big)$.

   [Hint: Use Workout 8.6 on page 484.]

2. Give two proofs of the following proposition

   For all positive integers m, n, p, q such that $\gcd(m, n) = \gcd(p, q) = 1$, if $m \cdot q = p \cdot n$ then $m = p$ and $n = q$.

   respectively using Theorem 63 and Equation $(\star)$ on page 291.

Workout 22
from page 305

1. Write an ML function

```
subset: ''a list * ''a list -> bool
```

such that for every list `xs` representing a finite set X and every list `ys` representing a finite set Y, `subset(xs,ys)=true` iff $X \subseteq Y$.

2. Prove the following statements:

   (a) Reflexivity.

   $\forall$ sets A. $A \subseteq A$.

   (b) Transitivity.

   $\forall$ sets A, B, C. $(A \subseteq B \wedge B \subseteq C) \implies A \subseteq C$.

   (c) Antisymmetry.

   $\forall$ sets A, B. $(A \subseteq B \wedge B \subseteq A) \iff A = B$.

Workout 23
from page 310

Prove the following statements:

1. $\forall \text{ set } S.\, \emptyset \subseteq S$.
2. $\forall \text{ set } S.\, (\forall x.\, x \notin S) \iff S = \emptyset$.

Workout 24
from page 326

1. Referring to the definitions on pages 193 and 194, show that $\mathrm{CD}(m, n) = \mathrm{D}(m) \cap \mathrm{D}(n)$.

2. Find the union and intersection of:

   (a) $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$;

   (b) $\{x \in \mathbb{R} \mid x > 7\}$ and $\{x \in \mathbb{N} \mid x > 5\}$.

3. Write ML functions

```
union:  'a list * 'a list -> 'a list
intersection:  ''a list * ''a list -> 'a list
```

such that for every list `xs` representing a finite set X and every list `ys` representing a finite set Y, the lists `union(xs,ys)` and `intersection(xs,ys)` respectively represent the finite sets $X \cup Y$ and $X \cap Y$.

Use these functions to check your answer to the first part of the previous item.

4. Give an explicit description of $\mathcal{P}\big(\mathcal{P}(\mathcal{P}(\emptyset))\big)$, and draw its Hasse diagram.

5. Write an ML function

```
powerset:  'a list -> 'a list list
```

such that for every list `as` representing a finite set A, the list of lists `powerset(as)` represents the finite set $\mathcal{P}(A)$.

6. Establish the laws of the powerset Boolean algebra.

7. Either prove or disprove that, for all sets A and B,

   (a) $A \subseteq B \implies \mathcal{P}(A) \subseteq \mathcal{P}(B)$,

   (b) $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$,

   (c) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

   (d) $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$,

   (e) $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

8. Let $\mathcal{U}$ be a set. For all $A, B \in \mathcal{P}(\mathcal{U})$ prove that the following statements are equivalent.

   (a) $A \cup B = B$.

   (b) $A \subseteq B$.

   (c) $A \cap B = A$.

   (d) $B^c \subseteq A^c$.

9. Let $\mathcal{U}$ be a set. For all $A, B \in \mathcal{P}(\mathcal{U})$ prove that

   (a) $A^c = B \iff (A \cup B = \mathcal{U} \wedge A \cap B = \emptyset)$,

   (b) $(A^c)^c = A$, and

   (c) the De Morgan's laws:

$$(A \cup B)^c = A^c \cap B^c \text{ and } (A \cap B)^c = A^c \cup B^c \; .$$

10. Draw Venn diagrams for the following constructions on sets.

(a) Difference:

$$A \setminus B = \{x \in A \mid x \notin B\}$$

(b) Symmetric difference:

$$A \vartriangle B = (A \setminus B) \cup (B \setminus A)$$

11. Prove that for all sets A, B, C,

(a) $A \setminus B = A \setminus (A \cap B)$, and

(b) $A \setminus B \subseteq C \implies A \setminus C \subseteq B$.

If you like this kind of stuff, push on.

12. Let $\mathcal{U}$ be a set. Prove that, for all $A, B \in \mathcal{P}(\mathcal{U})$,

(a) $A \subseteq B \implies \big(A \setminus B = \emptyset \;\wedge\; A \triangle B = B \setminus A\big)$.

(b) $A \cap B = \emptyset \implies A \triangle B = A \cup B$,

(c) $(A \triangle B) \cap (A \cap B) = \emptyset \;\wedge\; (A \triangle B) \cup (A \cap B) = A \cup B$,

and establish as corollaries that

(d) $A^c = \mathcal{U} \triangle A$.

(e) $A \cup B = (A \triangle B) \triangle (A \cap B)$,

thereby expressing complements and unions in terms of symmetric difference and intersections.

13. The purpose of this exercise is to show that, for a set $\mathcal{U}$, the structure $\big(\mathcal{P}(\mathcal{U}), \emptyset, \triangle, \mathcal{U}, \cap\big)$ is a commutative ring.

    (a) Prove that $(\mathcal{P}(\mathcal{U}), \emptyset, \triangle)$ is a commutative group; that is, a commutative monoid (refer to page 161) in which every element has an inverse (refer to page 166).

    (b) Prove that $\mathcal{P}(\mathcal{U})$ with additive structure $(\emptyset, \triangle)$ and multiplicative structure $(\mathcal{U}, \cap)$ is a commutative semiring.

Workout 25
from page 335

1. Find the product of $\{1, 2, 3, 4, 5\}$ and $\{-1, 1, 3, 5, 7\}$.

2. Write an ML function

```
product: 'a list * 'b list -> ( 'a * 'b ) list
```

   such that for every list `as` representing a finite set A and every list `bs` representing a finite set B, the list of pairs `product(as,bs)` represents the product set $A \times B$.

   Use this function to check your answer to the previous item.

3. For sets A, B, C, D, either prove or disprove the following statements.

   (a) $(A \subseteq B \ \wedge \ C \subseteq D) \implies A \times C \subseteq B \times D$.

   (b) $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$.

   (c) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

   (d) $A \times (B \cup D) \subseteq (A \times B) \cup (A \times D)$.

   (e) $(A \times B) \cup (A \times D) \subseteq A \times (B \cup D)$.

   What happens with the above when $A \cap C = \emptyset$ and/or $B \cap D = \emptyset$?

Workout 26
from page 347

1. Let $I = \{2, 3, 4, 5\}$, and for each $i \in I$ let $A_i = \{i, i + 1, i - 1, 2 \cdot i\}$.
   (a) List the elements of all the sets A_i for $i \in I$.
   (b) Let $\{ A_i \mid i \in I \}$ stand for $\{A_2, A_3, A_4, A_5\}$.
   Find $\bigcup\{A_i \mid i \in I\}$ and $\bigcap\{A_i \mid i \in I\}$.

2. Write ML functions

```
bigunion:  'a list list -> 'a list
bigintersection:  'a list list -> 'a list
```

such that for every list of lists `as` representing a finite set of finite sets A, the lists `bigunion(as)` and `bigintersection(as)` respectively represent the finite sets $\bigcup X$ and $\bigcap X$.

Use these functions to check your answer to the previous item.

3. For $\mathcal{F} \subseteq \mathcal{P}(A)$, let $\mathcal{U} = \{ X \subseteq A \mid \forall S \in \mathcal{F}.\ S \subseteq X \} \subseteq \mathcal{P}(A)$. Prove that $\bigcup \mathcal{F} = \bigcap \mathcal{U}$.

   Analogously, define $\mathcal{L} \subseteq \mathcal{P}(A)$ such that $\bigcap \mathcal{F} = \bigcup \mathcal{L}$. Also prove this statement.

NB For intuition when tackling the following exercises it might help considering the case of finite collections first.

4. Prove that, for all collections $\mathcal{F}$, it holds that

$$\forall \text{ set } U.\ \bigcup \mathcal{F} \subseteq U \iff (\forall X \in \mathcal{F}.\ X \subseteq U) \quad .$$

State and prove the analogous property for big intersections of non-empty collections.

5. Prove that for all collections $\mathcal{F}_1$ and $\mathcal{F}_2$,

$$\left(\bigcup \mathcal{F}_1\right) \cup \left(\bigcup \mathcal{F}_2\right) = \bigcup(\mathcal{F}_1 \cup \mathcal{F}_2) \quad .$$

State and prove the analogous property for intersections of non-empty collections.

Workout 27
from page 354

1. Find the disjoint union of $\{1,2,3,4,5\}$ and $\{-1,1,3,5,7\}$.

2. Let

```
datatype ('a,'b) sum = one of 'a | two of 'b  .
```

   Write an ML function

```
dunion:  'a list * 'b list -> ('a ,'b) sum list
```

   such that for every list `as` representing a finite set A and every list `bs` representing a finite set B, the list of tagged elements `dunion(as,bs)` represents the disjoint union $A \uplus B$.

   Use this function to check your answer to the previous item.

3. Prove or disprove the following statements for all sets A, B, C, D:

   (a) $(A \subseteq B \wedge C \subseteq D) \implies A \uplus C \subseteq B \uplus D$,

   (b) $(A \cup B) \uplus C \subseteq (A \uplus C) \cup (B \uplus C)$,

   (c) $(A \uplus C) \cup (B \uplus C) \subseteq (A \cup B) \uplus C$,

   (d) $(A \cap B) \uplus C \subseteq (A \uplus C) \cap (B \uplus C)$,

   (e) $(A \uplus C) \cap (B \uplus C) \subseteq (A \cap B) \uplus C$.

4. Give a proof of Workout 10.2 (on page 486) using the Generalised Pigeonhole Principle (on page 353).

Workout 28
from page 378

1. Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c, d\}$, and $C = \{x, y, z\}$. Let $R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\} : A \nrightarrow B$ and $S = \{(b, x), (b, x), (c, y), (d, z)\} : B \nrightarrow C$. What is their composition $S \circ R : A \nrightarrow C$?

2. Prove Theorem 101 (on page 362).

3. For a relation $R : A \longrightarrow\!\!\!\!\!\!\!+\;\; B$, let its *opposite*, or *dual*, $R^{\mathrm{op}} : B \longrightarrow\!\!\!\!\!\!\!+\;\; A$ be defined by

$$b \, R^{\mathrm{op}} \, a \iff a \, R \, b \quad .$$

For $R, S : A \longrightarrow\!\!\!\!\!\!\!+\;\; B$, prove that

(a) $R \subseteq S \implies R^{\mathrm{op}} \subseteq S^{\mathrm{op}}$.

(b) $(R \cap S)^{\mathrm{op}} = R^{\mathrm{op}} \cap S^{\mathrm{op}}$.

(c) $(R \cup S)^{\mathrm{op}} = R^{\mathrm{op}} \cup S^{\mathrm{op}}$.

4. Show that in a directed graph on a finite set with cardinality n there is a path between two nodes iff there is a path of length $n - 1$.

Workout 29
from page 383

1. For a relation R on a set A, prove that R is antisymmetric iff $R \cap R^{op} \subseteq \mathrm{id}_A$.

2. Let $\mathcal{F} \subseteq \mathcal{P}(A \times B)$ be a collection of relations from A to B. Prove that,

   (a) for all $R : X \mathrel{\longrightarrow\!\!\!\!\!\!\!+} A$,
   $$\left(\bigcup \mathcal{F}\right) \circ R \;=\; \bigcup \left\{ S \circ R \mid S \in \mathcal{F} \right\} \;: X \mathrel{\longrightarrow\!\!\!\!\!\!\!+} B \quad ,$$
   and that,

   (b) for all $R : B \mathrel{\longrightarrow\!\!\!\!\!\!\!+} Y$,
   $$R \circ \left(\bigcup \mathcal{F}\right) \;=\; \bigcup \left\{ R \circ S \mid S \in \mathcal{F} \right\} \;: A \mathrel{\longrightarrow\!\!\!\!\!\!\!+} Y \quad .$$

   What happens in the case of big intersections?

3. For a relation R on a set A, let

$$\mathcal{T}_R = \{ Q \subseteq A \times A \mid R \subseteq Q \wedge Q \text{ is transitive} \} .$$

For $R^{\circ +} = R \circ R^{\circ *}$, prove that (i) $R^{\circ +} \in \mathcal{T}_R$ and (ii) $R^{\circ +} \subseteq \bigcap \mathcal{T}_R$. Hence, $R^{\circ +} = \bigcap \mathcal{T}_R$.

Workout 30
from page 394

1. Let $A_2 = \{1, 2\}$ and $A_3 = \{a, b, c\}$. List the elements of the four sets $(A_i \rightrightarrows A_j)$ for $i, j \in \{2, 3\}$.

2. Prove that a relation $R : A \rightarrow\!\!\!\!\!+\,\, B$ is a partial function iff

$$R \circ R^{op} \subseteq id_B \quad .$$

   [Hint: Workout 8.7 on page 484 will be handy here.]

3. Prove Theorem 120 (on page 388).

4. Show that $(\mathrm{PFun}(A, \mathrm{B}), \subseteq)$ is a partial order.
5. Show that the intersection of a collection of partial functions in $\mathrm{PFun}(A, \mathrm{B})$ is a partial function in $\mathrm{PFun}(A, \mathrm{B})$.

6. Show that the union of two partial functions in $\mathrm{PFun}(A, B)$ is a relation that need not be a partial function. But that for $f, g \in \mathrm{PFun}(A, B)$ such that $f \subseteq h \supseteq g$ for some $h \in \mathrm{PFun}(A, B)$, the union $f \cup g$ is a partial function in $\mathrm{PFun}(A, B)$.

Workout 31
from page 400

1. Let $A_2 = \{1, 2\}$ and $A_3 = \{a, b, c\}$. List the elements of the four sets $(A_i \Rightarrow A_j)$ for $i, j \in \{2, 3\}$.

2. A relation $R : A \longrightarrow\!\!\!\!\!\!\!+\;\; B$ is said to be total whenever

$$\forall\, a \in A.\, \exists\, b \in B.\, a \mathrel{R} b \quad .$$

   Prove that this is equivalent to $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$.

   Conclude that a relation $R : A \longrightarrow\!\!\!\!\!\!\!+\;\; B$ is a function iff $R \circ R^{\mathrm{op}} \subseteq \mathrm{id}_B$ and $\mathrm{id}_A \subseteq R^{\mathrm{op}} \circ R$.

3. Prove Theorem 125 (on page 399).

4. Find endofunctions $f, g : A \to A$ such that $f \circ g \neq g \circ f$. Prove your claim.

5. The aim of this exercise is to show the *Knaster-Tarski Fixed-Point Theorem*:

Every monotone endofunction on a powerset has a least and a greatest fixed-point.

   We start with the definitions of monotonicity and fixed-points:

   - A function $f : \mathcal{P}(A) \to \mathcal{P}(A)$ is said to be ***monotone*** whenever

     $$\forall X, Y \in \mathcal{P}(A).\, X \subseteq Y \implies f(X) \subseteq f(Y) \quad .$$

- A *fixed-point* of $f : \mathcal{P}(A) \to \mathcal{P}(A)$ is an element $X \in \mathcal{P}(A)$ such that

$$f(X) = X \quad .$$

Henceforth, let $f : \mathcal{P}(A) \to \mathcal{P}(A)$ be a monotone function.

(a) The least pre-fixed point.

A *pre-fixed point* is an element $X \in \mathcal{P}(A)$ such that

$$f(X) \subseteq X \quad .$$

Consider the set

$$\mathcal{F} = \{ X \in \mathcal{P}(A) \mid f(X) \subseteq X \} \subseteq \mathcal{P}(A)$$

of pre-fixed points.

You will now show that

$$f\Big(\bigcap \mathcal{F}\Big) = \bigcap \mathcal{F} \quad .$$

i. Show that

$$\forall X \in \mathcal{F}.\ X \in \mathcal{F} \implies f(X) \in \mathcal{F} \quad .$$

ii. Prove that

$$f\left(\bigcap \mathcal{F}\right) \subseteq \bigcap \mathcal{F}$$

by establishing the following equivalent statement:

$$\forall X \in \mathcal{F}.\ f\left(\bigcap \mathcal{F}\right) \subseteq X \quad .$$

iii. Use the above two items to conclude that

$$f\left(\bigcap \mathcal{F}\right) \in \mathcal{F}$$

and thereby argue that

$$\bigcap \mathcal{F} \subseteq f\left(\bigcap \mathcal{F}\right) \quad .$$

(b) The greateast post-fixed point.

A ***post-fixed point*** is an element $X \in \mathcal{P}(A)$ such that

$$X \subseteq f(X) \quad .$$

Consider the set

$$\mathcal{G} = \left\{ X \in \mathcal{P}(A) \mid X \subseteq f(X) \right\} \subseteq \mathcal{P}(A)$$

of post-fixed points.

You will now show that

$$f\left(\bigcup \mathcal{G}\right) = \bigcup \mathcal{G} \quad .$$

i. Show that

$$\forall X \in \mathcal{G}.\ X \in \mathcal{G} \implies f(X) \in \mathcal{G} \quad .$$

ii. Prove that

$$\bigcup \mathcal{G} \subseteq f\left(\bigcup \mathcal{G}\right)$$

by establishing the following equivalent statement:

$$\forall X \in \mathcal{G}.\ X \subseteq f\left(\bigcup \mathcal{G}\right) \quad .$$

iii. Use the above two items to conclude that

$$f\left(\bigcup \mathcal{G}\right) \in \mathcal{G}$$

and thereby argue that

$$f\left(\bigcup \mathcal{G}\right) \subseteq \bigcup \mathcal{G} \quad .$$

(c) Finally, conclude that

$$\forall X \in \mathcal{P}(A).\ f(X) = X \implies \bigcap \mathcal{F} \subseteq X \subseteq \bigcup \mathcal{G} \quad .$$

Workout 32
from page 406

1. (a) Give examples of functions that have
   (i) none,
   (ii) exactly one, and
   (iii) more than one

   retraction.

   (b) Give examples of functions that have
   (i) none,
   (ii) exactly one, and
   (iii) more than one

   section.

2. Let n be an integer.

   (a) How many sections are there for the absolute-value map $[-n..n] \to [0..n] : x \mapsto |x|$?

   (b) How many retractions are there for the exponential map $[0..n] \to [0..2^n] : x \mapsto 2^x$?

3. Give an example of two sets A and B and a map $f : A \to B$ satisfying both:

   (i) there is a retraction for f, and

   (ii) there is no section for f.

   Explain how you know that f has these two properties.

4. Prove Theorem 129 (on page 404).

5. For $f : A \longrightarrow B$, prove that if there are $g, h : B \longrightarrow A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$ then $g = h$.

   Conclude as a corollary that, whenever it exists, the inverse of a function is unique.

6. We say that two functions $s : A \longrightarrow B$ and $r : B \longrightarrow A$ are a ***section-retraction*** pair whenever $r \circ s = \mathrm{id}_A$; and that a function $e : B \longrightarrow B$ is an ***idempotent*** whenever $e \circ e = e$.

   (a) Show that if $s : A \longrightarrow B$ and $r : B \longrightarrow A$ are a section-retraction pair then the composite $s \circ r : B \longrightarrow B$ is an idempotent.

   (b) Prove that for every idempotent $e : B \longrightarrow B$ there exists a set A and a section-retraction pair $s : A \longrightarrow B$ and $r : B \longrightarrow A$ such that $s \circ r = e$.

7. Let $p : C \to D$ and $q : D \to C$ be functions such that $p \circ q \circ p = p$. Can you conclude that

- $p \circ q$ is idempotent? If so, how?
- $q \circ p$ is idempotent? If so, how?

Workout 33
from page 412

1. For a relation R on a set A, prove that
   - R is reflexive iff $\mathrm{id}_A \subseteq R$,
   - R is symmetric iff $R \subseteq R^{\mathrm{op}}$,
   - R is transitive iff $R \circ R \subseteq R$.
2. Prove that the isomorphism relation $\cong$ between sets is an equivalence relation.
3. Prove that the identity relation id_A on a set A is an equivalence relation and that $A/_{\mathrm{id}_A} \cong A$.

4. Let E_1 and E_2 be two equivalence relations on a set A. Either prove or disprove the following statements.

   (a) $E_1 \cup E_2$ is an equivalence relation on A.

   (b) $E_1 \cap E_2$ is an equivalence relation on A.

5. For an equivalence relation E on a set A, show that $[a_1]_E = [a_2]_E$ iff $a_1 \mathrel{E} a_2$, where $[a]_E = \{ x \in A \mid x \mathrel{E} a \}$ as on page 410.

6. Let E be an equivalence relation on a set A. We want to show here that to define a function out of the quotient set $A_{/E}$ is, essentially, to define a function out of A that identifies equivalent elements.

   To formalise this, you are required to show that for any function $f : A \to B$ such that $f(x) = f(y)$ for all $(x, y) \in E$ there exists a unique function $f_{/E} : A_{/E} \to B$ such that $f_{/E} \circ q = f$, where $q : A \twoheadrightarrow A_{/E}$ denotes the quotient function $a \mapsto [a]_E$.

   Btw This proof needs some care, so please revise your argument. Sample applications of its use follow.

7. For a positive integer m, let $\equiv_m$ be the equivalence relation on $\mathbb{Z}$ given by

$$x \equiv_m y \iff x \equiv y \pmod{m} \quad .$$

Define a mapping $\mathbb{Z}_{/\equiv_m} \to \mathbb{Z}_m$ and prove it bijective.

8. Show that the relation $\equiv$ on $\mathbb{Z} \times \mathbb{N}^+$ given by

$$(a, b) \equiv (x, y) \iff a \cdot y = x \cdot b$$

is an equivalence relation. Define a mapping $(\mathbb{Z} \times \mathbb{N}^+)_{/\equiv} \to \mathbb{Q}$ and prove it bijective.

9. Let B be a subset of a set A. Define the relation E on $\mathcal{P}(A)$ by

$$(X, Y) \in E \iff X \cap B = Y \cap B \quad .$$

Show that E is an equivalence relation. Define a mapping $\mathcal{P}(A)_{/E} \to \mathcal{P}(B)$ and prove it bijective.

10. For a function $f : A \longrightarrow B$ define a relation $\equiv_f$ on A by the rule

$$a \equiv_f a' \iff f(a) = f(a')$$

for all $a, a' \in A$.

(a) Show that for every function $f : A \longrightarrow B$, the relation $\equiv_f$ is an equivalence on A.

(b) Prove that every equivalence relation E on a set A is equal to $\equiv_q$ for q the quotient function $A \twoheadrightarrow A_{/E} : a \mapsto [a]_E$.

(c) Prove that for every surjection $f : A \twoheadrightarrow B$,

$$B \cong \left(A_{/\equiv_f}\right) \quad .$$

11. We will see here that there is a canonical way in which every preorder can be turned into a partial order.

(a) Let $(P, \sqsubseteq)$ be a preorder. Define $\simeq \subseteq P \times P$ by setting

$$x \simeq y \iff (x \sqsubseteq y \wedge y \sqsubseteq x)$$

for all $x, y \in P$.

Prove that $\simeq$ is an equivalence relation on P.

(b) Consider now $P_{/\simeq}$ and define $\sqsubseteq_{\sim} \subseteq P_{/\simeq} \times P_{/\simeq}$ by setting

$$X \sqsubseteq_{\sim} Y \iff \forall x \in X. \exists y \in Y. x \sqsubseteq y$$

for all $X, Y \in P_{/\simeq}$.

Prove that $\left(P_{/\simeq}, \sqsubseteq_{\sim}\right)$ is a partial order.

Workout 34
from page 417

1. Make sure that you understand the calculus of bijections on pages 413 and 414.

2. Write ML functions describing the calculus of bijections, where the set-theoretic product $\times$ is interpreted as the product type `*`, the set-theoretic disjoint union $\uplus$ is interpreted as the sum datatype `sum` (see page 528), and the set-theoretic function $\Rightarrow$ is interpreted as the arrow type `->`.

   Btw The theory underlying this question is known as the *Curry-Howard correspondence*.

For instance,

- for the bijection

$$\big((A \times B) \Rightarrow C\big) \cong \big(A \Rightarrow (B \Rightarrow C)\big)$$

  you need provide ML functions of types

```
(('a*'b)->'c) -> ('a->('b->'c))
```

  and

```
(('a->('b->'c)) -> (('a*'b)->'c)
```

  such that when understood as functions on sets yield a bijection, and

- for the implication

$$(X \cong A \;\wedge\; B \cong Y) \implies (A \Rightarrow B) \cong (X \Rightarrow Y)$$

you need provide an ML function of type

```
('x->'a)*('b->'y) -> ('a->'b)->('x->'y)
```

such that when understood as a function between sets it constructs the required compound bijection from the two given component ones.

3. Let $\chi : \mathcal{P}(U) \to (U \Rightarrow [2])$ be the function mapping subsets S of U to their characteristic (or indicator) functions $\chi_S : U \to [2]$.

   (a) Prove that, for all $x \in U$,

   - $\chi_{A\cup B}(x) = \big(\chi_A(x) \text{ OR } \chi_B(x)\big) = \max\big(\chi_A(x), \chi_B(x)\big)$,
   - $\chi_{A\cap B}(x) = \big(\chi_A(x) \text{ AND } \chi_B(x)\big) = \min\big(\chi_A(x), \chi_B(x)\big)$,
   - $\chi_{A^c}(x) = \text{NOT}\big(\chi_A(x)\big) = \big(1 - \chi_A(x)\big)$.

   (b) For what construction $A?B$ on sets A and B it holds that

$$\chi_{A?B}(x) = \big(\chi_A(x) \text{ XOR } \chi_B(x)\big) = \big(\chi_A(x) +_2 \chi_B(x)\big)$$

   for all $x \in U$? Prove your claim.

Workout 35
from page 420

1. Prove Theorem 136 (on page 419).
2. For sets $A \subseteq B$, show that $B \cong A \uplus (B \setminus A)$, and argue that for finite B, $\#(B \setminus A) = \#B - \#A$.
3. For sets A and B, show that

$$A \cup B \cong \big(A \setminus (A \cap B)\big) \uplus (A \cap B) \uplus \big(B \setminus (A \cap A)\big) \quad .$$

Argue that for finite A and B,

$$\#(A \cup B) = \#A + \#B - \#(A \cap B) \quad .$$

4. The *Sieve Principle* (or *Principle of Inclusion and Exclusion*).

Prove by the Principle of Induction that, for all natural numbers n,

for all families of finite sets $\{A_1, \ldots, A_n\}$,

$$\#\left(\bigcup\left\{A_i \mid i \in [1..n]\right\}\right)$$
$$= \sum_{k\in[1..n]} (-1)^{k+1} \cdot \sum_{S\in\mathcal{P}_k([1..n])} \#\left(\bigcap\{A_i \mid i \in S\}\right)$$

where $\mathcal{P}_k(X) = \left\{ S \subseteq X \mid \#S = k \right\}$.

Workout 36
from page 428

1. Give three examples of functions that are surjective and three examples of functions that are not.

2. Prove Theorem 139 (on page 425).

3. From surjections $A \twoheadrightarrow B$ and $X \twoheadrightarrow Y$ define, and prove surjective, functions $A \times X \twoheadrightarrow B \times Y$ and $A \uplus X \twoheadrightarrow B \uplus Y$.

4. For an infinite set S, prove that if there is a surjection $\mathbb{N} \to S$ then there is a bijection $\mathbb{N} \to S$.

Workout 37
from page 435

1. Prove Proposition 143 (on page 434).

Workout 38
from page 441

1. Give three examples of functions that are injective and three of functions that are not.

2. Prove Theorem 145 (on page 439).

3. For a set X, prove that there is no injection $\mathcal{P}(X) \to X$.

   [Hint: By way of contradiction, assume an injection $f : \mathcal{P}(X) \to X$, consider

   $$W = \{ x \in X \mid \exists Z \in \mathcal{P}(X). x = f(Z) \wedge x \notin Z \} \in \mathcal{P}(X) \quad ,$$

   and ask whether or not $f(W) \in X$ is in W.]

4. For an infinite set S, prove that the following are equivalent:

   (a) There is a bijection $\mathbb{N} \longrightarrow S$.

   (b) There is an injection $S \longrightarrow \mathbb{N}$.

   (c) There is a surjection $\mathbb{N} \longrightarrow S$

Workout 39
from page 446

1. What is the direct image of $\mathbb{N}$ under the integer square root relation $R_2 = \{ (m, n) \mid m = n^2 \} : \mathbb{N} \longrightarrow\!\!\!\!\!\!\!+\,\, \mathbb{Z}$? And the inverse image of $\mathbb{N}$?

2. For a relation $R : A \longrightarrow\!\!\!\!\!\!\!+\,\, B$, show that

   (a) $\overrightarrow{R}(X) = \bigcup_{x \in X} \overrightarrow{R}\big(\{x\}\big)$ for all $X \subseteq A$, and

   (b) $\overleftarrow{R}(Y) = \big\{ a \in A \mid \overrightarrow{R}\big(\{a\}\big) \subseteq Y \big\}$ for all $Y \subseteq B$.

3. For a relation $R : A \to\!\!\!\!\!+\!\!\!\to B$, prove that

(a) $\overrightarrow{R}\left(\bigcup \mathcal{F}\right) = \bigcup\left\{\overrightarrow{R}(X) \mid X \in \mathcal{F}\right\} \in \mathcal{P}(B)$ for all $\mathcal{F} \in \mathcal{P}(\mathcal{P}(A))$, and

(b) $\overleftarrow{R}\left(\bigcap \mathcal{G}\right) = \bigcap\left\{\overleftarrow{R}(Y) \mid Y \in \mathcal{G}\right\} \in \mathcal{P}(A)$ for all $\mathcal{G} \in \mathcal{P}(\mathcal{P}(B))$.

4. Show that

the inverse and direct images of a relation form a *Galois connection*[a]

That is, for all $R : A \leftrightarrow B$, the direct image and inverse image functions

$$\mathcal{P}(A) \underset{\overleftarrow{R}}{\overset{\overrightarrow{R}}{\rightleftarrows}} \mathcal{P}(B)$$

are such that

- for all $X \subseteq X'$ in $\mathcal{P}(A)$, $\overrightarrow{R}(X) \subseteq \overrightarrow{R}(X')$;
- for all $Y \subseteq Y'$ in $\mathcal{P}(B)$, $\overleftarrow{R}(Y) \subseteq \overleftarrow{R}(Y')$;
- for all $X \in \mathcal{P}(A)$ and $Y \in \mathcal{P}(B)$, $\overrightarrow{R}(X) \subseteq Y \iff X \subseteq \overleftarrow{R}(Y)$.

[a] This is a fundamental mathematical concept, with many applications in computer science (e.g. in the context of abstract interpretations for static analysis).

Workout 40
from page 449

1. What is the direct image of $\mathbb{Z}$ under the negative-doubling function $\mathbb{Z} \to \mathbb{Z} : n \mapsto -2 \cdot n$? And the direct image of $\mathbb{N}$?

2. Prove that

   (a) for all sets A,

   $$\overrightarrow{\mathrm{id}_A} = \mathrm{id}_{\mathcal{P}(A)} \quad \text{and} \quad \overleftarrow{\mathrm{id}_A} = \mathrm{id}_{\mathcal{P}(A)} \quad ,$$

   and

   (b) for all functions $f : A \to B$ and $g : B \to C$,

   $$\overrightarrow{g \circ f} = \overrightarrow{g} \circ \overrightarrow{f} \quad \text{and} \quad \overleftarrow{g \circ f} = \overleftarrow{f} \circ \overleftarrow{g} \quad .$$

3. For $X \subseteq A$, prove that the direct image $\overrightarrow{f}(X) \subseteq B$ under an injective function $f : A \rightarrowtail B$ is in bijection with X; that is, $X \cong \overrightarrow{f}(X)$.

4. (a) How many sections are there for a surjective function between finite sets?

   (b) How many retractions are there for an injective function between finite sets?

5. Prove that for a surjective function $f : A \twoheadrightarrow B$, the direct image function $\overrightarrow{f} : \mathcal{P}(A) \to \mathcal{P}(B)$ is surjective.

6. For sets A and X, show that the mapping

$$f \mapsto \{\, b \subseteq A \mid \exists x \in X.\, b = \overleftarrow{f}\big(\{x\}\big) \,\}$$

yields a function $\mathrm{Sur}(A, X) \to \mathrm{Part}(A)$. Is it surjective? And injective?

7. Show that, by inverse image,

every map $A \longrightarrow B$ induces a
Boolean algebra map $\mathcal{P}(B) \longrightarrow \mathcal{P}(A)$.

That is, for every function $f : A \longrightarrow B$,

- $\overleftarrow{f}(\emptyset) = \emptyset$
- $\overleftarrow{f}(X \cup Y) = \overleftarrow{f}(X) \cup \overleftarrow{f}(Y)$
- $\overleftarrow{f}(B) = A$
- $\overleftarrow{f}(X \cap Y) = \overleftarrow{f}(X) \cap \overleftarrow{f}(Y)$
- $\overleftarrow{f}(X^c) = \left(\overleftarrow{f}(X)\right)^c$

for all $X, Y \subseteq B$.

(If you like this kind of stuff, investigate what happens with partial functions and relations; and also look at direct images.)

8. The aim of this exercise is to give a proof of the Cantor-Schroeder-Bernstein Theorem (Theorem 148 on page 443).

Given functions $f : A \to B$ and $g : B \to A$ define the relation $\perp \subseteq \mathcal{P}(A) \times \mathcal{P}(B)$ by letting

$$X \perp Y \iff X^c \cong \overrightarrow{g}(Y) \wedge \overrightarrow{f}(X) \cong Y^c \quad .$$

(a) Prove that,

for injections f and g, if $\perp$ is non-empty then $A \cong B$.

[Hint: Use that $A \cong X \uplus X^c$, $Y^c \uplus Y \cong B$, the calculus of bijections (see page 413), and that every set is in bijection with its direct image under an injection (Workout 40.3 on page 566).]

(b) Prove that $\perp$ is non-empty.

[Hint: Show that the function $h : \mathcal{P}(A) \longrightarrow \mathcal{P}(A)$ given by $h(X) = \left(\overrightarrow{g}\left(\left(\overrightarrow{f}(X)\right)^{c}\right)\right)^{c}$ is monotone, and hence by the Knaster-Tarski Fixed-Point Theorem (Workout 31.5 on page 538) has fixed-points, and consider pairs $\left(F, \left(\overrightarrow{f}(F)\right)^{c}\right) \in \mathcal{P}(A) \times \mathcal{P}(B)$ where F is a fixed-point of h.[a]]

[a] Alternatively, you may learn about the more general *Tarski's Fixed-Point Theorem*, use it to show that the function $h : \mathcal{P}(A) \times \mathcal{P}(B) \longrightarrow \mathcal{P}(A) \times \mathcal{P}(B)$ given by $h(X, Y) = \left(\left(\overrightarrow{g}(Y)\right)^{c}, \left(\overrightarrow{f}(X)\right)^{c}\right)$ has fixed-points, and consider such pairs.

Workout 41
from page 458

1. Prove Corollary 154 on page 455.
2. Make sure that you understand the calculus of bijections on page 456.

Workout 42
from page 465

1. Which of the following sets are finite, which are infinite but countable, and which are uncountable?

   (a) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \leq f(n+1) \}$

   (b) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(2 \cdot n) \neq f(2 \cdot n + 1) \}$

   (c) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \neq f(n+1) \}$

   (d) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \leq f(n+1) \}$

   (e) $\{ f \in (\mathbb{N} \Rightarrow [2]) \mid \forall n \in \mathbb{N}.\, f(n) \geq f(n+1) \}$

Workout 43
from page 468

1. Let $f : \mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ be a monotone function. Show that for all $\mathcal{F} \subseteq \mathcal{P}(A)$,

$$\bigcup_{\alpha \in \mathcal{F}} f(\alpha) \subseteq f\left(\bigcup \mathcal{F}\right) \quad .$$

In particular, note that

$$\bigcup_{\alpha \in \mathcal{P}_{\text{fin}}(X)} f(\alpha) \subseteq f(X)$$

for all $X \in \mathcal{P}(A)$.

2. A function $f : \mathcal{P}(A) \to \mathcal{P}(B)$ is said to be *continuous* whenever:
   - it is monotone, and
   - for all $X \in \mathcal{P}(A)$,

$$f(X) = \bigcup_{\alpha \in \mathcal{P}_{\text{fin}}(X)} f(\alpha) \quad .$$

   We write $\mathrm{Cont}\big(\mathcal{P}(A), \mathcal{P}(B)\big)$ for the set of continuous functions from $\mathcal{P}(A)$ to $\mathcal{P}(B)$.

   Prove that

$$\mathrm{Cont}\big(\mathcal{P}(A), \mathcal{P}(B)\big) \cong \big(\mathcal{P}_{\text{fin}}(A) \Rightarrow \mathcal{P}(B)\big) \cong \mathcal{P}\big(\mathcal{P}_{\text{fin}}(A) \times B\big) \quad .$$

3. Deduce that for $D = \mathcal{P}(\mathbb{N})$,

$$D \cong \mathrm{Cont}(D, D) \quad .$$