The Haskell Road to Logic, Math and Programming

Solutions to the Exercises

Kees Doets and Jan van Eijck

August 26, 2012

Contents

Important Advice to the Reader

This companion volume to **The Haskell Road to Logic, Math and Programming** will enable you to check your solutions to the exercises. It should be used wisely. You should only turn to the solution of an exercise *after* you have tried to solve the exercise on your own. What the following pages do *not* provide is a shortcut to understanding.

You don't expect to improve your swimming or iceskating skills by watching swimming or iceskating contests on TV. If you want to learn how to swim you must be willing to get wet. If you want to learn how to skate, you must venture on the ice skating ring and take the risk of falling. Likewise, you can't expect to improve your skills in reasoning or programming by watching others reason or program. Just reading through the following pages, to watch how the authors reason and program, is next to useless. You have to tackle the problems yourself, at the risk of making mistakes, only using the solutions as checks on your understanding.

We can make this advice still more specific. When learning skills in formal reasoning it is easy to deceive yourself into thinking you have thought hard enough. Therefore, a honest attempt to solve a problem should always include *a written account of how far you got*. Thus, if you find you cannot solve a problem, you should have an attempted solution on paper. Your account should always end with "I can get this far, but then I am stuck because ..." or "I follow the rules like on page ... of the book, but then I get the wrong answer because ...". Proceeding like this, you will make very rapid progress. On the other hand, if you think you can disregard this advice you might as well not bother with the book at all, for skills in formal reasoning and computation can only be acquired by training, and without proper exercise you will never be any good at it.

You are completely free to do as you please, of course. Only don't tell anyone you haven't been warned.

Solutions to the Exercises from Chapter 1

```
module Sol1  where

import GS
```

1.1 The precedences are: `^` binds more strongly than `*` and `/`, and these in turn bind more strongly than `+` and `-`.

1.4 Replacing `k^2 > n` by `k^2 >= n` would make no difference in this case. The reason is that it follows from `k^2 == n` that k divides n. This case was already covered by the previous line, and therefore `k^2 >= n` in the second line would still only cover the case of `k^2 > n`.

1.6. The type declaration for `rem` should run something like

```
rem :: Integer -> Integer -> Integer
```

In actual fact, the type is slightly more general than this.

1.7. If `divides` has type `Integer -> Integer -> Bool`, this means that `divides` takes an argument of type `Integer`, and then produces a result of type `Integer -> Bool`. Thus, `divides 5` indeed has this type. In other words, `divides 5` is itself a function that expects an argument of type `Integer` to give a result of type `Bool`. Providing this argument creates a boolean expression, i.e., `divides 5 7` is of type `Bool`. This expression evaluates to `False`, by the way, since `5` is not a divisor of `7`.

1.9

```
mxmInt :: [Int] -> Int
mxmInt [] = error "empty list"
mxmInt [x] = x
mxmInt (x:xs) = max x (mxmInt xs)
```

1.10

```
removeFst :: Eq a => a -> [a] -> [a]
removeFst x [] = []
removeFst x (y:ys) | x == y    = ys
                   | otherwise = y : (removeFst x ys)
```

1.13

```
count :: Char -> String -> Int
count c [] = 0
count c (x:xs) | c==x      = 1 + (count c xs)
               | otherwise = (count c xs)
```

1.14

```
copy :: Int -> Char -> String
copy 0 c = []
copy n c = c:(copy (n-1) c)

blowup :: String -> String
blowup xs = blowup' xs 1

blowup' :: String -> Int -> String
blowup' [] n = []
blowup' (x:xs) n = (copy n x) ++ (blowup' xs (n+1))
```

Haskell hackers may appreciate the following alternative. To understand the details, look up the code for `zip`, `take` and `repeat` in *Prelude.hs*.

```
spread :: [a] -> [a]
spread xs = [ x | (n,y) <- zip [1..] xs , x <- take n (repeat y)]
```

1.15 The best way to approach this is to generalize `mnmInt` and `srtInt`, and use these to implement a general sorting algorithm based on insertion. In Haskell, types for which we can do size comparison are put in a so-called *type class*, the type class `Ord`. In Haskell, we can make this type class requirement part of the type declaration. `f :: Ord a => a` means that `f` is a type in class `Ord`. `f :: Ord a => [a] -> a` means that `f` is a function from lists over `a` to `a` objects, where `a` is a type in class `Ord`. In other words, `f` picks an object from a list of things, where the list contains objects that can be compared for size. That is the type we need for the generalized minimum function.

```
mnm :: Ord a => [a] -> a
mnm [] = error "empty list"
mnm [x] = x
mnm (x:xs) = min x (mnm xs)

srt :: Ord a => [a] -> [a]
srt [] = []
srt xs = m : (srt (removeFst m xs)) where m = mnm xs
```

1.17

```
substring :: String -> String -> Bool
substring [] ys = True
substring (x:xs) [] = False
substring (x:xs) (y:ys) = ((x==y) && (prefix xs ys))
                        || (substring (x:xs) ys)
```

1.18

1. `[String]` is an abbreviation of `[[Char]]`. We have:

   ```
   Prelude> :t ["Alan","Turing"]
   ["Alan","Turing"] :: [[Char]]
   ```

2. `(Bool,String)` is an abbreviation of `(Bool,[Char])`. We have:

   ```
   Prelude> :t (True,"Turing")
   (True,"Turing") :: (Bool,[Char])
   ```

3. `[(Bool,String)]` is an abbreviation of `[(Bool,[Char])]`. We have:

   ```
   Prelude> :t [(True,"Turing")]
   [(True,"Turing")] :: [(Bool,[Char])]
   ```

4. `([Bool],String)` is an abbreviation of `([Bool],[Char])`. We have:

   ```
   Prelude> :t ([True],"Turing")
   ([True],"Turing") :: ([Bool],[Char])
   ```

5. `Bool -> Bool` is the type of the Haskell negation operator:

   ```
   Prelude> :t not
   not :: Bool -> Bool
   ```

1.20

```
lengths :: [[a]] -> [Int]
lengths = map length
```

1.21

```
sumLengths :: [[a]] -> Int
sumLengths lists = sum (map length lists)
```

Here is another way to express this, using `(.)` for function composition:

```
sumLengths :: [[a]] -> Int
sumLengths = sum . lengths
```

1.24 The change makes no difference. The final argument `n` in the definition can be left out, for saying that `ldp` is the function that results from applying `ldpf` to `primes1` is equivalent to saying that `ldp` is the function that for any argument `n` does the same as what `(ldpf primes1)` does for argument `n`.

Solutions to the Exercises from Chapter 2

```
module Sol2  where

import GS
import TAMO
```

2.2

P	Q	$P \oplus Q$
t	**t**	**f**
t	**f**	**t**
f	**t**	**t**
f	**f**	**f**

2.4

P	Q	$P \oplus Q$	$P \Leftrightarrow Q$	$\neg(P \Leftrightarrow Q)$
t	**t**	**f**	**t**	**f**
t	**f**	**t**	**f**	**t**
f	**t**	**t**	**f**	**t**
f	**f**	**f**	**t**	**f**

2.9

P	Q	$P \oplus Q$	$(P \oplus Q) \oplus Q$
t	**t**	**f**	**t**
t	**f**	**t**	**t**
f	**t**	**t**	**f**
f	**f**	**f**	**f**

2.13

```
tst1a = not True <=> False
tst1b = not False <=> True
tst2  = logEquiv1 (\ p -> p ==> False) (\ p -> not p)
tst3a = logEquiv1 (\ p -> p || True) (const True)
tst3b = logEquiv1 (\ p -> p && False) (const False)
tst4a = logEquiv1 (\ p -> p || False) id
tst4b = logEquiv1 (\ p -> p && True) id
tst5  = logEquiv1 excluded_middle (const True)
tst6  = logEquiv1 (\ p -> p && not p) (const False)
```

The implementation uses `excluded_middle`; this is defined in Chapter 2 as a name for the function

```
\ p -> p || not p)
```

`const k` is the function which gives value `k` for any argument.

Note that the implementation of `tst4a` and `tst4b` makes clear *why* $P \vee \bot \equiv P$ and $P \wedge \top \equiv P$ are called laws of identity.

2.15

```
contrad1 :: (Bool -> Bool) -> Bool
contrad1 bf =  not (bf True) && not (bf False)

contrad2 :: (Bool -> Bool -> Bool)  -> Bool
contrad2 bf = and [not (bf p q) | p <- [True,False], q <- [True,False]]

contrad3 :: (Bool -> Bool -> Bool -> Bool) -> Bool
contrad3 bf = and [ not (bf p q r) | p <- [True,False],
                                     q <- [True,False],
                                     r <- [True,False]]
```

2.16.1 The equation $x^2 + 1 = 0$ has no solutions. $\leadsto$ $\neg\exists x(x^2 + 1 = 0)$.

2.16.2 There is a largest natural number. $\leadsto$ $\exists n(n \in \mathbb{N} \wedge \forall m(m \in \mathbb{N} \Rightarrow m \leqslant n))$.

2.16.3 The number 13 is not prime. $\leadsto$ $\exists m(m \in \mathbb{N} \wedge 1 < m \wedge m < 13 \wedge m|13)$.

2.16.4 The number n is not prime. $\leadsto$ $n \in \mathbb{N} \wedge \exists m(m \in \mathbb{N} \wedge 1 < m \wedge m < n \wedge m|n)$.

2.16.5 There are only finitely many primes. $\leadsto$

$$\exists p((p \in \mathbb{N} \wedge \neg\exists m(m \in \mathbb{N} \wedge 1 < m \wedge m < p \wedge m|p)) \wedge \forall q((q \in \mathbb{N} \wedge q > p) \Rightarrow \exists n(n \in \mathbb{N} \wedge 1 < n \wedge n < q \wedge n|q))).$$

2.17 The statement $x < y < z$ is an abbreviation of $x < y \wedge y < z$. The negation of this, $\neg(x < y \wedge y < z)$, is equivalent to $x \geqslant y \vee y \geqslant z$.

2.18.1 $(\Phi \Leftrightarrow \Psi) \equiv (\neg\Phi \Leftrightarrow \neg\Psi)$, for we have:

$$\begin{aligned} \Phi \Leftrightarrow \Psi &\equiv (\Phi \Rightarrow \Psi) \wedge (\Psi \Rightarrow \Phi) \\ &\equiv (\neg\Psi \Rightarrow \neg\Phi) \wedge (\neg\Phi \Rightarrow \neg\Psi) \\ &\equiv (\neg\Phi \Rightarrow \neg\Psi) \wedge (\neg\Psi \Rightarrow \neg\Phi) \\ &\equiv \neg\Phi \Leftrightarrow \neg\Psi. \end{aligned}$$

2.18.2 $(\neg\Phi \Leftrightarrow \Psi) \equiv (\Phi \Leftrightarrow \neg\Psi)$, for we have:

$$\begin{aligned} \neg\Phi \Leftrightarrow \Psi &\equiv (\neg\Phi \Rightarrow \Psi) \wedge (\Psi \Rightarrow \neg\Phi) \\ &\equiv (\neg\Psi \Rightarrow \neg\neg\Phi) \wedge (\neg\neg\Phi \Rightarrow \neg\Psi) \\ &\equiv (\neg\Psi \Rightarrow \Phi) \wedge (\Phi \Rightarrow \neg\Psi) \\ &\equiv \Phi \Leftrightarrow \neg\Psi. \end{aligned}$$

2.19 $\Phi \equiv \Psi$ is true iff Φ and Ψ are equivalent iff Φ and Ψ have the same truth value no matter what the truth values are of their proposition letters iff $\Phi \Leftrightarrow \Psi$ is logically valid.

2.21.1 Here is an example formula:

P	Q	$Q \Rightarrow P$
t	**t**	**t**
t	**f**	**t**
f	**t**	**f**
f	**f**	**t**

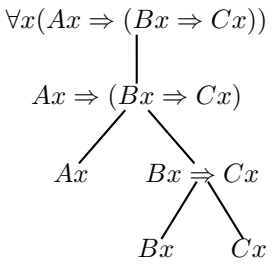
2.21.2 A two-letter formula has a truth table with four rows. The value at every row can be either **t** of **f**, so there are $2^4 = 16$ truth tables altogether.

2.21.3 and 4 To find a formula for a given four-row truth table, construct a formula that describes the table. In the first item above, the description would run: $(P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$. In this example, the formula happens to be equivalent to $Q \Rightarrow P$. It is clear that the method of describing a truth table always works.

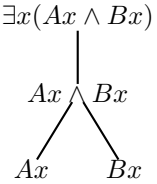
2.21.5 With 3-letter formulas, we get truth tables with $2^3 = 8$ rows, so there are 2^8 different meanings to express, but these again can be described in so-called disjunctive normal form. And so on: for formulas with n letters, there are $2^{(2^n)}$ different truth tables, and any of these tables can be described by a formula in disjunctive normal form.

2.22 'Between every two rational numbers there is a third one.' Take two arbitrary rationals x, y with $x < y$. Then $x < \frac{x+y}{2} < y$. $\frac{x+y}{2}$ is rational, for assume $x = \frac{p}{q}$ and $y = \frac{m}{n}$. Then $\frac{x+y}{2} = \frac{1}{2}(\frac{p}{q} + \frac{m}{n}) = \frac{1}{2}(\frac{pn+qm}{qn})$.

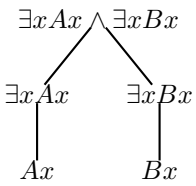
2.23.1 Structure tree for $\forall x(Ax \Rightarrow (Bx \Rightarrow Cx))$.



2.23.2 Structure tree for $\exists x(Ax \wedge Bx)$.



2.23.3 Structure tree for $\exists x Ax \wedge \exists x Bx$.



2.26.1 $\exists x \exists y(x \in \mathbb{Q} \wedge y \in \mathbb{Q} \wedge x < y)$. With restricted quantifiers this becomes:

$$\exists x \in \mathbb{Q}\ \exists y \in \mathbb{Q}\ (x < y).$$

2.26.2 $\forall x(x \in \mathbb{R} \Rightarrow \exists y(y \in \mathbb{R} \wedge x < y))$. With restricted quantifiers this becomes:

$$\forall x \in \mathbb{R}\ \exists y \in \mathbb{R}\ (x < y).$$

2.26.3 $\forall x(x \in \mathbb{Z} \Rightarrow \exists m, n(m \in \mathbb{N} \wedge n \in \mathbb{N} \wedge x = m - n))$. With restricted quantifiers this becomes:

$$\forall x \in \mathbb{Z}\ \exists m, n \in \mathbb{N}\ (x = m - n).$$

2.27.1 $\forall x \in \mathbb{Q} \exists m, n \in \mathbb{Z}(n \neq 0 \wedge x = m/n)$. Without restricted quantifiers this becomes:

$$\forall x(x \in \mathbb{Q} \Rightarrow \exists m, n(m \in \mathbb{Z} \wedge n \in \mathbb{Z} \wedge n \neq 0 \wedge x = m/n)).$$

2.27.2 $\forall x \in F \forall y \in D(Oxy \Rightarrow Bxy)$. Without restricted quantifiers this becomes:

$$\forall x(Fx \Rightarrow \forall y(Dy \Rightarrow (Oxy \Rightarrow Bxy))).$$

2.31.1 The equation $x^2 + 1 = 0$ has a solution $\rightsquigarrow$ $\exists x(x^2 + 1 = 0)$.

2.31.2 A largest natural number does not exist $\rightsquigarrow$ $\neg\exists n(n \in \mathbb{N} \wedge \forall m(m \in \mathbb{N} \Rightarrow m \leqslant n))$.

2.31.3 The number 13 is prime (use $d|n$ for 'd divides n') $\rightsquigarrow$

$$\neg\exists m(m \in \mathbb{N} \wedge 1 < m \wedge m < 13 \wedge m|13).$$

2.31.4 The number n is prime $\rightsquigarrow$ $n \in \mathbb{N} \wedge \neg\exists m(m \in \mathbb{N} \wedge 1 < m \wedge m < n \wedge m|n)$.

2.31.5 There are infinitely many primes $\rightsquigarrow$

$$\forall p(p \in \mathbb{N} \Rightarrow \exists q(q \in \mathbb{N} \wedge q > p \wedge \neg\exists n(n \in \mathbb{N} \wedge 1 < n \wedge n < q \wedge n|q))).$$

2.32 We assume that the domain of discussion consists of all human beings.

2.32.1 Everyone loved Diana $\rightsquigarrow$ $\forall x Lxd$.

2.32.2 Diana loved everyone $\rightsquigarrow$ $\forall x Ldx$.

2.32.3 Man is mortal. $\rightsquigarrow$ $\forall x(Mx \Rightarrow M'x)$.

2.32.4 Some birds do not fly. $\rightsquigarrow$ $\exists x(Bx \wedge \neg Fx)$.

2.33.1 Dogs that bark do not bite (B for barking, B' for biting). $\rightsquigarrow$ $\forall x((Dx \wedge Bx) \Rightarrow \neg B'x)$.

2.33.2 All that glitters is not gold (G for glitter, G' for gold) $\rightsquigarrow$ $\neg\forall x(Gx \Rightarrow G'x)$.

2.33.3 Friends of Diana's friends are her friends. $\rightsquigarrow$ $\forall x\forall y((Fxy \wedge Fyd) \Rightarrow Fxd)$.

2.33.4 The limit of $\frac{1}{n}$ as n approaches infinity is zero. $\rightsquigarrow$

$$\forall\epsilon > 0\exists n \in \mathbb{N}\forall k \in \mathbb{N}(k \geqslant n \Rightarrow \frac{1}{k} < \epsilon).$$

2.34.1 Everyone loved Diana except Charles. $\rightsquigarrow$ $\forall x(\neg x = c \Rightarrow Lxd)$.

2.34.2 Every man adores at least two women. $\rightsquigarrow$ $\forall x(Mx \Rightarrow \exists y\exists z(\neg z = y \wedge Wy \wedge Wz \wedge Axy \wedge Axz))$.

2.34.3 No man is married to more than one woman. $\rightsquigarrow$ $\neg\exists x(Mx \wedge \exists y\exists z(\neg z = y \wedge Wy \wedge Wz \wedge Maxy \wedge Maxz)$.

2.35.1 The King is not raging $\rightsquigarrow$ $\exists x(Kx \wedge \forall y(Ky \Rightarrow x = y) \wedge \neg Rx)$.

2.35.2 The King is loved by all his subjects $\rightsquigarrow$ $\exists x(Kx \wedge \forall y(Ky \Rightarrow x = y) \wedge \forall z(Szx \Rightarrow Lzx))$.

2.36.1 $\exists x \in \mathbb{R}(x^2 = 5)$. $\rightsquigarrow$ The equation $x^2 = 5$ has a real solution.

2.36.2 $\forall n \in \mathbb{N}\exists m \in \mathbb{N}(n < m)$. $\rightsquigarrow$ There is no largest natural number.

2.36.3 $\forall n \in \mathbb{N}\neg\exists d \in \mathbb{N}(1 < d < (2^n + 1) \wedge d|(2^n + 1))$. $\rightsquigarrow$ for all natural numbers n it holds that $2^n + 1$ is prime (a false statement, by the way; the smallest counterexample is $2^3 + 1$).

2.36.4 $\forall n \in \mathbb{N} \exists m \in \mathbb{N}(n < m \ \wedge \ \forall p \in \mathbb{N}(p \leqslant n \ \vee \ m \leqslant p))$. $\rightsquigarrow$ every natural number has an immediate successor.

2.36.5 $\forall \varepsilon \in \mathbb{R}^{+} \exists n \in \mathbb{N} \forall m \geqslant n(|a - a_m| \leqslant \varepsilon)$. $\rightsquigarrow$ the sequence $a_0, a_1, a_2, \ldots$ converges to a.

As a bonus, here is how to generate primes of the form $2^n + 1$ in Haskell (assuming you have the code for `prime` loaded):

```
Sol2> [ 2^n + 1 | n <- [0..], prime (2^n + 1) ]
[2,3,5,17,257,65537
```

And here is how to generate non-primes of that form:

```
Sol2> [ 2^n + 1 | n <- [0..], not (prime (2^n + 1)) ]
[9,33,65,129,513,1025,2049,4097,8193,16385,32769,131073,262145,524289,1048577,
2097153,4194305,8388609,16777217,33554433,67108865,134217729,268435457,
536870913,1073741825,2147483649,4294967297,8589934593,17179869185,34359738369,
68719476737,137438953473,274877906945,549755813889,1099511627777,
2199023255553,4398046511105,8796093022209,17592186044417,35184372088833,
70368744177665,140737488355329{Interrupted!}
```

2.37.a This is the case where the domain is $\mathbb{N} = \{0, 1, 2, \ldots\}$, and where the meaning of $\mathbf{R}$ is $<$.

1. $\forall x \forall y(x\mathbf{R}y)$ expresses that every pair of natural numbers is in the 'less than' relation. This is false.
2. $\forall x \exists y(x\mathbf{R}y)$ expresses that for every natural number there is a larger number. This is true.
3. $\exists x \forall y(x\mathbf{R}y)$ expresses that there is a natural number that is less than any natural number. This is false, for no natural number is less than itself.
4. $\exists x \forall y(x = y \vee x\mathbf{R}y)$ expresses that there is a natural number that is less than or equal to any natural number. This is true, for the natural number 0 has this property.
5. $\forall x \exists y(x\mathbf{R}y \ \wedge \ \neg \exists z(x\mathbf{R}z \ \wedge \ z\mathbf{R}y))$ expresses that every natural number has an immediate successor. This is true.

2.37.b This is the case where the domain is $\mathbb{N} = \{0, 1, 2, \ldots\}$, and where the meaning of $\mathbf{R}$ is $>$.

1. $\forall x \forall y(x\mathbf{R}y)$ expresses that every pair of natural numbers is in the 'greater than' relation. This is false.
2. $\forall x \exists y(x\mathbf{R}y)$ expresses that for every natural number there is a smaller number. This is false.
3. $\exists x \forall y(x\mathbf{R}y)$ expresses that there is a natural number that is greater than any natural number. This is false, for there is no largest natural number.
4. $\exists x \forall y(x = y \ \vee \ x\mathbf{R}y)$ expresses that there is a natural number that is greater than or equal to any natural number. This is false.
5. $\forall x \exists y(x\mathbf{R}y \wedge \neg \exists z(x\mathbf{R}z \wedge z\mathbf{R}y))$ expresses that every natural number has an immediate predecessor. This is false, for 0 has no immediate predecessor.

2.37.c This is the case where the domain is $\mathbb{Q}$, and where the meaning of $\mathbf{R}$ is $<$.

1. $\forall x \forall y(x\mathbf{R}y)$ expresses that every pair of rational numbers is in the 'less than' relation. This is false.
2. $\forall x \exists y(x\mathbf{R}y)$ expresses that for every rational number there is a larger number. This is true.
3. $\exists x \forall y(x\mathbf{R}y)$ expresses that there is a rational number that is less than any rational number. This is false.
4. $\exists x \forall y(x = y \vee x\mathbf{R}y)$ expresses that there is a rational number that is less than or equal to any rational number. This is false.
5. $\forall x \exists y(x\mathbf{R}y \wedge \neg \exists z(x\mathbf{R}z \wedge z\mathbf{R}y))$ expresses that every rational number has an immediate successor. This is false.

2.37.d This is the case where the domain is $\mathbb{R}$, and where the meaning of $x\mathbf{R}y$ is $y^2 = x$.

1. $\forall x \forall y(x\mathbf{R}y)$. This is false.
2. $\forall x \exists y(x\mathbf{R}y)$ expresses that every real number has a real square root. This is false, the square root of a negative real number is not a real number.
3. $\exists x \forall y(x\mathbf{R}y)$ expresses that there is a real number that is a square of every real number. This is false.
4. $\exists x \forall y(x = y \vee x\mathbf{R}y)$ expresses that there is a real number that is equal to or is a square root of every real number. This is false.
5. $\forall x \exists y(x\mathbf{R}y \wedge \neg \exists z(x\mathbf{R}z \wedge z\mathbf{R}y))$ expresses that for every real number x there is a y with $x = y^2$ and for all z with $x = z^2$ it holds that $z \neq y^2$. This is false, for 0 and 1 are counterexamples.

2.37.e The case where the domain is the set of all human beings; meaning of $\mathbf{R}$: father-of.

1. $\forall x \forall y(x\mathbf{R}y)$. Everyone is everyone's father. This is false.
2. $\forall x \exists y(x\mathbf{R}y)$. Everyone is the father of a child. This is false.
3. $\exists x \forall y(x\mathbf{R}y)$. Somebody is everyone's father. This is false (we are only talking about earthly matters here).
4. $\exists x \forall y(x = y \vee x\mathbf{R}y)$. Somebody is everyone's self or father. False.
5. $\forall x \exists y(x\mathbf{R}y \wedge \neg \exists z(x\mathbf{R}z \wedge z\mathbf{R}y))$. Everyone is the father of a child that does not have a sibling that is also its father. False.

2.37.f This is the case where $x\mathbf{R}y$ means that x loves y. As judgements tend to be subjective here, this is better left to the imagination of the reader.

2.38.a This is the case where the domain is $\mathbb{N}$ and the meaning of $\mathbf{R}$ is $<$.

1. $\forall y(x\mathbf{R}y)$ expresses the property of being smaller than any natural number. No natural number has this property.
2. $\exists y(x\mathbf{R}y)$ expresses the property of not being the largest natural number. Every natural number has this property.

3. $\forall y(x\mathbf{R}y)$ expresses that the property of being less than any natural number. No natural number has this property.

4. $\forall y(x = y \vee x\mathbf{R}y)$ expresses that the property of being less than or equal to any natural number. The natural number 0 is the only natural number with this property.

5. $\exists y(x\mathbf{R}y \wedge \neg\exists z(x\mathbf{R}z \wedge z\mathbf{R}y))$ expresses the property of having an immediate successor. Every natural number has this property.

2.38.b,c,d,e,f: left to the reader.

2.39 $\Phi \equiv \Psi$ is true iff Φ and Ψ are true in the same structures iff whenever Φ is true in a structure, Ψ is true in that structure as well and vice versa, iff $\Phi \Rightarrow \Psi$ and $\Psi \Rightarrow \Phi$ are true in any structure, iff $\Phi \Leftrightarrow \Psi$ is valid.

2.41.1 $\neg\exists x \in \mathbb{R}(x^2 = 5)$ can be expressed equivalently as $\forall x \in \mathbb{R}(x^2 \neq 5)$.

2.41.2 $\neg\forall n \in \mathbb{N}\exists m \in \mathbb{N}(n < m)$ can be expressed equivalently as $\exists n \in \mathbb{N}\forall m \in \mathbb{N}(n \geqslant m)$.

2.41.3 $\neg\forall n \in \mathbb{N}\neg\exists d \in \mathbb{N}(1 < d < (2^n + 1) \wedge d|(2^n + 1))$ can be expressed equivalently as

$$\exists n \in \mathbb{N}\exists d \in \mathbb{N}(1 < d < (2^n + 1) \wedge d|(2^n + 1)).$$

2.41.4 $\neg\forall n \in \mathbb{N}\exists m \in \mathbb{N}(n < m \wedge \forall p \in \mathbb{N}(p \leqslant n \vee m \leqslant p))$ can be expressed equivalently as

$$\exists n \in \mathbb{N}\forall m \in \mathbb{N}(n \geqslant m \vee \exists p \in \mathbb{N}(p > n \wedge m > p)).$$

2.41.5 $\neg\forall \varepsilon \in \mathbb{R}^+\exists n \in \mathbb{N}\forall m \geqslant n(|a - a_m| \leqslant \varepsilon)$ can be expressed equivalently as

$$\exists \varepsilon \in \mathbb{R}^+\forall n \in \mathbb{N}\exists m \geqslant n(|a - a_m| > \varepsilon).$$

2.46 $\neg\exists x \in A\ \Phi(x)$ is not equivalent to $\exists x \notin A\ \Phi(x)$. Take A to be the set of all computer scientists, and let $\Phi(x)$ express that x is clever. It is certainly the case that there are clever people who are not computer scientists ($\exists x \notin A\ \Phi(x)$), but this is quite different from the statement that no computer scientist is clever ($\neg\exists x \in A\ \Phi(x)$).

2.47 $\exists x \notin A\ \neg\Phi(x)$ is not equivalent to $\exists x \in A\ \neg\Phi(x)$. Reading A and Φ as above we get that $\exists x \notin A\ \neg\Phi(x)$ amounts to "there are stupid people who are not computer scientists", while $\exists x \in A\ \neg\Phi(x)$ expresses "there are stupid computer scientists". Both true, but quite different truths.

2.50 "The sequence $a_0, a_1, a_2, \ldots$ does not converge to a" can be expressed formally as

$$\exists \delta > 0\forall n\exists m \geqslant n(|a - a_m| \geqslant \delta).$$

2.51

```
unique :: (a -> Bool) -> [a] -> Bool
unique p xs = length (filter p xs) == 1
```

2.52

```
parity :: [Bool] -> Bool
parity [] = True
parity (x:xs) = x /= (parity xs)
```

2.53

```
evenNR :: (a -> Bool) -> [a] -> Bool
evenNR p = parity . map p
```

The following works as well:

```
evenNR :: (a -> Bool) -> [a] -> Bool
evenNR p xs = even (length (filter p xs))
```

Solutions to the Exercises from Chapter 3

```
module Sol3

where

import TUOLP
```

3.2 Given: $P \Rightarrow Q,\ P \Rightarrow (Q \Rightarrow R)$.
To be proved: $P \Rightarrow R$.
Proof:
Suppose P.
To be proved: R.
Proof:
From $P \Rightarrow Q$ and P we get Q.
From $P \Rightarrow (Q \Rightarrow R)$ and P we get $Q \Rightarrow R$.
From $Q \Rightarrow R$ and Q we get R.
Thus $P \Rightarrow R$.

3.4 Assume that $n, m \in \mathbb{N}$.
To show: (m is odd $\wedge$ n is odd) $\Rightarrow m + n$ is even.
Proof:
Assume that (m is odd $\wedge$ n is odd)
For instance, $m = 2p + 1$, $n = 2q + 1$, $p, q \in \mathbb{N}$.
Then $m + n = 2p + 2q + 2 = 2(p + q + 1)$ is even.

3.5.1 To show: From $P \Leftrightarrow Q$ it follows that $(P \Rightarrow R) \Leftrightarrow (Q \Rightarrow R)$.
Proof:
Assume $P \Leftrightarrow Q$
Suppose $P \Rightarrow R$.
Assume Q.
Then from $Q, P \Leftrightarrow Q$, we get P, and from $P, P \Rightarrow R$ we get R.
Thus $Q \Rightarrow R$.

Suppose $Q \Rightarrow R$.
Assume P.
Then from $P, P \Leftrightarrow Q$, we get Q, and from $Q, Q \Rightarrow R$ we get R.
Thus $P \Rightarrow R$.
Thus $(P \Rightarrow R) \Leftrightarrow (Q \Rightarrow R)$.

3.5.2 To show: From $P \Leftrightarrow Q$ it follows that $(R \Rightarrow P) \Leftrightarrow (R \Rightarrow Q)$.
Proof:
Assume $P \Leftrightarrow Q$
Suppose $R \Rightarrow P$.
Assume R.
Then from $R \Rightarrow P$ and R we get P, and from $P, P \Leftrightarrow Q$, we get Q.
Thus $R \Rightarrow Q$.
Suppose $R \Rightarrow Q$.
Assume R.
Then from $R \Rightarrow Q$ and R we get Q, and from $Q, P \Leftrightarrow Q$, we get P.
Thus $R \Rightarrow P$.
Thus $(R \Rightarrow P) \Leftrightarrow (R \Rightarrow Q)$.

3.7.1 Given: $P \Rightarrow Q$.
To show: $\neg Q \Rightarrow \neg P$.
Proof:
Assume $\neg Q$
Assume P
Then from $P \Rightarrow Q$ and P we get Q, and contradiction with $\neg Q$.
Thus $\neg P$.
Thus $\neg Q \Rightarrow \neg P$.

3.7.2 Given: $P \Leftrightarrow Q$.
To show: $\neg P \Leftrightarrow \neg Q$.
Proof:
Assume $\neg P$
If Q then from $P \Leftrightarrow Q$ and Q we get P, and contradiction. Thus $\neg Q$.
Thus $\neg P \Rightarrow \neg Q$.
Assume $\neg Q$
If P, then from $P \Leftrightarrow Q$ and P we get Q, and contradiction. Thus $\neg P$.
Thus $\neg Q \Rightarrow \neg P$.
Thus $\neg P \Leftrightarrow \neg Q$.

3.9 Given: $(P \Rightarrow Q) \Rightarrow P$.
To be proved: P.
Proof:
Assume $\neg P$.
If $P \Rightarrow Q$, then from the given, P, and contradiction. So $\neg(P \Rightarrow Q)$.
But then P, and contradiction with assumption $\neg P$.
Thus P.

3.11.1 Given: $A \Rightarrow B \vee C$, $B \Rightarrow \neg A$.
To be proved: $A \Rightarrow C$.
Proof:
Suppose A.
To be proved: C.
From A and $A \Rightarrow B \vee C$, we get $B \vee C$.
If B then from the given $B \Rightarrow \neg A$ we get $\neg A$, and contradiction. So $\neg B$.
From $B \vee C$ and $\neg B$ we get C, by the reasoning of 3.10.
Thus $A \Rightarrow C$.

3.11.2 Given: $A \vee B \Rightarrow C \vee D$, $C \Rightarrow A$, $B \Rightarrow \neg A$.
To be proved: $B \Rightarrow D$.
Proof:
Assume B.
To be proved: D.
From $B, B \Rightarrow \neg A$ we get $\neg A$.
From $\neg A$ and $C \Rightarrow A$ we get $\neg C$.
From B we get $A \vee B$, and with $A \vee B \Rightarrow C \vee D$ we get $C \vee D$.
By the reasoning of 3.10, from $C \vee D$ and $\neg C$, we get D.
Thus, $B \Rightarrow D$.

3.15 Let $n \in \mathbb{N}$. *To be proved:* division of n^2 by 4 gives remainder 0 or 1.
Proof:
Assume n even.
Then $n = 2m$, so $n^2 = 4m^2$, so division of n^2 by 4 gives remainder 0.
Assume n odd.
Then $n = 2m + 1$, so $n^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1$.
In this case, division of n^2 by 4 gives remainder 1.
Thus division of n^2 by 4 gives remainder 0 or 1.

3.17 Left to the reader.

3.18 Given: From $\Gamma, P(c)$ it follows that $Q(c)$.
To be proved: From Γ it follows that $\forall x(P(x) \Rightarrow Q(x))$.
Proof:
Assume Γ. Let c be arbitrary.
Suppose $P(c)$. Then from the given: $Q(c)$.
Thus (deduction rule) $P(c) \Rightarrow Q(c)$.
Thus ($\forall$ introduction) $\forall x(P(x) \Rightarrow Q(x))$.

3.25.1 Given: $\forall x(P(x) \Rightarrow Q(x))$, $\forall x P(x)$.
To be proved: $\forall x Q(x)$.
Proof:
Let c be arbitrary. Then from $\forall x P(x)$ we get that $P(c)$.
From the given $\forall x(P(x) \Rightarrow Q(x))$, we get $P(c) \Rightarrow Q(c)$.
From $P(c)$ and $P(c) \Rightarrow Q(c)$, we get $Q(c)$.
Thus ($\forall$ introduction) $\forall x Q(x)$.

3.25.2 Given: $\exists x(P(x) \Rightarrow Q(x)), \forall x P(x)$.
To be proved: $\exists x Q(x)$.
Proof:
Suppose c is an object that satisfies $P(c) \Rightarrow Q(c)$.
From the given $\forall x P(x)$ we get that $P(c)$.
From $P(c)$ and $P(c) \Rightarrow Q(c)$, we get $Q(c)$.
Thus $\exists x Q(x)$.

From $\exists x(P(x) \Rightarrow Q(x)), \exists x P(x)$ it does *not* follow that $\exists x Q(x)$. The snag is that if c is an object that does *not* have property P, then c trivially satisfies $P(c) \Rightarrow Q(c)$. But this situation is consistent with $\neg Q(c)$.

3.26 Given: $\forall x \exists y(x\mathbf{R}y), \forall x \forall y(x\mathbf{R}y \Rightarrow y\mathbf{R}x), \forall x \forall y \forall z(x\mathbf{R}y \wedge y\mathbf{R}z \Rightarrow x\mathbf{R}z)$.
To be proved: $\forall x(x\mathbf{R}x)$.
Proof:
Let c be arbitrary. Then from the given $\forall x \exists y(x\mathbf{R}y)$ we get $\exists y(c\mathbf{R}y)$.
Let d be such that $c\mathbf{R}d$. Then from this and the given $\forall x \forall y(x\mathbf{R}y \Rightarrow y\mathbf{R}x)$, we get $d\mathbf{R}c$.
From $c\mathbf{R}d$, $d\mathbf{R}c$, and the given $\forall x \forall y \forall z(x\mathbf{R}y \wedge y\mathbf{R}z \Rightarrow x\mathbf{R}z)$, we get $c\mathbf{R}c$.
Thus ($\forall$ introduction) $\forall x(x\mathbf{R}x)$.

3.27.1 Given: $\forall x \forall y \forall z(x\mathbf{R}y \wedge y\mathbf{R}z \Rightarrow x\mathbf{R}z), \forall x \neg x\mathbf{R}x$.
To be proved: $\forall x \forall y(x\mathbf{R}y \Rightarrow \neg y\mathbf{R}x)$.
Proof:
Let c, d be arbitrary objects such that $c\mathbf{R}d$. We have to show that $\neg d\mathbf{R}c$.
Suppose $d\mathbf{R}c$. Then from $c\mathbf{R}d$, $d\mathbf{R}c$ and the first given, $c\mathbf{R}c$.
Contradiction with the second given.
Thus $\neg d\mathbf{R}c$.
Thus $\forall x \forall y(x\mathbf{R}y \Rightarrow \neg y\mathbf{R}x)$.

3.27.2 Given: $\forall x \forall y(x\mathbf{R}y \Rightarrow \neg y\mathbf{R}x)$.
To be proved: $\forall x \neg x\mathbf{R}x$.
Proof:
Let c be arbitrary object. We have to show that $\neg c\mathbf{R}c$.
Suppose $c\mathbf{R}c$. Then with the given, $\neg c\mathbf{R}c$, and contradiction. Thus $\neg c\mathbf{R}c$.
Thus $\forall x \neg x\mathbf{R}x$.

3.27.3 Given: $\forall x \forall y(x\mathbf{R}y \wedge x \neq y \Rightarrow \neg y\mathbf{R}x)$.
To be proved: $\forall x \forall y(x\mathbf{R}y \wedge y\mathbf{R}x \Rightarrow x = y)$.
Proof:
Let c and d be arbitrary objects with $c\mathbf{R}d$ and $d\mathbf{R}c$. We have to show that $c = d$.
Suppose $c \neq d$. Then from this, $c\mathbf{R}d$, and the given, $\neg d\mathbf{R}c$, and contradiction. Thus $c = d$.
Thus $\forall x \forall y(x\mathbf{R}y \wedge y\mathbf{R}x \Rightarrow x = y)$.

3.27.4 Given: $\forall x \neg x\mathbf{R}x, \forall x \forall y(x\mathbf{R}y \Rightarrow y\mathbf{R}x), \forall x \forall y \forall z(x\mathbf{R}y \wedge y\mathbf{R}z \Rightarrow x\mathbf{R}z)$.
To be proved: $\neg \exists x \exists y(x\mathbf{R}y)$.
Proof:
Suppose $\exists x \exists y(x\mathbf{R}y)$, e.g., $c\mathbf{R}d$.

Then from this and the second given, $d\mathbf{R}c$.
From $c\mathbf{R}d$ and $d\mathbf{R}c$, with the third given, $c\mathbf{R}c$, and contradiction with the first given.
So $\neg\exists x\exists y(x\mathbf{R}y)$.

3.28 Given: $\forall y\exists z\forall x P(x,y,z)$.
To be proved: $\forall x\forall y\exists z P(x,y,z)$.
Proof:
Let c, d be arbitrary. We have to show that $\exists z P(c,d,z)$.
From the given, $\exists z\forall x P(x,d,z)$.
Let e be such that $\forall x P(x,d,e)$. Then $P(c,d,e)$.
Thus $\exists z P(c,d,z)$.

3.31.1 The equivalences $\forall x\forall y\Phi(x,y) \equiv \forall y\forall x\Phi(x,y)$ and $\exists x\exists y\Phi(x,y) \equiv \exists y\exists x\Phi(x,y)$ are straightforward. As an example, we prove that $\forall x\forall y\Phi(x,y) \Rightarrow \forall y\forall x\Phi(x,y)$.

Given: $\forall x\forall y\Phi(x,y)$.
To be proved: $\forall y\forall x\Phi(x,y)$
Proof:
Let y be arbitrary. We have to show that $\forall x\Phi(x,y)$.
Let x be arbitrary. We have to show that $\Phi(x,y)$.
This is immediate from the given.
Therefore $\forall x\Phi(x,y)$.
Therefore $\forall y\forall x\Phi(x,y)$.

3.31.2 As an example, we prove $\exists x\neg\Phi(x) \Rightarrow \neg\forall x\Phi(x)$.

To be proved: $\exists x\neg\Phi(x) \Rightarrow \neg\forall x\Phi(x)$.
Proof:
Suppose $\exists x\neg\Phi(x)$. We have to show that $\neg\forall x\Phi(x)$.
Assume $\forall x\Phi(x)$. Then from the given, there is an a with $\neg\Phi(a)$.
From the assumption $\Phi(a)$. Contradiction.
Therefore $\neg\forall x\Phi(x)$.
Thus $\exists x\neg\Phi(x) \Rightarrow \neg\forall x\Phi(x)$.

3.31.3 As an example, we prove $\forall x(\Phi(x) \wedge \Psi(x)) \equiv (\forall x\Phi(x) \wedge \forall x\Psi(x))$.

To be proved: $\forall x(\Phi(x) \wedge \Psi(x)) \equiv (\forall x\Phi(x) \wedge \forall x\Psi(x))$.
Proof:
$\Rightarrow$: Assume $\forall x(\Phi(x) \wedge \Psi(x))$.
We have to show that $\forall x\Phi(x) \wedge \forall x\Psi(x)$.
Let x be arbitrary. Then from the assumption, $\Phi(x) \wedge \Psi(x)$. Thus $\Phi(x)$ and $\Psi(x)$.
This proves $\forall x\Phi(x)$ and $\forall x\Psi(x)$. Thus $\forall x\Phi(x) \wedge \forall x\Psi(x)$.
$\Leftarrow$: Assume $\forall x\Phi(x) \wedge \forall x\Psi(x)$.
We have to show that $\forall x(\Phi(x) \wedge \Psi(x))$.
Let x be arbitrary. Then from the assumption, $\Phi(x)$ and $\Psi(x)$. Thus $\Phi(x) \wedge \Psi(x)$.
This proves $\forall x(\Phi(x) \wedge \Psi(x))$.

3.32

Restricted universal quantifier introduction:

Given: ...
To be proved: $\forall x \in A\ \Phi(x)$.
Proof:
What is to be proved is equivalent to $\forall x(x \in A \Rightarrow \Phi(x))$.
Let x be arbitrary. We now have to prove that $x \in A \Rightarrow \Phi(x)$.
Assume $x \in A$.
To show: $\Phi(x)$.
Proof: ...
Thus $\forall x \in A\ \Phi(x)$.

Restricted universal quantifier elimination:

Given: $\forall x \in A\ \Phi(x)$, $t \in A$.
The first given is equivalent to $\forall x(x \in A \Rightarrow \Phi(x))$.
So it follows that for any t we have that $t \in A \Rightarrow \Phi(t)$.
Therefore, from the givens $\forall x \in A\ \Phi(x)$, $t \in A$, it follows that $\Phi(t)$.

Restricted existential quantifier introduction:

Given: $t \in A$ and $\Phi(t)$. To be proved: $\exists x \in A \Phi(x)$.
Proof:
What is to be proved is equivalent to $\exists x(x \in A \wedge \Phi(x))$.
This follows from the given $t \in A$ and $\Phi(t)$.

Restricted existential quantifier elimination:

Given: $\exists x \in A \Phi(x)$.
To be proved: P.
Proof:
The given is equivalent to $\exists x(x \in A \wedge \Phi(x))$.
Suppose c is an object that satisfies $(c \in A \wedge \Phi(c))$.
So suppose $c \in A$ is an object that satisfies $\Phi(c)$.
To be proved: P.
Proof: ...
Thus P.

3.34 To be proved: $A = \{4n + 3 \mid n \in \mathbb{N}\}$ contains infinitely many prime numbers.
Proof: A variation on Euclid's proof of the infinity of primes works.
Assume that there are only finitely many prime numbers in A.
I.e., assume that $\{p_1, \ldots, p_k\}$ is the set of all prime numbers in A,
and consider $N = 4p_1 \cdots p_k - 1 = 4(p_1 \cdots p_k - 1) + 3$.
If N is prime, we have a contradiction with the assumption, and the result follows.
Otherwise, N has a prime factor q, different from all the p_i.
This is because each of the p_i divides N with a remainder -1.

If q has form $4n+3$, then done, so suppose q has form $4n+1$.
Since $(4a+1)(4b+1)$ has the form $(4c+1)$, we know that $\frac{N}{q}$ has form $4n+3$.
Also, $\frac{N}{q}$ has a prime factor q_1.
After a finite number of steps this will yield a prime factor q_i of the form $4n+3$,
with $q_i \neq p_1, \ldots, p_k$.

3.36 To be proved: if n is composite, then $2^n - 1$ is composite as well.
Proof: Assume there are $a, b \in \mathbb{N}$ with $n = ab$. Let $x = 2^b - 1$ and $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$.
Then $xy = (2^b - 1)(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) =$

$$\begin{array}{ccccccccccc} & & & 2^b & + & 2^{2b} & + & \cdots & + & 2^{(a-1)b} & + & 2^{ab} \\ - & 1 & - & 2^b & - & 2^{2b} & - & \cdots & - & 2^{(a-1)b} & & \end{array}$$

So $xy = 2^{ab} - 1$. In other words, $xy = 2^n - 1$, and $2^n - 1$ is composite.

3.38

```
fasterprimes :: [Integer]
fasterprimes = 2 : sieve oddsFrom3
```

3.39

```
examples = [ take n primes | n <- [0..],
                             not (prime (product (take n primes) + 1)) ]
```

This generates:

```
[[2,3,5,7,11,13],
 [2,3,5,7,11,13,17],
 [2,3,5,7,11,13,17,19],
 [2,3,5,7,11,13,17,19,23],
 [2,3,5,7,11,13,17,19,23,29],
 [2,3,5,7,11,13,17,19,23,29,31,37],
 [2,3,5,7,11,13,17,19,23,29,31,37,41],
 [2,3,5,7,11,13,17,19,23,29,31,37,41,43],
 [2,3,5,7,11,13,17,19,23,29,31,37,41,43,47],
 [2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53],
 [2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59],
 [2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61]
  ...
```

3.41 To be proved: For all $n \in \mathbb{N}$: if $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect.
Proof:
Let $n \in \mathbb{N}$, with $2^n - 1$ prime. Then the proper divisors of $2^{n-1}(2^n - 1)$ are

$$1, 2, 2^2, \ldots, 2^{n-1}, 2^n - 1, 2(2^n - 1), 2^2(2^n - 1), \ldots, 2^{n-2}(2^n - 1).$$

Observe that $1 + (1 + 2 + 2^2 + \cdots + 2^{n-1}) = 2^n$, so $A = 1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$.
Next, observe that

$$B = (2^n - 1) + 2(2^n - 1) + 2^2(2^n - 1) + \cdots + 2^{n-2}(2^n - 1) = (1 + 2 + 2^2 + \cdots + 2^{n-2})(2^n - 1).$$

By the same observation as above, we see that $1 + 2 + 2^2 + \cdots + 2^{n-2} = 2^{n-1} - 1$. Therefore, the sum of the proper divisors of $2^{n-1}(2^n - 1)$ equals

$$\begin{aligned} A + B &= (2^n - 1) + (1 + 2 + 2^2 + \cdots + 2^{n-2})(2^n - 1) \\ &= (2^n - 1) + (2^{n-1} - 1)(2^n - 1) = 2^{n-1}(2^n - 1), \end{aligned}$$

which proves that $2^{n-1}(2^n - 1)$ is perfect.

3.42 We will prove that $(3, 5, 7)$ is the only prime triple.
Any prime triple different from $(3, 5, 7)$ has the form $(n, n + 2, n + 4)$, with $3 \nmid n$.
There are two cases to consider.

Case 1. There is an $a \in \mathbb{N}$ with $n = 3a + 1$.
In this case $n + 2 = 3a + 3 = 3(a + 1)$, so $n + 2$ is not a prime.

Case 2. There is an $a \in \mathbb{N}$ with $n = 3a + 2$.
In this case $n + 4 = 3a + 6 = 3(a + 2)$, so $n + 4$ is not a prime.

In either case, $(n, n + 2, n + 4)$ is not a prime triple.

3.43 Any prime greater than 3 has the form $3q + 1$ or $3q + 2$. If $p = 3q + 1$ then $p^2 + 2 = (3q + 1)^2 + 2 = 9q^2 + 6q + 3 = 3(3q^2 + 2q + 1)$, which means that $p^2 + 2$ is composite. If $p = 3q + 2$ then $p^2 + 2 = (3q + 2)^2 + 2 = 9q^2 + 12q + 6 = 3(3q^2 + 4q + 2)$, which means that $p^2 + 2$ is composite in this case as well.

Solutions to Exercises from Chapter 4

```
module Sol4

where

import STAL
import Data.List
import SetEq
```

4.2 To be proved: $A \supseteq A$.
Proof: same as the proof of $A \subseteq A$.

To be proved: $A \supseteq B \wedge B \supseteq A \Longrightarrow A = B$.
Proof: note that $A \supseteq B \wedge B \supseteq A \Longrightarrow A = B$ is equivalent to $B \supseteq A \wedge A \supseteq B \Longrightarrow A = B$,
which is in turn equivalent to $A \subseteq B \wedge B \subseteq A \Longrightarrow A = B$, which is extensionality again.

To be proved: $A \supseteq B \wedge B \supseteq C \Longrightarrow A \supseteq C$.
This is equivalent to $B \subseteq A \wedge C \subseteq B \Longrightarrow C \subseteq A$,
which is in turn equivalent to $C \subseteq B \wedge B \subseteq A \Longrightarrow C \subseteq A$,
i.e., transitivity of $\subseteq$, and same proof as before.

4.4 To be proved: $\{\{1,2\},\{0\},\{2,1\}\} = \{\{0\},\{1,2\}\}$.
Proof:
$\subseteq$: $\{1,2\} \in \{\{0\},\{1,2\}\}$, $\{0\} \in \{\{0\},\{1,2\}\}$, and $\{2,1\} \in \{\{0\},\{1,2\}\}$,
since $\{1,2\} = \{2,1\}$ because $\{1,2\}$ and $\{2,1\}$ have the same elements.
$\supseteq$: $\{0\} \in \{\{1,2\},\{0\},\{2,1\}\}$ and $\{1,2\} \in \{\{1,2\},\{0\},\{2,1\}\}$.

4.7 Given: A is a set of sets.
To be proved: $\{x \in A \mid x \notin x\} \notin A$.
Proof:
Let $B := \{x \in A \mid x \notin x\}$, and assume $B \in A$.
Suppose $B \in B$. Then, from the definition of B, $B \notin B$, and contradiction.

Suppose $B \notin B$. Then, since $B \in A$ and $B \notin B$, $B \in B$, and contradiction again.
Therefore $\{x \in A \mid x \notin x\} \notin A$.

4.8 If we check the type of `elem`, we find: `elem :: Eq a => a -> [a] -> Bool`. This means that `elem` takes an object of any type `a` for which `==` is defined as first argument, a list over the same type as second argument, and produces a truth value. Therefore, the first argument of `elem` constrains the type of list that is needed for a second argument. If `elem` is called with `elem 1 1`, then the second argument is a numeral (an object of class `Num`), while the argument that is needed is a list argument `[a]`. The error message expresses that the type of the second argument in the call does not match the type for the second argument that Haskell infers from the type of `elem`.

4.10.1 To be proved: $\{a\} = \{b\}$ iff $a = b$.
Proof:
$\Rightarrow$: Suppose $\{a\} = \{b\}$.
Then $\{a\}$ and $\{b\}$ have the same elements, so $a = b$.
$\Leftarrow$: Suppose $a = b$.
Then $\forall x(x \in \{a\} \Leftrightarrow x \in \{b\})$.
Therefore, by extensionality, $\{a\} = \{b\}$.

4.10.2 To be proved: $\{a_1, a_2\} = \{b_1, b_2\}$ iff $a_1 = b_1 \wedge a_2 = b_2$, or $a_1 = b_2 \wedge a_2 = b_1$.
Proof:
$\Rightarrow$: Suppose $\{a_1, a_2\} = \{b_1, b_2\}$.
We show that $a_1 = b_1 \wedge a_2 = b_2$ or $a_1 = b_2 \wedge a_2 = b_1$.
Assume not $(a_1 = b_1 \wedge a_2 = b_2)$.
To show: $a_1 = b_2 \wedge a_2 = b_1$.
The assumption is equivalent to $a_1 \neq b_1 \vee a_2 \neq b_2$.
Case 1: $a_1 \neq b_1$.
Then since $a_1 \in \{b_1, b_2\}$ (from the given), $a_1 = b_2$.
Since $b_1 \in \{a_1, a_2\}$ (again from the given), $a_2 = b_1$.
Case 2: $a_2 \neq b_2$.
Since $b_2 \in \{a_1, a_2\}$ (from the given), $a_1 = b_2$.
Then since $a_2 \in \{b_1, b_2\}$ (from the given), $a_2 = b_1$.
This proves $a_1 = b_2 \wedge a_2 = b_1$.
$\Leftarrow$: Suppose $a_1 = b_1 \wedge a_2 = b_2$, or $a_1 = b_2 \wedge a_2 = b_1$.
To show: $\{a_1, a_2\} = \{b_1, b_2\}$.
$\subseteq$:
Suppose $a_1 = b_1 \wedge a_2 = b_2$.
Then $a_1 \in \{b_1, b_2\}$ and $a_2 \in \{b_1, b_2\}$, so $\{a_1, a_2\} \subseteq \{b_1, b_2\}$.
Suppose $a_1 = b_2 \wedge a_2 = b_1$.
Then $a_1 \in \{b_1, b_2\}$ and $a_2 \in \{b_1, b_2\}$, so $\{a_1, a_2\} \subseteq \{b_1, b_2\}$.
$\supseteq$:
Suppose $a_1 = b_1 \wedge a_2 = b_2$.
Then $b_1 \in \{a_1, a_2\}$ and $b_2 \in \{a_1, a_2\}$, so $\{a_1, a_2\} \supseteq \{b_1, b_2\}$.
Suppose $a_1 = b_2 \wedge a_2 = b_1$.
Then $b_1 \in \{a_1, a_2\}$ and $b_2 \in \{a_1, a_2\}$, so $\{a_1, a_2\} \supseteq \{b_1, b_2\}$.

4.11 $\emptyset \neq \{\emptyset\}$, for $\emptyset$ has no elements, while $\{\emptyset\}$ has one element, namely $\emptyset$.

$\{\emptyset\} \neq \{\{\emptyset\}\}$, for although both $\{\emptyset\}$ and $\{\{\emptyset\}\}$ are singletons, the elements they contain are different, because, as we have seen, $\emptyset \neq \{\emptyset\}$.

4.13 The type of the set difference operator $-$ is $s \to s \to s$. The type for the inclusion operator $\subseteq$ is $s \to s \to t$.

4.14

1. $x \in \{x \mid E(x)\} \ :: \ t$.
2. $\{x \mid E(x)\} \ :: \ s$.
3. $(A \cap B) \subseteq C \ :: \ t$.
4. $(A \cup B) \cap C \ :: \ s$.
5. $\forall x(x \in A \Rightarrow x \in B) \ :: \ t$.
6. $A = B \ :: \ t$.
7. $a \in A \Leftrightarrow a \in B \ :: \ t$.

4.17.1 To show that $A \not\subseteq B$ iff $A - B \neq \emptyset$, we rewrite the two sides as logical formulas. For $A \not\subseteq B$, this gives $\neg\forall x(x \in A \Rightarrow x \in B)$. For $A - B \neq \emptyset$, this gives: $\exists x(x \in A \wedge x \notin B)$. That these two formulas are equivalent can be seen from the quantifier rules in Chapter 2.

4.17.2 Compare the formula for $A \cap B$ with that for $A-(A-B)$: $x \in A \wedge x \in B$ versus $x \in A \wedge \neg(x \in A \wedge x \notin B)$. Formula $\neg(x \in A \wedge x \notin B)$ is equivalent to $x \notin A \vee x \in B$, and this in turn to $x \in A \Rightarrow x \in B$. Thus, $x \in A \wedge \neg(x \in A \wedge x \notin B)$ is equivalent to $x \in A \wedge x \in B$.

4.19 With the distributivity law for $\cap$, we get that

$$(A \cup B) \cap (C \cup D) = ((A \cup B) \cap C) \cup ((A \cup B) \cap D).$$

By $\cap$ commutativity we get:

$$((A \cup B) \cap C) \cup ((A \cup B) \cap D) = (C \cap (A \cup B)) \cup (D \cap (A \cup B)).$$

Using $\cap$ distributivity to rewrite $C \cap (A \cup B))$ and $D \cap (A \cup B)$, we get:

$$(C \cap (A \cup B)) \cup (D \cap (A \cup B)) = (C \cap A) \cup (C \cap B) \cup (D \cap A) \cup (D \cap B).$$

4.21 Immediate from the propositional validities $P \oplus Q \equiv (P \wedge \neg Q) \vee (Q \wedge \neg P)$ and $P \oplus Q \equiv (P \vee Q) \wedge \neg(P \wedge Q)$. The truth table checks are left to the reader.

4.23 Given: X has at least two elements.
To be proved: $\subseteq$ on $\wp(X)$ is not linear.
Proof:
We have to show that there are $A, B \in \wp(X)$ with $A \not\subseteq B$ and $B \not\subseteq A$.
Let a, b be arbitrary elements of X, with $a \neq b$ (from the given).
Define $A := \{a\}$ and $B := \{b\}$.
Then $A, B \in \wp(X)$. Because of $a \notin B$, we have $A \not\subseteq B$. Because of $b \notin A$, we have $B \not\subseteq A$.

4.26 The translation of $\cap\mathcal{F} \subseteq \cup\mathcal{G}$ is: $\forall x(\forall y(y \in \mathcal{F} \Rightarrow x \in y) \Rightarrow \exists z(z \in \mathcal{G} \wedge x \in z))$.

4.27 We show that $A = \cup\mathcal{F}$ fits the bill.

Given: $A = \cup\mathcal{F}$.
To be proved: $\mathcal{F} \subseteq \wp(A)$.
Proof:
Assume that X is an arbitrary element of $\mathcal{F}$.
Then $X \subseteq \cup\mathcal{F}$, so $X \in \wp(A)$.
This establishes $\mathcal{F} \subseteq \wp(A)$.

Given: $A = \cup\mathcal{F}$.
To be proved: For all sets B: if $\mathcal{F} \subseteq \wp(B)$ then $A \subseteq B$.
Proof:
Let B be an arbitrary set.
Suppose $\mathcal{F} \subseteq \wp(B)$.
To show: $A \subseteq B$.
Let x be an arbitrary element of A.
To show: $x \in B$.
By the definition of A we get from $x \in A$ that there is an $X \in \mathcal{F}$ with $x \in X$.
By $\mathcal{F} \subseteq \wp(B)$, $X \subseteq B$. Therefore, $x \in B$.
Thus, $A \subseteq B$.

4.29
$(A^c)^c = A$, for $x \in (A^c)^c \Leftrightarrow x \notin A^c \Leftrightarrow x \in A$.
$X^c = \emptyset$, for $x \in X^c \Leftrightarrow x \in X \wedge x \notin X \Leftrightarrow x \in \emptyset$.
$\emptyset^c = X$, for $x \in \emptyset^c \Leftrightarrow x \in X \wedge x \notin \emptyset \Leftrightarrow x \in X$.
$A \cup A^c = X$, for $x \in A \cup A^c \Leftrightarrow (x \in A \wedge x \in X) \vee (x \notin A \wedge x \in X) \Leftrightarrow x \in X$.
$A \cap A^c = \emptyset$, for $x \in A \cap A^c \Leftrightarrow x \in A \wedge x \notin A \Leftrightarrow x \in \emptyset$.
$A \subseteq B \Leftrightarrow B^c \subseteq A^c$, for $\forall x(x \in A \Rightarrow x \in B) \Leftrightarrow \forall x(x \notin B \Rightarrow x \notin A)$.
$(A \cap B)^c = A^c \cup B^c$, for:

$$\begin{array}{lcl} x \in (A \cap B)^c & \Leftrightarrow & \neg(x \in A \cap B) \\ & \Leftrightarrow & \neg(x \in A \wedge x \in B) \\ & \overset{*}{\Leftrightarrow} & x \notin A \vee x \notin B \\ & \Leftrightarrow & x \in A^c \vee x \in B^c \\ & \Leftrightarrow & x \in A^c \cup B^c, \end{array}$$

where again, the step $(*)$ is justified by one of the De Morgan laws of propositional reasoning.

4.30.1 $\wp(\emptyset) = \{\emptyset\}$, $\wp\wp(\emptyset) = \wp(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$, $\wp\wp\wp(\emptyset) = \wp(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.

4.30.2 We see from the above that $|\wp(\emptyset)| = 1$, $|\wp^2(\emptyset)| = 2$, $|\wp^3(\emptyset)| = 4$. Since the elements of $\wp^{n+1}(\emptyset)$ are the subsets of $\wp^n(\emptyset)$, we know that $|\wp^4(\emptyset)| = 2^4 = 16$, and $|\wp^5(\emptyset)| = 2^{16} = 65536$.

4.30.3 Suppose A has n elements. Since the elements of $\wp(A)$ are the subsets of A, how many different subsets does A have? To fully determine an arbitrary subset B of A, we have to decide for each of the n elements of A whether to put it in B or not. There are 2^n possible ways of doing this. Thus $|\wp(A)| = 2^n$.

4.31 This is true, for here is a proof.
Given: $\wp(A) = \wp(B)$.
To be proved: $A = B$.
Proof:
$\subseteq$: Let $x \in A$. Then $\{x\} \in \wp(A)$, so by the given, $\{x\} \in \wp(B)$, and thus $x \in B$.
$\supseteq$: Let $x \in B$. Then $\{x\} \in \wp(B)$, so by the given, $\{x\} \in \wp(A)$, and thus $x \in A$.

4.32.1 The proof poses no problem.
To be proved: $\wp(A \cap B) = \wp(A) \cap \wp(B)$.
Proof:
$\subseteq$: Let $X \in \wp(A \cap B)$. Then $X \subseteq A \cap B$, i.e., $X \subseteq A$ and $X \subseteq B$.
It follows that $X \in \wp(A)$ and $X \in \wp(B)$, and therefore $X \in \wp(A) \cap \wp(B)$.
$\supseteq$: Let $X \in \wp(A) \cap \wp(B)$. Then $X \in \wp(A)$ and $X \in \wp(B)$, i.e., $X \subseteq A$ and $X \subseteq B$.
It follows that $X \subseteq A \cap B$, and therefore $X \in \wp(A \cap B)$.

4.32.2 During the proof attempt of the left to right inclusion (the case $\wp(A \cup B) \subseteq \wp(A) \cup \wp(B)$) we get stuck, for the assumption that $X \in \wp(A \cup B)$ does yield that $X \subseteq A \cup B$, but from this we cannot draw the conclusion that $X \subseteq A$ or $X \subseteq B$.

Indeed, look at the example $A = \{1, 2\}$ and $B = \{2, 3\}$. Then $\{1, 3\} \subseteq A \cup B$ but $\{1, 3\} \not\subseteq A$, and $\{1, 3\} \not\subseteq B$. This provides a counterexample to $\wp(A \cup B) \subseteq \wp(A) \cup \wp(B)$. Note that the inclusion in the other direction still holds, for the following proof works:

To be proved: $\wp(A \cup B) \supseteq \wp(A) \cup \wp(B)$.
Proof:
Let $X \in \wp(A) \cup \wp(B)$. Then $X \in \wp(A)$ or $X \in \wp(B)$, i.e., $X \subseteq A$ or $X \subseteq B$.
It follows that $X \subseteq A \cup B$, and therefore $X \in \wp(A \cup B)$.

4.33.1 To be proved: $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$.
Proof:
$\subseteq$: Assume $x \in B \cap (\bigcup_{i \in I} A_i)$.
To show: $x \in \bigcup_{i \in I} (B \cap A_i)$.
From the assumption, $x \in B$, and $x \in \bigcup_{i \in I} A_i$.
Thus, $x \in B$ and there is an $i \in I$ with $x \in A_i$.
Thus, there is an $i \in I$ with $x \in B \cap A_i$, i.e., $x \in \bigcup_{i \in I} (B \cap A_i)$.
$\supseteq$: Assume $x \in \bigcup_{i \in I} (B \cap A_i)$
To show: $x \in B \cap (\bigcup_{i \in I} A_i)$.
From the assumption, there is an $i \in I$ with $x \in B \cap A_i$.
Thus, $x \in B$ and $x \in A_i$ for some $i \in I$.
Therefore, $x \in B$ and $x \in \bigcup_{i \in I} A_i$. Thus, $x \in B \cap (\bigcup_{i \in I} A_i)$.

4.33.2 To be proved: $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$.
Proof:

$\subseteq$: Assume $x \in B \cup (\bigcap_{i\in I} A_i)$.
To show: $x \in \bigcap_{i\in I}(B \cup A_i)$.
From the assumption, $x \in B$ or $x \in \bigcap_{i\in I} A_i$.
Thus, $x \in B$ or for all $i \in I$ $x \in A_i$.
Thus, for all $i \in I$ we have $x \in B \cup A_i$, i.e., $x \in \bigcap_{i\in I}(B \cup A_i)$.
$\supseteq$: Assume $x \in \bigcap_{i\in I}(B \cup A_i)$
To show: $x \in B \cup (\bigcap_{i\in I} A_i)$.
From the assumption, for all $i \in I$ we have $x \in B \cup A_i$.
Thus, $x \in B$ or $x \in A_i$ for all $i \in I$.
Therefore, $x \in B$ or $x \in \bigcap_{i\in I} A_i$. Thus, $x \in B \cup (\bigcap_{i\in I} A_i)$.

4.33.3 Given: For all $i \in I$, $A_i \subseteq X$.
To be proved: $(\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} A_i^c$.
$\subseteq$: Assume $x \in (\bigcup_{i\in I} A_i)^c$.
To show: $x \in \bigcap_{i\in I} A_i^c$.
From the assumption, $x \in X$ and $x \notin \bigcup_{i\in I} A_i$. Then there is no $i \in I$ with $x \in A_i$.
Therefore, for all $i \in I$ it holds that $x \in A_i^c$, i.e., $x \in \bigcap_{i\in I} A_i^c$.
$\supseteq$: Assume $x \in \bigcap_{i\in I} A_i^c$.
To show: $x \in (\bigcup_{i\in I} A_i)^c$.
From the assumption, it holds for all $i \in I$ that $x \in A_i^c$.
Therefore, there is no $i \in I$ with $x \in A_i$, i.e., $x \notin \bigcup_{i\in I} A_i$. Thus, $x \in (\bigcup_{i\in I} A_i)^c$.

4.33.4 Given: For all $i \in I$, $A_i \subseteq X$.
To be proved: $(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c$.
$\subseteq$: Assume $x \in (\bigcap_{i\in I} A_i)^c$.
To show: $x \in \bigcup_{i\in I} A_i^c$.
From the assumption, $x \in X$ and $x \notin \bigcap_{i\in I} A_i$. Then there is an $i \in I$ with $x \notin A_i$.
Therefore, for some $i \in I$ it holds that $x \in A_i^c$, i.e., $x \in \bigcup_{i\in I} A_i^c$.
$\supseteq$: Assume $x \in \bigcup_{i\in I} A_i^c$.
To show: $x \in (\bigcap_{i\in I} A_i)^c$.
From the assumption, it holds for some $i \in I$ that $x \in A_i^c$.
Therefore, there is an $i \in I$ with $x \notin A_i$, i.e., $x \notin \bigcap_{i\in I} A_i$. Thus, $x \in (\bigcap_{i\in I} A_i)^c$.

4.34 To be proved: Any sequence of sets $A_0, A_1, \ldots$ with $\wp(A_{i+1}) \subseteq A_i$ is finite.
Proof:
Assume there exists an infinite sequence of sets $A_0, A_1, \ldots$ with for all $i \in \mathbb{N}$, $\wp(A_{i+1}) \subseteq A_i$.
Then we can show that $\wp(\bigcap_{i\in\mathbb{N}} A_i) \subseteq \bigcap_{i\in\mathbb{N}} A_i$.
Indeed, let $X \in \wp(\bigcap_{i\in\mathbb{N}} A_i)$ be arbitrary.
Then $X \subseteq \bigcap_{i\in\mathbb{N}} A_i$.
We show that $X \in A_i$ for all $i \in \mathbb{N}$.
Let $k \in \mathbb{N}$ be arbitrary.
Then $X \subseteq A_{k+1}$, and from $\wp(A_{k+1}) \subseteq A_k$ we get that $X \in A_k$.
It follows that $B = \bigcap_{i\in\mathbb{N}} A_i$ has the property $\wp(B) \subseteq B$, i.e., every subset of B is an element of B.
In particular, the subset $\{x \in B \mid x \notin x\}$ has to be an element of B.
This gives a contradiction with what was established in Exercise 4.7.

4.35 Given: a collection $\mathcal{K}$ of sets satisfying the condition $\forall A \in \mathcal{K}(A = \emptyset \vee \exists B \in \mathcal{K}(A = \wp(B)))$.
To be proved: every element of $\mathcal{K}$ has the form $\wp^n(\emptyset)$ for some $n \in \mathbb{N}$.
Proof:
Let $A_0 \in \mathcal{K}$ be arbitrary.
From the previous exercise we know that any sequence $A_0, A_1, \ldots$ with $\wp(A_{i+1}) \subseteq A_i$ is finite.
Applying this to the sequence $A_0, A_1, \ldots$ where $\wp(A_{i+1}) = A_i$ we get from the condition on $\mathcal{K}$,
this gives an $n \in \mathbb{N}$, and a sequence $A_0, \ldots, A_n$,
with $\forall i < n\ \wp(A_{i+1}) = A_i$, and for no B, $\wp(B) \subseteq A_n$.
In particular $\wp(\emptyset) \not\subseteq A_n$, i.e., $\emptyset \notin A_n$.
From $A_n \in \mathcal{K}$ and $\emptyset \notin A_n$ we get $A_n = \emptyset$. But then $A_0 = \wp^n(\emptyset)$.

4.39 Left to the reader.

4.40 Given: $A \neq \emptyset$, $B \neq \emptyset$, $A \times B = B \times A$.
To be proved: $A = B$.
Proof:
$\subseteq$: Let $x \in A$ be arbitrary. Since $B \neq \emptyset$ there is an $y \in B$,
and we can consider the pair $(x, y) \in A \times B$.
From $A \times B = B \times A$, we get that $(x, y) \in B \times A$, and therefore $x \in B$.
$\supseteq$: Let $y \in B$ be arbitrary. Since $A \neq \emptyset$ there is an $x \in A$,
and we can consider the pair $(y, x) \in B \times A$.
From $A \times B = B \times A$, we get that $(y, x) \in A \times B$, and therefore $y \in A$.

The non-emptiness condition is necessary, for if $A = \emptyset$ and $B = \{1\}$, then $A \neq B$, but $A \times B = \emptyset = B \times A$.

4.41.1 Given: $\{a, b\} = \{a, c\}$.
To be proved: $b = c$.
Proof:
Suppose, for a contradiction, that $b \neq c$.
Assume $a \neq b$. Then $b \in \{a, b\}$, $b \notin \{a, c\}$, for $b \neq a$ and $b \neq c$.
Contradiction with the given.
Assume $a = b$. Then $c \in \{a, c\}$, $c \notin \{a, b\} = \{b\}$, for $c \neq b$.
Contradiction with the given.

4.41.2 Given: $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$.
To be proved: $a = x \wedge b = y$.
Proof:
Case 1: $a = b$. In this case, $\{a\} = \{a, b\}$, so from the given, $\{\{a\}\} = \{\{x\}, \{x, y\}\}$.
This gives $\{a\} = \{x\}$, and therefore $a = x$, and $\{a\} = \{x, y\}$, and therefore $a = b = y$.
Case 2: $a \neq b$. In this case, $\{a\} \neq \{a, b\}$, and $\{a, b\} \neq \{x\}$, for $\{a, b\}$ is not a singleton.
Thus, from the given, $\{a\} = \{x\}$, and therefore $a = x$.
Also, from the given, $\{a, b\} = \{x, y\}$, so from this and $a = x$ we get that $b = y$.

4.43 To see how the Haskell implementation of list equality accomplishes that lists of different length are classified as unequal, we distinguish two cases. In case there is a first position n with $\text{list}_1[n] \neq \text{list}_2[n]$, the matter is clear: at the n-th comparison, a call to `(x:xs) == (y:ys)` will yield `False`. Suppose therefore that we have two lists

$\text{list}_1, \text{list}_2$, with list_1 a proper prefix of list_2. In other words, list_1 has length k, and for all $i < k$, $\text{list}_1[i] = \text{list}_2[i]$. Then after k comparison steps we are at the end of list_1, but not at the end of list_2. In other words, we now process a call of the form `[] == (y:ys)`. This is the case that is covered by the catch-all phrase `_ == _ = False`, so in this case the test will yield `False`.

4.44 The definition could run like this:

$$\begin{aligned} L < K \quad :\equiv \quad & |L| < |K| \\ & \vee (|L| = |K| \\ & \quad \wedge \exists x, \text{xs}, y, \text{ys}\ (L = x : \text{xs} \wedge K = y : \text{ys} \wedge (x < y \vee (x = y \wedge \text{xs} < \text{ys})))). \end{aligned}$$

Here is an implementation:

```
compare' :: Ord a => [a] -> [a] -> Ordering
compare' [] [] = EQ
compare' (x:xs) (y:ys) | length (x:xs) < length (y:ys) = LT
                       | length (x:xs) > length (y:ys) = GT
                       | otherwise = compare (x:xs) (y:ys)
```

And here is how it compares with the standard implementation of `compare`:

```
Main> compare [1,3] [1,2,3]
GT
Main> compare' [1,3] [1,2,3]
LT
Main> compare [1,3] [1,2]
GT
Main> compare' [1,3] [1,2]
GT
```

4.45 When `init` is called with an empty list, we get an error message (for there is no equation to cover this case). If `init` is called with a non-empty list, the list is returned minus its last element.

4.46 Since `reverse` is predefined, we call our version `reverse'`.

```
reverse' :: [a] -> [a]
reverse' [] = []
reverse' (x:xs) = reverse' xs ++ [x]
```

4.47

```
splitList :: [a] -> [([a],[a])]
splitList [x,y] = [([x],[y])]
splitList (x:y:zs) = ([x],(y:zs)): addLeft x (splitList (y:zs))
   where addLeft u [] = []
         addLeft u ((vs,ws):rest) = (u:vs,ws): addLeft u rest
```

A neater version results when we avail ourselves of the `map` function:

```
split :: [a] -> [([a],[a])]
split [x,y] = [([x],[y])]
split (x:y:zs) =
    ([x],(y:zs)) : (map (\ (us,vs) -> ((x:us),vs)) (split (y:zs)))
```

4.48

```
q11 = [ y | (x,y) <- act, x == "Robert De Niro" || x == "Kevin Spacey"]
```

4.49

```
q12 = nub ([ y | ("Quentin Tarantino",y) <- act, releaseP (y,"1994") ]
       ++  [ y | ("Quentin Tarantino",y) <- direct, releaseP (y,"1994") ])
```

4.50

```
q13 = [ x | (x,y) <- release, y > "1997", not (actP ("William Hurt",x)) ]
```

4.51

```
difference :: Eq a => [a] -> [a] -> [a]
difference xs []  = xs
difference xs (y:ys) = difference (delete y xs) ys
```

4.53

```
genUnion :: Eq a => [[a]] -> [a]
genUnion [] = []
genUnion [xs] = xs
genUnion (xs:xss) = union xs (genUnion xss)

genIntersect :: Eq a => [[a]] -> [a]
genIntersect [] = error "list of lists should be non-empty"
genIntersect [xs] = xs
genIntersect (xs:xss) = intersect xs (genIntersect xss)
```

4.54

```
unionSet :: (Eq a) => Set a -> Set a -> Set a
unionSet (Set [])     set2  =  set2
unionSet (Set (x:xs)) set2  =
   insertSet x (unionSet (Set xs) (deleteSet x set2))
```

```
intersectSet :: (Eq a) => Set a -> Set a -> Set a
intersectSet (Set [])     set2  =  Set []
intersectSet (Set (x:xs)) set2
   | inSet x set2 = insertSet x (intersectSet (Set xs) set2)
   | otherwise    = intersectSet (Set xs) set2
```

```
differenceSet :: (Eq a) => Set a -> Set a -> Set a
differenceSet set1 (Set []) = set1
differenceSet set1 (Set (y:ys)) =
   differenceSet (deleteSet y set1) (Set ys)
```

4.55 `insertSet` will now have to insert an item at the right position to keep the underlying list sorted. This can be done in terms of an auxiliary function `insertList`, as follows:

```
insertSet :: (Ord a) => a -> Set a -> Set a
insertSet x (Set s) = Set (insertList x s)

insertList x [] = [x]
insertList x ys@(y:ys') = case compare x y of
                                GT -> y : insertList x ys'
                                EQ -> ys
                                _  -> x : ys
```

4.56 The only thing that is needed is a small patch in the function `showSet`, like this:

```
showSet []     str = showString "0" str
showSet (x:xs) str = showChar '' ( shows x ( showl xs str))
     where showl []     str = showChar '' str
           showl (x:xs) str = showChar ',' (shows x (showl xs str))
```

4.57.1 Assuming set A has N elements, and a curly braces representation with P pairs of braces. Then for $\wp(A)$ you need:

1. one new pair of outermost braces,
2. for each of the 2^N elements of $\wp(A)$ a pair of outermost braces,
3. each of the N elements of A occurs in half of the elements of $\wp(A)$, i.e., in 2^{N-1} elements of $\wp(A)$; for these we need $P-1$ brace pairs (all brace pairs of A, minus the outermost brace pair); all in all this gives $2^{N-1}(P-1)$ brace pairs.

Writing $\#$ for number of elements, and $\sharp$ for number of brace pairs, this gives:

$$\begin{array}{lll}
V_0 = \emptyset & \#(V_0) = 0 & \sharp(V_0) = 1 \\
V_1 = \wp(\emptyset) & \#(V_1) = 1 & \sharp(V_1) = 2 \\
V_2 = \wp^2(\emptyset) & \#(V_2) = 2 & \sharp(V_2) = 4 \\
V_3 = \wp^3(\emptyset) & \#(V_3) = 4 & \sharp(V_3) = 11 \\
V_4 = \wp^4(\emptyset) & \#(V_4) = 16 & \sharp(V_4) = 1 + 16 + 8 \times 10 = 97 \\
V_5 = \wp^5(\emptyset) & \#(V_5) = 2^{16} = 65536 & \sharp(V_5) = 1 + 2^{16} + 2^{15} \times 96 = 3211265
\end{array}$$

4.57.2 Assume N is the number of elements of A, and E the number of occurrences of $\emptyset$ in the standard representation of A. Then $\wp(A)$ has $2^{N-1}E+1$ occurrences of $\emptyset$, since each element of A occurs in half of the elements of $\wp(A)$, and we need one extra occurrence of $\emptyset$ for the empty subset of A. Writing $\flat$ for the number of occurrences

of $\emptyset$, this gives:

$$\begin{array}{lll}
V_0 = \emptyset & \#(V_0) = 0 & \flat(V_0) = 1 \\
V_1 = \wp(\emptyset) & \#(V_1) = 1 & \flat(V_1) = 1 \\
V_2 = \wp^2(\emptyset) & \#(V_2) = 2 & \flat(V_2) = 2 \\
V_3 = \wp^3(\emptyset) & \#(V_3) = 4 & \flat(V_3) = 5 \\
V_4 = \wp^4(\emptyset) & \#(V_4) = 16 & \flat(V_4) = 8 \times 5 + 1 = 41 \\
V_5 = \wp^5(\emptyset) & \#(V_5) = 2^{16} = 65536 & \flat(V_5) = 2^{15} \times 41 + 1 = 1343489
\end{array}$$

4.57.3 The number of brace pairs in the standard representation equals the number of brace pairs in the representation where $\emptyset$ appears as $\{\}$ minus the number of occurrences of $\emptyset$ in the standard representation. Thus, the number we need is $\sharp(V_5) - \flat(V_5) = 3211265 - 1343489 = 1867776$.

Solutions to Exercises from Chapter 5

```
module Sol5

where

import SetOrd
import Data.List
import REL
```

5.13 To be proved: $\forall x\, \forall y\, \exists R\, (xRy)$.
Proof:
Let c, d be arbitrary objects. Consider the set $R = \{(c, d)\}$.
Then cRd. Thus, there is a relation R with cRd.

5.17 Given: $R \subseteq A^2$.
To be proved: $\forall x \neg xRx$ iff $\Delta_A \cap R = \emptyset$.
Proof:
only if: Suppose $\forall x \neg xRx$.
  Assume $(c, d) \in \Delta_A \cap R$. Then $c = d$, $c \in A$ and $(c, c) \in R$.
  Contradiction with $\forall x \neg xRx$.
if: Suppose $\Delta_A \cap R = \emptyset$.
  Assume cRc. Then, because $R \subseteq A^2$, $c \in A$.
  Therefore $(c, c) \in \Delta_A$, so $(c, c) \in \Delta_A \cap R$.
  Contradiction with $\Delta_A \cap R = \emptyset$.

5.19.1 It is easy to prove that $\forall x \forall y (xRy \Leftrightarrow yRx)$ follows from $\forall x \forall y (xRy \Rightarrow yRx)$, so that the two formulas are equivalent.

5.19.2 Note that $R \subseteq R^{-1}$ iff for arbitrary $(c, d) \in R$ it holds that $(c, d) \in R^{-1}$, i.e., that $(d, c) \in R$. This is equivalent to $\forall x \forall y (xRy \Rightarrow yRx)$. Similarly, note that $R = R^{-1}$ is equivalent to $\forall x \forall y (xRy \Leftrightarrow yRx)$. Next, use the previous item.

5.20 Given: $\forall x \forall y(xRy \Rightarrow \neg yRx)$.
To be proved: $\forall x \neg xRx$.
Proof:
Let c be an arbitrary object, and suppose, for a contradiction, that cRc.
Then from the given, $\neg cRc$, and contradiction. Thus $\neg cRc$.
Therefore $\forall x \neg xRx$.

5.22 Given: $\forall x \forall y(xRy \Rightarrow \neg yRx)$.
To be proved: $\forall x \forall y(xRy \wedge yRx \Rightarrow x = y)$.
Proof:
Let c, d be arbitrary, and assume cRd and dRc.
Then contradiction with the given.
Thus, trivially, $c = d$.

5.23 This follows from the fact that the formulas $\forall x, z \in A(\exists y \in A(xRy \wedge yRz) \Rightarrow xRz)$ and $\forall x, y, z \in A(xRy \wedge yRz) \Rightarrow xRz)$ are equivalent.

5.28 To show that every strict partial order is asymmetric one has to prove $\forall x \forall y(x\mathbf{R}y \Rightarrow \neg y\mathbf{R}x)$ (asymmetry) from the givens $\forall x \forall y \forall z(x\mathbf{R}y \wedge y\mathbf{R}z \Rightarrow x\mathbf{R}z)$ (transitivity) and $\forall x \neg x\mathbf{R}x$ (irreflexivity). You already did this, in Exercise 3.27.1.

5.29 To show that every transitive and asymmetric relation is a strict partial order, we have to establish that from $\forall x \forall y \forall z(x\mathbf{R}y \wedge y\mathbf{R}z \Rightarrow x\mathbf{R}z)$ (transitivity) and $\forall x \forall y(x\mathbf{R}y \Rightarrow \neg y\mathbf{R}x)$ (asymmetry), $\forall x \neg x\mathbf{R}x$ (irreflexivity) can be proved. In fact, irreflexivity follows already from asymmetry, as you already proved in Exercise 3.27.2.

5.30 Here is the proof:
Given: $\forall x, y, z \in A(xRy \wedge yRz \Rightarrow xRz), \forall x \in A(\neg xRx)$.
To be proved: $S = R \cup \Delta_A$ is a partial order (reflexive, transitive, antisymmetric).
Proof:
Reflexivity: immediate from the fact that $\Delta_A \subseteq R \cup \Delta_A$.
Transitivity: Assume for arbitrary $c, d, e \in A$ that cSd and dSe.
We have to show that cSe.
If $c = d$ and $d = e$, then $c = e$, so cSe.
If cRd and $d = e$, then cRe, so cSe.
If $c = d$ and dRe, then cRe, so cSe.
If cRd and dRe, then cRe by transitivity of R, so cSe.
Antisymmetry: Assume cSd and dSc. We have to show $c = d$.
Suppose $c \neq d$.
Then cRd and dRc, and by transitivity of R, cRc. Contradiction with irreflexivity of R.

5.31 Given: R is transitive, reflexive, and antisymmetric.
To be proved: R^{-1} is transitive, reflexive, and antisymmetric.
Proof:
Transitivity: Assume $cR^{-1}d$ and $dR^{-1}e$. Then eRd and dRc.
So by transitivity of R, eRc, and therefore $cR^{-1}e$.
Reflexivity: Assume $cR^{-1}c$. Then cRc.

Antisymmetry: Assume $cR^{-1}d$ and $dR^{-1}c$. Then cRd and dRc.
By antisymmetry of R, $c = d$.

5.32 Given: $S \subseteq A^2$ is reflexive and symmetric, for all $a, b \in A$ there is one S-path connecting a with b.
$r \in A$, $a \leqslant b$ iff a is on the path connecting r with b.
To be proved:
1. $\leqslant$ is reflexive.
Proof: Let $c \in A$ be arbitrary. Then there is path $r, \ldots, c$ from r to c, so $c \leqslant c$.
2. $\leqslant$ is antisymmetric.
Proof: Let $c, d \in A$ be arbitrary, and suppose $c \leqslant d$ and $d \leqslant c$.
Then c is on the path $r, \ldots, d$, and d is on the path $r, \ldots, c$.
Since the paths $r, \ldots, c$ and $r, \ldots, d$ are unique, it follows that $c = d$.
3. $\leqslant$ is transitive.
Proof: Let $c, d, e \in A$ be arbitrary, and suppose $c \leqslant d$ and $d \leqslant e$.
Then c is on the path $r, \ldots, d$, and d is on the path $r, \ldots, e$.
Since paths are unique, it follows that c is on the path $r, \ldots, e$.
4. For all $a \in A$, $r \leqslant a$.
Proof: Let $c \in A$ be arbitrary. Then there is a path from r to c, and r is on that path. So $r \leqslant c$.
5. For every $a \in A$, the set $X_a = \{x \in A \mid x \leqslant a\}$ is finite and if $b, c \in X_a$ then $b \leqslant c$ or $c \leqslant b$.
Proof: Let $a \in A$ be arbitrary. Then there is a single path $r = a_1, \ldots, a_n = a$.
The set X_a consists of $\{a_1, \ldots, a_n\}$, because for each a_i on the path $a_1, \ldots, a_n$
there is a single path from the root to a_i, namely, $r = a_1, \ldots, a_i$.
Let $b, c \in X_a$. Then b and c are on the same path $r = a_1, \ldots, a_n = a$.
Thus, b, c are among the a_i and we have $b \leqslant c$ or $c \leqslant b$.

5.33

	$<$	$\leqslant$	successor	divisor	coprime
irreflexive	√		√		
reflexive		√		√	
asymmetric	√		√		
antisymmetric	√	√	√	√	
symmetric					√
transitive	√	√		√	
linear	√	√			

Note that the *coprime* relation is not irreflexive, for 1 and 1 are coprime.
5.35.1 We show that $R \cup \Delta_A$ is the reflexive closure of R:

First we show that $R \subseteq R \cup \Delta_A$ and that $R \cup \Delta_A$ is reflexive.
Proof: the first is immediate, the second follows from the fact that $\Delta_A \subseteq R \cup \Delta_A$.
Next we show that $R \cup \Delta_A$ is the smallest reflexive relation having R as a subset:
If $R \subseteq S$ and S is reflexive, then $R \cup \Delta_A \subseteq S$.
Proof: Let S be such that $R \subseteq S$ and S is reflexive. Assume $(c, d) \in R \cup \Delta_A$.
We have to show that cSd.
From $(c, d) \in R \cup \Delta_A$ we get cRd or $c = d$.
If cRd then by $R \subseteq S$, cSd.
If $c = d$ then by reflexivity of S, cSd.

5.35.2 We show that $R \cup R^{-1}$ is the symmetric closure of R.
To be proved: $R \subseteq R \cup R^{-1}$ and $R \cup R^{-1}$ is symmetric.
Proof: both are immediate.
To be proved: If $R \subseteq S$ and S is symmetric, then $R \cup R^{-1} \subseteq S$.
Proof: Let S be such that $R \subseteq S$ and S is symmetric. Assume $(c, d) \in R \cup R^{-1}$.
We have to show that cSd.
From $(c, d) \in R \cup R^{-1}$ we get cRd or dRc.
If cRd then by $R \subseteq S$, cSd.
If dRc then by $R \subseteq S$, dSc, and by symmetry of S, cSd.

5.36 From the transitivity of $R \subseteq A^2$ it does not follow that $R \cup R^{-1} \cup \Delta_A$ is transitive. Consider $A = \{1, 2, 3\}$ with $R = \{(1, 2), (1, 3)\}$. Then R is transitive, but

$$R \cup R^{-1} \cup \Delta_A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 3), (3, 1)\}$$

is not, for $(2, 1)$ and $(1, 3)$ are in it, but $(2, 3)$ is not.

5.38 The composition of the relation "father of" with itself gives the relation "paternal grandfather of". The composition of "brother of" and "parent of", in that order, gives the relation "uncle of". This gives an example showing that $R \circ S$ and $S \circ R$ may well be different: a brother of a parent of mine is an uncle, but a parent of my brother is my own parent.

5.39 $R^2 = \{(0, 0), (0, 3), (1, 2), (1, 3), (2, 2), (2, 3)\}$,
$R^3 = \{(0, 2), (0, 3), (1, 0), (1, 3), (2, 0), (2, 3)\}$
and $R^4 = \{(0, 0), (0, 3), (1, 2), (1, 3), (2, 2), (2, 3)\}$.
From these results we see that $R \cup R^2$ is a good candidate for S. And indeed, if we put

$$S = \{(0, 0), (0, 2), (0, 3), (1, 0), (1, 2), (1, 3), (2, 0), (2, 2), (2, 3)\},$$

we get that $R \cup (S \circ R) = S$.

5.40.1 To be proved: R is transitive iff $R \circ R \subseteq R$.
Proof:
Only If: Suppose R is transitive, and assume c, d are such that $cR \circ Rd$.
We have to show that cRd.
From $c(R \circ R)d$ we get that there is an e with cRe and eRd.
But then transitivity of R gives cRd.
If: Suppose $R \circ R \subseteq R$, and assume cRd and dRe.
We have to show that cRe.
From cRd and dRe, we get $c(R \circ R)e$, and because $R \circ R \subseteq R$ this gives cRe.

5.40.2 An example of a transitive relation R for which $R \circ R \neq R$ is $<$ on $\mathbb{N}$. We have that $0 < 1$, but $\neg 0(< \circ <)1$.

5.41.1 To be proved: $Q \circ (R \circ S) = (Q \circ R) \circ S$.
Proof:
$\subseteq$: Let $(c, d) \in Q \circ (R \circ S)$. Then there is an e with cQe and $(e, d) \in R \circ S$.
Therefore, there is an f with eRf and fSd.

It follows that $(c, f) \in Q \circ R$, and $(c, d) \in (Q \circ R) \circ S$.
$\supseteq$: Let $(c, d) \in (Q \circ R) \circ S$. Then there is an e with $(c, e) \in (Q \circ R)$ and eSd.
Therefore, there is an f with cQf and fRe.
It follows that $(f, d) \in R \circ S$, and $(c, d) \in Q \circ (R \circ S)$.

5.41.2 To be proved: $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.
Proof:
$\subseteq$: Let $(c, d) \in (R \circ S)^{-1}$. Then $(d, c) \in R \circ S$, so there is an e with dRe and eSc.
Therefore, $cS^{-1}e$ and $eR^{-1}d$, and thus $(c, d) \in S^{-1} \circ R^{-1}$.
$\supseteq$: Let $(c, d) \in S^{-1} \circ R^{-1}$. Then there is an e with $cS^{-1}e$ and $eR^{-1}d$.
Thus, dRe and eSc. Therefore, $(d, c) \in R \circ S$, and it follows that $(c, d) \in (R \circ S)^{-1}$.

5.45 Given: $R = \{(n, n + 1) \mid n \in \mathbb{N}\}$.
To be proved: $R^+ = <$.
Proof:
$\subseteq$: Let $(n, m) \in R^+$. Then there is a $k \in \mathbb{N}$, $k > 0$, with $(n, m) \in R^k$.
Applying the definition of R we get that $n + k = m$, i.e., $n < m$.
$\supseteq$: Let $n < m$. Then there is a $k \in \mathbb{N}$, $k > 0$, with $n + k = m$.
Thus, $(n, m) \in R^k$, and therefore $(n, m) \in R^+$.

5.46 Given: $R \subseteq A^2$.
To be proved: $R^* = R^+ \cup \Delta_A$ is the smallest transitive and reflexive relation on A that includes R.
Proof:
First, we have to check that R^* includes R, and is reflexive and transitive.
The first two of these are immediate from the definition.
For transitivity, pick arbitrary $c, d, e \in A$ with cR^*d and dR^*e. We have to show that cR^*e.
Putting $R^0 = \Delta_A$, we get that there are $n, m \geqslant 0$ with cR^nd and dR^me.
Therefore there is a $k \geqslant 0$ with cR^ke, i.e., $c = e$ or cR^+e.
Next, let $R \subseteq S \subseteq A^2$, with S reflexive and transitive.
We have to show that $R^* \subseteq S$.
Take an arbitrary pair c, d with cR^*d. Then there is a $k \geqslant 0$ with cR^kd.
If $k = 0$ then $c = d$, and cSd by reflexivity of S.
If $k > 0$ then there are $c_1, \ldots c_{k-1}$ with $cRc_1, \ldots, c_{k-1}Rd$.
By the fact that $R \subseteq S$, $cSc_1, \ldots, c_{k-1}Sd$, and by transitivity of S, cSd.

5.47 If $R = \{(n, n + 1) \mid n \in \mathbb{N}\}$, then R^* equals $\leqslant$.

5.48.1 Given: for each $i \in I$, $R_i \subseteq A^2$, with R_i transitive.
To be proved: $\bigcap_{i \in I} R_i$ is transitive.
Proof:
Let $(c, d), (d, e) \in \bigcap_{i \in I} R_i$. We have to show that $(c, e) \in \bigcap_{i \in I} R_i$.
From $(c, d), (d, e) \in \bigcap_{i \in I} R_i$ we get that cR_id, dR_ie for all $i \in I$.
Since each R_i is transitive, cR_ie for all $i \in I$. Thus $(c, e) \in \bigcap_{i \in I} R_i$.

5.48.2 Given: $R \subseteq A^2$, $Q = \bigcap\{S \mid R \subseteq S \subseteq A^2, S \text{ transitive}\}$.
To be proved: $R^+ = Q$.

Proof:
Since A^2 is transitive, $\{S \mid R \subseteq S \subseteq A^2, S \text{ transitive}\} \neq \emptyset$.
Immediately from the definition of Q, we have that $R \subseteq Q$.
Also, from 5.48.2 we get that Q is transitive.
R^+ is included in each transitive S with $R \subseteq S \subseteq A^2$, and therefore $R^+ = Q$.

5.49.1 To be proved: $(R^*)^{-1} = (R^{-1})^*$.
Proof:
$\subseteq$: Suppose $(c, d) \in (R^*)^{-1}$. We have to show that $(c, d) \in (R^{-1})^*$.
From $(c, d) \in (R^*)^{-1}$ we get $(d, c) \in R^*$, so there is a $k \geqslant 0$ with $dR^k c$.
Thus, there are $c_1, \ldots, c_{k-1}$ with dRc_1, …, $c_{k-1}Rc$.
Therefore, $cR^{-1}c_{k-1}$, …, $c_1R^{-1}d$, i.e., $c(R^{-1})^k d$, and we see that $(c, d) \in (R^{-1})^*$.
$\supseteq$: Suppose $(c, d) \in (R^{-1})^*$. We have to show that $(c, d) \in (R^*)^{-1}$.
From $(c, d) \in (R^{-1})^*$ we get that there is a $k \geqslant 0$ with $c(R^{-1})^k d$.
Thus, there are $c_1, \ldots, c_{k-1}$ with $cR^{-1}c_1$, …, $c_{k-1}R^{-1}d$.
Therefore, dRc_{k-1}, …, c_1Rc, i.e., $dR^k c$, so dR^*c, and thus, $(c, d) \in (R^*)^{-1}$.

5.49.2 To see that $(R \cup R^{-1})^* = R^* \cup R^{-1*}$ may be false, note that $(R \cup R^{-1})^*$ surely is transitive. If we can find a case where $R^* \cup R^{-1*}$ is not transitive, we are done. For this, the example used in the solution to Exercise 5.36 may serve again. Consider $A = \{1, 2, 3\}$ with $R = \{(1, 2), (1, 3)\}$. Then $R^* = \{(1, 1), (1, 2), (1, 3), (2, 2), (3, 3)\}$, $R^{-1} = \{(2, 1), (3.1)\}$, and $R^{-1*} = \{(1, 1), (2, 1), (2, 2), (3, 1), (3, 2)\}$. The union of R^* and R^{-1*} is not transitive, for $(2, 1)$ and $(1, 3)$ are in it, but $(2, 3)$ is not.

5.49.3 Given: $S \circ R \subseteq R \circ S$.
To be proved: $(R \circ S)^* \subseteq R^* \circ S^*$.
Proof:
Let (c, d) be an arbitrary element of $(R \circ S)^*$. We have to show that $(c, d) \in R^* \circ S^*$.
Since $(c, d) \in (R \circ S)^*$, there is a $k \geqslant 0$ with $(c, d) \in (R \circ S)^k$.
Thus, there are $c_1, \ldots, c_{k-1}$ with $c(R \circ S)c_1$, …, $c_{k-1}(R \circ S)d$.
So there are $d_1, \ldots, d_k$ with cRd_1, d_1Sc_1, …, $c_{k-1}Rd_k$, d_kSd.
By what is given, we can replace any pattern xSy, yRz by xRy, ySz.
After a finite number of such replacements we get $c(R^k \circ S^k)d$, i.e., $(c, d) \in R^* \circ S^*$.

5.50

property	*reflexivity*	*symmetry*	*transitivity*
preserved under $\cap$?	yes	yes	yes
preserved under $\cup$?	yes	yes	no
preserved under inverse?	yes	yes	yes
preserved under complement?	no	yes	no
preserved under composition?	yes	no	no

5.52 To define `restrictR`, we need a version of `intersectSet` for sets as ordered lists:

```
intersectSet :: (Ord a) => Set a -> Set a -> Set a
intersectSet (Set [])     set2  =  Set []
intersectSet (Set (x:xs)) set2
   | inSet x set2 = insertSet x (intersectSet (Set xs) set2)
   | otherwise    = intersectSet (Set xs) set2
```

Now computing the restriction of a relation R to a set A is a matter of intersecting R with A^2 (the total relation on A):

```
restrictR :: Ord a => Set a -> Rel a -> Rel a
restrictR set rel = intersectSet (totalR set) rel
```

Note that it is assumed that the lists used in the representations of set and relation are *ordered*.

5.53

```
rclosR :: Ord a => Rel a -> Rel a
rclosR r = unionSet r (idR background)
  where background = unionSet (domR r) (ranR r)
```

```
sclosR :: Ord a => Rel a -> Rel a
sclosR r = unionSet r (invR r)
```

5.54

```
tclosR :: Ord a => Rel a -> Rel a
tclosR r | transR r  = r
         | otherwise = tclosR (unionSet r (r @@ r))
```

5.55

```
inDegree :: (Eq a) => Rel a -> a -> Int
inDegree (Set r) = \ x -> length [ y | (_,y) <- r, y == x ]

outDegree :: (Eq a) => Rel a -> a -> Int
outDegree (Set r) = \ x -> length [ y | (y,_) <- r, y == x ]
```

5.56

```
sources :: (Eq a) => Rel a -> Set a
sources (Set r) = Set [ x | x <- union (map fst r) (map snd r),
                            inDegree  (Set r) x == 0,
                            outDegree (Set r) x >= 1           ]

sinks :: (Eq a) => Rel a -> Set a
sinks (Set r) = Set [ x | x <- union (map fst r) (map snd r),
                          outDegree (Set r) x == 0,
                          inDegree  (Set r) x >= 1             ]
```

5.57 It is not hard to see that the successor relation $S = \{(n, m) \in \mathbb{Z} \mid n + 1 = m\}$ has the property that $S \cup S^2 \neq S^*$.

```
successor :: Rel' Int
successor = \ n m -> n+1 == m

rel = unionR' successor (repeatR' [0..1000] successor 2)
```

We get:

```
REL> rel 1 3
True
REL> rel 1 4
False
```

This shows that `rel` is *not* the less-than relation on $[1..1000]$.

5.58

```
transClosure' :: [a] -> Rel' a -> Rel' a
transClosure' xs r | transR' xs r = r
                   | otherwise    =
                     transClosure' xs (unionR' r (compR' xs r r))
```

5.68 We have to check reflexivity, symmetry and transitivity. $\equiv_n$ is reflexive for $n \mid m - m$. $\equiv_n$ is symmetric, for $n \mid m - k$ iff $n \mid k - m$. For transitivity of $\equiv_n$, assume $n \mid m - k$ and $n \mid k - p$. Then $n \mid (m - k) + (k - p)$, i.e., $n \mid m - p$.
5.71.1 $\{(2, 3), (3, 5), (5, 2)\}$ is not reflexive on $\mathbb{N}$, not symmetric, and not transitive.

5.71.2 $\{(n, m) \mid |n - m| \geqslant 3\}$ is not reflexive on $\mathbb{N}$, is symmetric, is not transitive.

5.72.1 Since $A = \{1, 2, 3\}$ has three elements, A^2 has 9 elements. The number of relations on A equals the number of different subsets of A^2, so there are $2^9 = 512$ relations on A.

5.72.2 An example of a relation on A is that is reflexive, but neither symmetric nor transitive is

$$\{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)\}.$$

Here is the check by computer:

```
REL> reflR (Set [1,2,3]) (Set [(1,1),(1,2),(2,2),(2,3),(3,3)])
True
REL> symR (Set [(1,1),(1,2),(2,2),(2,3),(3,3)])
False
REL> transR (Set [(1,1),(1,2),(2,2),(2,3),(3,3)])
False
```

5.72.3 An example of a relation on d A that is not reflexive, that is symmetric, and that is not transitive is $\{(1, 2), (2, 1), (2, 3), (3, 2)\}$. Here is the check by computer:

```
REL> reflR (Set [1,2,3]) (Set [(1,2),(2,1),(2,3),(3,2)])
False
REL> symR (Set [(1,2),(2,1),(2,3),(3,2)])
True
REL> transR (Set [(1,2),(2,1),(2,3),(3,2)])
False
```

5.72.4 Reflexive, symmetric, not transitive: $\{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$. Reflexive, symmetric, transitive: the total relation on A. Reflexive not symmetric, transitive: $\{1, 1), (1, 2), (2, 2), (3, 3)\}$. Not reflexive, symmetric, transitive: the empty relation on A. Not reflexive, not symmetric, transitive: $\{(1, 2), (2, 3), (1, 3)\}$. Not reflexive, not symmetric, not transitive: $\{(1, 2), (2, 3)\}$. The checks are left to the reader.

5.73

A	A^2	$\wp(A^2)$	reflexive	symmetric	transitive	equivalence
0	0	1	1	1	1	1
1	1	2	1	2	2	1
2	4	16	4	8	13	—
3	9	512	$2^6 = 64$	$2^6 = 64$	—	—
4	16	$2^{16} = 65536$	$2^{12} = 4096$	$2^{10} = 1024$	—	—
5	25	$2^{25} = 33554432$	$2^{20} = 1048576$	$2^{15} = 32768$	—	—
n	n^2	$2^{(n^2)}$	$2^{n(n-1)}$	$2^{(\frac{n^2+n}{2})}$	—	—

The explanation for the formula $2^{n(n-1)}$ for the number of reflexive relations over a universe A with n elements is that any relation that contains all objects of the form (c, c) is reflexive. Next, observe that A^2 contains $n(n-1)$ pairs (c, d) with $c \neq d$. All of these pairs may or may not be part of a reflexive relation, so there are $2^{n(n-1)}$ different reflexive relations on A.

The explanation for the formula $2^{(\frac{n^2+n}{2})}$ for the number of symmetric relations over a universe A with n elements is that any pair of the form (c, c) can be in a symmetric relation, and there are n such pairs. Next, if (c, d) with $c \neq d$ is in a symmetric relation, then (d, c) has to be in as well, and there are $\frac{1}{2}n(n-1)$ sets $\{(c, d), (d, c)\}$ with $c \neq d$. All in all this gives $n + \frac{1}{2}n(n-1) = \frac{n^2+n}{2}$ objects to choose from, giving $2^{(\frac{n^2+n}{2})}$ different possibilities.

5.75 Given: $R \subseteq A^2$, R symmetric and transitive, $\forall x \in A \exists y \in A(xRy)$.
To be proved: R is reflexive on A.
Proof:
Let $c \in A$ be arbitrary. We have to show that cRc.
From $\exists y \in A(cRy)$, let $d \in A$ be an object with cRd.
From cRd and symmetry of R, dRc.
From cRd, dRc and transitivity of R, cRc.

5.76 Given: $R \subseteq A^2$.
To be proved: R is an equivalence iff $\Delta_A \subseteq R$ and $R = R \circ R^{-1}$.
Proof:
Only if: Suppose R is an equivalence. We have to show $\Delta_A \subseteq R$ and $R = R \circ R^{-1}$.
$\Delta_A \subseteq R$ is immediate from the reflexivity of R.
Next we show $R = R \circ R^{-1}$.
$\subset$: Assume cRd. Then by reflexivity of R, cRc, and by symmetry of R, dRc, hence $cR^{-1}d$.
Thus $(c, d) \in R \circ R^{-1}$.
$\supset$: Assume $(c, d) \in R \circ R^{-1}$. Then there is an e with cRe and $eR^{-1}d$.
From $eR^{-1}d$, dRe, and by symmetry of R, eRd. By transitivity of R, cRd.
If: Suppose $\Delta_A \subseteq R$ and $R = R \circ R^{-1}$. We have to show that R is an equivalence.
Reflexivity of R is immediate from the fact that $\Delta_A \subseteq R$.
Symmetry: suppose cRd. Then dRd from reflexivity of R, and $dR^{-1}c$ from cRd.
Thus, $(d, c) \in R \circ R^{-1}$, and dRc from $R = R \circ R^{-1}$.
Transitivity: suppose cRd and dRe. Then eRd from symmetry of R, so $dR^{-1}e$.
From cRd and $dR^{-1}e$, $(c, d) \in R \circ R^{-1}$, so from $R = R \circ R^{-1}$, cRe.

5.84

```
rclass :: Rel' a -> a -> [a] -> [a]
rclass r x ys = [ y | y <- ys, r x y ]
```

5.87 Given: $\{A_i \mid i \in I\}$ is a partition of A, $\{B_j \mid j \in J\}$ is a partition of B.
To be proved: $\{A_i \times B_j \mid (i,j) \in I \times J\}$ is a partition of $A \times B$.
Proof: we have to check the three properties of a partition.
$\emptyset \notin \{A_i \times B_j \mid (i,j) \in I \times J\}$:
Immediate from the fact that for no i, j, $A_i = \emptyset$ or $B_j = \emptyset$.
$\bigcup\{A_i \times B_j \mid (i,j) \in I \times J\} = A \times B$:
Immediate from the fact that $\bigcup\{A_i \mid i \in I\} = A$ and $\bigcup\{B_j \mid j \in J\} = B$.
For all $X, Y \in \{A_i \times B_j \mid (i,j) \in I \times J\}$: if $X \neq Y$ then $X \cap Y = \emptyset$:
Let $X, Y \in \{A_i \times B_j \mid (i,j) \in I \times J\}$, with $X \neq Y$.
We show that $X \cap Y = \emptyset$.
Suppose $(a,b) \in X \cap Y$. Let $X = A_p \times B_q$ and $Y = A_r \times B_s$.
Since $(a,b) \in X = A_p \times B_q$, $a \in A_p$ and $b \in B_q$.
Since $(a,b) \in Y = A_r \times B_s$, $a \in A_r$ and $b \in B_s$.
Since $\{A_i \mid i \in I\}$ is a partition, $A_p \cap A_r \neq \emptyset$ implies $A_p = A_r$.
Since $\{B_j \mid j \in J\}$ is a partition, $B_q \cap B_s \neq \emptyset$ implies $B_q = B_s$.
Contradiction with the fact that $X \neq Y$.

5.94 $R = \{(n,m) \mid n, m \in \mathbb{N}$ and $n + m$ is even $\}$ induces the partition $\{\{2n \mid n \in \mathbb{N}\}, \{2n+1 \mid n \in \mathbb{N}\}\}$.

5.98 The relation

$$\{(0,0),(0,3),(0,4),(1,1),(1,2),\\ (2,1),(2,2),(3,0),(3,3),(3,4),(4,0),(4,3),(4,4)\}.$$

is an equivalence. The corresponding partition is: $\{\{0,3,4\},\{1,2\}\}$.

5.100.1 The equivalence on $\{0,1,2,3,4\}$ that corresponds to $\{\{0,3\},\{1,2,4\}\}$ is:

$$\{(0,0),(0,3),(3,0),(3,3),(1,1),(1,2),(2,1),(2,2),(1,4),(2,4),(4,2),(4,1),(4,4)\}$$

5.100.2 $\{(n,m) \in \mathbb{Z}^2 \mid n = m = 0 \vee n \times m > 0\}$.

5.100.3 $(\mathrm{mod}\ 2)$.

5.101 The example relation R is an equivalence on $\{1,2,3,4,5\}$. $|2|_R = \{1,2,4\}$. $A/R = \{\{1,2,4\},\{3,5\}\}$.

5.103 Given: $\sim$ on $\wp(\mathbb{N})$ defined by: $A \sim B :\equiv\ (A - B) \cup (B - A)$ is finite.
To be proved: $\sim$ is symmetric and transitive.
Proof:
Symmetry: Assume $A \sim B$. Then $(A - B) \cup (B - A)$ is finite.
Thus $(B - A) \cup (A - B)$ is finite, i.e., $B \sim A$.
Transitivity: Assume $A \sim B$ and $B \sim C$.
Then $(A - B) \cup (B - A)$ and $(B - C) \cup (C - B)$ are finite.

Since both $A - B$ and $B - C$ are finite, $(A - B) \cup (B - C)$ is finite.
Since $A - C \subseteq (A - B) \cup (B - C)$, we get that $A - C$ is finite.
Similarly, both $B - A$ and $C - B$ are finite, so $(B - A) \cup (C - B)$ is finite.
Since $C - A \subseteq (B - A) \cup (C - B)$, we get that $C - A$ is finite.
Since $A - C$ and $C - A$ are finite, $(A - C) \cup (C - A)$ is finite, i.e., $A \sim C$.

5.104.1 The relation R on all people given by $aRb \ :\equiv a$ and b have a common ancestor is not transitive. Consider a case of a man a who has a half-brother b who in turn has a half-sister c; a and b have the same father, but different mothers, and b and c have the same mother, but different fathers. Then a and b have a common ancestor (their father), b and c have a common ancestor (their mother), but a and c need not have an ancestor in common.

5.104.2 The relation S defined by: $aSb \ :\equiv a$ and b have a common ancestor along the male line is transitive, for if a and b have a common ancestor e along the male line, and b and c have a common ancestor f along the male line, then e is an ancestor of f along the male line or vice versa, so in either case a and c have an ancestor along the male line in common.

5.106

```
bell :: Integer -> Integer
bell 0 = 1
bell n = sum [stirling n k | k <- [1..n]]

stirling :: Integer -> Integer -> Integer
stirling n 1             = 1
stirling n k | n == k    = 1
             | otherwise = k * (stirling (n-1) k) + stirling (n-1) (k-1)
```

5.107 The table can be computed with the Haskell code of the previous exercise:

A	A^2	$\wp(A^2)$	equivalences
0	0	1	1
1	1	2	1
2	4	16	2
3	9	512	5
4	16	$2^{16} = 65536$	15
5	25	$2^{25} = 33554432$	52
n	n^2	$2^{(n^2)}$	$\sum_{k=1}^{n} \left\{ {n \atop k} \right\}$

5.108 Given: For all $X \in \mathcal{A}$ it holds that $X \subseteq A$.
To be proved: $\bigcup \mathcal{A} = A$ and for all $X, Y \in \mathcal{A}$: if $X \neq Y$ then $X \cap Y = \emptyset$
iff for every $a \in A$ there exists exactly one $K \in \mathcal{A}$ such that $a \in K$.
Proof:
Only if: Assume $\bigcup \mathcal{A} = A$ and for all $X, Y \in \mathcal{A}$: if $X \neq Y$ then $X \cap Y = \emptyset$.
We show that for every $a \in A$ there exists exactly one $K \in \mathcal{A}$ such that $a \in K$.

Let $a \in A$ be arbitrary. Since $\bigcup \mathcal{A} = A$, there is an $X \in \mathcal{A}$ with $a \in X$.
Assume there a $Y \in \mathcal{A}, Y \neq X$ with $a \in Y$. Then contradiction with $X \cap Y = \emptyset$.
If: Assume for every $a \in A$ there exists exactly one $K \in \mathcal{A}$ such that $a \in K$.
We first show that $\bigcup \mathcal{A} = A$.
From the given, $\bigcup \mathcal{A} \subseteq A$, so we only have to show $A \subseteq \bigcup \mathcal{A}$.
Let $a \in A$ be arbitrary, and let K be the element of $\mathcal{A}$ that has $a \in K$.
Then from $a \in K \in \mathcal{A}$ we get $a \in \bigcup \mathcal{A}$. Thus $A \subseteq \bigcup \mathcal{A}$.
Next we show that for all $X, Y \in \mathcal{A}$: if $X \neq Y$ then $X \cap Y = \emptyset$.
Let $X, Y \in \mathcal{A}$, with $X \neq Y$, and assume $a \in X \cap Y$.
Then contradiction with the fact that there exists exactly one $K \in \mathcal{A}$ with $a \in K$.

5.109 If R and S are equivalences, $R \cap S$ is an equivalence as well, for reflexivity, symmetry and transitivity are all preserved under intersection (see the table of Exercise 5.50). Since, according to that same table, transitivity is not preserved under union, it should be possible to find relations R, S, with R and S transitive, but $R \cup S$ not transitive. E.g., consider the set $A = \{1, 2, 3\}$, and let $R = \{(1, 2)\}$ and $S = \{(2, 3)\}$. Then R, S are both transitive, but $R \cup S$ is not, for the pair $(1, 3)$ is lacking. To turn this into an example where R and S are equivalences, take $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$ and $S = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$. Then R and S are equivalences, but

$$R \cup S = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$$

is not an equivalence, because of failure of transitivity.

5.110 Given: R and S are equivalences on A, $R \subseteq S$.
To be proved: Every S-equivalence class is a union of R-equivalence classes.
Proof:
Let $c \in A$ be arbitrary, and consider $|c|_S$.
We have to show that for all members d of $|c|_S$, $|d|_R \subseteq |c|_S$.
Let d be an arbitrary element of $|c|_S$, and let $e \in |d|_R$.
We show that $e \in |c|_S$.
From $e \in |d|_R$, we get eRd. From eRd and $R \subseteq S$, eSd.
From $d \in |c|_S$, we get dSc. From eSd and dSc, by transitivity of S, eSc.
Thus, $e \in |c|_S$.

5.111

```
listPartition :: Eq a => [a] -> [[a]] -> Bool
listPartition xs xss =
     all (‘elem‘ xs) (concat xss) && all (‘elem‘ (concat xss)) xs
  && listPartition’ xss []
  where
  listPartition’ []       _      = True
  listPartition’ ([]:xss) _      = False
  listPartition’ (xs:xss) domain
     | intersect xs domain == [] = listPartition’ xss (union xs domain)
     | otherwise                 = False
```

5.112

```
listpart2equiv :: Ord a => [a] -> [[a]] -> Rel a
listpart2equiv dom xss
  | not (listPartition dom xss) = error "argument not a list partition"
  | otherwise                   = list2set [(x,y) | xs<-xss, x<-xs, y<-xs]
```

5.113.1 If $R = \{(0,3),(1,5),(2,0)\}$; $A = \{0,1,2,3,4,5\}$, then the smallest equivalence $S \supseteq R$ on A is the equivalence that corresponds to the partition $\{\{0,2,3\},\{1,5\},\{4\}\}$. Thus, we have:

$$S = \{(0,0),(0,2),(0,3),(1,1),(1,5),(2,0),(2,2),(2,3),(3,0),(3,2),(3,3),(4,4),(5,1),(5,5)\},$$

as you can check by means of `listpart2equiv [[0, 2, 3],[1,5],[4]]`.

5.113.2 $A/S = \{\{0,2,3\},\{1,5\},\{4\}\}$.

5.113.3 The equivalences on A that include R correspond to all the ways of making $0,2,3$ equivalent, and $1,5$ equivalent. There are 5 ways of doing this.

5.113.4 The corresponding partitions are

$$\begin{array}{l}\{\{0,2,3\},\{1,5\},\{4\}\},\\ \{\{0,2,3,4\},\{1,5\}\},\\ \{\{0,2,3\},\{1,4,5\}\},\\ \{\{0,1,2,3,5\},\{4\}\},\\ \{\{0,1,2,3,4,5\}\}.\end{array}$$

5.114

```
equiv2listpart :: Ord a => Set a -> Rel a -> [[a]]
equiv2listpart s@(Set xs) r | not (equivalenceR s r) =
  error "equiv2listpart: relation argument not an equivalence"
                            | otherwise              =
  genListpart r xs
    where
      genListpart r []     = []
      genListpart r (x:xs) = xclass : genListpart r (xs \\ xclass)
        where xclass = x : [ y | y <- xs, inSet (x,y) r ]
```

5.115

```
equiv2part :: Ord a => Set a -> Rel a -> Set (Set a)
equiv2part s r = list2set (map list2set (equiv2listpart s r))
```

5.116 Given: $R \subseteq A^2$.
To be proved: $\Delta_A \cup (R \cup R^{-1})^+$ is the smallest equivalence on A that includes R.
Proof:

In the first place, $\Delta_A \cup (R \cup R^{-1})^+$ includes R, and is an equivalence:
The relation is reflexive because Δ_A is contained in it.
The relation is symmetric because $R \cup R^{-1}$ is symmetric.
The relation is transitive because it is a transitive closure.

Next, assume S is an equivalence on A that includes R.
We will show that $\Delta_A \cup (R \cup R^{-1})^+ \subseteq S$.
Let $(c, d) \in \Delta_A \cup (R \cup R^{-1})^+$. We have to show that cSd.
From $(c, d) \in \Delta_A \cup (R \cup R^{-1})^+$, $c = d$ or $(c, d) \in (R \cup R^{-1})^+$.
If $c = d$, then from reflexivity of S, cSd.
Otherwise, there is a $k \geqslant 1$ with $(c, d) \in (R \cup R^{-1})^k$.
Thus, there are $c_1, \ldots, c_{k-1}$ with cR_1c_1, …, $c_{k-1}R_kd$, where each R_i is either R or R^{-1}.
Since $R \subseteq S$, we get from this that cS_1c_1, …, $c_{k-1}S_kd$, where each S_i is either S or S^{-1}.
Since S is symmetric, cSc_1, …, $c_{k-1}Sd$, and from transitivity of S we get cSd.

5.117.1 Given: $R \subseteq A^2$.
To be proved: $S = R^* \cap R^{-1*}$ is an equivalence on A.
Proof:
We have to show reflexivity, symmetry and transitivitity of S.
Reflexivity: since $\Delta_A \subseteq R^*$, $\Delta_A \subseteq R^{-1*}$, $\Delta_A \subseteq S$.
Symmetry: Suppose cSd. Then $(c, d) \in R^*$ and $(c, d) \in R^{-1*}$.
Thus, there are $i, j \geqslant 0$ with cR^id and $cR^{-1j}d$. Therefore, $dR^{-1i}c$ and dR^jc.
It follows that $(d, c) \in R^*$ and $(d, c) \in R^{-1*}$, so dSc.
Transitivity: Suppose cSd and dSe. Then $(c, d) \in R^*$, $(c, d) \in R^{-1*}$, $(d, e) \in R^*$, $(d, e) \in R^{-1*}$.
Thus, there are i, j, k, m with cR^id, $cR^{-1j}d$, dR^ke, $dR^{-1m}e$.
Therefore, $cR^{i+k}e$, $cR^{-1j+m}e$, and thus cR^*e, $cR^{-1*}e$. It follows that cSe.

5.117.2 Given: $R \subseteq A^2$, $S = R^* \cap R^{-1*}$, $|a|_S T |b|_S :\equiv aR^*b$.
To be proved: T is a partial order.
Proof:
We have to show reflexivity, anti-symmetry, and transitivity of T.
Reflexivity: let $c \in A$ be arbitrary. We have to show $|c|_S T |c|_S$.
This follows immediately from cR^*c and the definition of T.
Anti-symmetry: let $c, d \in A$ be objects with $|c|_S T |d|_S$, $|d|_S T |c|_S$. We show $|c|_S = |d|_S$.
From $|c|_S T |d|_S$, cR^*d, from $|d|_S T |c|_S$, dR^*c, and thus $cR^{-1*}d$.
Since cR^*d and $cR^{-1*}d$, cSd, i.e., $c \in |d|_S$, or in other words, $|c|_S = |d|_S$.
Transitivity: $c, d, e \in A$ be objects with $|c|_S T |d|_S$, $|d|_S T |e|_S$. We show $|c|_S T |e|_S$.
From $|c|_S T |d|_S$, cR^*d, from $|d|_S T |e|_S$, dR^*e, and thus cR^*e. It follows that $|c|_S T |e|_S$.

5.119.1 The relation $\sim$ on $\mathbb{R}$ given by $p \sim q :\equiv p \times q \in \mathbb{Z}$ is not an equivalence. E.g., reflexivity fails, for, e.g., $\frac{1}{2} \not\sim \frac{1}{2}$, for $\frac{1}{4} \notin \mathbb{Z}$.
5.119.2 The relation $\approx$ on $\mathbb{R}$ given by $p \approx q :\equiv p - q \in \mathbb{Z}$ is an equivalence. $\approx$ is reflexive, for $p - p = 0 \in \mathbb{Z}$, so $p \approx p$ for any $p \in \mathbb{R}$. $\approx$ is symmetric, for if $p - q = m \in \mathbb{Z}$, then $q - p = -m \in \mathbb{Z}$. $\approx$ is transitive, for if

$p-q=m\in\mathbb{Z}$ and $q-r=n\in\mathbb{Z}$, then $p-r=(m+q)-(q-n)=m+n\in\mathbb{Z}$. The partition that corresponds with $\approx$ consists of the classes of real numbers that all are at integer distances from one another. E.g., $\approx_0=\mathbb{Z}$, and $\approx_\pi=\{\pi+m\mid m\in\mathbb{Z}\}$.

5.120.1 Given: Relation R on $\mathbb{R}\times\mathbb{R}$, with $(x,y)R(u,v)$ iff $3x-y=3u-v$.
To be proved: R is an equivalence.
Proof: Reflexivity: Let $(x,y)\in\mathbb{R}^2$. Then $3x-y=3x-y$, so $(x,y)R(x,y)$.
Symmetry: Let $(x,y),(u,v)\in\mathbb{R}^2$, and suppose $(x,y)R(u,v)$.
Then $3x-y=3u-v$, so $3u-v=3x-y$, i.e., $(u,v)R(x,y)$.
Transitivity: Let $(x,y),(u,v),(p,q)\in\mathbb{R}^2$, and suppose $(x,y)R(u,v)$ and $(u,v)R(p,q)$.
Then $3x-y=3u-v$ and $3u-v=3p-q$, so $3x-y=3p-q$, i.e., $(x,y)R(p,q)$.

5.120.2 The equivalence class of $(0,0)$ is the set of points on the real plane given by $\{(x,y)\mid y=3x\}$, i.e., the straight line through the points $(0,0)$ and $(1,3)$. The equivalence class of $(1,1)$ is the set of points on the real plane given by $\{(x,y)\mid y=3x-2\}$, i.e., the straight line through the points $(1,1)$ and $(2,4)$.

5.120.3 R partitions $\mathbb{R}^2$ in the set of all straight lines parallel to the line given by the equation $y=3x$.

5.121 Let R be given by $(x,y)R(u,v):\equiv x^2+y^2=u^2+v^2$. Then every point (u,v) in the class $[(x,y)]_R$ is on the circle with centre $(0,0)$ and radius $\sqrt{x^2+y^2}$.

5.122.1 Given: $Q=\{(0,0),(0,1),(0,5),(2,4),(5,0)\}$,
R is an equivalence on $\{0,1,2,3,4,5\}$, $Q\subseteq R$, $(0,2)\notin R$.
To be proved: $(1,5)\in R$ and $(4,5)\notin R$.
Proof:
Since $Q\subseteq R$ and R transitive we get $Q^+\subseteq R$. Thus, $(1,5)\in R$.
Suppose $(4,5)\in R$. Since R is an equivalence with $(2,4)\in R$ and $(5,0)\in R$, $(2,0)\in R$.
By symmetry of R, $(0,2)\in R$, and contradiction with the given.

5.122.2 The partition corresponding to the smallest equivalence $\supseteq Q$ is the partition induced by Q^*. This is:

$$\{\{0,1,5\},\{2,4\},\{3\}\}.$$

5.122.3 Any equivalence S with $Q\subseteq S$ will have $Q^*\subseteq S$. Any equivalence S with $(0,2)\notin S$ will induce at least two equivalence classes $[0]_S\neq[2]_S$. There are three possibilities altogether: put 3 in a class of its own, put 3 in a class with 0, or put 3 in a class with 2. The corresponding partitions are:

$$\{\{0,1,5\},\{2,4\},\{3\}\},\{\{0,1,3,5\},\{2,4\}\},\{\{0,1,5\},\{2,3,4\}\}.$$

5.123 To be proved: For every partition $\mathcal{A}$ of a set A
there is an equivalence relation R with $A/R=\mathcal{A}$.
Proof:
Let R be given by $xRy:\equiv\exists X\in\mathcal{A}$ with $x,y\in X$.
We first show that R is an equivalence.
Reflexivity holds because $\bigcup\mathcal{A}=A$; symmetry is immediate from the definition of R.
Transitivity: Let xRy and yRz. We show that xRz.

From xRy: $\exists X \in \mathcal{A}$ with $x, y \in X$. From yRz: $\exists Y \in \mathcal{A}$ with $y, z \in Y$.
Since $y \in X \cap Y$ and $\mathcal{A}$ is a partition, $X = Y$. Thus, $x, z \in X$, and therefore xRz.

Next, $A/R = \mathcal{A}$, since $[x] \in A/R \Leftrightarrow \{y \mid yRx\} \in A/R \Leftrightarrow \{y \mid yRx\} \in \mathcal{A}$.

5.124 To find a recurrence for the maximum number of enmities among $2n$ countries, first observe that certainly, $E(1) = 1$, for if there are just two countries, nothing prevents them being at war (the exercise is wonderfully realistic). Next, given that we know that $E(n)$ is the maximum number of enmities among $2n$ countries, how many enmities can be added if we introduce one more pair of countries, say a and b? Certainly, a and b can be at war with each other. Also, a can only have enemies among the old countries that have mutual peace treaties (for the countries that have a as common enemy are obliged to be at peace with each other). Similarly for b. Furthermore, the enemies of a among the old countries have to sign peace treaties with b, and vice versa (this is to avoid war-triangles). Thus, a can be at war with at most n old countries, and similarly for b. All in all, this gives $E(n+1) = E(n) + 2n + 1$ possible enmities among $2(n+1)$ countries. It is clear that this can be solved by $(n+1)^2 = n^2 + 2n + 1$, and that $E(n) = n^2$ gives the general solution. The minimal number of peace treaties among $2n$ countries equals the number of pairs of different countries minus the maximum number of enmities, and is given by $f(n) = 2n(2n-1) - n^2 = 3n^2 - 2n$. For $n = 10$, this gives $300 - 20 = 280$ peace treaties at least.

5.125

```
coins :: [Int]
coins = [1,2,5,10,20,50,100,200]

change :: Int -> [Int]
change n = moneyback n (n,[]) where
    moneyback n (m,xs) | m == 0                  = xs
                       | n <= m && elem n coins  = moneyback n (m-n,n:xs)
                       | otherwise               = moneyback (n-1) (m,xs)
```

5.126

```
packCoins :: Int -> CmprPart -> CmprPart
packCoins k (m,xs) | k == 1                 = (m,xs)
                   | k <= m && elem k coins = packCoins k (m-k,k:xs)
                   | otherwise              = packCoins (k-1) (m,xs)

nextCpartition :: CmprPart -> CmprPart
nextCpartition (k,(x:xs)) = packCoins (x-1) ((k+x),xs)
```

```
generateCps :: CmprPart -> [Part]
generateCps p@(n,[])     = [expand p]
generateCps p@(n,(x:xs))
        | elem x coins = (expand p: generateCps (nextCpartition p))
        | otherwise    = generateCps (nextCpartition p)

partC :: Int -> [Part]
partC n | n < 1     = error "part: argument <= 0"
        | n == 1    = [[1]]
        | otherwise = generateCps (packCoins n (n,[]))
```

5.127

```
Sol5> length (partC 100)
4563
```

Solutions to Exercises from Chapter 6

```
module Sol6

where

import Data.Char
import Data.List
import SetOrd
import FCT
```

6.10

```
h' n = n * (n + 1)
```

6.11

```
k' n = n^2
```

6.14.1 R is not a function.

6.14.1 R^{-1} is a function. $\mathrm{dom}\,(R^{-1}) = \{2, 3, 4\}$ and ran$(R^{-1}) = \{0, 1\}$.

6.15.1 $f[A] = \{f(x) \mid x \in A\} =$ ran$(f \restriction A)$.

6.15.2 $f[\mathrm{dom}\,(f)] = f[X] = \{f(x) \mid x \in X\} =$ ran(f).

6.15.3 $f^{-1}[B] = \{f^-1(y) \mid y \in B\} = \{x \in X \mid f(y) \in B\} = \mathrm{dom}\,(f \cap (X \times B))$.

6.15.4 $f^{-1}[\text{ran}(f)] = f^{-1}[\{f(x) \mid x \in X\}] = \{f^{-1}(f(x)) \mid x \in X\} = X = \text{dom}\,(f)$.

6.15.5 $f{\restriction}A = \{(x, f(x)) \mid x \in A\} = \{(x, f(x)) \mid x \in A, f(x) \in Y\} = f \cap (A \times Y)$.

6.16 $f{\restriction}\{0,3\} = \{(0,3),(3,2)\}$, $f[\{1,2,3\}] = \{2,4\}$, $f^{-1}[\{2,4,5\}] = \{1,2,3\}$. Here is the code for the checks:

```
l_0 = [(0,3),(1,2),(2,4),(3,2)]
f_0 = list2fct l_0
test_1 = fct2list (restrict f_0 [0,3]) [0,3]
test_2 = image f_0 [1,2,3]
test_3 = coImage f_0 [0,1,2,3] [2,4,5]
```

6.17 Given: $f : A \to Y$, $g : B \to Y$, and $A \cap B = \emptyset$.
To be proved: $f \cup g : A \cup B \to Y$.
Proof:
$f \cup g = \{(a, f(a)) \mid a \in A\} \cup \{(b, g(b)) \mid b \in B\}$.
To show that this is a function in $A \cup B \to Y$, we must show:
for all $x \in A \cup B$ there is precisely one $y \in Y$ with $(f \cup g)(x) = y$.
Let $x \in A \cup B$. Since $A \cap B = \emptyset$, there are two cases:
(i) $x \in A$. In this case $(f \cup g)(x) = f(x)$.
(ii) $x \in B$. In this case $(f \cup g)(x) = g(x)$.

In case $A \cap B \neq \emptyset$, $f \cup g$ is a function iff $f{\restriction}(A \cap B) = g{\restriction}(A \cap B)$.

6.18 Given: $\mathcal{A}$ is a partition of X. For every component $A \in \mathcal{A}$ there is a function $f_A : A \to Y$.
To be proved: $\bigcup_{A \in \mathcal{A}} f_A : X \to Y$.
Proof:
Let $g = \bigcup_{A \in \mathcal{A}} f_A$.
We have to show that for any $x \in X$ there is exactly one $y \in Y$ with $g(x) = y$.
Let $x \in X$ be arbitrary.
Since $\mathcal{A}$ is a partition of X, there is exactly one $A \in \mathcal{A}$ with $x \in A$.
Thus $g(x) = f_A(x)$.
Suppose there is a $y' \neq f_A(x)$ with $g(x) = y'$.
Since $g(x) = f_A(x)$, this contradicts the fact that f_A is a function.

6.20.1a Given: $f : X \to Y$, $A, B \subseteq X$.
To be proved: $A \subseteq B \;\Rightarrow\; f[A] \subseteq f[B]$.
Proof: Let $y \in f[A]$. We have to show that $y \in f[B]$.
From $y \in f[A]$: there is an $x \in A$ with $f(x) = y$.
From $A \subseteq B$ and $x \in A$: $x \in B$.
Thus, there is an $x \in B$ with $f(x) = y$, i.e., $y \in f[B]$.

6.20.1b Given: $f : X \to Y$, $C, D \subseteq Y$.
To be proved: $C \subseteq D \;\Rightarrow\; f^{-1}[C] \subseteq f^{-1}[D]$.

Proof: Suppose $C \subseteq D$ and assume $x \in f^{-1}[C]$. We have to show that $x \in f^{-1}[D]$.
From $x \in f^{-1}[C]$, $f(x) \in C$. From $C \subseteq D$ and $f(x) \in C$: $f(x) \in D$.
Thus, $x \in f^{-1}[D]$.

6.20.2a Given: $f : X \to Y$, $A, B \subseteq X$.
To be proved: $f[A \cup B] = f[A] \cup f[B]$.
Proof:
$y \in f[A \cup B]$ iff $\exists x \in A \cup B : f(x) = y$ iff $\exists x \in A : f(x) = y$ or $\exists x \in B : f(x) = y$
iff $y \in f[A]$ or $y \in f[B]$ iff $y \in f[A] \cup f[B]$.

6.20.2b Given: $f : X \to Y$, $A, B \subseteq X$.
To be proved: $f[A \cap B] \subseteq f[A] \cap f[B]$.
Proof:
Suppose $y \in f[A \cap B]$. We have to show that $y \in f[A] \cap f[B]$.
From $y \in f[A \cap B]$: $\exists x \in A \cap B$ with $f(x) = y$.
So $x \in A : f(x) = y$, and $x \in B : f(x) = y$.
Therefore, $y \in f[A]$ and $y \in f[B]$, i.e., $y \in f[A] \cap f[B]$.

To see that the inclusion cannot be replaced by an equality, consider the function $f : \{0, 1, 2\} \to \{0, 1\}$ given by $f(0) = 0$, $f(1) = 0$, $f(2) = 1$. For this f we have $f[\{0, 2\}] = f[\{1, 2\}] = \{0, 1\} \neq f[\{0, 2\} \cap \{1, 2\}] = f[\{2\}] = \{1\}$. Here is an implementation:

```
l_1 = [(0,0),(1,0),(2,1)]
f_1 = list2fct l_1
```

We get:

```
Sol6> image f_1 [0,2]
[0,1]
Sol6> image f_1 [1,2]
[0,1]
Sol6> image f_1 (intersect [0,2] [1,2])
[1]
```

6.20.3a Given: $f : X \to Y$, $C, D \subseteq Y$.
To be proved: $f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]$.
Proof:
$x \in f^{-1}[C \cup D]$ iff $\exists y \in C \cup D$ with $x = f^{-1}(y)$
iff $\exists y \in C$ with $x = f^{-1}(y)$ or $\exists y \in D$ with $x = f^{-1}(y)$,
iff $x \in f^{-1}[C]$ or $x \in f^{-1}[D]$, iff $x \in f^{-1}[C] \cup f^{-1}[D]$.

6.20.3b Given: $f : X \to Y$, $C, D \subseteq Y$.
To be proved: $f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]$.
Proof:

$x \in f^{-1}[C \cap D]$ iff $\exists y \in C \cap D$ with $x = f^{-1}(y)$
iff $\exists y \in C$ with $x = f^{-1}(y)$ and $\exists y \in D$ with $x = f^{-1}(y)$,
iff $x \in f^{-1}[C]$ and $x \in f^{-1}[D]$, iff $x \in f^{-1}[C] \cap f^{-1}[D]$.

6.20.4a Given: $f : X \to Y$, $C \subseteq Y$.
To be proved: $f[f^{-1}[C]] \subseteq C$.
Proof: Suppose $y \in f[f^{-1}[C]]$. We have to show that $y \in C$.
From $y \in f[f^{-1}[C]]$, there is an $x \in f^{-1}[C]$ with $f(x) = y$.
From $x \in f^{-1}[C]$, we get $f(x) \in C$, and therefore $y \in C$.

To see that the inclusion cannot be replaced by an equality, consider again the function f that we used above (implemented as `f_1`), but now with co-domain $\{0, 1, 2\}$. Letting $C = \{0, 1, 2\}$, we get:

```
Sol6> coImage f_1 [0,1,2] [0,1,2]
[0,1,2]
Sol6> image f_1 [0,1,2]
[0,1]
```

6.20.4b Given: $f : X \to Y$, $A \subseteq X$.
To be proved: $f^{-1}[f[A]] \supseteq A$.
Proof: Suppose $x \in A$. We have to show that $x \in f^{-1}[f[A]]$.
From $x \in A$ and what is given about f, we get $f(x) \in f[A]$.
From $f(x) \in f[A]$ we get $f^{-1}(f(x)) \in f^{-1}[f[A]]$.
Since $f^{-1}(f(x)) = x$ this means $x \in f^{-1}[f[A]]$.

To see that the inclusion cannot be replaced by an equality, look at this:

```
Sol6> coImage f_1 [0,1,2] (image f_1 [0,2])
[0,1,2]
```

6.23

```
bijective :: Eq b => (a -> b) -> [a] -> [b] -> Bool
bijective f xs ys = injective f xs && surjective f xs ys
```

6.24

```
injectivePairs :: (Eq a, Eq b) => [(a,b)] -> [a] ->  Bool
injectivePairs f xs = injective (list2fct f) xs

surjectivePairs :: (Eq a, Eq b) => [(a,b)] -> [a] -> [b] -> Bool
surjectivePairs f xs ys = surjective (list2fct f) xs ys

bijectivePairs :: (Eq a, Eq b) => [(a,b)] -> [a] -> [b] -> Bool
bijectivePairs f xs ys = bijective (list2fct f) xs ys
```

Instead of this, it is also possible to use something more direct, such as:

```
injectivePairs :: Eq b => [(a,b)] -> [a] -> Bool
injectivePairs f xs = length (nub [b | (a,b) <- f]) == length xs

surjectivePairs :: (Eq a, Eq b) => [(b,a)] -> [b] -> [a] -> Bool
surjectivePairs f xs ys = and (map (`elem` im) ys)
  where im = imagePairs f xs
```

6.25

1. $\sin : \mathbb{R}^+ \to \mathbb{R}$ is not injective, for $\sin(0) = \sin(\pi)$, and not surjective, for, e.g., 2, is not in the range.
2. $\sin : \mathbb{R} \to [-1, +1]$ is not injective, but is surjective.
3. $\sin : [-1, +1] \to [-1, +1]$ is both injective and surjective.
4. $e^x : \mathbb{R} \to \mathbb{R}$ is injective, but not surjective (for the values are always positive).
5. $\tan : \mathbb{R} \to \mathbb{R}$ is not injective, for $\tan(0) = \tan(\pi)$, but is surjective.
6. $\log : \mathbb{R}^+ \to \mathbb{R}$ is injective and surjective.
7. $\surd : \mathbb{R}^+ \to \mathbb{R}^+$ is injective and surjective.

6.26 Let $f : A \to B$ be an injection, and suppose $|A| = n$ and $|B| = k$. Then $A = \{a_1, \ldots, a_n\}$, and there are k possible choices for $f(a_1)$, $k - 1$ possible choices for a_2, …, $k - n + 1$ possible choices for a_n. Thus, all in all, there are $k(k-1)\cdots(k-n+1)$ such f.
6.27

```
injs :: [Int] -> [Int] -> [[(Int,Int)]]
injs [] xs = [[]]
injs xs [] = []
injs (x:xs) ys =
  concat [ map ((x,y):) (injs xs (ys \\ [y])) | y <- ys ]
```

6.28

```
perms :: [a] -> [[a]]
perms [] = [[]]
perms (x:xs) = concat (map (insrt x) (perms xs))
  where
  insrt :: a -> [a] -> [[a]]
  insrt x [] = [[x]]
  insrt x (y:ys) = (x:y:ys) : map (y:) (insrt x ys)
```

Here is another way, but note that this version assumes that the list is over a type in the class `Eq`.

```
permuts :: Eq a => [a] -> [[a]]
permuts [] = [[]]
permuts xs = [ a:ys | a <- xs, ys <- permuts (xs \\ [a]) ]
```

6.32

```
comp :: Eq b => [(b,c)] -> [(a,b)] -> [(a,c)]
comp g f = [ (x,list2fct g y) | (x,y) <- f ]
```

6.37 Let $f : \{0\} \to \{0,1\}$ be given by $f = \{(0,0)\}$. Then f is not surjective. Let $g : \{0,1\} \to \{0\}$ be given by $g = \{(0,0),(1,0)\}$. Then g is not injective. Still, $g \circ f = \{(0,0\}$ is a bijection.

Here is the computational check:

```
Sol6> comp [(0,0),(1,0)] [(0,0)]
[(0,0)]
```

6.38.1 We can use `comp` to find the values:

```
Sol6> comp [(0,1),(1,2),(2,0),(3,0),(4,3)] [(0,1),(1,2),(2,0),(3,0),(4,3)]
[(0,2),(1,0),(2,1),(3,1),(4,0)]
Sol6> comp [(0,1),(1,2),(2,0),(3,0),(4,3)] [(0,2),(1,0),(2,1),(3,1),(4,0)]
[(0,0),(1,1),(2,2),(3,2),(4,1)]
Sol6> comp [(0,1),(1,2),(2,0),(3,0),(4,3)] [(0,0),(1,1),(2,2),(3,2),(4,1)]
[(0,1),(1,2),(2,0),(3,0),(4,2)]
```

This gives the following table:

x	0	1	2	3	4
$f(x)$	1	2	0	0	3
$(ff)(x)$	2	0	1	1	0
$(fff)(x)$	0	1	2	2	1
$(ffff)(x)$	1	2	0	0	2

6.38.2 The set $\{f, f \circ f, f \circ f \circ f, \ldots\}$ has 4 elements.
6.38.3 Take $g = \{(0,1),(1,0),(2,3),(3,4),(4,2)\}$. Then we get:

```
Sol6> comp [(0,1),(1,0),(2,3),(3,4),(4,2)] [(0,1),(1,0),(2,3),(3,4),(4,2)]
[(0,0),(1,1),(2,4),(3,2),(4,3)]
Sol6> comp [(0,1),(1,0),(2,3),(3,4),(4,2)] [(0,0),(1,1),(2,4),(3,2),(4,3)]
[(0,1),(1,0),(2,2),(3,3),(4,4)]
Sol6> comp [(0,1),(1,0),(2,3),(3,4),(4,2)] [(0,1),(1,0),(2,2),(3,3),(4,4)]
```

```
[(0,0),(1,1),(2,3),(3,4),(4,2)]
Sol6> comp [(0,1),(1,0),(2,3),(3,4),(4,2)] [(0,0),(1,1),(2,3),(3,4),(4,2)]
[(0,1),(1,0),(2,4),(3,2),(4,3)]
Sol6> comp [(0,1),(1,0),(2,3),(3,4),(4,2)] [(0,1),(1,0),(2,4),(3,2),(4,3)]
[(0,0),(1,1),(2,2),(3,3),(4,4)]
```

6.39.1 Given: A finite, $f : A \to A$ is a bijection.
To be proved: for some $n \in \mathbb{N}$, $f^n = 1_A$.
Proof:
Observe that there are only finitely many bijections on A.
Thus, there must be an n with f^n equal to $f^0 = 1_A$.

6.39.2 Since the bijections on A correspond to permutations of A, their number cannot exceed $k!$, the number of permutations of a domain of size k.

6.40 Given: $h : X \to X$ satisfies $h \circ h \circ h = 1_X$.
To be proved: h is a bijection.
Proof:
To show injectivity, let $a_1, a_2 \in X$ be arbitrary, and suppose $h(a_1) = h(a_2)$.
Then $h^3(a_1) = h^3(a_2)$, and from the given about h^3 we get $a_1 = a_2$.

To show surjectivity, let $b \in X$ be arbitrary.
From the given about h^3, $h^3(b) = b$. Thus $h(h^2(b)) = b$, so there is an $a \in X$ with $h(a) = b$.

For a simple example of a set X and a function $h : X \to X$ such that $h \circ h \circ h = 1_X$, whereas $h \neq 1_X$, take $X = \{0, 1, 2\}$ and $h = \{(0, 1), (1, 2), (2, 0)\}$.

6.41 Given: $f : X \to Y$, $g : Y \to Z$, f and g injective.
To be proved: $g \circ f$ injective.
Proof:
Let $a_1, a_2 \in X$ be arbitrary, and suppose $(g \circ f)(a_1) = (g \circ f)(a_2)$.
Then $g(f(a_1)) = g(f(a_2))$. By injectivity of g, $f(a_1) = f(a_2)$.
From this we get $a_1 = a_2$ by injectivity of f.

6.42 Given: $f : X \to Y$, $g : Y \to Z$, and $g \circ f$ bijective.
To be proved: f is surjective iff g is injective.
Proof:
Only if: Suppose f is surjective.
To show injectivity of g, let $b_1, b_2 \in Y$ be arbitrary, and assume $g(b_1) = g(b_2)$.
Then by surjectivity of f, there are $a_1, a_2 \in X$ with $f(a_1) = b_1$ and $f(a_2) = b_2$.
This gives $g(f(a_1)) = g(f(a_2))$, so by the fact that $g \circ f$ is a bijection, $a_1 = a_2$.
From this and the functionality of f, $b_1 = b_2$.

If: Suppose g is injective.
To show surjectivity of f, let $b \in Y$ be arbitrary.
Then $g(b) \in Z$, and by bijectivity of $g \circ f$, there is an $a \in X$ with $(g \circ f)(a) = g(b)$.
From $(g \circ f)(a) = g(f(a)) = g(b)$, by injectivity of g, $f(a) = b$.

6.43 Given: $\lim_{i\to\infty} a_i = a$, $f : \mathbb{N} \to \mathbb{N}$ injective.
To be proved: $\lim_{i\to\infty} a_{f(i)} = a$.
Proof:
We have to show that $\forall\epsilon > 0\ \exists n\ \forall i \geqslant n\ (|a - a_{f(i)}| < \epsilon)$.
Let ϵ be arbitary, and let n_0 be such that $\forall i \geqslant n_0\ (|a - a_i| < \epsilon)$ (from the first given).
From the injectivity of f we get that there is an m_0 with $\forall k \geqslant m_0\ (f(k) > n_0)$.
It follows that $\exists n\ \forall i \geqslant n\ (|a - a_{f(i)}| < \epsilon)$.

6.48 Given: $f : X \to Y$ has left-inverse g and right-inverse h.
To be proved: f is a bijection and $g = h = f^{-1}$.
Proof:
$h = 1_X \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ 1_X = g$.
Also, g is the inverse of f, for if $x \in X$ then $g(f(x)) = 1_X(x) = x$,
and if $y \in Y$ then $f(g(y)) = f(h(y)) = 1_Y(y) = y$.

6.49 Given: $f : X \to Y$ and $g : Y \to X$.
To be proved: $g \circ f = 1_X$ iff $\{(f(x), x) \mid x \in X\} \subseteq g$.
Proof:
Only if: Suppose $g \circ f = 1_X$. Let $x \in X$ be arbitrary.
We have to show that $(f(x), x) \in g$.
From $g \circ f = 1_X$ we get $g(f(x)) = x$, and we are done.
If: Suppose $\{(f(x), x) \mid x \in X\} \subseteq g$.
Then for all $x \in X$, $(g \circ f)(x) = g(f(x)) = x$, i.e., $g \circ f = 1_X$.

6.50 To get $g \circ f = 1_X$, it is sufficient that $g(3) = 0$ and $g(4) = 1$. The values for the arguments 2 and 5 are free, and for both of these there are two possible choices. Thus, all in all there are four functions g with $g \circ f = 1_X$.

6.51 The function $\Lambda : \emptyset \to \{0\}$ is (trivially) an injection. But there is no function $g : \{0\} \to \emptyset$, and therefore the condition $g \circ \lambda = 1_\emptyset$ cannot be fulfilled.

6.52 Given: $f : X \to Y$ is surjective.
To be proved: there is a $g : Y \to X$ with $f \circ g = 1_Y$.
Proof:
Let g be given by $g(y) :=$ an arbitrary $x \in X$ with $f(x) = y$.
By surjectivity of f, this is well-defined.
To show $f \circ g = 1_Y$, take an arbitrary $y \in Y$. Then $g(y)$ equals some $x \in X$ with $f(x) = y$.
So indeed, $(f \circ g)(y) = f(g(y)) = f(x) = y$.

6.53 A right-inverse g to the function $\{(0,5), (1,5), (2,5), (3,6), (4,6)\}$ with domain: $\{0,1,2,3,4\}$, codomain: $\{5,6\}$ has to satisfy two properties: (i) $g(5) \in \{0,1,2\}$, and (ii) $g(6) \in \{3,4\}$. This can be done in $3 \times 2 = 6$ ways, so there are 6 such g.

6.54.1 The following $g, g', g'' : \mathbb{R}^+ \to \mathbb{R}$ are all right inverses to f. $g(x) := \sqrt{x}$, $g'(x) := -\sqrt{x}$, $g''(x) := \sqrt{x}$ if $x > 1$, $g''(x) := -\sqrt{x}$ otherwise.

6.54.2 The function $\arcsin : [0,1] \to [0,\pi]$ is a right inverse of $\sin$, but so are h given by $h(x) = \pi - \arcsin(x)$, and h' given by $h'(x) = \arcsin(x)$ if $x < \frac{1}{2}$, $h'(x) = \pi - \arcsin(x)$ otherwise. Note: $\arcsin$, the inverse of the $\sin$ function, is predefined in Haskell as `asin`.

6.55 Given: $f : X \to Y$ is a surjection, $h : Y \to X$.
To be proved: h is right-inverse of f iff $h \subseteq \{(f(x), x) \mid x \in X\}$.
Proof:
Only if: Suppose h is right-inverse of f, i.e., $f \circ h = 1_Y$.
Let $(y, x) \in h$ be arbitrary. We have to show that $y = f(x)$.
Since $x = h(y)$, we get from $f \circ h = 1_Y$ that $f(x) = f(h(y)) = (f \circ h)(y) = 1_Y(y) = y$.

If: Suppose $h \subseteq \{(f(x), x) \mid x \in X\}$. Let $y \in Y$ be arbitrary.
Since $h \subseteq \{(f(x), x) \mid x \in X\}$, there is an $x \in X$ with $y = f(x)$ and $h(y) = x$.
Thus $f(x) = f(h(y)) = f \circ h(y) = y$.

6.56.1 To be proved: Every function that has a surjective right-inverse is a bijection.
Proof:
Let $f : X \to Y$, $g : Y \to X$, g surjective, and $f \circ g = 1_Y$.
We show that f is injective:
Let $a_1, a_2 \in X$ be arbitrary, and suppose $f(a_1) = f(a_2)$.
Then, by surjectivity of g, there are $b_1, b_2 \in Y$ with $a_1 = g(b_1)$ and $a_2 = g(b_2)$.
Since $f \circ g = 1_Y$, $f(a_1) = f(g(b_1)) = b_1$, and $f(a_2) = f(g(b_2)) = b_2$.
It follows that $b_1 = f(a_1) = f(a_2) = b_2$. By functionality of g, $a_1 = g(b_1) = g(b_2) = a_2$.

We show that f is surjective:
Let $y \in Y$ be arbitrary. Then $g(y) \in X$, and by $f \circ g = 1_Y$, $f(g(y)) = y$.
So there is an $x \in X$ with $f(x) = y$.

6.56.2 To be proved: Every function that has an injective left-inverse is a bijection.
Proof:
Let $f : X \to Y$, $g : Y \to X$, g injective, and $g \circ f = 1_X$.
We show that f is injective:
Let $a_1, a_2 \in X$ be arbitrary, and suppose $f(a_1) = f(a_2)$.
Then $g(f(a_1)) = g(f(a_2))$, and by $g \circ f = 1_X$, $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$.

We show that f is surjective:
Let $y \in Y$ be arbitrary. Then $g(y) \in X$. We show that $f(g(y)) = y$.
By $g \circ f = 1_X$, $g(f(g(y))) = g(y)$. By injectivity of g, we get from this that $f(g(y)) = y$.

6.57

```
stringCompare :: String -> String -> Maybe Ordering
stringCompare xs ys | any (not . isAlpha) (xs ++ ys) = Nothing
                    | otherwise                      = Just (compare xs ys)
```

6.58.1 Given: $f : A \to I$ is a surjection. $aRb :\equiv f(a) = f(b)$.
To be proved: R is an equivalence on A.
Proof:
Reflexivity: For all $a \in A$, aRa, since $f(a) = f(a)$.
Symmetry: Let aRb. Then $f(a) = f(b)$. Thus $f(b) = f(a)$, and bRa.
Transitivity: Let aRb and bRc. Then $f(a) = f(b)$ and $f(b) = f(c)$.
So $f(a) = f(c)$, and therefore aRc.

6.58.2 Given: $f : A \to I$ is a surjection. $aRb :\equiv f(a) = f(b)$.
To be proved: $A/R = \{f^{-1}[\{i\}] \mid i \in I\}$.
Proof:
$\subseteq$: Let $a \in A$ be arbitrary. We have to show that $|a|_R \in \{f^{-1}[\{i\}] \mid i \in I\}$.
Since $f(a) \in I$, there is an $i \in I$ with $|a|_R = \{b \mid f(b) = f(a)\} = f^{-1}[\{i\}]$.
$\supseteq$: Let $i \in I$ be arbitrary. We have to show that $f^{-1}[\{i\}] \in A/R$.
From surjectivity of f, there is an $a \in A$ with $f(a) = i$.
Thus $f^{-1}[\{i\}] = \{b \mid f(b) = i\} = \{b \mid f(b) = f(a)\} = \{b \mid bRa\} = |a|_R$.

6.58.3 Given: S is an equivalence on A.
To be proved: there is a function g on A with $aSb \;\Leftrightarrow\; g(a) = g(b)$.
Proof:
Take $g : A \to A/S$ given by $g(a) = |a|_S$. Then $aSb \Leftrightarrow b \in |a|_S \Leftrightarrow g(a) = g(b)$.

6.60.1 Given: $f : A \to B$; f an injection.
To be proved: For all sets C and for every $g : A \to C$ there is a $h : B \to C$ with $g = h \circ f$.
Proof:
Let C be arbitrary, with $g : A \to C$.
Since f is an injection, for every $b \in \text{ran}(f)$ there is a unique $a \in A$ with $f(a) = b$.
Define h by means of: if $b \in \text{ran}(f)$ then $h(b) := g(a)$ for the unique a with $f(a) = b$,
otherwise $h(b) = c$ for some arbitrary $c \in C$.
Let $a \in A$ be arbitrary. Then $(h \circ f)(a) = h(f(a)) = g(a)$.

6.60.2 Given: $f : A \to B$;
for all sets C and for every $g : A \to C$ there is a $h : B \to C$ with $g = h \circ f$.
To be proved: f is an injection.
Proof:
Let $a_1, a_2 \in A$ and assume $f(a_1) = f(a_2)$.
Then for any h, $h(f(a_1)) = h(f(a_2))$. Take for g the function 1_A.
Then $a_1 = 1_A(a_1) = (h \circ f)(a_1) = h(f(a_1)) = h(f(a_2)) = (h \circ f)(a_2) = 1_A(a_2) = a_2$.

6.61 Given: R is an equivalence on A.
To be proved: for every equivalence $S \supseteq R$ on A there exists a function $g : A/R \to A/S$
such that, for $a \in A$: $| a |_S = g(| a |_R)$.
Proof:
All we have to show is that $g : A/R \to A/S$ given by $g(| a |_R) = | a |_S$ is well-defined.
Let $x \in A$ be such that xRa. We have to show that $g(| a |_R) = g(| x |_R)$.
From xRa, $|a|_R = |x|_R$, and from $R \subseteq S$, $|a|_S = |x|_S$.
Thus $g(| a |_R) = |a|_S = |x|_S = g(| x |_R)$.

6.62 Given: $\sim$ is an equivalence on A, and $f : A^2 \to A$ is a binary function such that
for all $a, b, x, y \in A$: $a \sim x \ \wedge \ b \sim y \implies f(a, b) \sim f(x, y)$.
To be proved: There is a unique function $f^{\sim} : (A/\sim)^2 \to (A/\sim)$ with, for $a, b \in A$:
$f^{\sim}(|a|, |b|) = |f(a, b)|$.
Proof:
We have to show that $f^{\sim}(|a|, |b|) = |f(a, b)|$ defines a function.
Let $a \sim x$, $b \sim y$. Then $|a| = |x|$, $|b| = |y|$, and $|f(a, b)| = |f(x, y)|$.
Therefore, $f^{\sim}(|a|, |b|) = |f(a, b)| = |f(x, y)| = f^{\sim}(|x|, |y|)$.
This proves that the definition of $f^{\sim}$ is "independent of the representatives of $|a|, |b|$".

6.63 Given: $\sim$ is an equivalence on A, and $R \subseteq A^2$ is a relation such that for all $a, b, x, y \in A$:
$a \sim x \ \wedge \ b \sim y \ \wedge \ aRb \ \Rightarrow \ xRy$.
To be proved: there is a unique relation $R^{\sim} \subseteq (A/\sim)^2$
with for all $a, b \in A$: $|a|R^{\sim}|b| \ \Leftrightarrow \ aRb$.
Proof:
Again, we must show that $R^{\sim}$ is well-defined.
Let $a \sim x$ and $b \sim y$. Then $aRb \Leftrightarrow xRy$.
Therefore, $|a|R^{\sim}|b| \Leftrightarrow aRb \Leftrightarrow xRy \Leftrightarrow |x|R^{\sim}|y|$.
The fact that $R^{\sim} \subseteq (A/\sim)^2$ is immediate from the definition of $R^{\sim}$.

6.64.1 Given: $\sim$ on $A \times B$ defined by $(a, b) \sim (x, y) \ \equiv \ a = x$.
To be proved: $\sim$ is an equivalence on $A \times B$.
Proof:
Reflexivity: $(a, b) \sim (a, b)$, since $a = a$.
Symmetry: If $(a, b) \sim (x, y)$ then $a = x$, so also $(x, y) \sim (a, b)$.
Transitivity: If $(a, b) \sim (x, y)$ and $(x, y) \sim (u, v)$, then $a = x$ and $x = u$.
Therefore $a = u$, and thus $(a, b) \sim (u, v)$.

6.64.2 Given: $\sim$ on $A \times B$ defined by $(a, b) \sim (x, y) \ \equiv \ a = x$. $B \neq \emptyset$.
To be proved: There is a bijection : $(A \times B)/\sim \ \longrightarrow \ A$.
Proof:
We show that $f(|(a, b)|) = a$ defines a bijection.
Firstly, this is well-defined, for let $(a, b) \sim (x, y)$.
Then $a = x$, and therefore $f(|(a, b)|) = a = x = f(|(x, y)|)$.
Next, we show that f is injective and surjective.
For injectivity, assume $f(|(a, b)|) = f(|(x, y)|)$.
Then $a = x$ and therefore $|(a, b)| = |(x, y)|$.
For surjectivity, assume $a \in A$.
Then, since $B \neq \emptyset$, there is a $b \in B$ with $(a, b) \in A \times B$, and $f(|(a, b)|) = a$.

6.64.3 Given: $\sim$ on $A \times B$ defined by $(a, b) \sim (x, y) \ \equiv \ a = x$.
To be proved: For every equivalence class $|(a, b)|$ there is a bijection between $|(a, b)|$ and A.
Proof:
Let $|(a, b)|$ be arbitrary. We show that $F : |(a, b)| \to A$ given by $F(x, y) = y$ is a bijection.
F is injective, for suppose $F(x, y) = F(u, v)$.
Then, since $(x, y) \in |(a, b)|$, $x = a$, and since $(u, v) \in |(a, b)|$, $u = a$.

From the definition of F, $y = v$. So $(x, y) = (u, v)$.
F is surjective, for suppose $y \in B$.
Then $(a, y) \in |(a, b)|$, and $F(a, y) = y$.

6.65

```
fct2listpart :: (Eq a, Eq b) => (a -> b) -> [a] -> [[a]]
fct2listpart f [] = []
fct2listpart f (x:xs) = xclass : fct2listpart f (xs \\ xclass)
   where xclass =  x : [ y | y <- xs, f x == f y ]
```

6.66 Let $f : A \to B$ be a surjection, and suppose $|A| = n$ and $|B| = k$. We can decompose f into $h \cdot g$, where g is the surjection $g : A \to A/R$ ($R = \{(a, b) \in A^2 \mid f(a) = f(b)\}$) given by $g(a) = [a]_R$, and h is the bijection $h : A/R \to B$, given by $h([a]_R) = f(a)$. By Example 5.105, A has $\left\{ {n \atop k} \right\}$ partitions into k blocks, so there are $\left\{ {n \atop k} \right\}$ such g. Since there are $k!$ bijections h on a set of size k, all in all, there are $k!\left\{ {n \atop k} \right\}$ surjections f.

6.68 There is no harm in the two ways to interpret $X_0 \times X_1$, since there is a bijection $F : \prod_{i \in \{0,1\}} X_i \to \{(x, y) \mid x \in X_0 \wedge y \in X_1\}$, given by $Ff = (f(0), f(1))$.

6.69 $F : \wp(A) \to \{0, 1\}^A$ given by $F(X) = \lambda a.(a \in A \wedge a \in X)$ is a bijection. Another bijection is $G : \wp(A) \to \{0, 1\}^A$ given by $G(X) = \lambda a.(a \in A \wedge a \notin X)$.

6.70.1 Given: A relation $\approx$ on $Y^X = \{f \mid f : X \to Y\}$ defined by
$f \approx g \equiv$ there are bijections $i : Y \to Y$ and $j : X \to X$ such that $i \circ f = g \circ j$.
To be proved: $\approx$ is an equivalence.
Proof:
$\approx$ is reflexive, for since $1_Y \circ f = f \circ 1_X$ we have $f \approx f$.
$\approx$ is symmetric, for suppose $f \approx g$.
Then there are bijections $i : Y \to Y$ and $j : X \to X$ with $i \circ f = g \circ j$.
Thus $f = i^{-1} \circ i \circ f = i^{-1} \circ g \circ j$, so $i^{-1} \circ g = i^{-1} \circ g \circ j \circ j^{-1} = f \circ j^{-1}$.
It follows that $g \approx f$.
$\approx$ is transitive, for suppose $f \approx g$ and $g \approx h$.
Then there are bijections i_1, i_2, j_1, j_2 with $i_1 \circ f = g \circ j_1$ and $i_2 \circ g = h \circ j_2$.
Thus, $i_2 \circ i_1 \circ f = i_2 \circ g \circ j_1$ and $i_2 \circ g \circ j_1 = h \circ j_2 \circ j_1$.
Therefore, $i_2 \circ i_1 \circ f = h \circ j_2 \circ j_1$, and it follows that $f \approx h$.

6.70.2 If $f, g : X \to Y$ are injective, then $f \approx g$, for consider the function $i : Y \to Y$ given by

$$i(y) = \begin{cases} g(y) & \text{if } y \in \text{ran}(f), \\ y & \text{otherwise.} \end{cases}$$

From the injectivity of g it follows that i is a bijection. Moreover, $i \circ f = g \circ 1_X$.

6.70.3.1 Let $f = \{(0, 0), (1, 0), (2, 1)\}$ and $g = \{(0, 1), (1, 3), (2, 3)\}$. To show that $f \approx g$ we must find bijections i, j with $i \circ f = g \circ j$. Taking $i = \{(0, 3), (3, 0), (1, 1), (2, 2)\}$ and $j = \{(0, 2), (1, 1), (2, 0)\}$, we get

$$i \circ f = \{(0, 3), (1, 3), (2, 1)\} = g \circ j.$$

6.70.3.2 There are three $\approx$ equivalence classes: the class of the functions that lump all objects together, the class of the functions that lump two of the objects together, and the class of the functions that keep the three objects separate. Representatives for these classes are $f = \{(0,0),(1,0),(2,0)\}$, $f' = \{(0,0),(1,0),(2,1)\}$, $f'' = \{(0,0),(1,1),(2,2)\}$.

6.71.1 Given: X, Y and Z are sets, $h : Y \to Z$, $F : Y^X \to Z^X$ defined by $F(g) := h \circ g$.
To be proved: if h is injective, then F is injective.
Proof:
Suppose h is injective. Let $g_1, g_2 \in Y^X$, i.e., $g_1, g_2 : X \to Y$, with $g_1 \neq g_2$.
From $g_1 \neq g_2$ we get that there is an $x \in X$ with $g_1(x) \neq g_2(x)$.
From the fact that h is injective, $h(g_1(x)) \neq h(g_2(x))$.
But this means that $F(g_1)(x) = (h \circ g_1)(x) = h(g_1(x)) \neq h(g_2(x)) = (h \circ g_2)(x) = F(g_2)(x)$.
Thus, $F(g_1) \neq F(g_2)$, i.e., F is an injection.

6.71.2 Given: X, Y and Z are sets, $h : Y \to Z$, $F : Y^X \to Z^X$ defined by $F(g) := h \circ g$.
To be proved: if h is surjective, then F is surjective.
Proof:
Suppose h is surjective. Let $f \in Z^X$, i.e., $f : X \to Z$.
We have to show that there is a $g : X \to Y$ with $F(g) = f$.
Since h is surjective, we can define g by means of $g(x) =$ some $y \in Y$ with $h(y) = f(x)$.
To show that $F(g) = f$, let $x \in X$ be arbitrary.
Then: $F(g)(x) = (h \circ g)(x) = h(g(x)) = f(x)$.

6.72.1 Given: X, Y and Z are sets, $X \neq \emptyset$, $h : X \to Y$, $F : Z^Y \to Z^X$ defined by $F(g) := g \circ h$.
To be proved: if h is injective, then F is surjective.
Proof:
Suppose h is injective. Let $f : X \to Z$. We have to find $g : Y \to Z$ with $F(g) = f$.
Define g by means of $g(y) = f \circ h^{-1}(y)$ if $y \in \text{ran}(h)$,
and $g(y) =$ some arbitrary member of Z otherwise.
By the injectivity of h this is well-defined.
We have: $F(g)(x) = (g \circ h)(x) = g(h(x)) = (f \circ h^{-1})(h(x)) = f(x)$. So $F(g) = f$.

6.72.2 Given: X, Y and Z are sets, $X \neq \emptyset$, $h : X \to Y$, $F : Z^Y \to Z^X$ defined by $F(g) := g \circ h$.
To be proved: if h is surjective, then F is injective.
Proof:
Suppose h is surjective. Let $g_1, g_2 : Y \to Z$, with $g_1 \neq g_2$.
Since $g_1 \neq g_2$, there is a $y \in Y$ with $g_1(y) \neq g_2(y)$.
Since h is surjective, there is an $x \in X$ with $h(x) = y$, so $g_1(h(x)) \neq g_2(h(x))$.
Now $F(g_1)(x) = (g_1 \circ h)(x) = g_1(h(x)) \neq g_2(h(x)) = (g_2 \circ h)(x) = F(g_2)(x)$. So $F(g_1) \neq F(g_2)$.

6.75 Suppose $m \equiv_n m'$ and $k \equiv_n k'$. We have to show that $m \cdot k \equiv_n m' \cdot k'$.

From $m \equiv_n m'$ we get that there is an $a \in \mathbb{Z}$ with $m' = m + an$. From $k \equiv_n k'$ we get that there is a $b \in \mathbb{Z}$ with $k' = k + bn$. Therefore $m'k' = mk + akn + bmn + abn^2 = mk + (ak + bm + abn)n \equiv_n mk$. It follows that we can define:

$$[m]_n \cdot [k]_n := [m \cdot k]_n.$$

6.78 Given: R on $\mathbb{N}$ given by $(m_1, m_2)R(n_1, n_2) :\equiv m_1 + n_2 = m_2 + n_1$.
$\cdot : \mathbb{N}^2 \to \mathbb{N}$ given by $(m_1, m_2) \cdot (n_1, n_2) = (m_1n_1 + m_2n_2, m_1n_2 + n_1m_2)$.
To be proved: R is a congruence for $\cdot$ on $\mathbb{N}^2$.
Proof:
Assume $(m_1, m_2)R(p_1, p_2)$ and $(n_1, n_2)R(q_1, q_2)$.
We have to show that $(m_1, m_2) \cdot (n_1, n_2)R(p_1, p_2) \cdot (q_1, q_2)$.
From $(m_1, m_2)R(p_1, p_2)$ and $(n_1, n_2)R(q_1, q_2)$:
$(1)\ m_1 + p_2 = p_1 + m_2$ and $(2)\ n_1 + q_2 = q_1 + n_2$.
Multiplying (1) by n_1 and by q_1, and multiplying (2) by m_2 and p_2 we get:

$$\begin{aligned} m_1n_1 + n_1p_2 &= n_1p_1 + m_2n_1 \\ m_2n_1 + n_2p_2 &= m_1n_2 + n_2p_2 \\ p_1q_1 + n_1p_1 &= p_1q_1 + n_2p_1 \\ p_2q_1 + n_2p_2 &= n_1p_2 + p_2q_2. \end{aligned}$$

Add lefthand and righthand sides, and delete terms that occur both left and right:
$m_1n_1 + m_2n_2 + p_1q_2 + p_2q_1 = m_2n_1 + m_1n_2 + p_1q_1 + p_2q_2$.
It follows that $(m_1n_1 + m_2n_2, m_1n_2 + n_1m_2)R(p_1q_1 + p_2q_2, p_1q_2 + q_1p_2)$,
i.e., that $(m_1, m_2) \cdot (n_1, n_2)R(p_1, p_2) \cdot (q_1, q_2)$.

Solutions to Exercises from Chapter 7

```
module Sol7

where

import Data.List
import IAR
```

7.6 To be proved: $\forall n : \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
Proof:
Basis: $\sum_{k=1}^{1} k^2 = 1 = \frac{1 \cdot 2 \cdot 3}{6}$.
Induction step: Assume $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.
We have to show that $\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$.
We have: $\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 \stackrel{ih}{=} \frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$
$= \frac{(n+1)(2n^2+n)}{6} + \frac{(n+1)(6n+6)}{6} = \frac{(n+1)(2n^2+n+6n+6)}{6} = \frac{(n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$.

7.8 To be proved: $\forall n : \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.
Proof:
Basis: $\sum_{k=1}^{1} k^3 = 1 = \left(\frac{1 \cdot 2}{2}\right)^2$.
Induction step: Assume $\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.
We have to show that $\sum_{k=1}^{n+1} k^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2$.
We have: $\sum_{k=1}^{n+1} k^3 = \sum_{k=1}^{n} k^3 + (n+1)^3 \stackrel{ih}{=} \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + \frac{4(n+1)^3}{4} =$
$= \frac{n^2(n+1)^2}{4} + \frac{(4n+4)(n+1)^2}{4} = \frac{(n^2+4n+4)(n+1)^2}{4} = \frac{(n+1)^2(n+2)^2}{4} = \left(\frac{(n+1)(n+2)}{2}\right)^2$.

7.9 Induction proof that for all $n \in \mathbb{N}$: $3^{2n+3} + 2^n$ is divisible by 7.
Basis: $3^{2\cdot 0+3} + 2^0 = 3^3 + 1 = 28 = 7 \cdot 4$.
Induction step: Assume that $3^{2n+3} + 2^n$ is divisible by 7, i.e., $\exists a \in \mathbb{N} : 3^{2n+3} + 2^n = 7a$.
We have to show that $3^{2(n+1)+3} + 2^{n+1}$ is divisible by 7.
We have:

$$\begin{aligned} 3^{2(n+1)+3} + 2^{n+1} &= 3^{2n+2+3} + 2^{n+1} \\ &= 3^2 \cdot 3^{2n+3} + 3^2 \cdot 2^n - (3^2 - 2) \cdot 2^n \\ &= 3^2(3^{2n+3} + 2^n) - 7 \cdot 2^n \\ &\overset{ih}{=} 3^2(7a) - 7 \cdot 2^n = 7(3^2 \cdot a - 2^n). \end{aligned}$$

This proves that $3^{2(n+1)+3} + 2^{n+1}$ is divisible by 7.

7.12.1 $m \cdot 1 \overset{+.1}{=} m \cdot (1+0) \overset{+\text{comm}}{=} m \cdot (0+1) \overset{\cdot 2}{=} (m \cdot 0) + m \overset{\cdot 1}{=} 0 + m \overset{+\text{comm}}{=} m + 0 \overset{+.1}{=} m$.

7.12.2 We prove $m \cdot (n+k) = (m \cdot n) + (m \cdot k)$ by induction on k.
Basis:

$$m \cdot (n+0) \overset{+.1}{=} m \cdot n \overset{+.1}{=} m \cdot n + 0 \overset{\cdot 1}{=} m \cdot n + m \cdot 0.$$

Induction step:

$$\begin{aligned} m \cdot (n + (k+1)) &\overset{+\text{ass}}{=} m \cdot ((n+k)+1) \\ &\overset{\cdot 2}{=} m \cdot (n+k) + m \\ &\overset{ih}{=} (m \cdot n + m \cdot k) + m \\ &\overset{+\text{ass}}{=} m \cdot n + (m \cdot k + m) \\ &\overset{\cdot 2}{=} m \cdot n + m \cdot (k+1). \end{aligned}$$

7.12.3 We prove $m \cdot (n \cdot k) = (m \cdot n) \cdot k$ by induction on k.
Basis:

$$m \cdot (n \cdot 0) \overset{\cdot 1}{=} m \cdot 0 \overset{\cdot 1}{=} 0 \overset{\cdot 1}{=} (m \cdot n) \cdot 0.$$

Induction step:

$$\begin{aligned} m \cdot (n \cdot (k+1)) &\overset{\cdot 2}{=} m \cdot (n \cdot k + n) \\ &\overset{\cdot \text{dist}}{=} m \cdot (n \cdot k) + m \cdot n \\ &\overset{ih}{=} (m \cdot n) \cdot k + m \cdot n \\ &\overset{\cdot 2}{=} (m \cdot n) \cdot (k+1). \end{aligned}$$

7.12.4 To prove $m \cdot n = n \cdot m$, we use induction on n.
Basis:

$$m \cdot 0 \overset{\cdot 1}{=} 0 \overset{\cdot 1}{=} 0 \cdot 0 \overset{\cdot 1}{=} 0 \cdot (m \cdot 0) \overset{\cdot 1}{=} 0 \cdot m.$$

Induction step:

$$m \cdot (n+1) \stackrel{\cdot 2}{=} m \cdot n + m \stackrel{+\text{ass}}{=} m + m \cdot n \stackrel{\cdot \text{id}}{=} m \cdot 1 + m \cdot n \stackrel{\cdot \text{dist}}{=} m \cdot (1+n).$$

7.13 We prove $k^{m+n} = k^m \cdot k^n$ by induction on n.
Basis:

$$k^{m+0} \stackrel{+.1}{=} k^m \stackrel{\cdot \text{id}}{=} k^m \cdot 1 \stackrel{\exp 1}{=} k^m \cdot k^0.$$

Induction step:

$$\begin{array}{lll} k^{m+(n+1)} & \stackrel{+\text{ass}}{=} & k^{(m+n)+1} \\ & \stackrel{\exp 2}{=} & k^{m+n} \cdot k \\ & \stackrel{ih}{=} & (k^m \cdot k^n) \cdot k \\ & \stackrel{\cdot \text{ass}}{=} & k^m \cdot (k^n \cdot k) \\ & \stackrel{\exp 2}{=} & k^m \cdot k^{n+1}. \end{array}$$

7.14

```
subtr :: Natural -> Natural -> Natural
subtr Z _         = Z
subtr m Z         = m
subtr (S m) (S n) = subtr m n
```

7.15

```
qrm :: Natural -> Natural -> (Natural,Natural)
qrm m n | gt n m    = (Z,m)
        | otherwise = (S (fst qr), snd qr) where qr = qrm (subtr m n) n

quotient ::  Natural -> Natural -> Natural
quotient m n  = fst (qrm m n)

remainder ::  Natural -> Natural -> Natural
remainder m n  = snd (qrm m n)
```

7.16

```
pre :: Natural -> Natural
pre Z = Z
pre (S n) = n

subtr :: Natural -> Natural -> Natural
subtr = foldn pre
```

7.17 Basis: $F_2F_0 - F_1^2 = 0 - 1 = -1 = (-1)^1$.
Induction step: Assume $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. Then:

$$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= (F_n + F_{n+1})F_n - F_{n+1}^2 = F_n^2 + F_nF_{n+1} - F_{n+1}^2 \\ &= F_n^2 - F_{n+1}(F_{n+1} - F_n) = F_n^2 - F_{n+1}F_{n-1} \\ &\stackrel{ih}{=} -(-1)^n = (-1)^{n+1} \end{aligned}$$

7.18.1 The empty list satisfies bittest, so $a_0 = 1$. Both $[1]$ and $[0]$ satisfy bittest, so $a_1 = 2$. $[1,1], [1,0], [0,1]$ are the lists of length 2 satisfying bittest, so $a_2 = 3$.

$$[0,1,1], [0,1,0, [1,1,1], [1,1,0], [1,0,1]$$

are the satisfying lists of length 3, so $a_3 = 5$.
7.18.2 Here is a proof by induction of $a_n = F_{n+2}$ for all $n \geqslant 0$. Basis: $a_0 = 1 = F_2$, $a_1 = 2 = F_3$.
Induction step: assume that $a_n = F_{n+2}$ en $a_{n+1} = F_{n+3}$. We have to show that $a_{n+2} = F_{n+4}$.
From the bittest we know that the bitlists of length $n+2$ satisfying the test can be got by either prefixing $[1]$ to a bitlist of length $n+1$ or prefixing $[0,1]$ to a bitlist of length n. According to the induction hypothesis, the first can be done in $a_{n+1} = F_{n+3}$ ways, the second in $a_n = F_{n+2}$ ways. Together this gives $a_{n+2} = F_{n+3} + F_{n+2} = F_{n+4}$.
7.19 We show that for all i, n it holds that `fib2 (fib i) (fib (i+1)) n = fib (i+n)`, by induction on n.
Basis: `fib2 (fib i) (fib (i+1)) 0 = fib (i)`: immediate from the definition of `fib2`.
Induction step: Suppose $\forall i$: `fib2 (fib i) (fib (i+1)) n = fib (i+n)`.
We have to show that $\forall i$: `fib2 (fib i) (fib (i+1)) (n+1) = fib (i+n+1)`.
Let i be arbitrary.

```
fib2 (fib i) (fib (i+1)) (n+1)  =fib2 2=  fib2 (fib (i+1)) ((fib i) + (fib (i+1))) n
                                =fib 3=  fib2 (fib (i+1)) (fib (i+2)) n
                                =ih=     fib (i+n+1)
```

Note that the induction hypothesis applies to the case of $i+1$ since it holds for all i. Since i was arbitrary we have established the claim for all n and i.

7.20

```
catalan :: Integer -> Integer
catalan 0     = 1
catalan (n+1) = sum [ (catalan i) * (catalan (n-i)) | i <- [0..n] ]
```

7.21 Basis: in case there is just one variable x_0 there is just one possible bracketing.

Induction step: We assume as induction hypothesis that for any i with $0 \leqslant i \leqslant n$, for any sequence of $i+1$ variables $x_0 \cdots x_i$ it holds that C_i gives the number of bracketings for that sequence. We have to show that C_{n+1} is the number of bracketings for $n+2$ variables.

Any bracketing for a sequence $x_0 \cdots x_{n+1}$ of $n+2$ variables has a main operator: the operator for the final multiplication that takes place. This is the operator outside brackets. Suppose this operator is between x_i and x_{i+1}, with $0 \leqslant i \leqslant n$. Then, by the induction hypothesis, there are C_i ways to bracket $x_0 \cdots x_i$ and C_{n-i} ways to bracket $x_{i+1} \cdots x_{n+1}$. This gives $C_i C_{n-i}$ bracketings. Summing over i we get $\sum_{i=0}^{n} C_i C_{n-i}$ for the number of bracketings, which by definition equals C_{n+1}.

7.25

```
data TernTree = L' | N' TernTree TernTree TernTree deriving Show

makeTernTree :: Integer -> TernTree
makeTernTree 0       = L'
makeTernTree (n + 1) = N'
   (makeTernTree n) (makeTernTree n) (makeTernTree n)

count3 :: TernTree -> Integer
count3 L'            = 1
count3 (N' t1 t2 t3) = 1 + count3 t1 + count3 t2 + count3 t3
```

7.27 Proof that $\sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$, by induction on n.
Basis: $\sum_{k=0}^{0} q^k = q^0 = 1 = \frac{q-1}{q-1}$.
Induction step: Assume $\sum_{k=0}^{n} q^k = \frac{q^{n+1}-1}{q-1}$. Then: $\sum_{k=0}^{n+1} q^k = \sum_{k=0}^{n} q^k + q^{n+1} \stackrel{ih}{=} \frac{q^{n+1}-1}{q-1} + q^{n+1} = \frac{q^{n+1}-1}{q-1} + \frac{q^{n+1}(q-1)}{q-1} = \frac{q^{n+2}-1}{q-1}$.

7.28

```
insertTree :: Int -> Tree -> Tree
insertTree n Lf = (Nd n Lf Lf)
insertTree n t@(Nd m left right)
     | m < n     = Nd m left (insertTree n right)
     | m > n     = Nd m (insertTree n left) right
     | otherwise = t
```

7.29

```
list2tree :: [Int] -> Tree
list2tree [] = Lf
list2tree (n:ns) = insertTree n (list2tree ns)

tree2list :: Tree -> [Int]
tree2list Lf = []
tree2list (Nd n left right) = tree2list left ++ [n] ++ tree2list right
```

7.30

```
inTree :: Int -> Tree -> Bool
inTree n Lf = False
inTree n (Nd m left right) | n == m = True
                           | n <  m = inTree n left
                           | n >  m = inTree n right
```

7.31

```
mergeTrees :: Tree -> Tree -> Tree
mergeTrees t1 t2 = foldr insertTree t2 (tree2list t1)
```

7.32

```
findDepth :: Int -> Tree -> Int
findDepth _ Lf = -1
findDepth n (Nd m left right)
    | n == m = 0
    | n <  m = if d1 == -1 then -1 else d1 + 1
    | n >  m = if d2 == -1 then -1 else d2 + 1
  where d1 = findDepth n left
        d2 = findDepth n right
```

7.33

```
mapT ::  (a -> b) -> Tr a -> Tr b
mapT f Nil = Nil
mapT f (T x left right) = T (f x) (mapT f left) (mapT f right)
```

7.34

```
foldT :: (a -> b -> b -> b) -> b -> (Tr a) -> b
foldT h c Nil = c
foldT h c (T x left right) = h x (foldT h c left) (foldT h c right)
```

This gives:

```
Sol7>  foldT (\ x y z -> sum [x,y,z]) 0 (T 4 (T 5 Nil Nil)(T 6 Nil Nil))
15
```

7.35

```
preorderT, inorderT, postorderT :: Tr a -> [a]
preorderT = foldT preLists []
  where preLists x ys zs = (x:ys) ++ zs
inorderT = foldT inLists []
  where inLists x ys zs = ys ++ [x] ++ zs
postorderT = foldT postLists []
  where postLists x ys zs = ys ++ zs ++ [x]
```

7.36

```
orderedT :: Ord a => Tr a -> Bool
orderedT tree = ordered (inorderT tree)
  where
  ordered xs = (sort (nub xs) == xs)
```

7.37

```
lookupD :: String -> Dict -> [String]
lookupD _ Nil = []
lookupD x (T (v,w) left right) | x == v    = [w]
                               | x < v     = lookupD x left
                               | otherwise = lookupD x right
```

7.38

```
buildTree :: [a] -> Tr a
buildTree [] = Nil
buildTree xs = T m (buildTree left) (buildTree right)
   where (left,m,right) = split xs
```

7.39

```
mapLT :: (a -> b) -> LeafTree a -> LeafTree b
mapLT f (Leaf x) = Leaf (f x)
mapLT f (Node left right) =  Node (mapLT f left) (mapLT f right)
```

7.40

```
reflect :: LeafTree a -> LeafTree a
reflect (Leaf x) = Leaf x
reflect (Node left right) = Node (reflect right) (reflect left)
```

7.41 We show with induction on the structure of `t` that `reflect (reflect t) == t`.
Basis: Because `reflect (Leaf x) == (Leaf x)` it certainly holds that

```
reflect (reflect (Leaf x)) == (Leaf x).
```

Induction step: Assume that

```
reflect (reflect left) == left
reflect (reflect right) == right.
```

Now consider `reflect (Node left right)`. According to the definition of `reflect` this is equal to:

```
Node (reflect right) (reflect left).
```

Applying `reflect` on this again gives:

```
reflect (Node (reflect right) (reflect left)).
```

Again according to the definition of `reflect`, this is equal to:

```
Node (reflect (reflect left)) (reflect (reflect right)).
```

Applying the induction hypothesis twice we get:

```
reflect (reflect (Node left right)) == Node left right.
```

This completes the inductive argument.

7.42

```
mapR :: (a -> b) -> Rose a -> Rose b
mapR f (Bud x)  = Bud (f x)
mapR f (Br roses) = Br (map (mapR f) roses)
```

7.44 Proof that `cat xs [] = cat [] xs` by list induction on `xs`.
Basis: Immediate from `(cat [] [])` $\stackrel{\text{cat.1}}{=}$ `[]`.
Induction step:

$$\begin{aligned}
\texttt{cat (x:xs) []} &\stackrel{\text{cat.2}}{=} \texttt{x : (cat xs [])} \\
&\stackrel{ih}{=} \texttt{x : (cat [] xs)} \\
&\stackrel{\text{cat.1}}{=} \texttt{(x:xs)} \\
&\stackrel{\text{cat.1}}{=} \texttt{cat [] (x:xs)}.
\end{aligned}$$

7.45 Proof that `len (cat xs ys) = (len xs) + (len ys)`, by list induction on `xs`.
Basis: If `xs = []` then

$$\texttt{len (cat [] ys)} \stackrel{\text{cat.1}}{=} \texttt{len ys} = 0 + \texttt{len ys} \stackrel{\text{len.1}}{=} \texttt{len []} + \texttt{len ys}.$$

Induction step: Assume `len (cat xs ys) = (len xs) + (len ys)`. Then:

$$\begin{aligned}
\texttt{len (cat (x:xs) ys)} &\stackrel{\text{cat.2}}{=} \texttt{len (x:(cat xs ys))} \\
&\stackrel{\text{len.2}}{=} 1 + \texttt{len (cat xs ys)} \\
&\stackrel{ih}{=} 1 + \texttt{len xs} + \texttt{len ys} \\
&\stackrel{len.2}{=} \texttt{len (x:xs)} + \texttt{len ys}.
\end{aligned}$$

7.46

```
genUnion :: Eq a => [[a]] -> [a]
genUnion = foldr union []

genIntersect :: Eq a => [[a]] -> [a]
genIntersect = foldr1 intersect
```

7.47

```
insrt :: Ord a => a -> [a] -> [a]
insrt x [] = [x]
insrt x (y:ys) = if x <= y then (x:y:ys) else y : (insrt x ys)

srt :: Ord a => [a] -> [a]
srt = foldr insrt []
```

7.48 The relation between h and h' is given by

$$h\ x\ (h'\ z\ y) = h'\ (h\ x\ z)\ y. \qquad (*)$$

Here is the inductive proof.

Basis:

$$h\ x\ (\text{foldl}\ h'\ y\ []) \overset{\text{foldl.1}}{=} h\ x\ y \overset{\text{foldl.1}}{=} \text{foldl}\ h'\ (h\ x\ y)\ [].$$

Induction step: Assume

```
h x (foldl h' y zs) = foldl h' (h x y) zs
```

We have to show:

```
h x (foldl h' y (z:zs)) = foldl h' (h x y) (z:zs)
```

We have:

$$\begin{aligned} h\ x\ (\text{foldl}\ h'\ y\ \text{(z:zs)}) &\overset{\text{foldl.2}}{=} h\ x\ (\text{foldl}\ h'\ (h'\ y\ z)\ \text{zs}) \\ &\overset{\text{ih}}{=} \text{foldl}\ h'\ (h\ x\ (h'\ y\ z))\ \text{zs} \\ &\overset{(*)}{=} \text{foldl}\ h'\ (h'\ (h\ x\ y)\ z)\ \text{zs} \\ &\overset{\text{foldl.2}}{=} \text{foldl}\ h'\ (h\ x\ y)\ \text{(z:zs)}. \end{aligned}$$

7.50 In fact, `rev1` follows the recursive definition pattern of `foldl`, so `rev` and `rev1` behave almost the same, and are both much more effficient than `rev'`.

7.52 Proof by induction on `xs` that

$$\text{filter}\ p\ (\text{map}\ f\ \text{xs}) = \text{map}\ f\ (\text{filter}\ (p \cdot f)\ \text{xs}).$$

Basis:

$$\text{filter}\ p\ (\text{map}\ f\ []) = [] = \text{map}\ f\ (\text{filter}\ (p.f)\ []).$$

Induction step: Assume

$$\text{filter}\ p\ (\text{map}\ f\ \text{xs}) = \text{map}\ f\ (\text{filter}\ (p.f)\ \text{xs}).$$

Consider `(x:xs)`. There are two cases: (i) $p(fx) =$ **t** and (ii) $p(fx) =$ **f**.
In case (i) we have:

$$\begin{aligned}
\text{filter } p \text{ (map } f \text{ (x:xs))} &\overset{\text{map}}{=} \text{filter } p \text{ } (f\ x) : (\text{map } f \text{ (x:xs)}) \\
&\overset{\text{filter}}{=} (f\ x) : (\text{filter } p \text{ (map } f \text{ (x:xs)})) \\
&\overset{\text{ih}}{=} (f\ x) : (\text{map } f \text{ (filter } (p.f) \text{ xs})) \\
&\overset{\text{map}}{=} \text{map } f \text{ } (x : (\text{filter } (p.f) \text{ xs})) \\
&\overset{\text{filter}}{=} \text{map } f \text{ (filter } (p.f) \text{ (x:xs)}).
\end{aligned}$$

In case (ii) we have:

$$\begin{aligned}
\text{filter } p \text{ (map } f \text{ (x:xs))} &\overset{\text{map}}{=} \text{filter } p \text{ } (f\ x) : (\text{map } f \text{ (x:xs)}) \\
&\overset{\text{filter}}{=} \text{filter } p \text{ (map } f \text{ (x:xs))} \\
&\overset{\text{ih}}{=} \text{map } f \text{ (filter } (p.f) \text{ xs)} \\
&\overset{\text{map}}{=} \text{map } f \text{ (filter } (p.f) \text{ xs)} \\
&\overset{\text{filter}}{=} \text{map } f \text{ (filter } (p.f) \text{ (x:xs)}).
\end{aligned}$$

7.51

```
ln' :: [a] -> Natural
ln' = foldl S Z
```

7.53.1 $2^n - 1$ moves.

7.53.2 Assume that A is the source peg, B the auxiliary peg, and C the destination peg. We show by induction on n that $2^n - 1$ moves suffice for transferring a Hanoi tower of n disks, and that transfer in less than $2^n - 1$ moves is impossible.
Basis: Transferring a tower with no disks takes no moves at all.
Induction step: Assume that it takes $2^n - 1$ moves to transfer a Hanoi tower of n disks.
We have to show that it takes $2^{n+1} - 1$ moves to transfer a tower of $n + 1$ disks.
As induction hypothesis we assume that n disks can be moved in $2^n - 1$ moves, but not in less than that. Then to move the largest disk from A to C, all other disks must be stacked on B. By the induction hypothesis this can be done in $2^n - 1$, and not in less than $2^n - 1$ moves. Next, it takes one move to get the largest disk from A to C. Notice that this disk cannot go anywhere else, for peg B is occupied by the stack $[1..n]$. Finally, n disks have to be moved from B to C; again this can be done in $2^n - 1$, and not in less than $2^n - 1$ moves. This proves that, all in all, the optimal transfer procedure takes exactly $(2^n - 1) + 1 + (2^n - 1) = 2^{n+1} - 1$ moves.

7.53.3 $2^8 - 1 = 255$ moves.

7.54 Disk k makes exactly 2^{n-k} moves. To prove this with induction, we prove by induction on m that the disk of size $n - m$ makes 2^m moves. From this the result follows, since $k = n - m$ implies $m = n - k$.

Basis: For $m = 0$ we get that the disk of size $n = n - 0$ makes $2^0 = 1$ move. This is correct, for the largest disk moves exactly once, from source to destination.
Induction step: Assume that disk $n-m$ makes 2^{n-m} moves. Now there are two kinds of moves for disk $n-(m+1)$: (i) move it on top of disk $n - m$, or (ii) remove it from disk $n - m$. This makes clear that to every single move of disk $n - m$ there are two moves of disk $n - (m + 1)$, giving $2 \times 2^{n-m} = 2^{n-(m+1)}$ moves altogether.
Finally, note that this outcome squares with the result of the previous exercise, for if disk k makes 2^{n-k} moves the total number of moves is $\sum_{k=1}^{n} 2^{n-k}$. Since $1 + \sum_{k=1}^{n} 2^{n-k} = 2^n$ (use binary representation to see this) we get $\sum_{k=1}^{n} 2^{n-k} = 2^n - 1$.

7.55 Complete transfer of the tower of Brahma takes $2^{64} - 1 = 18446744073709551615$ moves, which, at a rate of one move per day, keeps the monks occupied for 50504432782230120 years, taking leap years into account.

7.56 We prove by induction on n that `check n (xs,ys,zs)` gives `True` iff `(xs,ys,zs)` is a correct configuration.
Basis. The only correct configuration with no disks at all is `([],[],[])`.
Induction step. Suppose that `check n (xs,ys,zs)` gives `True` iff `check n (xs,ys,zs)` is a correct configuration. Let `(xs,ys,zs)` be a configuration with largest disk $n + 1$. Then either `xs` has disk $n + 1$ at the bottom or `zs` has. In the first case, we are in the process of moving `init xs` to `ys`, with auxiliary stack `zs`, and `check n (xs,ys,zs)` holds iff `check (n-1) (init xs, zs, ys)` does. In the second case, we are in the process of moving `ys` to `init zs`, using `xs` as auxiliary stack, and we have:
`check n (xs,ys,zs)` holds iff `check (n-1) (ys, xs, init zs)` does.

7.57 Here is a proof by induction on n.
Basis: if `(xs,ys,zs) == ([],[],[])` there is nothing to check.
Induction step: Suppose `(xs,ys,zs)` with largest disk n is correct iff it holds that every disk m is either on top of a disk k with $k-m$ odd, or at the bottom of the source or destination peg, with $(n+1)-m$ odd, or at the bottom of the auxiliary peg, with $n - k$ odd. We have to show that `(xs,ys,zs)` with largest disk $n + 1$ is correct iff it holds that every disk m is either on top of a disk k with $k - m$ odd, or at the bottom of the source or destination peg, with $(n+1) - m$ even, or at the bottom of the auxiliary peg, with $(n+1) - k$ odd. For m on top of $k \neq n+1$, this follows from the fact that `(xs,ys,zs)` is correct iff either `xs` has $n + 1$ at the bottom and `(init xs, zs, ys)` is correct or `zs` has $n + 1$ at the bottom and `(ys, xs, init zs)` is correct. For m at the bottom of a stack, there are two cases: $m = n + 1$ and $m < n + 1$. In the first case, it follows from the fact that $n + 1$ must be at source or destatination. In the second case, if m is at source, $n + 1$ must be at destination, and the claim follows from the fact that `(ys, xs, init zs)` is correct. If m is at destination, $n + 1$ must be at source, and the claim follows from the fact that `(init xs, zs, ys)` is correct. If m is at auxiliary, either $n + 1$ is at source and the claim follows from the fact that `(ys,xs, init zs)` is correct, or $n + 1$ is at target, and the claim follows from the fact that `(init xs, zs, ys)` is correct.

7.58 Suppose `(xs, zs, ys)` is a correct configuration. Then if all stacks are empty, the law holds, for `parity ([],[],[])` equals $(1, 0, 1)$. Otherwise, one of the stacks has 1 on top, so this stack has parity 1. Now suppose either both other stacks have parity 1 or both other stacks have parity 0. It is easy to check that removing the largest disk and swapping auxiliary and destination (if the largest disk was on the source) or source and auxiliary (if the largest disk was on the destination) does not change parity. After n steps this gives a contradiction with the fact that the parity of `([],[],[])` equals $(1, 0, 1)$.

7.59 Moving 1 to a peg with an even disk at the top, or to an empty peg at even position are the only moves that

will result in a correct configuration.

7.60 If t and t' are two correct tower configurations, and the numbers of disks is different, then the configuration with the smallest number of disks comes first.

If the numbers of disks are the same, then configurations with the largest disk at the source are smaller than configurations with the largest disk at the destination. For the cases with largest disk at the same position we can use recursion.

In the implementation below, we let the output be of type `[Ordering]`, where `Ordering` is the predeclared type consisting of the constants `EQ`, `LT` and `GT`. The value `[]` indicates that at least one of the configurations to be compared is incorrect. In all other cases a unit list indicating the order is generated.

```
compareT :: Tower -> Tower -> [Ordering]
compareT t t' | maxT t < maxT t' = [ LT | checkT t && checkT t' ]
              | maxT t > maxT t' = [ GT | checkT t && checkT t' ]
              | otherwise        = [ compare' t t' | checkT t && checkT t' ]
```

```
compare' :: Tower -> Tower -> Ordering
compare' ([],[],[]) ([],[],[])   = EQ
compare' t@(xs,ys,zs) t'@(xs',ys',zs')
  | firstStage t && firstStage t' =
    compare' (init xs, zs, ys) (init xs', zs', ys')
  | lastStage t  && lastStage t'  =
    compare' (ys, xs, init zs) (ys', xs', init zs')
  | firstStage t && lastStage t'  = LT
  | lastStage t  && firstStage t' = GT
  where
  firstStage (xs,ys,zs) = xs /= [] && last xs == maxT t
  lastStage  t = not (firstStage t)
```

7.61

```
hanoi'' :: Int -> [Tower]
hanoi'' n = [ hanoiCount n k | k <- [0..2^(toInteger n)-1] ]
```

7.62 The key to the implementation is the observation that the initial configuration of a tower with disk size n is preceded in the ordering of all tower configurations by $2^n - 1$ configurations for towers of smaller sizes, as is easily proved by induction.

```
fromTower :: Tower -> Integer
fromTower t = (2^n - 1) + (fromT t n) where
  n = maxT t
  fromT (xs,ys,zs) k
    | xs == [1..k] = 0
    | elem k xs    = fromT  (init xs, zs, ys) (k-1)
    | elem k zs    = 2^(k-1) +  fromT  (ys, xs, init zs) (k-1)
    | otherwise    = error "not a proper tower configuration"
```

Solutions to Exercises from Chapter 8

```
module Sol8
where

import WWN
```

8.1

```
toBase :: Integral a => a -> a -> [Int]
toBase b n | b < 2 || b > 16 = error "base not in [2..16]"
           | n < 0           = error "negative argument"
           | otherwise       = reverse (toB b n)
    where
    toB b n | n < b     = [fromIntegral n]
            | otherwise = fromIntegral (rem n b) : toB b (quot n b)

hex :: (Integral a) => a -> String
hex = showDigits . toBase 16
```

8.2 Let $m, n \in \mathbb{N}$. Then there are $a, r \in \mathbb{N}$ with $m = an + r$ and $0 \leqslant r < n$. We show that for all $d \in \mathbb{N}$: $d \mid m \wedge d \mid n$ iff $d \mid n \wedge d \mid r$. From this it immediately follows that $\text{GCD}(m, n) = \text{GCD}(n, r)$.

Suppose $d \mid m$ and $d \mid n$. Then there are $e, f \in \mathbb{N}$ with $m = ed$ and $n = fd$. Then $r = m - an = ed - afd = (e - af)d$, i.e., $d \mid r$.
Conversely, suppose $d \mid n$ and $d \mid r$. Then there are $e, f \in \mathbb{N}$ with $n = ed$ and $r = fd$. Then $m = an + r = aed + fd = (ae + f)d$, i.e., $d \mid m$.

8.3 We have to establish that if m and n are coprime then m and $m + n$ are.
Assume m and n are coprime. Suppose that there is a $d > 1$ in $\mathbb{N}$ with $d \mid m$ and $d \mid (m + n)$. Then there are $a, b \in \mathbb{N}$ with $m = ad$ and $m + n = bd$. Thus $n = (m + n) - m = bd - ad = (b - a)d$. Contradiction with the fact that m and n are coprime.

8.9 The following establishes associativity of addition for difference pairs:

$$\begin{array}{lcl}
(m_1, m_2) + ((n_1, n_2) + (k_1, k_2)) & = & \text{[definition of } + \text{ for difference pairs]} \\
(m_1, m_2) + ((n_1 + k_1, n_2 + k_2)) & = & \text{[definition of } + \text{ for difference pairs]} \\
(m_1 + (n_1 + k_1), m_2 + (n_2 + k_2)) & = & \text{[commutativity of } + \text{ for } \mathbb{N}\text{]} \\
((m_1 + n_1) + k_1, (m_2 + n_2) + k_2) & = & \text{[definition of } + \text{ for difference pairs]} \\
((m_1 + n_1), (m_2 + n_2)) + (k_1, k_2) & = & \text{[definition of } + \text{ for difference pairs]} \\
((m_1, m_2) + (n_1, n_2)) + (k_1, k_2). & &
\end{array}$$

8.11

```
leq1 :: NatPair -> NatPair -> Bool
leq1 (m1,m2) (n1,n2) = (m1+n2) <= (m2+n1)

gt1 :: NatPair -> NatPair -> Bool
gt1 p1 p2  = not (p1 `leq1` p2)
```

8.14 Brute force comparision of all the decimal expansions of rationals p/q with p and q in the specified range is computationally unfeasible. Still, the following tool is all we need for finding an answer:

```
periods :: [Rational] -> [Int]
periods xs = map periodLength xs
  where
  periodLength x = length (third (decForm x))
  third (_,_,c)  = c
```

It helps to observe that the period of p/q is always less than or equal to that of $1/q$. Next, it helps to observe that the chances of finding a high period increase with the size of q. Therefore, the following query should contain the answer.

```
Sol8> periods [ 1 % q | q <- [971..999] ]
[970,27,138,486,6,60,976,81,44,42,108,490,982,5,98,112,138,18,
462,2,495,15,110,210,99,41,166,498,3]
```

The biggest period is that of $\frac{1}{983}$, which is 982.

8.16 Suppose $\exists p, q \in \mathbb{N}$ with $\left(\frac{p}{q}\right)^2 = 3$ and p and q coprime. Then $\frac{p^2}{q^2} = 3$, so $p^2 = 3q^2$. It follows that p has a factor 3, for if 3 is not a factor of p then 3 is not a factor of p^2. Therefore $p = 3a$ for some $a \in \mathbb{N}$.

Thus, $p^2 = (3a)^2 = 9a^2 = 3q^2$, and we get that $q^2 = 3a^2$. From this it follows that q also has a factor 3, and contradiction with the assumption that p and q are coprime.

8.17 To be proved: if p is prime then $\sqrt{p} \notin \mathbb{Q}$.
Proof: Assume p prime, and suppose $\sqrt{p} \in \mathbb{Q}$. Then there are $n, m \in \mathbb{N}$ with $\left(\frac{n}{m}\right)^2 = p$, with n and m coprime. Then $\frac{n^2}{m^2} = p$, and therefore $n^2 = pm^2$. From the fact that p is prime we get that n has a factor p, because squaring does not introduce any new prime factors. Thus, there is an $a \in \mathbb{N}$ with $n = pa$. From this we get $n^2 = p^2a^2 = pm^2$, and thus $m^2 = pa^2$. It follows that m also has p as a factor, and contradiction with the fact that n and m are coprime.

8.18 To be proved: if $n \in \mathbb{N}$ and $\sqrt{n} \notin \mathbb{N}$, then $\sqrt{n} \notin \mathbb{Q}$.
Proof: Assume $n \in \mathbb{N}$ and $\sqrt{n} \notin \mathbb{N}$, and suppose $\sqrt{n} \in \mathbb{Q}$. Then there are $p, q \in \mathbb{N}$ with $\sqrt{n} = \frac{p}{q}$, with p and q coprime. From p and q coprime it follows that p^2 and q^2 are coprime (squaring does not introduce new prime factors). On the other hand we get from $\sqrt{n} = \frac{p}{q}$ that $n = \frac{p^2}{q^2}$, and therefore $q^2 \mid p^2$, and contradiction.

8.19 Take $x = \sqrt{2}$ and $y = -\sqrt{2}$. Then $x + y = 0 \in \mathbb{Q}$, but x and y are both irrational.

8.20.1 Let $a_0 > 0$. For all $n \geqslant 0$ we get:

$$a_{n+1} - \sqrt{p} = \frac{1}{2}(a_n + \frac{p}{a_n}) - \sqrt{p} = \frac{a_n^2 + p - 2a_n\sqrt{p}}{2a_n} = \frac{(a_n - \sqrt{p})^2}{2a_n}.$$

Similarly, we get:

$$a_{n+1} + \sqrt{p} = \frac{(a_n + \sqrt{p})^2}{2a_n}.$$

From $a_0 > 0$ and the definition of a_{n+1}, it is clear that $a_n > 0$ for all n. Therefore,

$$\frac{a_{n+1} - \sqrt{p}}{a_{n+1} + \sqrt{p}} = \frac{(a_n - \sqrt{p})^2}{(a_n + \sqrt{p})^2}.$$

8.20.2 Since $a_0 > 0$ and $\sqrt{p} > 0$, we get $|a_0 - \sqrt{p}| < a_0 + \sqrt{p}$. Thus,

$$\frac{a_{n+1} - \sqrt{p}}{a_{n+1} + \sqrt{p}} = \left(\frac{a_0 - \sqrt{p}}{a_0 + \sqrt{p}}\right)^{2^n}$$

converges to 0, and therefore $\lim_{n=0}^{\infty} a_n = \sqrt{p}$.

8.20.3 From the first item we get that $\frac{a_{n+1}-\sqrt{p}}{a_{n+1}+\sqrt{p}} \geqslant 0$, for this is a fraction with squares in both numerator and denominator. This means that $a_{n+1} - \sqrt{p} \geqslant 0$, i.e., $a_{n+1} > \sqrt{p}$. In other words, $a_n \geqslant \sqrt{p}$, for all $n \geqslant 1$.

8.21.1 It is easy to see that $a_n - a_{n+1} \geqslant 0$ for every $n \geqslant 1$. For we have $a_n - a_{n+1} = a_n - \frac{1}{2}(a_n + \frac{p}{a_n}) = \frac{1}{2}(a_n - \frac{p}{a_n}) = \frac{a_n^2 - p}{2a_n} \geqslant 0$, because $a_n^2 \geqslant p$ for every $n \geqslant 1$.

Because $a_{n+1} \leqslant a_n$ for every $n \geqslant 1$, and also $\sqrt{p} \leqslant a_1$, we get for every $n \geqslant 1$ that $a_n + \sqrt{p} \leqslant a_1 + \sqrt{p} \leqslant 2a_1$. Together with the result from Exercise 8.20.2, this gives:

$$\frac{a_n - \sqrt{p}}{2a_1} \leqslant \left(\frac{a_0 - \sqrt{p}}{a_0 + \sqrt{p}}\right)^{2^n}.$$

From this we get the following estimate of the approximation:

$$0 \leqslant a_n - \sqrt{p} \leqslant 2a_1 \left(\frac{a_0 - \sqrt{p}}{a_0 + \sqrt{p}}\right)^{2^n}.$$

8.21.2 Now for the concrete case. In the approximation of $\sqrt{2}$ we start out from $a_0 = 1$ (the biggest natural number with a square $\leqslant 2$). Thus, $a_1 = 1.5$, and $2a_1 = 3$. Because $1 < \sqrt{2} < 1.5$ we get that $|a_0 - \sqrt{2}| < 0.5$ and $a_0 + \sqrt{2} > 2$. This gives:

$$0 < a_n - \sqrt{2} < 3 \cdot \left(\frac{1}{4}\right)^{2^n} = 3 \cdot 4^{-2^n}.$$

With the help of Hugs we can have a quick look at what this gets us for $n = 1..5$:

```
Prelude> [ 3 * (1 / 4^(2^n)) | n <- [1..5] ]
[0.1875,0.0117188,4.57764e-05,6.98492e-10,1.6263e-19]
```

The numbers of correct decimals for approximations $a_1, \ldots, a_5$, in that order, are $0, 1, 4, 9, 18$. The quadratic convergence property (at every successive approximation step the size of the remaining error gets squared) ensures that this continues as:

$$36, 72, 144, 288, 576, \ldots$$

It follows that the approximation a_{10} of $\sqrt{2}$ is sure to be correct in the first 576 decimals.

8.22 Given: $\lim_{i\to\infty} a_i = a$, $\lim_{i\to\infty} a_i = b$.
To be proved: $a = b$.
Proof:
Assume, for a contradiction, that $a \neq b$, i.e., assume $|a - b| > 0$.
From the given $\lim_{i\to\infty} a_i = a$, we get $\exists n\, \forall i \geqslant n\, (|a - a_i| < \varepsilon)$.
So some n_1 exists such that $\forall i \geqslant n_1\, (|a - a_i| < \varepsilon)$.
In a similar way, from the given $\lim_{i\to\infty} a_i = b$, we get an n_2 with $\forall i \geqslant n_2\, (|b - a_i| < \varepsilon)$.
Let $n = max(n_1, n_2)$. Then, since $n \geqslant n_1, n_2$, both $|a - a_n| < \varepsilon$ and $|b - a_n| < \varepsilon$.
Since $|x + y| \leqslant |x| + |y|$, we get $|a - b| = |a - a_n + a_n - b| \leqslant |a - a_n| + |b - a_n| < 2\varepsilon = |a - b|$, and contradiction.
This proves $a = b$.

8.23.1 Given: $\lim_{i\to\infty} a_i = a$.
To be proved: $\lim_{i\to\infty} a_{2i} = a$.
Proof:
Let ϵ be arbitrary, and let n_0 be an n_0 such that $\forall i \geqslant n_0(|a - a_i| < \epsilon)$ (from the given).
If $i \geqslant n_0$ then $2i \geqslant n_0$, so $\forall i \geqslant n_0(|a - a_{2i}| < \epsilon$.
Therefore $\forall \epsilon > 0 \exists n \forall i \geqslant n(|a - a_{2i}| < \epsilon)$, i.e., $\lim_{i\to\infty} a_{2i} = a$.

8.23.2 Given: $\lim_{i\to\infty} a_i = a$, $f : \mathbb{N} \to \mathbb{N}$ with $\forall n \exists m \forall i \geqslant m\, f(i) \geqslant n$.
To be proved: $\lim_{i\to\infty} a_{f(i)} = a$.
Proof:
Let ϵ be arbitrary, and let n_0 be such that $\forall i \geqslant n_0(|a - a_i| < \epsilon)$ (from the first given).
From the second given we know that there is an m_0 with $\forall i \geqslant m_0(f(i) \geqslant n_0)$.
Thus $\forall i \geqslant m_0(|a - a_{f(i)}| < \epsilon)$.
Therefore $\forall \epsilon > 0 \exists n \forall i \geqslant n(|a - a_{f(i)}| < \epsilon)$, i.e., $\lim_{i\to\infty} a_{f(i)} = a$.

8.24 Given: $\lim_{i\to\infty} a_i = a$, $\lim_{i\to\infty} b_i = b$, $a < b$.
To be proved: there is an n with $\forall m \geqslant n(a_m < b_m)$.
Proof:
Let n_1 be such that $\forall i \geqslant n_1(|a - a_i| < \epsilon)$ (from the first given).
Let n_2 be such that $\forall i \geqslant n_2(|b - b_i| < \epsilon)$ (from the second given).
Let $k = \max(n_1, n_2)$. Since $k \geqslant n_1$, we get from the above that $\forall i \geqslant k(|a - a_i| < \epsilon)$.
If $a_i < a$ then certainly $a_i < a + \epsilon$. If $a < a_i$, then $a_i - a < \epsilon$, and also $a_i < a + \epsilon$.
So in any case $a_i < a + \epsilon$.
Since $k \geqslant n_2$, we get from the above that $\forall i \geqslant k(|b - b_i| < \epsilon)$.
If $b < b_i$ then $b - \epsilon < b_i$. If $b_i < b$, then $b - b_i < \epsilon$, so $b - \epsilon < b_i$.
So in any case $b - \epsilon < b_i$.
Setting $\epsilon = \frac{a+b}{2}$ we get from $a < b$ that $a + \epsilon = b - \epsilon$, so $a_i < a + \frac{a+b}{2} < b_i$.
This proves $\forall m \geqslant k(a_m < b_m)$, so there is an n with $\forall m \geqslant n(a_m < b_m)$.

8.25 Given: $\lim_{i\to\infty} a_i = a$, $\lim_{i\to\infty} b_i = b$.
To be proved: $\lim_{i\to\infty}(a_i + b_i) = a + b$.
Proof:
We have to show that $\forall\epsilon > 0 \exists n \forall i \geqslant n(|(a + b) - (a_i + b_i)| < \epsilon$.
Let ϵ be arbitrary.
Let n_1 be such that $\forall i \geqslant n_1(|a - a_i| < \frac{1}{2}\epsilon)$, from the first given.
Let n_2 be such that $\forall i \geqslant n_2(|b - b_i| < \frac{1}{2}\epsilon)$, from the second given.
Let $k = \max(n_1, n_2)$. Since $k \geqslant n_1, n_2$, we get from the above
that $\forall i \geqslant k(|a - a_i| < \frac{1}{2}\epsilon)$ and that $\forall i \geqslant k(|b - b_i| < \frac{1}{2}\epsilon)$.
Thus $\forall i \geqslant k(|a - a_i| + |b - b_i| < \epsilon)$, and therefore $\forall i \geqslant k(|(a + b) - (a_i + b_i)| < \epsilon)$.
This proves $\lim_{i\to\infty}(a_i + b_i) = a + b$.

8.26 To be proved: $f : \mathbb{R} \to \mathbb{R}$ is continuous iff $\lim_{i\to\infty} f(a_i) = f(a)$ whenever $\lim_{i\to\infty} a_i = a$.
Proof:
$\Rightarrow$: Suppose $f : \mathbb{R} \to \mathbb{R}$ is continuous.
To show: if $\lim_{i\to\infty} a_i = a$ then $\lim_{i\to\infty} f(a_i) = f(a)$.
Assume $\lim_{i\to\infty} a_i = a$.
To show: $\lim_{i\to\infty} f(a_i) = f(a)$.
Proof:
Let ϵ be arbitrary.
We have to show that there is an n with $\forall i \geqslant n(|f(a) - f(a_i)| < \epsilon)$.
Since f is continuous, there is a δ with $|a - a_i| < \delta \Rightarrow |f(a) - f(a_i)| < \epsilon$.
From the assumption $\lim_{i\to\infty} a_i = a$, there is an n with $\forall i \geqslant n(|a - a_i| < \delta)$.
It follows that $\forall i \geqslant n(|f(a) - f(a_i)| < \epsilon)$.
This shows that $\lim_{i\to\infty} f(a_i) = f(a)$.
$\Leftarrow$: Suppose $\lim_{i\to\infty} f(a_i) = f(a)$ whenever $\lim_{i\to\infty} a_i = a$.
To show: $f : \mathbb{R} \to \mathbb{R}$ is continuous.
Let a and $\epsilon > 0$ be arbitrary.
We have to show that there is a $\delta > 0$ with $\forall y(|a - y| < \delta \Rightarrow |f(a) - f(y)| < \epsilon)$.
Suppose, for a contradiction, that there is no such δ.
Then for all δ, there is a y with $|a - y| < \delta$ and $|f(a) - f(y)| \geqslant \epsilon$.
Now we can construct a sequence $a_0, a_1, a_2, \ldots$ with a_0 arbitrary ($a_0 \neq a$),

$a_1 :=$ some y with $|a-y| < |a-a_0|$ and $|f(a)-f(y)| \geqslant \epsilon$,
and in general $a_{i+1} :=$ some y with $|a-y| < |a-a_i|$ and $|f(a)-f(y)| \geqslant \epsilon$.
Then $\lim_{i\to\infty} a_i = a$, while $\lim_{i\to\infty} f(a_i) \neq f(a)$, and contradiction with the given.
So there is a $\delta > 0$ with $\forall y(|a-y| < \delta \Rightarrow |f(a)-f(y)| < \epsilon)$.

8.27.1 Given: $\{a_n\}_{n=0}^{\infty}$ is Cauchy.
To be proved: $\{a_n\}_{n=0}^{\infty}$ is bounded.
Proof:
We have to show that there are b, c with $\forall i(b < a_i < c)$.
Take some $\epsilon > 0$. Then by the given, there is an n with $\forall i, j \geqslant n(|a_i - a_j| < \epsilon)$.
Let $b = \min\{a_0, \ldots, a_n\} - \epsilon$. We show that for all i, $b < a_i$.
For $i \in [0..n]$ this is immediate from the definition.
If $i > n$ and $a_n < a_i$, then again $b < a_i$ is immediate from the definition.
If $i > n$ and $a_i < a_n$, then, since $|a_n - a_i| < \epsilon$, $a_n - \epsilon < a_i$, so again $b < a_i$.
Analogously, we can take $c = \max\{a_0, \ldots, a_n\} + \epsilon$, and prove that $a_i < c$, for all i.

8.27.2 Given: $\{a_n\}_{n=0}^{\infty}$ is Cauchy; there is an $a \in \mathbb{R}$ with $\forall \varepsilon > 0 \forall n \exists i \geqslant n\ (|a - a_i| < \varepsilon)$.
To be proved: $\lim_{i\to\infty} a_i = a$.
Proof:
Let $\epsilon > 0$ be arbitrary. We have to prove that $\exists n \forall i \geqslant n(|a - a_i| < \epsilon)$.
Let n_1 be such that $\forall i, j \geqslant n_1(|a_i - a_j| < \frac{1}{2}\epsilon)$ (from the fact that $\{a_n\}_{n=0}^{\infty}$ is Cauchy).
By the second given there is a k with $k \geqslant n_1$ and $|a - a_k| < \frac{1}{2}\epsilon$.
Then $\forall i \geqslant k(|a_k - a_i| < \frac{1}{2}\epsilon)$, so $\forall i \geqslant k(|a - a_k| < \frac{1}{2}\epsilon \wedge |a_k - a_i| < \frac{1}{2}\epsilon)$.
Since $|a - a_i| \leqslant |a - a_k| + |a_k - a_i|$, this gives $\forall i \geqslant k(|a - a_i| < \epsilon)$.
This proves that $\lim_{i\to\infty} a_i = a$.

8.28 Take $\{a_n\}_{n=0}^{\infty} \sim \{b_n\}_{n=0}^{\infty}$ if $\{a_n - b_n\}_{n=0}^{\infty}$ converges to 0. This is easily shown to be an equivalence.

8.30 Left to the reader.

8.31.1 Basis: It is clear that

$$(\cos(\varphi) + i\sin(\varphi))^0 = 1 = \cos(0) + i\sin(0).$$

Suppose that

$$(\cos(\varphi) + i\sin(\varphi))^n = \cos(n\varphi) + i\sin(n\varphi).$$

Then:

$$\begin{aligned}(\cos(\varphi) + i\sin(\varphi))^{n+1} &= (\cos(\varphi) + i\sin(\varphi))^n \times (\cos(\varphi) + i\sin(\varphi)) \\ &\overset{ih}{=} (\cos(n\varphi) + i\sin(n\varphi)) \times (\cos(\varphi) + i\sin(\varphi)) \\ &= \cos((n+1)\varphi) + i\sin((n+1)\varphi).\end{aligned}$$

The final step is justified by the fact that $\cos(n\varphi) + i\sin(n\varphi)$ is the number with magnitude 1 and phase $n\varphi$, while $\cos(\varphi) + i\sin(\varphi)$ has magnitude 1 and phase φ. The result of multiplying them is the number with magnitude 1 and phase $n\varphi + \varphi = (n+1)\varphi$, i.e., the number

$$\cos((n+1)\varphi) + i\sin((n+1)\varphi).$$

8.31.2 If $m \in \mathbb{N}$ then:

$$\begin{aligned}
(\cos(\varphi) + i\sin(\varphi))^{-m} &= \frac{1}{(\cos(\varphi) + i\sin(\varphi))^m} \\
&\overset{\text{previous item}}{=} \frac{1}{\cos(m\varphi) + i\sin(m\varphi)} \\
&= \cos(m\varphi) - i\sin(m\varphi) \\
&= \cos((-m)\varphi) + i\sin((-m)\varphi).
\end{aligned}$$

Draw a picture to see why the penultimate step is justified.

Solutions to Exercises from Chapter 9

```
module Sol9

where

import POLS
```

9.3 Next 10 elements are: `[237,367,539,759,1033,1367,1767,2239,2789,3423]`. The sequence is of the form $\lambda n.n^3 + 3n + 3$.

9.5 Difference analysis yields that this sequence is generated by a polynomial of the third degree, so the sequence leads to the following set of equations:

$$\begin{aligned} a &= 13 \\ a + b + c &= 21 \\ a + 2b + 4c &= 35 \end{aligned}$$

Eliminate a:

$$\begin{aligned} b + c &= 8 \\ 2b + 4c &= 22 \end{aligned}$$

Subtracting the second equation from the 4-fold of the first gives $2b = 10$, whence $b = 5$ and $c = 3$. The sequence is generated by the form $\lambda n.(3n^2 + 5n + 13)$.

9.6 There is no need for an inductive proof anymore, for this time you did not arrive at the closed form by guesswork, but by solving a set of linear equations derived from a polynomial sequence for the pie cutting process.

9.9 The implementation `choose` is far more efficient. The computation for `choose n k` uses $2k-2$ multiplication operations plus one division operation. The computation for `choose' n k` constructs a 'lozenge' in the Pascal triangle with lower corner $\binom{n}{k}$ by means of addition, but with repeated computation of the same intermediate results. E.g., to compute $\binom{5}{3}$, the numbers $\binom{4}{2}$ and $\binom{4}{3}$ get added. To compute $\binom{4}{2}$ the number $\binom{3}{2}$ is needed. To compute $\binom{4}{3}$, the number $\binom{3}{2}$ is needed as well. So $\binom{3}{2}$ gets computed twice.

9.10

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n!}{(n-(n-k))!\,(n-k)!} = \binom{n}{n-k}.$$

9.12

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} = \frac{n}{k} \cdot \frac{(n-1)!}{(k-1)!\,(n-k)!} = \frac{n}{k} \cdot \frac{(n-1)!}{(k-1)!\,((n-1)-(k-1))!} = \frac{n}{k} \cdot \binom{n-1}{k-1}.$$

9.13 $\binom{n}{m} \cdot \binom{m}{k}$ gives the number of ways of first picking an m-sized subset B from an n-sized set A, and next picking a k-sized subset C from B. Alternatively, one might first pick a k-sized subset C from A, and next select $m-k$ elements from $A-C$, so that these $m-k$ elements together with C constitute an m-element set B with $C \subseteq B \subseteq A$. There are $\binom{n}{k} \cdot \binom{n-k}{m-k}$ ways of doing this. Clearly, the two procedures are equivalent.

9.14 First observe that $\binom{n}{n} = 1 = \binom{n+1}{n+1}$. Next, use the law of addition k times, as follows. Add $\binom{n+1}{n+1}$ and $\binom{n+1}{n}$ to yield $\binom{n+2}{n+1}$. Next add $\binom{n+2}{n+1}$ and $\binom{n+2}{n}$ to yield $\binom{n+3}{n+1}$, and so on, and finally add $\binom{n+k}{n+1}$ and $\binom{n+k}{n}$ to yield $\binom{n+k+1}{n+1}$.

9.20 Putting 1 on the positions for the prime exponents, we get:

```
COR> ([0,0,1,1,0,1,0,1,0,0,0]^3) !! 10
6
```

Solutions to Exercises from Chapter 10

```
module Sol10

where

import COR
```

10.1

```
evens = 0 : map (+2) evens
```

10.2

```
theEvens = iterate (+2) 0
```

10.3

```
swap ""        = ""
swap ('1': xs) = '0': swap xs
swap ('0': xs) = '1': swap xs

morse xs = xs ++ morse (xs ++ swap xs)

thue = '0' : morse "1"
```

10.5

```
random001s :: Int -> [Int]
random001s i =  map (‘mod‘ 2) (randomInts 2 i)
```

10.9 The first machine will always deliver mineral water after insertion of a single coin, while the second machine may refuse to do so.

10.10

```
vend, vend1, vend2, vend3, vend4  :: Process
vend  (0:xs) = "coin"     : vend1 xs
vend  (1:xs) = "coin"     : vend4 xs
vend1 (0:xs) = "coin"     : vend2 xs
vend1 (1:xs) =              vend1 xs
vend2 (0:xs) = "beer"     : vend xs
vend2 (1:xs) = "coin"     : vend3 xs
vend3 (0:xs) = "moneyback": vend  xs
vend3 (1:xs) =              vend3 xs
vend4 (0:xs) = "water"    : vend xs
vend4 (1:xs) =              vend4 xs
```

10.12 Take $D = \mathbb{Z}$ and $A = D$, under the standard ordering $\leqslant$. The set $\mathbb{Z}$ has no greatest and no least element.

10.13 The example of the previous exercise works.

10.14 $\mathbb{N}$ is not a domain for the set of all natural numbers has no lub. Let $\mathbb{N}^\infty$ be the set $\mathbb{N} \cup \{\infty\}$, and put $n \leqslant \infty$ for all $n \in \mathbb{N} \cup \{\infty\}$. Then we have: $\bot = 0$, and every chain in $\mathbb{N}^\infty$ has a lub, so $\mathbb{N}^\infty$ is a domain.

10.15 To show that $a \to b$ is a domain, we must show that there is a bottom element and that every chain has a lub. Take for $\bot$ the partial function that is everywhere undefined. Then it is clear from the definition of $\sqsubseteq$ that $\bot \sqsubseteq f$ for any $f : a \to b$. Let A be a chain in $a \to b$. Then we get from the definition of $\sqsubseteq$ that for all $g, g' \in A$ and for all $x \in a$ it will hold that if $g(x)$ and $g'(x)$ are both defined, then $g(x) = g'(x)$. Therefore, $\sqcup A$ can be defined as the function h given by $h(x) := \sqcup\{g(x) \mid g \in A\}$.

10.16 The partial list $\bot$ is the bottom of $[a]$. Let A be a chain in $[a]$. Then $\{\text{head ys} \mid \text{ys} \in A\}$ is a chain in a, and $\{\text{tail ys} \mid \text{ys} \in A\}$ is a chain in $[a]$. Thus, we can define $\sqcup A$ as the list xs given by

- head xs $:= \sqcup\{\text{head ys} \mid \text{ys} \in A\}$,
- tail xs $:= \sqcup\{\text{tail ys} \mid \text{ys} \in A\}$.

Note that head $\bot$ = head [] = $\bot$, and tail $\bot$ = tail [] = $\bot$.

10.20 Infinite lists always have a first element, so we may assume the list to be of the form `x:xs`. We give a proof by approximation that

$$\text{filter}\ p\ (\text{map}\ f\ \text{x:xs}) = \text{map}\ f\ (\text{filter}\ (p.f)\ \text{x:xs}).$$

Assume (induction hypothesis) that for any list ys the following holds:

$$\text{approx}\, n\ (\text{filter}\ p\ (\text{map}\ f\ \text{ys})) = \text{approx}\ n\ (\text{map}\ f\ (\text{filter}\ (p.f)\ \text{ys})).$$

There are two cases: (i) $p(fx) =$ **t** and (ii) $p(fx) =$ **f**. In case (i) we have:

$$\begin{array}{rcl}
\text{approx}\ (n+1)\ (\text{filter}\ p\ (\text{map}\ f\ (\text{x:xs}))) & \stackrel{\text{map}}{=} & \text{approx}\ (n+1)\ (\text{filter}\ p\ (f\ x) : (\text{map}\ f\ (\text{x:xs})))\\
& \stackrel{\text{filter}}{=} & \text{approx}\ (n+1)\ ((f\ x) : (\text{filter}\ p\ (\text{map}\ f\ (\text{x:xs}))))\\
& \stackrel{\text{approx}}{=} & (f\ x) : \text{approx}\ n\ (\text{filter}\ p\ (\text{map}\ f\ (\text{x:xs})))\\
& \stackrel{\text{ih}}{=} & (f\ x) : \text{approx}\ n\ (\text{map}\ f\ (\text{filter}\ (p.f)\ \text{xs}))\\
& \stackrel{\text{approx}}{=} & \text{approx}\ (n+1)\ ((f\ x) : (\text{map}\ f\ (\text{filter}\ (p.f)\ \text{xs})))\\
& \stackrel{\text{map}}{=} & \text{approx}\ (n+1)\ (\text{map}\ f\ (x : (\text{filter}\ (p.f)\ \text{xs})))\\
& \stackrel{\text{filter}}{=} & \text{approx}\ (n+1)\ (\text{map}\ f\ (\text{filter}\ (p.f)\ (\text{x:xs}))).
\end{array}$$

Case (ii) is similar.

10.23 To show that Δ is a bisimulation on A, we have to check the two bisimulation properties. Assume $a = b$.

1. Suppose $a \stackrel{o}{\longrightarrow} a'$. From $a = b$ it follows that $b \stackrel{o}{\longrightarrow} a'$, with $a' = a'$.
2. Similar.

10.25 State q_1 of the second vending machine cannot be linked to any state in the first vending machine. In particular, it cannot be linked to state q_1 in the first machine, for q_1 in the first machine has a water and a coin transition, q_1 in the second machine has only a coin transition.

10.26 Let R and S be bisimulations. Assume $a(R \cup S)b$. To show that $R \cup S$ is a bisimulation, we have to check the two bisimulation properties.

1. Suppose $a \stackrel{o}{\longrightarrow} a'$. From $a(R \cup S)b$, we know that either aRb or aSb. In the first case, it follows from the fact that R is a bisimulation that there is a b' with $b \stackrel{o}{\longrightarrow} b'$ and bRb'. Hence $b(R \cup S)b'$. In the second case, it follows from the fact that S is a bisimulation that there is a b' with $b \stackrel{o}{\longrightarrow} b'$ and bSb'. Hence $b(R \cup S)b'$.
2. The reasoning is similar.

10.27 Let $R = \cup\{B \mid B \text{ is a bisimulation on } A\}$. We show that R is a bisimulation, by checking the two bisimulation properties. Assume aRb.

1. Suppose $a \stackrel{o}{\longrightarrow} a'$. From aRb and the definition of R we know that there is a bisimulation B on A with aBb. It follows from the fact that B is a bisimulation that there is a b' with $b \stackrel{o}{\longrightarrow} b'$ and bBb'. Hence, by the definition of R, bRb'.
2. The reasoning is similar.

10.28 Take $B \cup \Delta_A \cup \{(c_3, c_4), (c_4, c_3)\}$, where A is the list of states $\{c, c_0, c_1, c_2, c_3, c_4\}$, and B is the bisimulation given in Example 10.24.

10.30 Let S be given by:

$$\{(\text{filter } p\ (\text{map } f\ \text{xs}), \text{map } f\ (\text{filter } (p.f)\ \text{xs})) \mid f : a \to b, p : b \to \{0,1\}, \text{xs} :: [a], |\text{xs}| = \infty\}$$

Let R be given by $\Delta_b \cup S$. We show that R is a bisimulation. Clearly,

$$\text{filter } p\ (\text{map } f\ \text{xs})\ R\ \text{map } f\ (\text{filter } (p.f)\ \text{xs}),$$

by definition of R. We have to show that head and tail observations on the items related by R satisfy the back and forth conditions.

Suppose filter p (map f xs) $\xrightarrow{\text{head}} z$.

Then, by the definition of filter and map, xs has the form $x_0 : \cdots : x_n : x : \text{xs}'$, and for all i with $0 \leqslant i \leqslant n$, $p(x_i) = 0$, and $p(x) = 1$, and $f(x) = z$.

But then also map f (filter $(p.f)$ xs) $\xrightarrow{\text{head}} z$, and by the definition of R, zRz.

Suppose map f (filter $(p.f)$ xs) $\xrightarrow{\text{head}} z$.

Then again, by the definition of filter and map, xs has the form $x_0 : \cdots : x_n : x : \text{xs}'$, and for all i with $0 \leqslant i \leqslant n$, $p(x_i) = 0$, and $p(x) = 1$, and $f(x) = z$.

But then also filter p (map f xs) $\xrightarrow{\text{head}} z$, and by the definition of R, zRz.

The reasoning for tail observations is similar.

10.37 Generating function for $[0,0,0,1,1,1,\ldots]$ is $\frac{z^3}{1-z}$. Generating function for $[1,1,1,0,0,0,\ldots]$ is $1+z+z^2$. Generating function for $[1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots]$ is $\frac{2}{2-z}$. Here are the checks:

```
COR> take 20 (z^3 * ones)
[0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]
COR> 1+z+z^2
[1,1,1]
COR> take 10 (2/(2-z))
[1 % 1,1 % 2,1 % 4,1 % 8,1 % 16,1 % 32,1 % 64,1 % 128,1 % 256,1 % 512]
```

10.40

1. In Example 10.32 we saw that $\frac{1}{1-z}$ is the generating function for $\lambda n.1$. Multiplication with a constant c gives that $\frac{c}{1-z}$ is the generating function for $\lambda n.c$.

2. $\frac{z}{(1-z)^2}$ is the generating function for $\lambda n.n$: this was shown in Example 10.33.

3. $\frac{f(z)}{z}$ is the generating function for $\lambda n.f_{n+1}$; division by z has the effect of shifting the coefficients one place to the left.

4. $cf(z) + dg(z)$ is the generating function for $\lambda n.cf_n + dg_n$:

$$\begin{array}{rcccccccc} cf(z) & = & cf_0 & + & cf_1 z & + & cf_2 z^2 & + & \cdots \\ dg(z) & = & dg_0 & + & dg_1 z & + & dg_2 z^2 & + & \cdots \\ cf(z)+dg(z) & = & (cf_0+dg_0) & + & (cf_1+dg_1)z & + & (cf_2+dg_2)z^2 & + & \cdots \end{array}$$

5. $(1-z)f(z)$ is the generating function for the difference sequence $\lambda n.f_n - f_{n-1}$: page 349, chapter 9.
6. $\frac{1-z}{z}f(z)$ is the generating function for the difference sequence $\lambda n.f_{n+1} - f_n$: from previous item, for division by z shifts the sequence of coefficients one place to the left.
7. $\frac{1}{1-z}f(z)$ is the generating function for $\lambda n.f_0 + f_1 + \cdots + f_n$: the n-th coefficient of the product of $\frac{1}{1-z} = (1 + z + z^2 + z^3 + \cdots)$ and $f(z) = f_0 + f_1 z + f_2 z^2 + \cdots$ is $f_0 + f_1 + \cdots + f_n$.
8. $f(z)g(z)$ is the generating function for $\lambda n.f_0 g_n + f_1 g_{n-1} + \cdots + f_{n-1} g_1 + f_n g_0$ (the convolution of f and g): the n-th coefficient in the list of coefficients of $f(z)g(z)$ has the form $f_0 g_n + f_1 g_{n-1} + \cdots + f_{n-1} g_1 + f_n g_0$.
9. $zf'(z)$ is the generating function for $\lambda n.nf_n$: $f'(z)$ generates $\lambda n.(n+1)f_{n+1}$; multiplication with z shifts one place to the right, and inserts a 0 in the first position.
10. $\frac{1}{z}\int_0^z f(t)dt$ is the generating function for $\lambda n.\frac{f_n}{n+1}$: integration gives $\lambda n.\frac{f_{n-1}}{n}$, division by z shifts one place to the left.

10.45 The appropriate corecursive definition is given by:

```
COR> take 20 lucs where lucs = 2 : 1 : (lucs + tail lucs)
[2,1,3,4,7,11,18,29,47,76,123,199,322,521,843,1364,2207,3571,5778,9349]
```

The corresponding instruction for a generating function is:

$$g(z) = z^2\left(g(z) + \frac{g(z)}{z}\right) + 2 - z.$$

Multiplying by z^2 inserts two 0's in front of the lucs sequence; adding 2 changes the first of these to 2; subtracting z indicates that the second coefficient is obtained from the first by subtracting 1. The tail of the lucs sequence is given by $\frac{g(z)}{z}$. From this we get:

$$\begin{aligned} g(z) - zg(z) - z^2 g(z) &= 2 - z \\ g(z) &= \frac{2-z}{1-z-z^2} \end{aligned}$$

This is easily verified, as follows:

```
COR> take 10 ((2-z)/(1-z-z^2))
[2 % 1,1 % 1,3 % 1,4 % 1,7 % 1,11 % 1,18 % 1,29 % 1,47 % 1,76 % 1]
```

10.52 The exponential generating function we need is $(\frac{z^2}{2} + \frac{z^3}{6} + \frac{z^4}{24})^3$. Again, the idea: if you pick n marbles of the same colour, then $n!$ of the marble orderings become indistinguishable. The answer is given by the following query:

```
COR> o2e ((z^2/2 + z^3/6 + z^4/24)^3)
[0 % 1,0 % 1,0 % 1,0 % 1,0 % 1,0 % 1,90 % 1,630 % 1,2940 % 1,
 9240 % 1,22050 % 1,34650 % 1,34650 % 1]
```

Alternatively, we can express this as follows:

```
COR> o2e ([0,0,1/2,1/6,1/24]^3)
[0 % 1,0 % 1,0 % 1,0 % 1,0 % 1,0 % 1,90 % 1,630 % 1,2940 % 1,
 9240 % 1,22050 % 1,34650 % 1,34650 % 1]
```

Thus, under the given constraints there are 90 different sequences of 6 marbles, 630 of 7 marbles, 2940 of 8 marbles, 9240 of 9 marbles, 22050 of 10 marbles, 34650 of 11 marbles and 34650 again of 12 marbles. The numbers of 11-sequences and 12-sequences are the same, for any 12-sequence can be viewed as the result of extending an 11-sequence with a marble of the only colour that occurs 3 times in the 11-sequence.

Solutions to Exercises from Chapter 11

```
module Sol11

where

import FAIS
```

11.5 To be proved: for every $X \subseteq \mathbb{N}$, if $m \in X$ and $\forall n \geqslant m(n \in X \Rightarrow n+1 \in X)$, then $\forall n \in \mathbb{N}(m \leqslant n \Rightarrow n \in X)$.
Proof: Assume $m \in X$ and $\forall n \geqslant m(n \in X \Rightarrow n+1 \in X)$. We prove by induction on n that $Y = \{n \mid m+n \in X\} = \mathbb{N}$.
Basis: $0 \in Y$. This follows from $m \in X$.
Induction hypothesis: $n \in Y$. Induction step. From the induction hypothesis we get $m+n \in X$. From the second assumption, $m+n+1 \in X$. From this and the definition of Y: $n+1 \in Y$.
We now show $\forall n \in \mathbb{N}(m \leqslant n \Rightarrow n \in X)$. Now let n an arbitrary natural number with $m \leqslant n$. Then $n-m \in \mathbb{N}$, so $n-m \in Y$. Thus, by the definition of Y, $(n-m)+m = n \in X$.

11.6 Given: $X \subseteq \mathbb{N}$, $1 \in X$, $\forall n \in \mathbb{N}(n \in X \Rightarrow n+2 \in X)$.
To be proved: every odd number is in X.
Proof: We show that $Y = \{n \in \mathbb{N} \mid 2n-1 \in X\} = \mathbb{N}$.
Basis: $0 \in Y$ follows from $1 \in X$.
Induction hypothesis: $n \in Y$.
Induction step: From the induction hypothesis we get that $2n-1 \in X$. From this and the third given: $2n+1 = 2(n+1)-1 \in X$. Thus $n+1 \in Y$.

11.9 To be proved: $<$ is well-founded on $\mathbb{N}$.
Proof: We show by strong induction that for no $n \in \mathbb{N}$ is there an infinite sequence $n > n_1 > n2 > \ldots$.
Basis: Since 0 is the smallest member of $\mathbb{N}$, there is no infinite sequence $0 > n_1 > \ldots$.
Induction hypothesis: For all $m < n$ it holds that there is no infinite sequence $m > n_1 > n_2 > \ldots$.
Induction step: Assume there is an infinite sequence $n > n_1 > n_2 > \ldots$. Since $n_1 < n$, this contradicts the induction hypothesis. Thus, there is no infinite sequence $n > n_1 > n_2 > \ldots$.

11.10.1 Given: $\prec$ on A is well-founded, $X \subseteq A$, $\forall a \in A(\forall b \prec a(b \in X) \Rightarrow a \in X)$.

To be proved: $X = A$.
Proof: Assume $X \neq A$. Then $\exists a_0 \in A - X$. SInce $a_0 \notin X$, by the third given there is an $a_1 \prec a_0$ with $a_1 \notin X$. Thus $a_0 \succ a_1$ and $a_1 \in A - X$. Repeating the argument we get an infinite sequence $a_0 \succ a_1 \succ a_2 \succ \ldots$ in A, and contradiction with the fact that A is well-founded. Thus $X = A$.

11.10.2 Given: Every $X \subseteq A$ with $\forall a \in A(\forall b \prec a(b \in X) \Rightarrow a \in X)$ coincides with A.
To be proved: $\prec$ is well-founded.
Proof: Suppose there is an infinite sequence $a_0 \succ a_1 \succ a_2 \succ \ldots$ in A. Let $X = A - \{a_0, a_1, a_2, \ldots\}$. Let $a \in A$ be arbitrary and assume $\forall b \prec a(b \in X)$. Then $a \notin \{a_0, a_1, a_2, \ldots\}$. Thus, $a \in X$. But then X satisfies $\forall a \in A(\forall b \prec a(b \in X) \Rightarrow a \in X)$, so by the given, $X = A$, and contradiction with the definition of X. Thus, there is no infinite sequence $a_0 \succ a_1 \succ a_2 \succ \ldots$ in A, i.e., A is well-founded.

11.11.1 Given: Let R be a relation on A and let $a, b_1, b_2 \in A$. If aRb_1 and aRb_2 then there is a $c \in A$ with b_1Rc and b_2Rc.
To be proved: R is confluent.
Proof: we will proceed by induction on the path length from a to b_1. Basis: $a = b_1$. If aR^*b_2, then b_2 satisfies $b_1R^*b_2$ and $b_2R^*b_2$.
Induction step: The induction hypothesis is that if aR^kb_1 and aR^*b_2 then there is a c with b_1R^*c and b_2R^*c. Suppose $aR^{k+1}b_1$ and aR^*b_2. Then there is an m with aR^mb_2. So there is a d with aR^kdRb_1. By the induction hypothesis, there is a c with dR^*c and b_2R^*c. From dR^*c, there is some $p \in \mathbb{N}$ with dR^pc. Let $d = c_0, c_1, \ldots, c_p = c$ be the R-path from d to c. Then from dRb_1 and dRc_1, by the given about R there is an e_1 with b_1Re_1 and c_1Re_1. Similarly, from c_iRe_i and c_iRc_{i+1}, by the given about R there is an e_{i+1} with e_iRe_{i+1} and $c_{i+1}Re_{i+1}$. This gives an R-path $b_1, e_1, \ldots, e_p$ with cRe_p. It follows that $b_1R^*e_p$ and $b_2R^*e_p$, which clinches the argument.

11.11.2 Assume R is weakly confluent, and suppose a is bad. We have to show that there is a bad b with aRb. If a is bad, then there are b_1, b_2 with aRb_1, aRb_2, and for no $c \in A$ is it the case that b_1R^*c and b_2R^*c. From b_1R^*c and b_2R^*c, there are $k, m \in \mathbb{N}$ with aR^mb_1 and aR^kb_2. Also, $k > 1$ and $m > 1$. For suppose, e.g., that $k = 1$. Then by m applications of weak confluence we get at an c with b_1R^*c and b_2R^*c, and contradiction with the fact that a is bad.

Thus, $k = n + 1$, and there is a b with $aRbR^nb_1$ and aR^mb_2. By m applications of weak confluence we get at an e with bR^*e and b_2R^*e. Assume b is not bad. Then there is a c with b_1R^*c and eR^*c. Since aR^*b_1 and $aR^*b_2R^*e$ this contradicts the assumption about a. Thus, b is bad.

11.11.3 Given: R is weakly confluent and R^{-1} is well-founded.
To be proved: R is confluent.
Proof: Suppose aR^*b_1 and aR^*b_2. If a is not bad, there is nothing to be proved. Assume therefore that a is bad. Then by 11.11.2 there is an a_1 with aRa_1 and a_1 bad. Continuing like this we get an infinite sequence $a_0, a_1, a_2, \ldots$, with $a = a_0$, a_iRa_{i+1}, with the a_i all bad. This gives a contradiction with the assumption that R^{-1} is well-founded.

11.12 Given: $\emptyset \neq X \subseteq \mathbb{N}$, there is an $m \in \mathbb{N}$ with for all $n \in X$ $(n \leqslant m)$.
To be proved: There is a $k \in X$ such that for all $n \in X$ $(n \leqslant k)$.
Proof: We show by induction on m that the property $E(m)$ holds, where $E(m) \stackrel{\text{def}}{\iff}$ every non-empty $X \subseteq \mathbb{N}$ with $\forall n \in X(n \leqslant m)$ has a maximum.
Basis: $E(0)$ holds by the fact that the only non-empty $X \subseteq \mathbb{N}$ with $\forall n \in X$ $(n \leqslant 0)$ is the set $\{0\}$, and this set has 0 as a maximum.

Induction step: Suppose $E(m)$ holds. Assume $\emptyset \neq X \subseteq \mathbb{N}$ and $\forall n \in X\ (n \leqslant m+1)$. We have to show that X has a maximum. Assume $m+1 \in X$. Then $m+1$ is a maximum of X. Assume $m+1 \notin X$. Then $\forall n \in X\ (n \leqslant m)$. By the induction hypothesis, X has a maximum.

11.13 Given: $f : \mathbb{N} \to \mathbb{N}$ with $n < m \ \Rightarrow\ f(n) < f(m)$.
To be proved: for all $n \in \mathbb{N}$: $n \leqslant f(n)$.
Proof: induction on n.
Basis: $0 \leqslant f(0)$ holds by virtue of the fact that 0 is the smallest member of $\mathbb{N}$.
Induction step: Assume $n \leqslant f(n)$. We have to show $n+1 \leqslant f(n+1)$. Since $n < n+1$ we get from the given about f that $f(n) < f(n+1)$. Therefore $f(n)+1 \leqslant f(n+1)$. From the induction hypothesis we get that $n+1 \leqslant f(n)+1$. Combining these gives $n+1 \leqslant f(n+1)$.

11.14 Let $a_0, a_1, a_2, \ldots$ be an infinite sequence of natural numbers. We have to show that there are i, j with $i < j$ and $a_i \leqslant a_j$. Suppose for a contradiction that for all i, j with $i < j$ it holds that $a_i > a_j$. This gives a contradiction with the well-foundedness of $<$ on $\mathbb{N}$.

11.15 Let n, m be arbitrary natural numbers. We will show that that $g(n, m)$ is the gcd of n and m. Let a sequence of natural number pairs $(a_0, b_0), (a_1, b_1), (a_2, b_2), \ldots$ be given by $(n, m) = (a_0, b_0)$, if $a_i < b_i$ then $a_{i+1} = a_i$, $b_{i+1} = b_i - a_i$, if $a_i > b_i$ then $a_{i+1} = b_i$, $b_{i+1} = a_i$, and if $a_i = b_i$ then $a_{i+1} = a_i$, $b_{i+1} = b_i$. Then it is immediate from the properties of g that $g(a_i, b_i) = g(n, m)$ for all i. Also, by the well-foundedness of $<$ on $\mathbb{N}$ there has to be a j with $a_j = b_j$. It follows, by the properties of g, that $g(n, m) = a_j$.

It was shown in Section 8.2 that if $p < q$ then p, q and $p, q - p$ have the same common divisors. It is clear that p is the greatest common divisor of p, p. It follows that $g(n, m) = a_j$ is the gcd of n, m.

11.16 To be proved: Smullyan's ball game terminates for any initial game situation of finitely many balls.
Proof: Assume the game goes on forever. Let B_k be the contents of the box after the k-th move. Then the initial situation from which you can play an infinite game is B_0. Let n be the greatest number present on one of the balls in B_0. We derive $\perp$ by strong induction on n.
Basis: $n = 0$. In this case the contents of box B_0 consists of a finite number, say m, of balls carrying number 0. Now every move *must* consist of removal of one of the balls without replacement (for there are no balls with smaller numbers available). Thus, the game ends after m moves, and contradiction with the assumption that we can go on forever.
Induction step: Assume that the game terminates for all situations where the greatest number on any ball in B_0 is $\leqslant n$. Suppose that the greatest number on a ball in B_0 is $n+1$. To show $\perp$, we use strong induction on the number m of balls in B_0 carrying the number $n+1$.

> Basis: $m = 1$. There is a single ball carrying number $n+1$. The move that replaces this ball cannot be postponed forever, for otherwise contradiction with the induction hypothesis for n. Thus, after a finite number of steps, this ball gets replaced by a finite number of balls carrying smaller numbers. The assumption that the game goes on forever after this leads to a contradiction with the induction hypothesis for n.
> Induction step: suppose the game terminates if there are up to m balls in B_0 carrying number $n+1$. Then by the induction hypothesis for m, after a finite number of moves the last ball carrying number $n+1$ has to be replaced. The assumption that the game goes on forever after this leads to a contradiction with the induction hypothesis for n.

Thus, we have proved that the game terminates for every initial situation.

11.17

```
ball :: Int -> [[Int]]
ball n = ballgame [n]

ballgame :: [Int] -> [[Int]]
ballgame xs | all (==1) xs = [xs]
            | otherwise    = xs : ballgame (reduce xs)
  where
  reduce (1 : ys) = 1 : reduce ys
  reduce (n : ys) = (n-1) : (n-1) : ys
```

`ball 50` or `ballgame [50]` takes centuries to terminate, for (as an easy induction argument shows) it will produce a list of 2^{49} integer lists. Since $2^{10} \approx 10^3$ we get:

$$2^{49} = 2^9 \cdot 2^{40} \approx 2^9 \cdot 10^{12} = 512 \cdot 10^{12}.$$

512 billion (in American terminology: "512 trillion") lists is a lot. If 1000 lists are being generated per second, then this makes $3600 \cdot 24 \cdot 365 \cdot 10^3 = 864 \cdot 365 \cdot 10^5 = 31536 \cdot 10^6$ lists a year, which means that the computation would go on for more than 160 centuries.

11.18 The argument is flawed, so there is no contradiction with common sense experience. The flaw is in the sentence 'choose $r \in A - \{p, q\}$'. This presupposes that $A - \{p, q\}$ is non-empty, an assumption not warranted by what is given about A.

11.25 From the given $A \sim B$ we know that there is a bijection $g : A \to B$. Let f be defined by $f(x) := b$ if $x = a$, $f(x) := g(a)$ if $x = g^{-1}(b)$ ($g^{-1}(b)$ exists, since g is bijective), and $f(x) := g(x)$ in all other cases. Then f is a bijection, and $f(a) = b$.

11.26 Given: $A \sim B$.
To be proved: $\wp(A) \sim \wp(B)$.
Proof: Let f be a bijection that witnesses $A \sim B$. Define $f^* : \wp(A) \to \wp(B)$, by means of $f^*(X) := f[X]$. We show that f^* is a bijection. Let $X \neq Y$, e.g., suppose that $a \in X, a \notin Y$. Then $f(a) \in f[X], f(a) \notin f[Y]$, so $f[X] \neq f[Y]$. Thus $f^*(X) \neq f^*(Y)$, which proves injectivity of f^*. Next, take an arbitrary $V \in \wp(B)$. Consider the set $X = f^{-1}[V]$, and observe that $f[X] = f[f^{-1}[V]] = V$. Thus, there is an $X \in \wp(A)$ with $f^*(X) = V$. This proves surjectivity of f^*.

11.27 The function $f : \wp(A) \to \{0, 1\}^A$ given by $f(X) := \text{char}_X$, where $\text{char}_X : A \to \{0, 1\}$ is given by $\text{char}_X(a) := 1$ iff $a \in X$ (char_X is the characteristic function of X in A), is a bijection.

11.28.1 Given: $A \sim B$.
To be proved: if A has n elements,then so has B.
Proof: Let $f : B \to A$ be a bijection that witnesses $A \sim B$. From the fact that A has n elements we get that there is a bijection $g : A \to \{0, \ldots, n-1\}$. But then $g \circ f$ is a bijection between B and $\{0, \ldots, n-1\}$, which shows that B has n elements.

11.28.2 Given: $A \sim B$.
To be proved: if A is finite, then so is B.
Proof: If A is finite then there is some $n \in \mathbb{N}$ such that A has n elements. By 11.28.1, in that case B also has n elements, so B is finite.

11.28.3 Given: $A \sim B$.
To be proved: if A is infinite, then so is B.
Proof: follows by contraposition from 'if B is finite, then so is A' (see 11.28.2).

11.29 If f is a function, then $\lambda x.(x, f(x))$ is a bijection between $\mathrm{dom}\,(f)$ and f. This establishes $f \sim \mathrm{dom}\,(f)$.

11.30 Let R be an equivalence on A, and let $V = A/R$. Let X be the set of all partitions on V and let Y be the set of all equivalences Q with $R \subseteq Q$. Consider the function $f : X \to Y$ given by

$$f(\mathcal{B}) = \{(a, b) \in A^2 \mid \exists B \in \mathcal{B} : [a]_R \in B \wedge [b]_R \in B\}.$$

Then f is well-defined, for every $Q = f(\mathcal{B})$ is an equivalence with $R \subseteq Q$. The latter fact holds because aRb implies $[a]_R = [b]_R$, together with the fact that $\cup\mathcal{B} = V = A/R$ for any partition $\mathcal{B}$.

We have to show that f is bijective. For injectivity, suppose $f(\mathcal{B}) = f(\mathcal{B}') = Q$. Let $B \in \mathcal{B}$. Then $B \neq \emptyset$, by the fact that $\mathcal{B}$ is a partition. Let $[b]_R \in B$. Then by the definition of f and the fact that $f(\mathcal{B}') = Q$ there is a B' in $\mathcal{B}'$ with $[b]_R \in B'$. So $B \subset B'$. Let $[a]_R \in B'$. Then aQb, so $[a]_R \in B$. Thus, $B' \subseteq B$, and therefore $B = B'$. This shows $\mathcal{B} \subseteq \mathcal{B}'$. In a similar way we can show that $\mathcal{B}' \subseteq \mathcal{B}$. Therefore, $\mathcal{B} = \mathcal{B}'$, which clinches the argument for injectivity of f. For surjectivity, let Q be an equivalence on A with $Q \supseteq R$. Then

$$\mathcal{B} = \{\{[b]_R \mid b \in [a]_Q\} \mid a \in A\}$$

is a partition of A/R with $f(\mathcal{B}) = Q$.

11.31 Let $m, m \in \mathbb{N}$ and suppose $n < m$. We show that $\forall n < m\ \{0, \ldots, n-1\} \not\sim \{0, \ldots, m-1\}$ by induction on m.
Basis: If $m = 0$ there is no $n < m$ so the statement $\forall n < m\ \{0, \ldots, n-1\} \not\sim \{0, \ldots, m-1\}$ trivially holds.
Induction step. Assume that $\forall n < m\ \{0, \ldots, n-1\} \not\sim \{0, \ldots, m-1\}$. We show that $\forall n < m+1\ \{0, \ldots, n-1\} \not\sim \{0, \ldots, m\}$.
Suppose for a contradiction that for some $n < m+1$ a bijection f from $\{0, \ldots, n-1\}$ to $\{0, \ldots, m\}$ exists. We may assume that $f(n-1) = m$ (exercise 11.25). Then $f \restriction \{0, \ldots, n-2\}$ is a bijection from $\{0, \ldots, n-2\}$ to $\{0, \ldots, m-1\}$, and contradiction with the induction hypothesis.

11.32 Let $X \subseteq \mathbb{N}$ and assume that for some $m \in \mathbb{N}\ \forall n \in X(n < m)$. We show that X is finite by establishing a bijection f between X and $\{0, \ldots, n-1\}$, for some n.
We first define a sequence of sets $X_0, \ldots, X_{n-1}$, as follows. If X is empty then put $n = 0$. Otherwise, put $X = X_0$ and $X_1 = X_0 - \{\min X_0\}$, where $\min(X_0)$ is the least element of X_0 that is guaranteed to exist by Fact 11.4. In general, if $X_i = 0$, then put $n = i$, otherwise put $X_{i+1} = X_i - \{\min X_i\}$. This defines the sequence $X_0, \ldots, X_{n-1}$. For every i, every non-empty X_i, $\min X_i < m$, so $n < m$. The function f given by $f(i) = \min X_i$ is a bijection between $\{0, \ldots, n-1\}$ and X.

11.33 Let E be a property of sets such that

1. $E(\emptyset)$,

2. for every set A and every object $x \notin A$: if $E(A)$, then also $E(A \cup \{x\})$.

Define $E'(n)$ as $\forall A$ (if A has n elements then $E(A)$). We show by induction on n that for all $n \in \mathbb{N}$, $E'(n)$. From this it follows immediately that E holds for any finite set A.
Basis: $E'(0)$ states that if A has 0 elements then $E(A)$. This follows immediately from $E(\emptyset)$.
Induction step: Assume $E'(n)$. We have to show $E'(n+1)$. Let A be an arbitrary set with $n+1$ elements, and let $x \in A$. Then $A - \{x\}$ has n elements, so the induction hypothesis applies, and we get $E(A - \{x\})$. By the second property of E, we get from $E(A - \{x\})$ and $x \notin A - \{x\}$ that $E(A)$. This establishes $E'(n+1)$.

11.34 We use 11.33. Let $E(A)$ be the property 'all subsets of A are finite'. It is clear that $E(\emptyset)$ holds, for $\emptyset$ has $\emptyset$ as its only subset, and $\emptyset$ is finite. Suppose that all subsets of A are finite. Let $x \notin A$. Then all subsets of $A \cup \{x\}$ are finite. For let $B \subseteq A$. Then by assumption $\{0, \ldots, n-1\} \sim B$ for some n. Since $x \notin B$, $\{0, \ldots, n\} \sim B \cup \{x\}$. This establishes E for every finite A.

11.35 Again, we use 11.33. Let A be a finite set. We show that for every finite set B, $A \cup B$ is finite. Let $E(B)$ be the property '$A \cup B$ is finite'. Then $E(\emptyset)$ follows from the fact that A is finite. Assume $E(B)$. Let $x \notin B$. We have to show that $A \cup B \cup \{x\}$ is finite. If $x \in A$ then $A \cup B \cup \{x\} = A \cup B$, which is finite by assumption $E(B)$. If $x \notin A$, then we get from assumption $E(B)$ that $\{0, \ldots, n-1\} \sim A \cup B$ for some n. Therefore, $\{0, \ldots, n\} \sim A \cup B \cup \{x\}$, i.e., $A \cup B \cup \{x\}$ is finite.

11.36 Let h be a finite injection with $\mathrm{dom}\,(h) \subseteq A$ and $\mathrm{ran}(h) \subseteq B$. Suppose $A \sim B$. We prove by induction on the size of h that a bijection $f : A \to B$ exists with $f \supseteq h$. If $h = \emptyset$ then every f fits the bill. Suppose that if h has n elements, the property holds. Let h have $n+1$ elements. Let $h' = h - \{(a, b)\}$, for some pair $(a, b) \in h$. Then by i.h. there is a bijection $f' : A \to B$ with $f' \supseteq h'$. Let $f'^{-1}(b) = a'$. Then $a' \notin \mathrm{dom}\,(f')$ by injectivity of f'. Define f by means of: $f(x) := f'(x)$ for $x \neq a, x \neq a'$, $f(a) := b$, $f(a') := f'(a)$. Then f is a bijection and $f \supseteq h$.
Note that the result does not extend to infinite injections h. Consider $h = \lambda n.2n$ on $\mathbb{N}$. Then h is injective, $\mathrm{dom}\,(h) \subseteq \mathbb{N}$ and $\mathrm{ran}(h) \subseteq \mathbb{N}$, but clearly there is no bijection f on $\mathbb{N}$ that extends h.

11.37 A proper subset of a finite set never is equipollent to that set. We prove by induction on the size of B that if $A \subseteq B$, $A \neq B$, B finite, then $A \not\sim B$.
Basis: If $B = \emptyset$ the property holds since $\emptyset$ has no proper subsets.
Induction step: Assume the property holds for sets B of size n. Let B be a set with $|B| = n+1$. Suppose, for a contradiction, that $f : B \to A$ is a bijection for some $A \subseteq B$, $A \neq B$. Since $A \neq B$, there is a $b \in B$ with $b \notin A$. Then $f(b) = a \in A$. Consider the set of pairs $f' = f - \{(b, a)\}$. The function f' is a bijection between $B - \{b\}$ and $A - \{a\}$. Also, $A - \{a\} \subseteq B - \{b\}$, by the fact that $f(b) = a$ and f is injective. Since $|B - \{b\}| = n$, this gives a contradiction with the induction hypothesis.

11.38.1 Let A and B be finite sets and $f : A \to B$ a bijection. Define $h : A \cap B \to B$ by means of $h(x) = x$. Then h is a finite injection of $A \cap B$ into B, so by Exercise 11.36 there is a bijection $g : A \to B$ with $g \supseteq h$. Consider $g \restriction A - B$. It is easy to see that this is a bijection between $A - B$ and $B - A$. This establishes $A - B \sim B - A$.

11.38.2 Let A and B be finite sets and $f : A \to B$ a bijection. Then by the previous item there is a bijection $h : B - A \to A - B$. Define $g : A \cup B \to A \cup B$ by means of: $g(x) = f(x)$ if $x \in A$, $g(x) = h(x)$ if $x \in B - A$. Then $f \subset g$ and g is a bijection on $A \cup B$.

11.39 Let A be finite. Let $E \subseteq \wp(A)$. Suppose $\emptyset \in E$, and assume $\forall B \in E \forall a \in A : B \cup \{a\} \in E$. We prove by

induction on the size of A that $A \in E$.
Basis: if $|A| = 0$ then the claim follows from $\emptyset \in E$.
Induction step: Suppose the property holds for all A with $|A| = n$. Let A be a set with $|A| = n+1$. Let $E \subseteq \wp(A)$ with $\emptyset \in E$ and $\forall B \in E \forall a \in A : B \cup \{a\} \in E$. Let $x \in A$. Consider $E' = \{B - \{x\} \mid B \in E\}$. Then $\emptyset \in E'$, $\forall B \in E' \forall a \in A - \{x\} : B \cup \{a\} \in E$. Thus, by induction hypothesis, $A - \{x\} \in E'$. Therefore, by the definition of E', $A \in E$.
Conversely, suppose A infinite. Let $E \subseteq \wp(A)$ be the collection of all finite subsets of A. Then $\emptyset \in E$, and $\forall B \in E \forall a \in A : B \cup \{a\} \in E$. Still, $A \notin E$, by the fact that A is infinite.

11.43.1 $A \preceq A$ since 1_A is an injection from A to A.

11.43.2 $A \sim B$ implies $A \preceq B$ since every bijection is an injection.

11.43.3 $A \preceq B \wedge B \preceq C \Longrightarrow A \preceq C$, since if there are injections $f : A \to B$ and $g : B \to C$, then $g \circ f : A \to C$ also is an injection.

11.43.4 $A \subseteq B \Longrightarrow A \preceq B$, since $A \subseteq B$ implies that the function $i : A \to B$ given by $i(x) = x$ is an injection.

11.44 To show that $\mathbb{N} \preceq A$ implies that A is infinite, we prove by induction on n that for all $n \in \mathbb{N}$, $\mathbb{N} \not\preceq \{0, \ldots, n-1\}$. From this we get immediately that for all $n \in \mathbb{N}$, $A \not\sim \{0, \ldots, n-1\}$, i.e., that A is infinite.
Basis: $\mathbb{N} \not\preceq \emptyset$. Obvious.
Inductions step: Assume $\mathbb{N} \not\preceq \{0, \ldots, , n-1\}$. We have to show $\mathbb{N} \not\preceq \{0, \ldots, n\}$. Suppose for a contradiction that there is an injection $f : \mathbb{N} \to \{0, \ldots, , n\}$. Then an injection $g : \mathbb{N} \to \{0, \ldots, n\}$ exists with $g(0) = n$ (swap the values of f on 0 and $f^{-1}(n)$, if necessary). Define $h : \mathbb{N} \to \{0, \ldots, n-1\}$ by means of $h(k) = g(k+1)$. Then h is an injection, and contradiction with the induction hypothesis.

11.45 Let $h : A \to A$ be an injection that is not surjective, and let $b \in A - \text{ran}(f)$. Let f be given by $f(0) = b$ and $f(n+1) = h(f(n))$. We prove by induction on n that $f(n)$ is different from $f(0), \ldots, f(n-1)$.
Basis: trivially true.
Induction step. Assume $f(n)$ is different from $f(0), \ldots, f(n-1)$. We have to show that $f(n+1)$ is different from $f(0), \ldots, f(n)$. By definition of h, $f(1) = h(f(0), \ldots, f(n+1) = h(f(n))$. By induction hypothesis, $f(n)$ is different from $f(0), \ldots, f(n-1)$, so by injectivity of h, $f(n+1) = h(f(n))$ is different from $h(f(0)) = f(1), \ldots, h(f(n-1)) = f(n)$. By the fact that $b \notin \text{ran}(f)$, $f(n+1) = h(f(n)) \neq b$, so $f(n+1)$ is also different from $f(0)$.

11.46 Let $\mathbb{N} \preceq A$. Then there is an injection $f : \mathbb{N} \to A$. Consider the function $h = f \circ s$, where s is the successor function on $\mathbb{N}$. Then h is inejective because s and f are, and $f(0) \notin \text{ran}(h)$.

11.47 Let A be infinite. Then (Thm 11.42) $\mathbb{N} \preceq A$. Thus (Ex 11.46) there is a non-surjective injection $h : A \to A$. But then $A \sim \text{ran}(h) \neq A$, i.e., A is equipollent with one of its proper subsets.
Conversely, let A be equipollent with one of its proper subsets B. Then a bijection $f : A \to B$ exists, so $h : A \to A$ given by $h(x) = f(x)$ is an injection that is not surjective. Thus (Ex 11.45), $\mathbb{N} \preceq A$, i.e., A is infinite.

11.48 Let A be infinite, and let $f : A \to A$. We show that f is surjective iff f is injective.
$\Rightarrow$: Since A is infinite there is an $n \in \mathbb{N}$ with $A = \{a_0, \ldots, a_{n-1}\}$. By surjectivity of f, $A = \{f(a_0), \ldots, f(a_{n-1})\}$. Since this set has n elements, $i \neq j$ implies $f(a_i) \neq f(a_j)$, i.e., f is injective.
$\Leftarrow$: Suppose $f : A \to A$ is surjective but not injective. Then (Ex 11.45) $\mathbb{N} \preceq A$ and therefore (Ex 11.44)

contradiction with the finiteness of A.

11.50 Let $B \subseteq A$ and $A \sim \mathbb{N}$. Then there is a bijection $f : A \to \mathbb{N}$. Define an enumeration of B as follows. $b_0 =$ the $b \in B$ such that $f(b) \leqslant f(a)$ for all $a \in B$, provided B is non-empty, $b_{n+1} =$ the $b \in B' = B - \{b_0, \ldots, b_n\}$ such that $f(b) \leqslant f(a)$ for all $a \in B'$, provided B' is non-empty. Then either there is a k with $B = \{b_0, \ldots, b_k\}$, in which case B is finite, or there is no such k, in which case $B \sim \mathbb{N}$.

11.51.1 $\mathbb{Z}$ is countably infinite, for $f : \mathbb{Z} \to \mathbb{N}$ given by $f(p) = 2p$ if $p \geqslant 0$ and $f(p) = -(2p + 1)$ if $p < 0$ is a bijection. This maps the non-negative integers to the even naturals, and the negative integers to the odd naturals.

11.51.2 Let A and B are both countably infinite. Assume $A \cap B = \emptyset$. Then there are bijections $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$. Define a bijection $h : \mathbb{N} \to A \cup B$ by means of $h(2n) = f(n)$ and $h(2n + 1) = g(n)$.

If $A \cap B \neq \emptyset$, then put $A' = A - B$ and $B' = A \cap B$, and enumerate $A' \cup B'$, next enumerate the union of $A' \cup B'$ and $C' = B - A$.

11.54 Map the non-negative rationals to the even naturals, and the negative rationals to the odd naturals.

11.55 By repeated application of the enumeration procedure F_2 for pairs we get enumerations F_3 of $\mathbb{N}^3$, F_4 of $\mathbb{N}^4$, and so on. To enumerate $\mathbb{N}^*$, first take [], next use the function $f(k) = F_n(m)$, where $j(n, m) = k$. Note that j is the function defined in Theorem 11.52. This generates the list

$$[[], [0], [1], [0, 0], [2], [0, 1], [0, 0, 0], [3], [1, 0], [0, 0, 1], [0, 0, 0, 0], [4], [0, 2], [1, 0, 0], [0, 0, 0, 1], \ldots$$

which is the result of taking $\swarrow$ slices from the following table, starting from the top left corner.

$$\begin{array}{llllllll}
[0], & [1], & [2], & [3], & [4], & [5], & \cdots \\
[0, 0], & [0, 1], & [1, 0], & [0, 2], & [1, 1], & [2, 0], & \cdots \\
[0, 0, 0], & [0, 0, 1], & [1, 0, 0], & [0, 1, 0], & [1, 0, 1], & [2, 0, 0], & \cdots \\
[0, 0, 0, 0], & [0, 0, 0, 1], & [1, 0, 0, 0], & [0, 1, 0, 0], & [1, 0, 0, 1], & [2, 0, 0, 0], & \cdots \\
[0, 0, 0, 0, 0], & \cdots & & & & &
\end{array}$$

11.56 A union of countably infinitely many countably infinite sets is countably infinite, by an obvious variation on the procedure of the previous exercise.

11.63.1 Since $A \sim A$, it is *not* the case that no bijection from A to A exists. Therefore $A \not\prec A$.

11.63.2 $A \preceq B$ iff an injection $h : A \to B$ exists iff either an injection $h : A \to B$ exists while A and B are not equipollent, or A and B are equipollent, iff $A \prec B \vee A \sim B$.

11.63.3 Suppose $A \prec B$ and $B \sim C$. Then an injection $h : A \to B$ exists, but there is no bijection between A and B. There is a bijection $f : B \to C$. Thus $f \circ h : A \to C$ is an injection. Suppose for a contradiction that a bijection $g : C \to A$ exists. Then $g \circ f : B \to A$ is a bijection, and contradiction with $A \not\sim B$. Thus $A \prec C$.

11.63.4 The flaw in the argument is that the fact that a particular injection $f : A \to B$ is not surjective does not warrant the conclusion that *no* function $f : A \to B$ is a bijection.

11.64 Suppose A is finite. Then there is an $n \in \mathbb{N}$ with $A = \{a_0, \ldots, a_n\}$, and therefore $f : A \to \mathbb{N}$ given by $f(a_i) = i$ is an injection. From Thm 11.24 ($\mathbb{N} \not\sim \{0, \ldots, n - 1\}$) it follows that $\mathbb{N} \not\sim \{a_0, \ldots, a_n\}$. Thus, $A \prec \mathbb{N}$.

11.65 The reals in the interval $(0, \frac{2}{9}]$ are exactly the numbers with decimal expansions $0, r_0 r_1 r_2 \cdots$ with decimal digits $r_i \in \{0, 1, 2\}$. The proof of uncountability of $(0, \frac{2}{9}]$ can therefore proceed exactly as the proof for the uncountability of $\mathbb{R}$, only with the decimal digits restricted to $\{0, 1, 2\}$.

11.66 Let A be a set, and let $h : A \to \wp(A)$ be given by $h(a) = \{a\}$. We show that $\{a \in A \mid a \notin h(a)\} = \emptyset$. For suppose, to the contrary, that $b \in \{a \in A \mid a \notin h(a)\}$. Then $b \in A$ and $b \notin h(b)$. Thus, $b \notin \{b\}$, and therefore $b \neq b$, and contradiction.

11.67 Clearly, $\mathbb{N} \preceq \{0, 1\}^{\mathbb{N}}$, for the function $h : \mathbb{N} \to \{0, 1\}^{\mathbb{N}}$ given by

$$h(k) = \lambda n. \text{ if } n = k \text{ then } 1 \text{ else } 0$$

is an injection. To see that $\mathbb{N} \not\sim \{0, 1\}^{\mathbb{N}}$, assume for a contradiction that $f : \mathbb{N} \to \{0, 1\}^{\mathbb{N}}$ is a bijection. Define a fucntion $g : \mathbb{N} \to \{0, 1\}$ by means of $g(i) = 0$ if $f(i)(i) = 1$, $= 1$ otherwise. Then $g \notin \text{ran}(f)$, and contradiction with the assumption that f is a bijection.

11.68 Clearly, $\mathbb{N} \preceq \mathbb{N}^{\mathbb{N}}$, for the function $h : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ given by

$$h(k) = \lambda n. \text{ if } n = k \text{ then } 1 \text{ else } 0$$

is an injection. To see that $\mathbb{N} \not\sim \mathbb{N}^{\mathbb{N}}$, assume for a contradiction that $\varphi : \mathbb{N} \to \mathbb{N}^{\mathbb{N}}$ is a bijection. Define a function $f : \mathbb{N} \to \mathbb{N}$ by means of $f(i) = k$ for some $k \in \mathbb{N}$ with $k \neq \varphi(i)(i)$. Then $f \notin \text{ran}(\varphi)$, and contradiction with the assumption that φ is a bijection.

11.69 A surjection $h : \mathbb{N} \to \mathbb{Q}$ exists. Now assume we produce a real r by the procedure from the proof of Theorem 11.60. Then it follows immediately from the procedure that $r \notin \text{ran}(h)$. Since h is surjective, this means that $r \notin \mathbb{Q}$.

11.74 Let $A \preceq B \subseteq A$. Then there is an injection $h : A \to B$, and $\text{ran}(h) \subseteq B \subset A$. Let $X_0 = A - B$, and in general, let $X_{n+1} = h[X_n]$. Let $X = \bigcup_{n \in \mathbb{N}} X_n$. Define a function $f : A \to B$ as follows. If $a \notin X$ then $f(a) = a$, if $a \in X$ then $f(a) = h(a)$. Verify that f is a bijection. For injectivity, let $a \neq b$.

1. If $a \notin X, b \notin X$, then $f(a) = a \neq b = f(b)$.
2. If $a \in X, b \in X$, then $f(a) = h(a) \neq h(b) = f(b)$, by injectivity of h.
3. If $a \notin X, b \in X$, then $f(a) = a \neq h(b) = f(b)$ by the fact that $a \notin X$ while $h(b) \in X$ by definition of X.
4. If $a \in X, b \notin X$, then $f(a) = h(a) \neq b = f(b)$ by the fact that $b \notin X$ while $h(a) \in X$ by definition of X.

For surjectivity, let $b \in B$. Then $b \notin X_0$. If $b \notin X$ then $f(b) = b$, otherwise $b \in X_k$ with $k > 0$, and therefore there is a $c \in X_{k-1}$ with $f(c) = h(c) = b$.

11.75 Let $A \preceq B$ and $B \preceq A$. Then there are injections $h : A \to B$ and $g : B \to A$. So $f : B \to \text{ran}(g)$ given by $f(b) = g(b)$ is a bijection, i.e., $B \sim \text{ran}(g)$. Therefore, $f \circ h : A \to \text{ran}(g)$ is an injection. Applying Lemma 11.73 to the injection $f \circ h : A \to \text{ran}(g) \subseteq A$ we get that $A \sim \text{ran}(g)$, which, together with $B \sim \text{ran}(g)$ gives $A \sim B$.

11.76.1 By Cantor-Bernstein it is enough to give injections $f : [0, 1] \to [0, \frac{2}{3})$ and $g : [0, \frac{2}{3}) \to [0, 1]$. This is easy. Let $f = \lambda x. \frac{1}{3} x$ and let $g = \lambda x. x$. This shows that a bijection between $[0, 1]$ and $[0, \frac{2}{3})$ must exist. For good

measure, we also give an explicit definition of such a bijection. Let $G : [0,1] \to [0, \frac{2}{3}]$ be the bijection $x \mapsto \frac{2}{3}x$, and let $H : [0,1] \to [0,1]$ be the injection $x \mapsto \frac{1}{2}x$. Then let $F : [0,1] \to [0, \frac{2}{3})$ be given by $F(x) = G(x)$ for all x not of the form $2^{-n} \cdot \frac{2}{3}$, and $F(x) = H \circ G(x)$ for all x of the form $2^{-n} \cdot \frac{2}{3}$. It is easily checked that F is a bijection.

11.76.2 By Cantor-Bernstein it is enough to give injections $f : \{(x,y) \mid x^2 + y^2 \leqslant 1\} \to \{(x,y) \mid x^2 + y^2 < 1\}$ and $g : \{(x,y) \mid x^2 + y^2 < 1\} \to \{(x,y) \mid x^2 + y^2 \leqslant 1\}$. This is easy: put $f = \lambda(x,y).(\frac{1}{2}x, \frac{1}{2}y)$ and $g = \lambda(x,y).(x,y)$.

11.76.3 Again, Cantor-Bernstein makes this easy. Here is a function $f : \{(x,y) \mid x^2 + y^2 \leqslant 1\} \to \{(x,y) \mid |x|, |y| < \frac{1}{2}\}$ that injects the disk $\{(x,y) \mid x^2 + y^2 \leqslant 1\}$ into a disk within the square $\{(x,y) \mid |x|, |y| < \frac{1}{2}\}$. Let $f = \lambda(x,y).(\frac{1}{2}x, \frac{1}{2}y)$. Since the square is already contained in the disk the function $g : \{(x,y) \mid |x|, |y| < \frac{1}{2}\} \to \{(x,y) \mid x^2 + y^2 \leqslant 1\}$ given by $g = \lambda(x,y).(x,y)$ is an injection.

11.77 Let A be finite or countably infinite. To show that $X = \mathbb{R} - A$ is uncountable, suppose for a contradiction that $f : \mathbb{N} \to X$ is a bijection. As in the proof of Theorem 11.60, every $f(n)$ can be written as $p_n + 0.r_0^n r_2^n r_2^n \cdots$, with $p_n \in \mathbb{Z}$ and $p_n \leqslant f(n) < p_n + 1$. Define a real number $f = 0.r_0 r_1 r_2 \cdots$ by means of picking r_n different from r_n^n, $r_n \neq 0$, $r_n \neq 9$. Then r is different from every $f(n)$, and contradiction with the fact that f is a bijection.

The above does not yet show that $\mathbb{R}$ and $\mathbb{R} - A$ are equipollent, for it does not exclude the possiblity $\mathbb{N} \prec \mathbb{R} - A \prec \mathbb{R}$ (we don't assume Cantor's continuum hypothesis).

To show that $\mathbb{R} \sim \mathbb{R} - A$, we need to establish an injection from $\mathbb{R}$ into $\mathbb{R} - A$. The result then follows from $\mathbb{R} \preceq \mathbb{R} - A$ and $\mathbb{R} - A \preceq \mathbb{R}$ by Cantor-Bernstein. If $A = \{a_0, \ldots, a_{n-1}\}$, then $\mathbb{R} - A \sim \mathbb{R} - \{p_0, \ldots, p_{n-1}\}$, where the p_i are different prime numbers. Define a function $h : \mathbb{R} \to \mathbb{R} - \{p_0, \ldots, p_{n-1}\}$ by putting $h(x) = x$ if x is not of the form p_i^k, with $0 \leqslant i < n$ and $k > 0$, and letting $h(p_i^k) = p_i^{k+1}$. Then h is an injection. Suppose $A \sim \mathbb{N}$. To show $\mathbb{R} \preceq \mathbb{R} - A$ we will show that $\mathbb{R} \preceq \mathbb{R} - P$, where P is the set of prime numbers. Since $P \sim \mathbb{N} \sim A$, this gives $\mathbb{R} \preceq \mathbb{R} - A$. Define a function $h : \mathbb{R} \to \mathbb{R} - P$ as follows. Let $h(x) = x$ if x is not of the form p^n, with $n > 0$, and let $h(p^n) = p^{n+1}$. Then h is an injection.

11.78 $(\mathbb{R} - \mathbb{Q}) \sim \mathbb{R}$ is a special case of $(\mathbb{R} - A) \sim \mathbb{R}$, with A countably infinite: see previous exercise.

11.79 The function `pair` is nothing but the function j defined in Theorem 11.52. Here it is (to check that it is the inverse of `natpairs`, you can use `map pair natpairs`):

```
pair (n,m) = (n + m) * (n + m + 1) `div` 2 + n
```

11.79 First, we need code for enumerating $\mathbb{N}^2$, $\mathbb{N}^3$, ..., as lists:

```
natpairs2 = [(x, fromInteger z-x) | z <- [0..], x <- [0..z]]

natlist 0 = [ [n] | n <- [0..] ]
natlist k = [ n : (natlist (k-1) !! fromInteger m) | (n,m) <- natpairs2 ]
```

Next, `natstar` can be defined in terms of `natlist`:

```
natstar = [] : [ natlist n !! fromInteger m  |  (n,m) <- natpairs2 ]
```

11.84.1 Unter the given assumptions we have: $|A_1 \cap B_1| = |A_1| + |B_1| = |A_2| + |B_2| = |A_2 \cap B_2|$. It follows that $A_1 \cap B_1 \sim A_2 \cap B_2$.

11.84.2 $|A_1 \times B_1| = |A_1| \times |B_1| = |A_2| \times |B_2| = |A_2 \times B_2|$. It follows that $A_1 \times B_1 \sim A_2 \times B_2$.

11.84.3 Let $f : A_1 \to A_2$ and $g : B_1 \to B_2$ be bijections. Establish a bijection $F : A_1^{B_1} \to A_2^{B_2}$ as follows. For $\varphi : B_1 \to A_1$, let $F(\varphi)$ be the function $g \circ \varphi \circ f^{-1}$. It is routine to check that this is a bijection. It follows that ${A_1}^{B_1} \sim {A_2}^{B_2}$.

11.85.1 Given: $A_1 \preceq A_2$ and $B_1 \preceq B_2$, $A_2 \cap B_2 = \emptyset$. We show that $A_1 \cup B_1 \preceq A_2 \cup B_2$ by establishing an injection. Let $f : A_1 \to A_2$ and $g : B_1 \to B_2$ be injections. Define $h : A_1 \cup B_1 \to A_2 \cup B_2$ by means of: $h(x) = f(x)$ if $x \notin B_1$, $h(x) = g(x)$ if $x \in B_1$. By the injectivity of f, g and the fact that $A_2 \cap B_2 = \emptyset$, this is an injection.

11.85.2 Let f, g be as before. Define $h : A_1 \times B_1 \to A_2 \times B_2$ by means of: $h(x, y) = (f(x), g(y))$. Then h is an injection.

11.85.3 Let $f : A_1 \to A_2$ be an injection. Then $h : \wp(A_1) \to \wp(A_2)$ defined by $h(X) = f[X]$ is an injection.

11.85.4 Assume $A_2 \neq \emptyset$. Let $a \in A_2$, let $f : A_1 \to A_2$ and $g : B_1 \to B_2$ be injections. Define a mapping $F : A_1^{B_1} \preceq A_2^{B_2}$ as follows. If $\varphi : B_1 \to A_2$, then $F(\varphi)$ is the function in $B_2 \to A_2$ given by $F(\varphi)(x) = g(\varphi(f^{-1}(x)))$ if $x \in \mathrm{ran}(f)$, and $F(\varphi)(x) = a$ otherwise. By injectivity of f this is well-defined. We show that F is an injection. Let $\varphi_1, \varphi_2 : B_1 \to A_2$ with $\varphi_1 \neq \varphi_2$. We have to show $F(\varphi_1) \neq F(\varphi_2)$. From $\varphi_1 \neq \varphi_2$ we get that there is a $b \in B_1$ with $\varphi_1(b) \neq \varphi_2(b)$. By the definition of F, $F(\varphi_1(f(b))) = g(\varphi_1(b))$ and $F(\varphi_2(f(b))) = g(\varphi_2(b))$, and by injectivity of g we get from $\varphi_1(b) \neq \varphi_2(b)$ that $F(\varphi_1(f(b))) = g(\varphi_1(b)) \neq g(\varphi_2(b)) = F(\varphi_2(f(b)))$.

11.86.1 $\emptyset \prec \{\frac{1}{2}\}$, but $\emptyset \cup \mathbb{N} = \mathbb{N} \sim \{\frac{1}{2}\} \cup \mathbb{N}$.

11.86.2 $\{0\} \prec \{0, 1\}$, but $\{0\} \times \mathbb{N} \sim \mathbb{N} \sim \mathbb{Z} \sim \{0, 1\} \times \mathbb{N}$.

11.86.3 $\{0, 1\} \prec \{0, 1, 2\}$, but $\{0, 1\}^{\mathbb{N}} \sim \{0, 1, 2\}^{\mathbb{N}}$.

11.86.4 $\{0\} \prec \{0, 1\}$, but $\mathbb{N}^{\{0\}} \sim \mathbb{N} \sim \mathbb{N}^2 \sim \mathbb{N}^{\{0,1\}}$.

11.87.1 If $B \cap C = \emptyset$ then $|B \cup C| = |B| + |C|$, and therefore:

$$|A^{B \cup C}| = |A|^{|B \cup C|} = |A|^{|B|+|C|} = |A|^{|B|} \times |A|^{|C|} = |A^B| \times |A^C| = |A^B \times A^C|.$$

11.87.2 Cardinal arithmetic:

$$|(A \times B)^C| = |A \times B|^{|C|} = (|A| \times |B|)^{|C|} = |A|^{|C|} \times |B|^{|C|}.$$

11.87.3 Note that a bijection between $(A^B)^C$ and $A^{C\times B}$ is provided by the *curry* operation that links $f : C \times B \to A$ to $(\text{curry} f) : C \to B \to A$. This gives $(A^B)^C \sim A^{C\times B} \sim A^{B\times C}$.

11.88.1 Clearly $\{0,1\}^{\mathbb{N}} \preceq \{0,\ldots,n\}^{\mathbb{N}} \preceq \mathbb{N}^{\mathbb{N}} \preceq \mathbb{R}^{\mathbb{N}}$, so if we can show $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$ we are done, for together with $\{0,1\}^{\mathbb{N}} \sim \wp(\mathbb{N}) \sim \mathbb{R}$ this gives the desired result, by Cantor-Bernstein. For $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$ we can use cardinal arithmetic:

$$|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|^{|\mathbb{N}|} = {\aleph_1}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0\times\aleph_0} = 2^{\aleph_0} = |\mathbb{R}|.$$

11.88.2 Clearly,

$$\{0,1\}^{\mathbb{R}} \preceq \{0,\ldots,n\}^{\mathbb{R}} \preceq \mathbb{N}^{\mathbb{R}} \preceq \mathbb{R}^{\mathbb{R}} \preceq (\wp(\mathbb{R}))^{\mathbb{R}} \preceq (\mathbb{R}^{\mathbb{R}})^{\mathbb{R}}.$$

It is therefore enough to show $(\mathbb{R}^{\mathbb{R}})^{\mathbb{R}} \sim \{0,1\}^{\mathbb{R}}$. Here is a proof by cardinal arithmetic:

$$|(\mathbb{R}^{\mathbb{R}})^{\mathbb{R}}| = (|\mathbb{R}|^{|\mathbb{R}|})^{|\mathbb{R}|} = ({\aleph_1}^{\aleph_1})^{\aleph_1} = {\aleph_1}^{\aleph_1\times\aleph_1} = {\aleph_1}^{\aleph_1} = (2^{\aleph_0})^{\aleph_1} = 2^{\aleph_0\times\aleph_1} = 2^{\aleph_1} = |\{0,1\}^{\mathbb{R}}|.$$

11.89.1 We show by induction on n that ${\aleph_0}^n = \aleph_0$ for all $n > 0$. Basis: clearly, ${\aleph_0}^1 = \aleph_0$. Induction step: suppose ${\aleph_0}^n = \aleph_0$. Then:

$${\aleph_0}^{n+1} = \aleph_0 \times {\aleph_0}^n \overset{ih}{=} \aleph_0 \times \aleph_0 = \aleph_0.$$

11.89.2 We show by induction on n that ${\aleph_1}^n = \aleph_1$ for all $n > 0$. Basis: clearly, ${\aleph_1}^1 = \aleph_1$. Induction step: suppose ${\aleph_1}^n = \aleph_1$. Then:

$${\aleph_1}^{n+1} = \aleph_1 \times {\aleph_1}^n \overset{ih}{=} \aleph_1 \times \aleph_1 = \aleph_1.$$

To show $\mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$, use cardinal arithmetic:

$$|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|^{|\mathbb{N}|} = {\aleph_1}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0\times\aleph_0} = 2^{\aleph_0} = \aleph_1 = |\mathbb{R}|.$$

11.90 Both sets have cardinality $\aleph_1$.

11.91 If A is infinite and B finite, then there are $n, m \in \mathbb{N}$ with $|B| = n$ and $|B - A| = m$. Since $(A - B) \cap (B - A) = \emptyset$ and A is infinite, we have:

$$|(A - B) \cup (B - A)| = |A - B| + |B - A| = (|A| - n) + m = |A| + m = |A|.$$