# Discrete Mathematics Problems

Irakli Diasamidze

# Contents

# Chapter 1

# Sets, induction and functions

## 1.1 Week 1 Central Exercises

### Exercise 1.1.1

Let $S$ denote the set of students enrolled in KIU. Let's further define the following sets

$$\begin{aligned}
&A = \{s \in S : s \text{ is registered for “Discrete Structures 2022” course}\},\\
&B = \{s \in S : s \text{ is studying on computer science program}\},\\
&C = \{s \in S : s \text{ is studying on math program}\},\\
&D = \{s \in S : s \text{ is studying on math or computer science programs}\}.
\end{aligned}$$

Now, try to describe $A \cup B$, $C \cap \mathbb{N}$, $D \setminus B$ and $\mathbb{N} \setminus A$. [I am going to assume “Discrete Structures” course was taught for CS major in 2022.]

Since every student who studies on computer science program also studies Discrete Structures, i.e., $B \subset A$, we have $A \cup B = A$. Elements of $C$ are students and elements of $\mathbb{N}$ are numbers, clearly, they have nothing in common. Hence, $C \cap \mathbb{N} = \varnothing$. Also, $D \setminus B = \{s \in S : s \text{ is studying on math or computer science programs and not on computer science program}\} = \{s \in S : s \text{ is studying on math program}\} = C$. Like previously, $\mathbb{N}$ and $A$ have no common elements, so $\mathbb{N} \setminus A = \mathbb{N} \setminus (A \cap \mathbb{N}) = \mathbb{N} \setminus \varnothing = \mathbb{N}$.

## Exercise 1.1.2

Given $A = \{a \in \mathbb{N} : a \text{ is odd}\}$, $B = \mathbb{Z}$, $C = \{x \in \mathbb{R} : 2 \leqslant x < 7\}$ and $D = \left\{2, \frac{1}{4}, 7, \pi\right\}$. Find

1. $A \cap C = \{3, 5\}$
2. $A \cup D = \left\{a : a = 2, a = \frac{1}{4}, a = \pi \text{ or } a \text{ is an odd natural number}\right\}$
3. $C \cap D \cap A = C \cap \{7\} = \varnothing$
4. $(A \cap D) \cup C = \{7\} \cup C = \{x \in \mathbb{R} : 2 \leqslant x \leqslant 7\}$
5. $(B \setminus A) \cap D = (B \cap D) \setminus A = \{2, 7\} \setminus A = \{2\}$ [Proof of the first equality is at the end of this Exercise.]
6. $D \setminus (A \cap B \cap C \cap D) = D \setminus \varnothing = D$
7. $\mathcal{P}(D) = \left\{\varnothing, \{2\}, \left\{\frac{1}{4}\right\}, \{7\}, \{\pi\}, \left\{2, \frac{1}{4}\right\}, \{2, 7\}, \{2, \pi\}, \left\{\frac{1}{4}, 7\right\}, \left\{\frac{1}{4}, \pi\right\},\right.$ $\left.\{7, \pi\}, \left\{2, \frac{1}{4}, 7\right\}, \left\{2, \frac{1}{4}, \pi\right\}, \left\{2, \frac{1}{4}, \pi\right\}, \{2, 7, \pi\}, \left\{\frac{1}{4}, 7, \pi\right\}, \left\{2, \frac{1}{4}, 7, \pi\right\}\right\}$
8. $\mathcal{P}(D) \cap D = \varnothing$

## Exercise 1.2.1

Triangle sequence is a sequence of natural numbers $T_n$, geometrically given by starting with a single point in space and then for each $n$th triangle drawing $n + 1$ equally spaced dots centered at the bottom of it to get the $(n + 1)$th triangle, $T_n$ is the amount of dots in the $n$th triangle. Show that

$$T_n = \frac{n(n+1)}{2}$$

The base case holds as, like we mentioned, the sequence starts with a single dot, i.e., $T_1 = 1$ and $\frac{1(1+1)}{2} = 1$. For the inductive step, assume $T_n = \frac{n(n+1)}{2}$ is true for some natural $n$ and consider $T_{n+1}$. Note that the way we construct the triangles gives us the recursive formula $T_{n+1} = T_n + (n+1)$. According to our assumption, we have the following:

$$T_{n+1} = T_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} =$$
$$= \frac{(n+2)(n+1)}{2} = \frac{(n+1)((n+1)+1)}{2}$$

Finishing the proof by induction.

## Exercise 1.2.2

By the principle of mathematical induction for $\forall n \in \mathbb{N}$ prove, the following:

1. $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$;

   The base case holds as $1^3 = 1 = \frac{1^2(1+1)^2}{4}$ indeed. For the inductive step, assume the equation is true for some natural $n$. Consider the following:

   $$1^3 + 2^3 + \cdots + n^3 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 =$$
   $$= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} = \frac{(n+1)^2(n^2+4n+4)}{4} =$$
   $$= \frac{(n+1)^2(n+2)^2}{4} = \frac{(n+1)^2((n+1)+1)^2}{4}$$

   Finishing the proof by induction. (Note how this implies that sum of first $n$ cubes is the same as the square of the sum of first $n$ naturals.)

2. $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$;

   The base case is satisfied as $1 \cdot 2 = 2 = \frac{1(1+1)(1+2)}{3}$ indeed. For the inductive step, assume the equation is true for some natural $n$. Consider the following:

   $$1 \cdot 2 + \cdots + n(n+1) + (n+1)(n+2) = \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) =$$
   $$= \frac{n(n+1)(n+2) + 3(n+1)(n+2)}{3} = \frac{(n+3)(n+1)(n+2)}{3} =$$
   $$= \frac{(n+1)((n+1)+1)(n+1)+2)}{3}$$

   Finishing the proof by induction. (interestingly enough, this can be shown via closed forms of sum of first $n$ natural and first $n$ squares.)

3. $n(n+1)(n+2)$ is divisible by 6;

   The base case indeed holds as $1(1+1)(1+2) = 6$ and $6 = 6 \cdot 1$ (i.e., 6 divides itself 6). For the inductive step, assume there exists an integer $k$ with $6k = n(n+1)(n+2)$. Consider the following:

   $$(n+1)((n+1)+1)((n+1)+2) = (n+1)(n+2)(n+3) = n(n+1)(n+2)+3(n+1)(n+2) =$$

   $$= 6k + 3(n+1)(n+2)$$

   For any $n$, either $n+1$ or $n+2$ will be even, so we have a sum of two multiples of 6, which is also a multiple of 6, finishing the proof by induction. (Using induction for this becomes more of a messy method when the amount of terms in the product get larger with the number that we are dividing by. An alternate and easier method would rather involve showing that any set of $n$ consecutive integers contains one multiple of $n$.)

4. $3^{2n} - 1$ is divisible by 8.

   The base case is held since $3^2 - 1 = 8 = 8 \cdot 1$. For the inductive step, assume there exists an integer $m$ with $8m = 3^{2n} - 1$. Consider the following:

   $$3^{2(n+1)} - 1 = 3^{2n+2} - 1 = 9 \cdot 3^{2n} - 1 = 8 \cdot 3^{2n} + 3^{2n} - 1 = 8 \cdot 3^{2n} + 8k =$$

   $$= 8(3^{2n} + k)$$

   Clearly, $3^{2n}$ and $k$ are integers and so is their sum. Finishing the proof by induction. (An easier proof would consist of using modular arithmetic or binomial theorem.)

## Exercise 1.3.1

Let $V$ denote the set of all arrows originating from a single point on a plane (see Figure 1). Can you find a bijection between $V$ and ordered pairs of real numbers (that is, $\mathbb{R} \times \mathbb{R}$)? Can you find another one? Hint: Consider a Cartesian plane and corresponding coordinates for each arrow.

Start by drawing a pair of distinct lines crossing the origin, we will refer to them as axes (axis 1 and axis 2) and assign values to points on each line on a numberline. For each arrow, draw two lines crossing its tip each of which is orthogonal to one of the axes (line 1 and line 2 respectively). Write down the value at the intersection of axis 1 and line 1 and then the value at the intersection of axis 2 and line 2. We claim function from $V$ to $\mathbb{R}^2$ defined with the procedure mentioned to be a bijection. Clearly, different arrows have different tips and hence at least one of the orthogonal projections should be distinct, meaning the corresponding outputs are also different; This proves injectivity. For surjectivity, for any $(r_1, r_2) \in \mathbb{R}$ find the points on axis 1 having the value $r_1$ and draw a line crossing that point which is orthogonal to axis 1. Do the same for axis 2 and draw an arrow from the origin to the intersection of the lines. What we get is a guarantee for an arrow whose output is $(r_1, r_2)$; This proves surjectivity. Due to 4 constraints of freedom, this gives us an infinite family of bijections from $V$ to $\mathbb{R}^2$, but there are still some actions we could do before applying $f$ to each arrow. They are reflections along any line or point, translations and scaling. (Existence of a bijection from $V$ and $\mathbb{R}^2$ explains the duality of a "vector" for non-mathematicians (i.e., the idea that vectors are lists of numbers and arrows in space at the same time). Later we will call some of these functions isomorphisms for vector spaces and also generalize the notion of a vector.)

## Exercise 1.3.2

Let $f : X \to Y$ be a function between sets $X$ and $Y$.

1. Recall the definition of the preimage of $Y$ under $f$.

   It is the set of elements $x$ in $X$ such that $f(x)$ is in $Y$. Obviously, that set is $X$ itself.

2. Show that there is a bijection between $X$ and range of $f$ if $f$ is injective.

$f$ is injective and surjectivity is guaranteed by the definition of range.

3. Can $f$ be surjective if $X$ and $Y$ are finite and $|X| < |Y|$?

Before we begin the proof, we need to show that composition (if defined) of any set of surjections is also surjective by induction. For base case take two surjective functions $f : A \to B$ and $g : B \to C$ and consider $g \circ f : A \to C$. Due to surjectivity of $g$, for all $c \in C$ there exists $b \in B$ such that $g(b) = c$. Also, due to surjectivity of $f$ and since $b \in B$, there exists $a \in A$ such that $f(a) = b$. Hence for all $c \in C$ we have $g(f(a)) = c$ for some $a \in A$, meaning $g \circ f$ is indeed surjective. For the inductive step, assume the hypothesis is true for $n$ amount of suitable functions. Let $\{f_1, \dots, f_{n+1}\}$ be a set of surjective functions with $f_i : A_i \to A_{i+1}$. Then $f_{n+1} \circ f_n \circ \dots f_1 : A_1 \to A_{n+2}$ is surjective since $f_n \circ \dots \circ f_1$ and $f_{n+1}$ are surjective. (The result of base case has been applied.)

Assume $|X| = n < m = |Y|$ and that there exists $f : X \to Y$ which is surjective. Since cardinalities of $|X|$ and $|Y|$ are $n$ and $m$ respectively, there exist bijections $\varphi_1 : X \to \{1, \dots, n\}$ and $\varphi_2 : Y \to \{1, \dots m\}$. Since $\varphi_2, f$ and $\varphi_1^{-1}$ are surjective, their composition, call it $\pi$, should also be surjective according to our claim. But $\pi : \{1, \dots, n\} \to \{1, \dots, m\}$ can't be surjective since $\{\pi(1), \dots, \pi(n)\}$ contains at most $n$ elements, which is less than $m$, meaning the image of $\pi$ can't have the same amount of elements as the codomain (Hence they can't be the same sets and surjectivity is not achievable). Since we arrived at a contradiction, no such $f$ exists.

Note: We can rephrase our result as follows: If for finite sets $X, Y$ there exists a surjective $f : X \to Y$, then $|X| \geqslant |Y|$.

4. Can $f$ be injective but not surjective if $X$ and $Y$ are finite and $|X| = |Y|$.

   We start by showing that composition (if defined) of a set of injections is also injective. For the base case, let $f : A \to B$ and $g : B \to C$ be injective and consider $g \circ f : A \to C$. Let $a_1, a_2 \in A$ be distinct, then $f(a_1) \neq f(a_2)$. Since $f(a_1)$ and $f(a_2)$ are distinct elements of $B$, we have $g(f(a_1)) \neq g(f(a_1))$. The inductive step is proven the same way as before.

   Like previously, we construct an injective function $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ where $n = |X| = |Y|$. $\{\pi(1), \ldots, \pi(n)\}$ should have $n$ elements due to injectivity and it also has be a subset of $\{1, \ldots, n\}$, whose amount of elements is also $n$. The only subset of a finite set with the same amount of elements is the set itself, so the image and codomain are equal, hence surjectivity.

   Note: The following exercise demonstrates how this exercise fails for infinite sets.

## Exercise 1.3.3

1. Can you find an injective function from $\mathbb{N}$ to $\mathbb{N}$? Can you find another one?

   Besides the identity function there is $f : \mathbb{N} \to \mathbb{N}$ given by $f : n \mapsto n - (-1)^n$.

2. Can you find a bijective function from $\mathbb{N}$ to $\mathbb{Z}$?

   Consider $g : \mathbb{N} \to \mathbb{Z}$ given by $g : n \mapsto (-1)^n \left\lfloor \frac{n}{2} \right\rfloor$. Let $(-1)^{n_1} \left\lfloor \frac{n_1}{2} \right\rfloor = (-1)^{n_2} \left\lfloor \frac{n_2}{2} \right\rfloor$ for some $n_1, n_2 \in \mathbb{N}$. Since the signs should be the same, we have that $n_1$ and $n_2$ with same parities. If both are even, i.e., there exist $k_1, k_2 \in \mathbb{N}$ with $n_1 = 2k_1$ and $n_2 = 2k_2$, then we have the following:

$$(-1)^{2k_1} \left\lfloor \frac{2k_1}{2} \right\rfloor = (-1)^{2k_2} \left\lfloor \frac{2k_2}{2} \right\rfloor$$

$$\lfloor k_1 \rfloor = \lfloor k_2 \rfloor$$

$$k_1 = k_2$$

This implies $n_1 = n_2$.

If, however, $n_1$ and $n_2$ are both odd, i.e., there exist $l_1, l_2 \in \mathbb{N}$ with $n_1 = 2l_1 - 1$ and $n_2 = 2l_2 - 1$, then we have:

$$(-1)^{2l_1-1} \left\lfloor \frac{2l_1 - 1}{2} \right\rfloor = (-1)^{2l_2-1} \left\lfloor \frac{2l_2 - 1}{2} \right\rfloor$$

$$(-1) \left\lfloor l_1 - \frac{1}{2} \right\rfloor = (-1) \left\lfloor l_2 - \frac{1}{2} \right\rfloor$$

$$\left\lfloor l_1 - \frac{1}{2} \right\rfloor = \left\lfloor l_2 - \frac{1}{2} \right\rfloor$$

$$l_1 - 1 = l_2 - 1$$

$$l_1 = l_2$$

This implies and finishes the proof of injectivity.

For surjectivity, take an arbitrary $y \in \mathbb{Z}$. If $y = 0$, then we have $g(0) = 0$. If $y > 0$, then $g(2y) = y$. And if $y < 0$, then $g(1 - 2y) = y$.

Hence $g$ is bijective.

3. This might be tricky: Can you find a surjective function from $\mathbb{Z}$ to $\mathbb{Q}$?

Let $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ be defined by the picture below.

$$\begin{tikzcd}
(-2,3) \arrow[r] & (-1,3) \arrow[r] & (0,3) \arrow[r] & (1,3) \arrow[r] & (2,3) \arrow[d] & \\
(-2,2) \arrow[u] & (-1,2) \arrow[d] & (0,2) \arrow[l] & (1,2) \arrow[l] & (2,2) \arrow[d] & \\
(-2,1) \arrow[u] & (-1,1) \arrow[l] & (0,1) \arrow[r] & (1,1) \arrow[u] & (2,1) \arrow[r] & ... \\
(-2.0) & (-1,0) & (0,0) & (1,0) & (2,0) & \\
(-2,-1) \arrow[r] & (-1,-1) \arrow[d] & (0,-1) \arrow[uu] & (1,-1) \arrow[l] & (2,-1) \arrow[d] & ... \arrow[l] \\
(-2,-2) \arrow[u] & (-1,-2) \arrow[r] & (0,-2) \arrow[r] & (1,-2) \arrow[u] & (2,-2) \arrow[d] & \\
(-2,-3) \arrow[u] & (-1,-3) \arrow[l] & (0,-3) \arrow[l] & (1,-3) \arrow[l] & (2,-3) \arrow[l] &
\end{tikzcd}$$

Pick any vertex with a nonzero second entry to be $f(0)$, let the arrow coming out of $f(n)$ indicate where $f(n+1)$ is and the arrow coming to $f(n)$ indicate where the $f(n-1)$ is. Clearly, $f$ takes on any pair of integers with the second integer being nonzero. Now, define $g$ : $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ with $g : (p, q) \mapsto \frac{p}{q}$. Clearly, $g$ is also surjective. A composition of surjective functions is also a surjective function (See Part 3 of Exercise 1.3.2 of this section.), so $g \circ f$ is a surjective function from $\mathbb{Z}$ to $\mathbb{Q}$.

4. This is actually hard: Can you find a bijective function from $\mathbb{R}$ to $\mathbb{R} \times \mathbb{R}$?

Let $h : (0, 1] \to (0, 1] \times (0, 1]$ given by $h : 0.x_1x_2x_3 \cdots \mapsto (0.x_1x_3x_5 \ldots, 0.x_2x_4x_6 \ldots)$. $f(\lfloor x \rfloor) + g(1 - x + \lfloor x \rfloor)$ is a bijection from $\mathbb{R}$ to $\mathbb{R} \times \mathbb{R}$. (For $f$, see the previous part, but redefine it so that it's surjective to the entire $\mathbb{Z} \times \mathbb{Z}$.)

## Exercise 1.3.4

1. How many functions are there from $\{1, 2\}$ to $\{3, 4, 5\}$?

   Since there are 3 possibilities for both $f(1)$ and $f(2)$, by combinatorics, the amount of functions should be 9.

2. Explain how all possible functions from the set $\{6\}$ to the set $D$ from Exercise 1.1.2 look like? What about to the set of all natural numbers? To the set of all real numbers?

   There are six functions from $\{6\}$ to $D$, each defined by $f(6) = a$ with $a \in D$. Same thing for the other functions but with $a \in \mathbb{N}$ and $a \in \mathbb{R}$.

3. Define a function $f : \mathbb{Z} \to \mathbb{Z}$ by $f(n) = n^2$. Is $f$ surjective? Injective? Why or why not?

   Is it not injective as $f(-1) = f(1)$ meanwhile $-1 \neq 1$ and it is neither surjective as $-1 \notin \operatorname{im} f$ whereas $-1 \in \mathbb{Z}$.

4. Find the pre-image of the set $\{k \in \mathbb{Z} : k \text{ is even}\}$ under $f$ from Exercise 1.3.4(3).

   It is $\{k \in \mathbb{Z} : k \text{ is even}\}$ itself.

## 1.2 Schaum's Outline of Abstract Algebra, Chapter 1

### Exercise 1.21

Exhibit the each of the following in tabular form:

1. The set of negative integers greater than $-6$. $\{-5, -4, -3, -2, -1\}$
2. The set of integers between $-3$ and 4. $\{-2, -1, 0, 1, 2, 3\}$
3. The set of integers whose squares are less than 20. $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
4. The set of all positive factors of 18. $\{1, 2, 3, 6, 9, 18\}$
5. The set of all common factors of 16 and 24. $\{-8, -4, -2, -1, 1, 2, 4, 8\}$
6. $\{p : p \in \mathbb{N}, p^2 < 10\} = \{1, 2, 3\}$
7. $\{b : b \in \mathbb{N}, 3 \leqslant b \leqslant 8\} = \{3, 4, 5, 6, 7, 8\}$
8. $\{x : x \in \mathbb{Z}, 3x^2 + 7x + 2 = 0\} = \{-2\}$
9. $\{x : x \in \mathbb{Q}, 2x^2 + 5x + 3 = 0\} = \left\{-\frac{3}{2}, -1\right\}$

### Exercise 1.22

Verify: (a) $\{x : x \in \mathbb{N}, x < 1\} = \varnothing$, (b) $\{x : x \in \mathbb{Z}, 6x^2 + 5x - 4 = 0\} = \varnothing$

A quick proof by induction shows that for all natural $x$ we have $x \geqslant 1$, meaning there is no natural number smaller than 1, hence the equality in (a).

A quick application of quadratic formula shows that $6x^2 + 5x - 4 = 0 \implies x = \frac{4}{3}$ or $x = -\frac{1}{2}$, but considering the sizes of cubic and quartic formulas and also the fact that there is no general formula for equations of degree $\geqslant 5$, this method becomes obsolete for equations of higher degrees. Using the rational root theorem is an alternate method. Here it tells us that if $6x^2+5x-4=0$ has a rational root $x$, then it must be one of $\pm1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{6}, \pm2, \pm\frac{2}{3}, \pm4, \pm\frac{4}{3}$, the only integers out of which are $\pm1, \pm2, \pm4$. As shown below, none of them is a root of $6x^2+5x-4=0$.

$$\begin{aligned}
6(1)^2+5(1)-4 &= 7 \neq 0\\
6(-1)^2+5(-1)-4 &= -3 \neq 0\\
6(2)^2+5(2)-4 &= 30 \neq 0\\
6(-2)^2+5(-2)-4 &= 10 \neq 0\\
6(4)^2+5(4)-4 &= 112 \neq 0\\
6(-4)^2+5(-4)-4 &= 72 \neq 0
\end{aligned}$$

Either way, the set presented in (b) is indeed empty.

## Exercise 1.23

Exhibit the 15 proper subsets of $\{a,b,c,d\}$.

$$\mathcal{P}(\{a,b,c,d\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a,b\}, \{a,c\}, \{a,d\}, \{b,c\}, \{b,d\}, \{c,d\},$$
$$\{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}\}.$$

## Exercise 1.24

Show that the number of proper subsets of $S=\{a_1,a_2,\ldots,a_n\}$ is $2^n-1$.

For a set of cardinality $n$ there are $2^n$ subsets with only one of them not being a proper subset (The original set itself). Hence there are $2^n-1$ proper subsets.

## Exercise 1.25

Using the sets in Problem 1.2, verify: (a) $(A\cup B)\cup C = A\cup(B\cup C)$, (b) $(A\cap B)\cap C = A\cap(B\cap C)$, (c) $(A\cup B)\cap C \neq A\cup(B\cap C)$. [For reference to the reader: $A=\{a,b,c,d\}, B=\{a,c,g\}, C=\{c,g,m,n,p\}$.]

$$(A \cup B) \cup C = \{a, b, c, d, g\} \cup \{c, g, m, n, p\} = \{a, b, c, d, g, m, n, p\}$$
$$A \cup (B \cup C) = \{a, b, c, d\} \cup \{a, c, g, m, n, p\} = \{a, b, c, d, g, m, n, p\}$$

$$(A \cap B) \cap C = \{a, c\} \cap \{c, g, m, n, p\} = \{c\}$$
$$A \cap (B \cap C) = \{a, b, c, d\} \cap \{c, g\} = \{c\}$$

$$(A \cup B) \cap C = \{a, b, c, d, g\} \cap \{c, g, m, n, p\} = \{c, g\}$$
$$A \cup (B \cap C) = \{a, b, c, d\} \cap \{c, g\} = \{c\}$$

Transitivity of = shows that the equalities in (a) and (b) are ubdeed true. However, $\{c, g\}$ and $\{c\}$ are not equal since the former contains $g$ whereas the latter does not.

## Exercise 1.26

Using the sets in Problem 1.3, verify: (a) $(K')' = K$, (b) $(K \cap L)' = K' \cup L'$, (c) $(K \cup L \cup M)' = K' \cap L' \cap M'$, (d) $K \cap (L \cup M) = (K \cap L) \cup (K \cap M)$ [For reference to the reader: $K = \{2, 4, 6, 8\}, L = \{1, 2, 3, 4\}, M = \{3, 4, 5, 6, 7, 8\}$ and $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is the universal set.]

$$(K')' = \{1, 3, 5, 7, 9, 10\}' = \{2, 4, 6, 8\} = K.$$
$$(K \cap L)' = \{2, 4\}' = \{1, 3, 5, 6, 7, 8, 9, 10\} =$$
$$= \{1, 3, 5, 7, 9, 10\} \cup \{5, 6, 7, 8, 9, 10\} = K' \cup L'.$$
$$(K \cup L \cup M)' = \{1, 2, 3, 4, 5, 6, 7, 8\}' = \{9, 10\} =$$
$$= \{1, 3, 5, 7, 9, 10\} \cap \{5, 6, 7, 8, 9, 10\} \cap \{1, 2, 9, 10\} = K' \cap L' \cap M'.$$

## Exercise 1.27

Let "$n|m$" mean "$n$ is a factor of $m$". Given $A = \{x : x \in \mathbb{N}, 3|x\}$ and $B = \{x : x \in \mathbb{N}, 5|x\}$, list 4 elements of each of the sets $A', B', A \cup B, A \cap B, A \cup B', A \cap B', A' \cup B'$ where $A'$ and $B'$ are the respective complements of $A$ and $B$ in $\mathbb{N}$.

$$\begin{aligned}
A' &= \{1, 2, 4, 5, 7, 8, \dots\} \\
B' &= \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, \dots\} \\
A \cup B &= \{3, 5, 6, 9, \dots\} \\
A \cap B &= \{15, 30, 45, 60, \dots\} \\
A \cup B' &= \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 15, \dots\} \\
A \cap B' &= \{3, 6, 9, 12, 18, 21, 24, 27, 33, 36, 39, 41, \dots\} \\
A' \cup B' &= \{1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 16 \dots\}
\end{aligned}$$

## Exercise 1.28

Prove the laws of (1.8)-(1.12'), which were not treated in Problems 1.8-1.13.

Not sure about what is meant by the author here, the proofs of those laws are already given.

## Exercise 1.29

Let $A$ and $B$ be subsets of a universal set $U$. Prove:

1. $A \cup B = A \cap B$ if and only if $A = B$,

   Assume $A \cup B = A \cap B$ and let $x \in A$. Then $x \in A \cup B$ by definition of union and $x \in A \cap B$ according to the assumption. The latter implies that $x \in B$, so we have $A \subset B$. Similarly $B \subset A$ can be achieved. Hence $A = B$.

For the other direction, start by assuming that $A = B$. then we have the following:

$$A \cup B = A \cup A = A = A \cap A = A \cap B$$

2. $A \cap B = A$ if and only if $A \subset B$.

Assume $A \cap B = A$ and let $x \in A$. According to the assumption, $x \in A \cap B$, which implies $x \in B$. So, $A \subset B$.

For the other direction, start by assuming $A \subset B$, i.e., $x \in B$ for $x \in A$. As shown below, $A \subset A \cap B$:

$$x \in A \iff x \in A \text{ and } x \in A \implies x \in A \text{ and } x \in B \iff x \in A \cap B$$

We also have $A \cap B \subset A$:

$$x \in A \cap B \iff x \in A \text{ and } x \in B \implies x \in A$$

Hence $A \cap B = B$.

3. $(A \cap B') \cup (A' \cap B) = A \cup B$ if and only if $A \cap B = \varnothing$.

Assume $(A \cap B') \cup (A' \cap B) = A \cup B$ and that there exists $x \in A \cap B$. Then $x \in (A \cap B') \cup (A' \cap B)$ according to the assumption, meaning we have two cases: $x \in A \cap B'$ or $x \in A' \cap B$. (both can't happen since $(A \cap B') \cap (A' \cap B) = \varnothing$.) On the one hand, since $x \in A$, we should have $x \in A \cap B'$ rather than $x \in A' \cap B$, meaning $x \notin B$, contradicting the definition of $x$. Hence no such $x$ exists, i.e., $A \cap B$ is empty.

For the other direction, start by assuming $A \cap B = \varnothing$. Then we have the following:

$$(A \cap B') \cup (A' \cap B) = (A - B) \cup (B - A) = (A \cup B) - (A \cap B) =$$

$$= (A \cup B) - \varnothing = A \cup B$$

(The proof of the second equality is given in 1.16)

## Exercise 1.30

Given $n(U) = 692$, $n(A) = 300$, $n(B) = 230$, $n(C) = 370$, $n(A \cap B) = 150$, $n(A \cap C) = 180$, $n(B \cap C) = 90$, $n(A \cap B' \cap C') = 10$ where $n(S)$ is the number of elements in the set $S$, find:

1. $n(A \cap B \cap C)$

   We have the equations $n(A) = n(A \cap B) + n(A \cap B') = n(A \cap B) + n(A \cap B' \cap C) + n(A \cap B' \cap C')$ and $n(A \cap C) = n(A \cap B \cap C) + n(A \cap B' \cap C)$, which, combined, yield

   $$n(A \cap B \cap C) = n(A \cap C) + n(A \cap B) + n(A \cap B' \cap C')) - n(A) =$$

   $$= 180 + 150 + 10 - 300 = 40$$

2. $n(A' \cap B \cap C')$

   We have equations $n(B \cap C) = n(A \cap B \cap C) + n(A' \cap B \cap C)$ and $n(B) = n(A \cap B) + n(A' \cap B) = n(A \cap B) + n(A' \cap B \cap C) + n(A' \cap B \cap C')$, which, combined, yield

   $$n(A' \cap B \cap C') = n(B) + n(A \cap B \cap C) - n(A \cap B) - n(B \cap C) =$$

   $$= 230 + 40 - 150 - 90 = 30$$

3. $n(A' \cap B' \cap C')$

   De morgan's laws and the inclusion-exclusion principle suggests that

   $$n(A' \cap B' \cap C') = n((A \cup B \cup C)') =$$

   $$= n(U) - n(A) - n(B) - n(C) + n(A \cap B) + n(A \cap C) + n(B \cap C) - n(A \cup B \cup C) =$$

   $$= 692 - 300 - 230 - 370 + 150 + 180 + 90 - 40 = 172$$

4. $n((A \cap B) \cup (A \cap C) \cup (B \cap C))$

Again, via the inclusion-exclusion principle, we obtain

$$n((A \cap B) \cup (A \cap C) \cup (B \cap C))$$

$$= n(A \cap B) + n(A \cap C) + n(B \cap C) - n((A \cap B) \cap (A \cap C)) - n((A \cap B) \cap (B \cap C)) -$$

$$- n((A \cap C) \cap (B \cap C)) + n((A \cap B) \cap (A \cap C) \cap (B \cap C))$$

$$= n(A \cap B) + n(A \cap C) + n(B \cap C) - 2n(A \cap B \cap C)$$

$$= 150 + 180 + 90 - 2 \cdot 40 = 340$$

## Exercise 1.31

Given the mappings $\alpha : n \mapsto n^2 + 1$ and $\beta : n \mapsto 3n + 2$ of $\mathbb{N}$ into $\mathbb{N}$, find $\alpha\beta$ and $\beta\alpha$.

$\alpha\beta, \beta\alpha : \mathbb{N} \to \mathbb{N}$ are given by $\beta\alpha : n \mapsto 3n^2 + 5$ and $\alpha\beta : n \mapsto 9n^2 + 12n + 5$.

## Exercise 1.32

Which of the following mappings of $\mathbb{Z}$ into $\mathbb{Z}$:

1. $x \mapsto x + 2$
2. $x \mapsto 3x$
3. $x \mapsto x^2$
4. $x \mapsto 4 - x$
5. $x \mapsto x^3$
6. $x \mapsto x^2 - x$

are (i) mappings of $\mathbb{Z}$ onto $\mathbb{Z}$, (ii) one-to-one mappings of $\mathbb{Z}$ onto $\mathbb{Z}$?

The first and fourth functions are surjective since for every $a \in \mathbb{Z}$ there exists $x \in \mathbb{Z}$ such that $x + 2 = a$ (namely, $x = a - 2$) and $y \in \mathbb{Z}$ such that $4 - y = a$ (namely, $y = 4 - a$). They are also injective (and therefore bijective) as shown below:

$$x_1 + 2 = x_2 + 2 \iff x_1 = x_2$$

$$4 - x_1 = 4 - x_2 \iff -x_1 = -x_2 \iff x_1 = x_2$$

The other functions are not surjective since $-2$ is not in the images.

## Exercise 1.33

Same as Problem 32 with $\mathbb{Z}$ replaced by $\mathbb{Q}$.

The first and fourth functions remain bijective for the same reasons. The second function obtains surjectivity since for every $q \in \mathbb{Q}$ there exists $x$ with $3x = q$ (namely, $x = \frac{q}{3}$). It it also injective as $3a = 3b \iff a = b$.

The other functions still don't contain $-2$ in their images.

## Exercise 1.34

Same as Problem 32 with $\mathbb{Z}$ replaced by $\mathbb{R}$.

The first, second and fourth functions remain bijective. The fifth function obtains surjectivity since for every $y \in \mathbb{R}$ we have $\sqrt[3]{y}^3 = y$. It is also injective as $a^3 = b^3 \iff a = b$.

The other functions still don't contain $-2$ in their images.

## Exercise 1.35

1. If $E$ is the set of all even positive integers, show that $x \mapsto x+1$, $x \in E$ is not a mapping onto the set $F$ of all odd positive integers.

   It is not onto since there is no $x \in E$ s.t. $x+1=1$.

2. If $E$ is a set consisting of zero and all even positive integers (i.e., the non-negative integers), show that $x \mapsto x+1$, $x \in E$ is a mapping of $E$ onto $F$.

   The function $g : E \to F$ given by $g : x \mapsto x+1$ is surjective since for every $y \in F$ we have $f(y-1) = y$. This presence of $y-1$ in $E$ is guaranteed by the fact that it is even and $y \geqslant 1$, meaning $y-1 \geqslant 0$.

## Exercise 1.36

Given the one-to-one mappings

$$\begin{array}{rllll}
\mathcal{J}: & \mathcal{J}(1)=1, & \mathcal{J}(2)=2, & \mathcal{J}(3)=3, & \mathcal{J}(4)=4 \\
\alpha: & \alpha(1)=2, & \alpha(2)=3, & \alpha(3)=4, & \alpha(4)=1 \\
\beta: & \beta(1)=4, & \beta(2)=1, & \beta(3)=2, & \beta(4)=3 \\
\gamma: & \gamma(1)=3, & \gamma(2)=4, & \gamma(3)=1, & \gamma(4)=2 \\
\delta: & \delta(1)=1, & \delta(2)=4, & \delta(3)=3, & \delta(4)=2
\end{array}$$

of $S = \{1,2,3,4\}$ onto itself, verify: (a) $\alpha\beta = \beta\alpha = \mathcal{J}$, hence, $\beta = \alpha^{-1}$, (b) $\alpha\gamma = \gamma\alpha = \beta$, (c) $\alpha\delta \neq \delta\alpha$, (d) $\alpha^2 = \gamma$, (e) $\gamma^2 = \mathcal{J}$, (f) $\alpha^4 = \mathcal{J}$, hence, $\alpha^3 = \alpha^{-1}$.

For part a,

$$\begin{array}{ll}
\alpha(\beta(1)) = \alpha(4) = 1 & \alpha(\beta(2)) = \alpha(1) = 2 \\
\beta(\alpha(1)) = \beta(2) = 1 & \beta(\alpha(2)) = \beta(3) = 2 \\
\mathcal{J}(1) = 1 & \mathcal{J}(2) = 2
\end{array}$$

$$\begin{array}{ll}
\alpha(\beta(3)) = \alpha(2) = 3 & \alpha(\beta(4)) = \alpha(3) = 4 \\
\beta(\alpha(3)) = \beta(4) = 3 & \beta(\alpha(4)) = \beta(1) = 4 \\
\mathcal{J}(3) = 3 & \mathcal{J}(4) = 4
\end{array}$$

For part b,

$$\begin{array}{ll}
\alpha(\gamma(1)) = \alpha(3) = 4 & \alpha(\gamma(2)) = \alpha(4) = 1 \\
\gamma(\alpha(1)) = \gamma(2) = 4 & \gamma(\alpha(2)) = \gamma(3) = 1 \\
\beta(1) = 4 & \beta(2) = 1
\end{array}$$

$$\begin{array}{ll}
\alpha(\gamma(3)) = \alpha(1) = 2 & \alpha(\gamma(4)) = \alpha(2) = 3 \\
\gamma(\alpha(3)) = \gamma(4) = 2 & \gamma(\alpha(4)) = \gamma(1) = 3 \\
\beta(3) = 2 & \beta(4) = 3
\end{array}$$

For part c, $\alpha(\delta(1)) = \alpha(1) = 2 \neq 4 = \delta(2) = \delta(\alpha(1))$

For part d,

$$\alpha(\alpha(1)) = \alpha(2) = 3 = \gamma(1)$$
$$\alpha(\alpha(2)) = \alpha(3) = 4 = \gamma(2)$$
$$\alpha(\alpha(3)) = \alpha(4) = 1 = \gamma(3)$$
$$\alpha(\alpha(4)) = \alpha(1) = 2 = \gamma(4)$$

For part c,

$$\gamma(\gamma(1)) = \gamma(3) = 1 = \mathcal{J}(1)$$
$$\gamma(\gamma(2)) = \gamma(4) = 2 = \mathcal{J}(2)$$
$$\gamma(\gamma(3)) = \gamma(1) = 3 = \mathcal{J}(3)$$
$$\gamma(\gamma(4)) = \gamma(2) = 4 = \mathcal{J}(4)$$

For part d, we can use the facts that parts a and b suggest that $\alpha^2\gamma = \mathcal{J}$ whereas part d tells us that $\gamma = \alpha^2$, hence we have $\alpha^2\gamma = \alpha^2\alpha^2 = \alpha^4 = \mathcal{J}$.

For part e, using our previous results, we have $\alpha^4 = 1$, so $\alpha^2 = (\alpha^2)^{-1}$ and $(\alpha^{-1})^2 = (\alpha^3)^2 = \alpha^6 = \alpha^2\alpha^4 = \alpha^2$. By transitivity of $=$, we have $(\alpha^{-1})^2 = (\alpha^2)^{-1}$

Later we will call such functions “permutations” of $\{1, 2, 3, 4\}$.

## 1.3 Schaum’s Outline of Abstract Algebra, Section 3.4

### Exercise 3.13

Prove by induction that $1 \cdot n = n$ for every $n \in \mathbb{N}$.

For the base case we have $1 \cdot 1 = 1$ according to the definition of multiplication. For the inductive step, assume $1 \cdot n = n$ for some $n \in \mathbb{N}$. Then we have $1 \cdot n^* = 1 \cdot n + 1 = n + 1$. Finishing the proof by induction.

### Exercise 3.14

Prove $\mathbf{M_1}$, $\mathbf{M_2}$, and $\mathbf{M_3}$ by induction. Hint: Use the result of Problem 3.13 and $\mathbf{D_2}$ in proving $\mathbf{M_2}$.

For $\mathbf{M_1}$, the base case yields $n \cdot 1 \in \mathbb{N}$ for $n \in \mathbb{N}$, which is indeed true as $n \cdot 1 = n$. (We are inducting on $m$.) For the inductive step, assume $n \cdot m \in \mathbb{N}$ for some $n, m \in \mathbb{N}$. Then $n \cdot m* = n \cdot m + n$, which is natural according to closure of addition. Hence the hypothesis holds for $m^*$ as well, ending the proof.

For $\mathbf{M_2}$, the base case (by inducting on $m$ again) yields $1 \cdot n = n \cdot 1$, which is indeed true according to our previous result. For the inductive step, assume $m \cdot n = n \cdot m$ for some $m, n \in \mathbb{N}$. Then $n \cdot m^* = n \cdot m + n = m \cdot n + 1 \cdot n = (m + 1) \cdot n = m^* \cdot n$. Hence the hypothesis holds for $m^*$ as well, ending the proof.

For $\mathbf{M_3}$, we shall induct on $n$ this time. The base case yields $m \cdot (1 \cdot p) = (m \cdot 1) \cdot p$, which is indeed true. (both sides equal $m \cdot p$.) For inductive step, assume $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ for some $m, n, p \in \mathbb{N}$. Then we have $(m \cdot n^*) \cdot p = (m \cdot n + m) \cdot p = (m \cdot n) \cdot p + m \cdot p = m \cdot (n \cdot p) + m \cdot p = m \cdot (n \cdot p + p) = m \cdot (n^* \cdot p)$. Hence the hypothesis holds for $m^*$ as well, ending the proof.

## Exercise 3.15

Prove: (a) $\mathbf{D_1}$ by following Problem 3.5, (b) $\mathbf{D_1}$ by using $\mathbf{M_2}$.

For part a, we shall induct on $p$. The base case yields $m \cdot (n+1) = m \cdot n^* = m \cdot n + m = m \cdot n + m \cdot 1$. For the inductive step, let $m \cdot (n+p) = m \cdot n + m \cdot p$ be true for some natural $m, n, p$. Then we have $m \cdot (n + p^*) = m \cdot (n+p)^* = m \cdot (n+p) + m = m \cdot n + m \cdot p + m = m \cdot n + m \cdot p^*$. Hence the hypothesis holds for $p^*$ as well, ending the proof.

For part b, it is unclear what the author meant unless we are also allowed to use $D_1$, in which case the result is immediate. Otherwise $\mathcal{M}_\in$ is irrelevant.

## Exercise 3.16

Prove the following:

1. $(m + n^*)^* = m^* + n^*$

$$(m + n^*)^* = (n^* + m)^* = n^* + m^* = m^* + n^*$$

2. $(m \cdot n^*)^* = m \cdot n + m^*$

$$(m \cdot n^*)^* = (m \cdot n + m)^* = m \cdot n + m^*$$

3. $(m^* \cdot n^*)^* = m^* + m \cdot n + n^*$

$$(m^* \cdot n^*)^* = (m^* \cdot n + m^*)^* = (n \cdot m^* + m^*)^* =$$
$$= (n \cdot m + n + m^*)^* = (m^* + m \cdot n + n)^* = m^* + m \cdot n + n^*$$

## Exercise 3.17

Prove the following:

1. $(m+n)\cdot(p+q)=(m\cdot p+m\cdot q)+(n\cdot p+n\cdot q)$

$$(m+n)\cdot(p+q)=m\cdot(p+q)+n\cdot(p+q)=(m\cdot p+m\cdot q)+(n\cdot p+n\cdot q)$$

2. $m\cdot(n+p)\cdot q=(m\cdot n)\cdot q+m\cdot(p\cdot q)$

$$m\cdot(n+p)\cdot q=m\cdot q\cdot(n+p)=(m\cdot q)\cdot(n+p)=(m\cdot q)\cdot n+(m\cdot q)\cdot p=$$
$$=m\cdot(q\cdot n)+m\cdot(q\cdot p)=m\cdot(n\cdot q)+m\cdot(p\cdot q)=(m\cdot n)\cdot q+m\cdot(p\cdot q)$$

3. $m^*+n^*=(m+n)^*+1$

$$(m+n)^*+1=(m+n^*)+1=(m+n^*)^*=m^*+n^* \text{ (See part 1.)}$$

## Exercise 3.18

Let $m,n,p,q\in\mathbb{N}$ and define $m\cdot n\cdot p\cdot q=(m\cdot n\cdot p)\cdot q$. (a) Show that in $m\cdot n\cdot p\cdot q$ we may insert parenthesis at will. (b) Prove that $m\cdot(n+p+q)=m\cdot n+m\cdot p+m\cdot q$.

For part a, we have

$$(m\cdot n\cdot p)\cdot q=m\cdot n\cdot p\cdot q$$
$$m\cdot(n\cdot p\cdot q)=m\cdot((n\cdot p)\cdot q)=(m\cdot(n\cdot p))\cdot q=((m\cdot n)\cdot p)\cdot q=(m\cdot n\cdot p)\cdot q=m\cdot n\cdot p\cdot q$$
$$(m\cdot n)\cdot p\cdot q=((m\cdot n)\cdot p)\cdot q=(m\cdot n\cdot p)\cdot q=m\cdot n\cdot p\cdot q$$
$$m\cdot(n\cdot p)\cdot q=(m\cdot(n\cdot p))\cdot q=((m\cdot n)\cdot p)\cdot q=(m\cdot n\cdot p)\cdot q=m\cdot n\cdot p\cdot q$$
$$m\cdot n\cdot(p\cdot q)=(m\cdot n)\cdot(p\cdot q)=((m\cdot n)\cdot p)\cdot q=(m\cdot n\cdot p)\cdot q$$

For part b, $m\cdot(n+p+q)=m\cdot((n+p)+q)=m\cdot(n+p)+m\cdot q=(m\cdot n+m\cdot p)+m\cdot q=m\cdot n+m\cdot p+m\cdot q$.

## Exercise 3.19

Identify the set $S = \{x : x \in \mathbb{N}, n < x < n^* \text{ for some } n \in \mathbb{N}\}$.

Assume there are $x, n \in \mathbb{N}$ such that $n < x < n^*$. Since $n < x$, there should exist $a \in \mathbb{N}$ with $x + a = n$. Similarly, there exists $b \in \mathbb{N}$ with $n^* + b = x$. And so we have $n^* + b + a = x + a = n$ and $n + 1 + b + a = n$, meaning $n > n$, implying $n \neq n$, which is a contradiction. Hence no such $x, n \in \mathbb{N}$ exist, i.e., $S$ is empty.

## Exercise 3.20

If $m, n, p, q \in \mathbb{N}$ and if $m < n$ and $p < q$, prove: (a) $m + p < n + q$, (b) $m \cdot p < n \cdot q$.

For part a, since $m < n$ and $p < q$, there should exist $a_1, a_2 \in \mathbb{N}$ s.t. $m + a_1 = n$ and $p + a_2 = q$. We then have $m + a_1 + p + a_2 = n + q$, meaning $m + p < n + q$.

For part b, we also have $(m + a_1) \cdot (p + a_2) = n \cdot q$. Expand the left hand side (See part 1 of Exercise 3.17) and we get $m \cdot p + m \cdot a_2 + a_1 \cdot p + a_1 \cdot a_2 = n \cdot q$, meaning $m \cdot p < n \cdot q$.

## Exercise 3.21

Let $m, n \in \mathbb{N}$. Prove: (a) If $m = n$, then $k^* \cdot m > n$ for every $k \in \mathbb{N}$. (b) If $k^* \cdot m = n$ for some $k \in \mathbb{N}$, then $m < n$.

For part a, we have $m \cdot k + m = m \cdot k + n$, meaning $m \cdot k + m > n$ and $m \cdot k^* > n$.

For part b, rewrite the equation as $m \cdot k^* = n$ and $m \cdot k + m = n$, this implies $m < n$ by definition.

## Exercise 3.22

Prove $\mathbf{A_4}$ and $\mathbf{M_4}$ using the Trichotomy Law and Theorems II and II'.

Theorems II and II' show that if $m > n$ or $m < n$ (i.e., $m \neq n$), then $m + p > n + p$ or $m + p < n + p$ respectively. By contrapositive, this means for $m + p = n + p$, we have $m = n$. Same reasoning for multiplication.

## Exercise 3.23

For all $m \in \mathbb{N}$ define $m^1 = m$ and $m^{p+1} = m^p \cdot m$ provided $m^p$ is defined. When $m, n, p, q \in \mathbb{N}$, prove: (a) $m^p \cdot m^q = m^{p+q}$, (b) $(m^p)^q = m^{p \cdot q}$, (c) $(m \cdot n)^p = m^p \cdot n^p$, (d) $(1)^p = 1$.

For part a, we shall induct on $q$. The base case indeed holds as $m^p \cdot m^1 = m^{p+1}$. (Both sides equal $m^p \cdot m$.) For inductive step, assume $m^p \cdot m^q = m^{p+q}$ is true for some $q \in \mathbb{N}$. Then $m^p \cdot m^{q+1} = m^p \cdot m^q \cdot m = m^{p+q} \cdot m = m^{p+q+1}$. Thus it holds for $(q + 1)$ as well, ending the proof.

For part b, we shall induct on $q$. The base case indeed holds as $(m^p)^1 = m^{p \cdot 1}$. (Both sides equal $m^p$.) For the inductive step, assume $(m^p)^q = m^{p \cdot q}$ is true for some $q \in \mathbb{N}$. Then $(m^p)^{q+1} = (m^p)^q \cdot m^p = m^{p \cdot q} \cdot m^p = m^{p \cdot q + p} = m^{q \cdot (p+1)}$. (See part a for the second from last equality.) Thus it holds for $(q + 1)$ as well, ending the proof.

For part c, we shall induct on $p$. The base case indeed holds as $(m \cdot n)^1 = m^1 \cdot n^1$. (Both sides equal $m \cdot n$.) For the inductive step, assume $(m \cdot n)^p = m^p \cdot n^p$ for some $p \in \mathbb{N}$. Then $(m \cdot n)^{p+1} = (m \cdot n)^p \cdot m \cdot n = m^p \cdot n^p \cdot m \cdot n = m^p \cdot m \cdot n^p \cdot n = m^{p+1} \cdot n^{p+1}$. Thus it holds for $(p + 1)$ as well, ending the proof.

For part d, the base case holds as $(1)^1 = 1$. Now assume $(1)^p = 1$ to be true for $p \in \mathbb{N}$. Then $(1)^{p+1} = (1)^p \cdot 1 = 1 \cdot 1 = 1$. Ending the proof.

## Exercise 3.24

For $m, n \in \mathbb{N}$ show that (a) $m^2 < m \cdot n < n^2$ if $m < n$, (b) $m^2 + n^2 > 2 \cdot m \cdot n$ if $m \neq n$.

For part a, simply multiply each side of the inequality $m < n$ by $m$ first and then by $n$, that yields $m \cdot m < n \cdot m$ and $n \cdot m < n \cdot n$, i.e., $m^2 < m \cdot n$ and $m \cdot n < n^2$. We shortly wrote those together as $m^2 < m \cdot n < n^2$.

For part b, we have two cases, $m > n$ or $m < n$. Thanks to the symmetry, we can be done by considering just one of these cases. Let $m < n$, meaning there exists $p \in \mathbb{N}$ with $m + p = n$. Consider the following:

$$2m^2 + p^2 > 2m^2$$
$$m^2 + m^2 + 2mp + p^2 > 2m^2 + 2mp$$
$$m^2 + (m+p)^2 > 2m(m+p)$$
$$m^2 + n^2 > 2mn$$

## Exercise 3.25

Prove, by induction, for all $n \in \mathbb{N}$:

1. $1 + 2 + 3 + \cdots + n = (1/2)n(n+1)$

The author has not yet defined (1/2), we assume that they meant to write $2\sum_{i=1}^{n} i = n(n+1)$.

For base case, $n = 1$, so $2\sum_{i=1}^{n} i = 2\sum_{i=1}^{1} i = 2 \cdot 1 = 1 \cdot 2 = 1 \cdot (1+1) = n \cdot (n+1)$.

For inductive step, assume that the statement is true for some $n$. We then have

$$2\sum_{i=1}^{n+1} i = 2\left(\sum_{i=1}^{n} i + (n+1)\right) = 2\sum_{i=1}^{n} i + 2(n+1) =$$
$$= n(n+1) + 2(n+1) = (n+1)(n+2) = (n+1)((n+1)+1)$$

2. $1^2 + 2^2 + 3^2 + \cdots + n^2 = (1/6)n(n+1)(2n+1)$

The author has not yet defined (1/6), we assume that they meant to write $6\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)$.

For base case, $n = 1$, so $6\sum_{i=1}^{n} i^2 = 6\sum_{i=1}^{1} i^2 = 6 \cdot 1^2 = 6 \cdot 1 = 1 \cdot 6 = 1 \cdot 2 \cdot 3 = 1 \cdot (1+1)(2 \cdot 1 + 1) = n(n+1)(2n+1)$.

For inductive step, assume that the statement is true for some $n$. We then have

$$6\sum_{i=1}^{n+1} i^2 = 6\left(\sum_{i=1}^{n} i^2 + (n+1)^2\right) = 6\sum_{i=1}^{n} i^2 + 6(n+1)^2 =$$

$$= n(n+1)(2n+1)+6(n+1)^2 = (n+1)(n(2n+1)+6(n+1)) = (n+1)(2n^2+n+6n+6) =$$

$$= (n+1)(2n^2+7n+6) = (n+1)(2n^2+4n+3n+6) =$$

$$= (n+1)((n+2)2n+(n+2)3) = (n+1)(n+2)(2n+3) = (n+1)((n+1)+1)(2(n+1)+1)$$

3. $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1/4)n^2(n+1)^2$

The author has not yet defined (1/4), we assume that they meant to write $4\sum_{i=1}^{n} i^3 = n^2(n+1)^2$.

For base case, $n = 1$, so $4\sum_{i=1}^{n} i^3 = 4\sum_{i=1}^{1} i^3 = 4 \cdot 1^3 = 4 \cdot 1^2 = 1^2 \cdot 4 = 1^2 \cdot 2^2 = n^2(n+1)^2$.

For inductive step, assume that the statement is true for some $n$. We then have

$$4\sum_{i=1}^{n+1} i^3 = 4\left(\sum_{i=1}^{n} i^3 + (n+1)^3\right) = 4\sum_{i=1}^{n} i^3 + 4(n+1)^3 =$$

$$= n^2(n+1)^2 + 4(n+1)^3 = (n^2 + 4(n+1))(n+1)^2 =$$

$$= (n^2+4n+4)(n+1)^2 = (n+2)^2(n+1)^2 = (n+1)^2((n+1)+1)^2$$

4. $1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$

   The author has not yet defined $-1$, we assume that they meant to write $2 + \sum_{i=1}^{n} 2^i = 2^{n+1}$.

   For base case, $n = 1$, so $2 + \sum_{i=1}^{n} 2^i = 2 + \sum_{i=1}^{1} 2^i = 2 + 2^1 = 2 + 2 = 2 \cdot 2 = 2^2 = 2^{1+1} = 2^{n+1}$.

   For inductive step, assume that the statement is true for some $n$. We then have

$$2 + \sum_{i=1}^{n+1} 2^i = 2 + \sum_{i=1}^{n} 2^i + 2^{n+1} = 2^{n+1} + 2^{n+1} = 2^{n+1} \cdot 2 = 2^{(n+1)+1}$$

## Exercise 3.26

For $a_1, a_2, a_3, \ldots, a_n \in \mathbb{N}$ define $a_1 + a_2 + a_3 + \cdots + a_k = (a_1 + a_2 + a_3 + \cdots + a_{k-1}) + a_k$ for $k = 3, 4, 5, \ldots, n$. Prove:

1. $a_1+a_2+a_3+\cdots+a_n = (a_1+a_2+a_3+\cdots+a_r)+(a_{r+1}+a_{r+2}+a_{r+3}+\cdots+a_n)$

   We shall induct on $n$. For $n = 3$, we have associativity of $+$, which has already been established.

   For induction, assume that the statement is true for any $n$ and $1 \leq r \leq n - 1$. If $q = n$, then the conclusion is trivial. If $1 \leq q \leq n - 1$, then

$$a_1+\cdots+a_n+a_{n+1} = (a_1+\cdots+a_n)+a_{n+1} = ((a_1+\cdots+a_q)+(a_{q+1}+\ldots a_n))+a_{n+1}$$

$$= (a_1+\cdots+a_q)+((a_{q+1}+\cdots+a_n)+a_{n+1}) = (a_1+\cdots+a_q)+(a_{q+1}+\cdots+a_{n+1})$$

2. In any sum of $n$ natural numbers, parenthesis may be inserted at will.

   ...

### Exercise 3.27

Prove each of the following alternate forms of the Induction Principle:

1. With each $n \in \mathbb{N}$ let there be associated a proposition $P(n)$. Then $P(n)$ is true for every $n \in \mathbb{N}$ provided:

   (a) $P(1)$ is true

   (b) For each $m \in \mathbb{N}$ the assumption $P(k)$ is true for all $k < m$ implies $P(m)$ is true.

   By induction we shall prove that the second condition implies that $P(k) \implies P(k+1)$ and the conclusion follows automatically from Induction Principle. Let $k = 1$, then $P(2)$ is indeed true given that $P(1)$ is true since 1 is the only natural number less than 2. Now assume that $P(k) \implies P(k+1)$.

   The base case is given to be true. For inductive step, assume

2. Let $b$ be some fixed natural number, and with each natural number $n \geq b$ let the be associated a proposition $P(n)$. Then $P(n)$ is true for all values of $n$ provided:

   (a) $P(b)$ is true.

   (b) For each $m > b$ the assumption $P(k)$ is true for all $k \in \mathbb{N}$ such that $b \leq k < m$ implies $P(m)$ is true.

## 1.4 Algebra by Waerden, Chapter 1

### Exercise 1.1

Let a property $E$ be true, first for $n = 3$, and second for $n + 1$ whenever it is true for $n \geqslant 3$. Prove that $E$ is true for all numbers $\geqslant 3$.

We first show that if $a \geqslant b$, then $a + c \geqslant b + c$. We have two cases: $a = b$ or $a > b$. In the first case, $a + c = b + c$, meaning $a + c \geqslant b + c$ is true. In the second case, $a > b$ and $a + c > b + c$, meaning $a + c \geqslant b + c$ is true.

Our claim is that $(n - 2)$ exists for $n \geqslant 3$. We have $n = 3$ or $n > 3$. Either way, $n > 2$ and hence $(n - 2)$ exists by definition of $>$.

Now that we have established the existence of $(n - 2)$, we shall define a property $P$ which holds for $(n - 2)$ if and only if $E$ holds for $n$ and prove $P$ for all $n \geqslant 1$ by inducting on $(n - 2)$. When $(n - 2) = 1$, we have $n = 2+(n-2) = 3$. $E$ holds for $n = 3$, so $P$ holds for $(n-2) = 1$. Now assume $P$ is true for some $(n-2) \geqslant 1$, meaning $E$ is true for $n = 2+(n-2) \geqslant 2+1 = 3$. By definition of $E$, it should also be true for $n + 1$. If $E$ is true for $n + 1$, then $P$ should be true for $((n + 1) - 2)$. The only remaining thing to show is that $((n + 1) - 2) = (n - 2) + 1$. Consider the following:

$$(2 + (n - 2)) + 1 = n + 1 = 2 + ((n + 1) - 2) = (((n + 1) - 2) + 1) + 1$$

$$2 + (n - 2) = ((n + 1) - 2) + 1$$
$$((n - 2) + 1) + 1 = ((n + 1) - 2) + 1$$
$$(n - 2) + 1 = (n + 1) - 2$$

Finishing the induction. Hence $P$ holds for $(n - 2) \geqslant 1$, meaning $E$ should hold for $n = 2 + (n - 2) \geqslant 2 + 1 = 3$.

## Exercise 1.2

Carry out the proofs of the above. [For context, see the book.]

To prove that addition of integers as defined above is indeed well-defined, we can show that replacing $(a, b)$ by $(a', b')$ does not change the result whenever $(a, b)$ and $(a', b')$ represent the same thing i.e., $a + b' = a' + b$. Note that if we add $c$ and $d$ and rearrange via commutativity and associativity, we get

$$b' + d + a + c = a' + c + b + d$$

Meaning we have

$$(a + c, b + d) = (a' + c, b' + d)$$

Hence

$$(a, b) + (c, d) = (a', b') + (c, d)$$

Note that integer of additions inherits commutativity as shown below:

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b)$$

Therefore we arrive at the same conclusion if we were to replace $(c, d)$ by $(c', d')$ given they represent the same number.

Associativity and cancellation is also inherited:

$$((a, b) + (c, d)) + (e, f) = (a + c, b + d) + (e, f) = ((a + c) + e, (b + d) + f) =$$

$$= (a + (c + e), b + (d + f)) = (a, b) + (c + e, d + f) = (a, b) + ((c, d) + (e, f)).$$

$$(a, b) + (c, d) = (e, f) + (c, d) \implies (a + c, b + d) = (e + c, f + d) \implies$$

$$\implies a + c + f + d = b + d + e + c \implies a + f = b + e \implies$$

$$\implies (a, b) = (e, f).$$

We shall now go through the same process for multiplication. Let $a + b' = a' + b$ so that $(a, b) = (a', b')$. Then we have the following:

$$(a + b')c + (a' + b)d = (a' + b)c + (a + b')d$$

$$ac + bd + a'd + b'c = ad + bc + a'c + b'd$$

$$(ac + bd, ad + bc) = (a'c + b'd, a'd + b'c)$$

$$(a, b) \cdot (c, d) = (a', b') \cdot (c, d)$$

Hence multiplication is well-defined.

$$(a, b) \cdot (c, d) = (ac + bd, ad + bc) = (ca + db, da + cb) = (c, d) \cdot (a, b)$$

Hence multiplication is commutative.

$$((a, b) \cdot (c, d)) \cdot (e, f) = (ac + bd, ad + bc) \cdot (e, f) =$$

$$= ((ac)e + (bd)e + (ad)f + (bc)f, (ac)f + (bd)f + (ad)e + (bc)e) =$$

$$= (a(ce) + b(de) + a(df) + b(cf), a(cf) + b(df) + a(de) + b(ce)) =$$

$$= (a(ce) + a(df) + b(de) + b(cf), a(cf) + a(de) + b(df) + b(ce)) =$$

$$= (a, b) \cdot (ce + df, cf + de) = (a, b) \cdot ((c, d) \cdot (e, f))$$

Hence multiplication is associative.

For this part, let $(c, d) > 0$, i.e., $c > d$, meaning $(c-d)$ exists (as a natural number).

$$(a, b) \cdot (c, d) = (e, f) \cdot (c, d)$$

$$(ac + bd, ad + bc) = (ec + fd, ed + fc)$$

$$ac + bd + ed + fc = ad + bc + ec + fd$$

$$(a + f)c + (b + e)d = (a + f)d + (b + e)c$$

Let us now rewrite $c$ as $d + (c - d)$.

$$(a + f)(d + (c - d)) + (b + e)d = (a + f)d + (b + e)(d + (c - d))$$

$$(a + f)d + (a + f)(c - d) + (b + e)d = (a + f)d + (b + e)d + (b + e)(c - d)$$

$$(a + f)(c - d) = (b + e)(c - d)$$

$$a + f = b + e$$

$$(a, b) = (e, f)$$

Hence cancellation law holds for multiplication.

$$(a, b)\cdot((c, d)+(e, f)) = (a, b)\cdot(c+e, d+f) = (ac+ae+bd+bf, ad+af+bc+be) =$$

$$= (ac + bd, ad + bc) + (ae + bf, af + be) = (a, b) \cdot (c, d) + (a, b) \cdot (e, f)$$

Hence multiplication distributes over addition.

For any naturals $a, b, c, d$ we have either $a + d < b + c$, $a + d = b + c$ or $a + d > b + c$, i.e., for all $(a, b), (c, d)$ we have $(a, b) < (c, d)$, $(a, b) = (c, d)$ or $(a, b) > (c, d)$.

Let $(a, b) < (c, d)$ and $(c, d) < (e, f)$, i.e., $a + d < b + c$ and $c + f < d + e$, meaning we have $a + d + f < b + c + f < b + d + e$, $a + f < b + e$ and $(a, b) < (e, f)$. Hence transitivity of $<$ also holds for integers.

Let $(a, b) < (c, d)$, i.e., $a + d < b + c$, meaning we have $a + e + d + f < b + f + c + e$, $(a + e, b + f) < (c + e, d + f)$ and $(a, b) + (e, f) < (c, d) + (e, f)$.

Now also let $(e, f) > 0$, i.e., $e > f$, meaning $(e - f)$ exists (as a natural number). We thus have the following:

$$a + d > b + c$$

$$(a + d)(e - f) > (b + c)(e - f)$$

$$(a+d)f+(a+d)(e-f)+(b+c)f > (b+c)f+(b+c)(e-f)+(a+d)f$$

$$(a+d)(f+(e-f))+(b+c)f > (b+c)(f+(e-f))+(a+d)f$$

$$(a+d)e+(b+c)f > (b+c)e+(a+d)f$$

$$ae+bf+cf+de > ce+df+af+be$$

$$(ae+bf, af+be) > (ce+df, cf+de)$$

$$(a,b)\cdot(e,f) > (c,d)\cdot(e,f)$$

Finally, we have proven that the same rules arithmetic are fulfilled. (although with in some cases an integer being required to be positive.)

We shall now show that the equation $(a,b)+(x,y)=(c,d)$ has a unique solution for $(x,y)$ this time without needing any restrictions. We start by showing existence of a solution. For any $(a,b)$ and $(c,d)$ we have $(a,b)+(b+c,a+d)=(c,d)$, so $x=b+c$ and $y=a+d$ yields a solution. Uniqueness of the number represented by $(x,y)$ is guranteed due to the cancellation law.

For the following part we need to show that multiplying an integer by zero yields zero.

$$(x,y)\cdot(a,a)=(ax+ay, ax+ay)=0$$

Another quick thing to show is that $(b,a)\cdot(d,c)=(a,b)\cdot(c,d)$.

$$(a,b)\cdot(c,d)=(ac+bd, ad+bc)=(bd+ac, bc+ad)=(b,a)\cdot(d,c)$$

For the fourth and final part, we could do a proof by contraposition. Let $(a,b)$ and $(c,d)$ be nonzero, i.e., either positive or negative and consider cases. If only one of them is positive (without loss of generality, assume $(a,b)$ is positive), then we will have $(a,b)\cdot(c,d) > (a,b)\cdot 0$ or $(a,b)\cdot(c,d) < (a,b)\cdot 0$ depending on the sign of $(c,d)$. In either case, $(a,b)\cdot(c,d)\neq 0$. For the other case let $(a,b)$ and $(c,d)$ both be negative, this implies $(b,a)$ and $(d,c)$ to be both positive and so we have $(a,b)\cdot(c,d)=(b,a)\cdot(d,c)>0$. We have thus proven that for integers $x,y\neq 0$ we have $xy\neq 0$. Contrapositive of the above implication is that if $xy=0$ for integers $x,y$, then $x=0$ or $y=0$.

## Exercise 1.3

The same as Exercise 1.1 with the number 3 replaced by 0.

Since $E$ is true for 0, it should also be true for $0+1$, which is just 1. So we have $E$ satisfied for 0, 1 and for $n+1$ whenever it's true for $n$. The last two statements can be combined into the fact that $E$ is true for any $n \geqslant 1$. (via principle of mathematican induction.) Since it's also true for 0, we have $E$ true for $n \geqslant 0$.

## Exercise 1.4

Prove by mathematical induction on $n$ that any subset of a finite set $\mathfrak{A} = \{a_1, \ldots, a_n\}$ is itself finite.

For base case, $n = 1$, so the only subsets of $\mathfrak{A}$ are the empty set and $\mathfrak{A}$ itself, both of which are finite. For inductive step, assume that every set with $n$ elements has subsets all finite and consider $\mathfrak{A}$ to be a set with $n+1$ elements with $\mathfrak{S}$ one of its subsets. If $\mathfrak{S} = \mathfrak{A}$, then $\mathfrak{S}$ is automatically finite since so is $\mathfrak{A}$. If, however, $\mathfrak{S}$ is a proper subset of $\mathfrak{A}$, then name $a$ to be the element in $\mathfrak{A}$ missing in $\mathfrak{S}$, then $\mathfrak{S}$ is a subset of $\mathfrak{A} \setminus \{a\}$. The latter has $n$ elemenents and, by inductive hypothesis, $\mathfrak{A}$ is finite. This finishes the proof by induction.

## Exercise 1.5

Prove that the number of elements in a union of two mutually exclusive finite sets is equal to the sum of the numbers of the individual sets. (Mathematical induction by means of recursion formulae (1.1), (1.2), Section 1.3.)

...

# Chapter 2

# Relations and order theory

## 2.1 Week 2 Central Exercises

### Exercise 1.1

On the set of integers $\mathbb{Z}$, define a relation $\mid$ by the following rule: for $x, y \in \mathbb{Z}$, let $x \mid y$ if and only if there exists an integer $k \in \mathbb{Z}$ such that $xk = y$.

1. Find all $x$ such that $x \mid 10$.

   Via fundamental theorem of arithmetic and the fact that the only units in $\mathbb{Z}$ are $-1$ and $1$, we get that $x \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$.

2. Is it true that $x \mid x$ for all $x \in \mathbb{Z}$? Explain why.

   For all $x \in \mathbb{Z}$ we have $x = x \cdot 1$, hence $x \mid x$.

3. Is it true that if $x \mid y$ then $y \mid x$ for all $x, y \in \mathbb{Z}$? Explain why.

By contradiction let it be true for all $x, y \in \mathbb{Z}$. Then $\exists k_1, k_2 \in \mathbb{Z}$ s.t. $y = k_1 x$ and $x = k_2 y$, meaning $y = k_1 k_2 y$ and $(1 - k_1 k_2)y = 0$. We want this to work for all $y$, so we can let $y$ be nonzero, so $1 = k_1 k_2$. But the only divisors of 1 are $-1$ and 1, so we have two cases: $k_1, k_2 = 1$ or $k_1, k_2 = -1$. Both cases restrict the suitable values of $x, y$ despite the assumption that the hypothesis is true for any $x, y$. Hence the contradiction.

4. Is it true that if $x \mid y$ and $y \mid z$ then $x \mid z$ for all $x, y, z \in \mathbb{Z}$?

By definition we can rewrite $x \mid y$ and $y \mid z$ as $\exists k_1, k_2 \in \mathbb{Z}$, $y = k_1 x$ and $z = k_2 y$, meaning $z = k_1 k_2 x$, i.e., there exists $k \in \mathbb{Z}$ with $z = kx$, meaning $x \mid z$ indeed.

## Exercise 1.2.1

Determine whether the relation described by all ordered pairs of real numbers $(x, y)$ such that $xy = 0$ is reflexive, symmetric, antisymmetric, and transitive.

The relation is not reflexive as $1 \in \mathbb{R}$ and $(1, 1)$ is absent as $1 \cdot 1 \neq 0$. The relation is symmetric since if $xy = 0$, then $yx = xy = 0$ due to commutativity of multiplication. The relation is not antisymmetric as $1 \cdot 0 = 0$ and $0 \cdot 2 = 0$ but $1 \cdot 2 \neq 0$.

## Exercise 1.2.2

Give an example of a relation on a set that is neither symmetric nor antisymmetric.

Consider the relation $\{(a, b), (b, a), (a, c)\}$ on the set $\{a, b, c\}$.

### Exercise 1.2.3

Determine whether the relations described by the conditions below are reflexive, symmetric, antisymmetric, or transitive.

1. All ordered pairs of real numbers $(x, y)$ such that $x - y$ is rational;

   It is reflexive as $x - x = 0 \in \mathbb{Q}$. It is symmetric as $(x - y) \in \mathbb{Q}$ implies $(y - x) = -(x - y) \in \mathbb{Q}$ thanks to closure of $\mathbb{Q}$ under negation. It is not antisymmetric as $2 - 1 = 1 \in \mathbb{Q}$ and $1 - 2 = -1 \in \mathbb{Q}$ but $2 \neq 1$. It is transitive as $(x - y) \in \mathbb{Q}$ and $(y - z) \in \mathbb{Q}$ imply $(x - z) = (x - y) + (y - z) \in \mathbb{Q}$ thanks to closure of $\mathbb{Q}$ under addition.

2. All ordered pairs of real numbers $(x, y)$ such that $x = 2y$.

   It is not reflexive as $1 \neq 1 \cdot 2$. It is neither symmetric since $2 = 2 \cdot 1$ but $1 \neq 2 \cdot 2$. It is antisymmetric as $x = 2y$ and $y = 2x$ imply $x = 4x$ and $x = 0$, meaning $y = 0$ and therefore $x = y$ thanks to transitivity of $=$. The relation is not transitive as $4 = 2 \cdot 2$ and $2 = 2 \cdot 1$ but $4 \neq 2 \cdot 1$.

3. All ordered pairs of real numbers $(x, y)$ such that $xy > 0$.

   The relation is not reflexive as $0 \cdot 0 = 0 \not> 0$. It is symmetric as $xy > 0$ implies $yx = xy > 0$ thanks to commutativity of multiplication. It is not antisymmetric as $2 \cdot 1 > 0$ and $1 \cdot 2 > 0$ but $1 \neq 2$. It is transitive as $xy > 0$ and $yz > 0$ imply $xy^2z > 0$; $y$ can't be 0 as it would contradict both $xy > 0$ and $yz > 0$, so $y^2 > 0$, meaning we can divide the inequality by it and get $xz > 0$, proving transitivity.

## Exercise 1.2.4

Give an example of a relation on a set that is both symmetric and antisymmetric.

The empty and diagonal relations.

## Exercise 1.3.1

Is the relation described below on the set of all people an equivalence relation? If not, determine the properties of an equivalence relation that it lacks.

$$\{(a, b) : a \text{ and } b \text{ speak a common language}\}$$

The only property it lacks is transitivity. As a counterexample to the relation being transitive, my friend Alex speaks only English, Eliana speaks Greek and English, but her mother speaks only Greek. Alex relates to Eliana, Eliana related to her mother, but Alex does not relate to Eliana's mother.

## Exercise 1.3.2

Which of the relations described below on the set of all people are equivalence relations? Determine the properties of an equivalence relation that the others lack.

1. $\{(a, b) : a$ and $b$ are the same age$\}$;

   Reflexivity is satisfied as a person has the same age as oneself. If person 1 has the same age as person 2, then person 2 has the same age as person 1, so symmetry is present. Transitivity also holds since if, on top of that, person 2 had the same age as person 3, then person 1 would have the same age as person 3. Hence this is an equivalence relation.

2. $\{(a, b) : a$ and $b$ have the same parents$\}$;

A person has the same parents as oneself, so reflexivity holds. Symmetry is also present since if person 1 and person 2 have the same parents, then person 2 and person 1 have the same parents. If, on top of that, person 2 had the same parents as person 3, then person 1 would have the same parents as person 3, so transitivity is satisfied. Hence the relation is an equivalence relation.

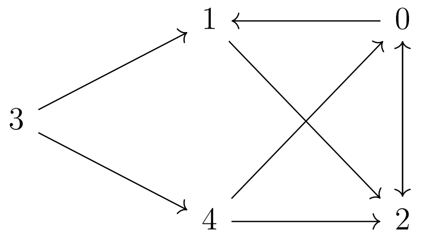
3. $\{(a, b) : a \text{ and } b \text{ have a common parent}\}$

The relation lacks only transitivity. For a counterexample, the read may look up any European royal family tree.

## Exercise 1.4

Let $R$ be a relation on $X = \{0, 1, 2, 3, 4\}$ defined by a directed graph on the graph below in the following way: for any two elements $a, b \in X$, we draw an arrow from $a$ to $b$ if and only if $aRb$.

Identity the smallest subset $R' \subset X \times X$, so that the relation $R \cup R'$ is symmetric.



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

## Exercise 1.5.1

Is the relation

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

on $\{0, 1, 2, 3\}$ a partial ordering. If not, determine the properties of a partial ordering that it lacks.

Each one of $(0, 0)$, $(1, 1)$, $(2, 2)$ and $(3, 3)$ is present, so reflexivity holds. For antisymmetry, we start by considering all pairs of symmetric pairs in the relation. Those happen to be $(0, 0)$ and $(0, 0)$, $(1, 1)$ and $(1, 1)$, $(2, 2)$ and $(2, 2)$, $(3, 3)$ and $(3, 3)$. Clearly, the elements in each case are equal, hence antisymmetry. Transitivity also holds as we have $(0, 0)$, $(0, 0)$ and $(0, 0)$; $(1, 1)$, $(1, 1)$ and $(1, 1)$; $(2, 0)$, $(0, 0)$ and $(2, 0)$; $(2, 2)$, $(2, 2)$ and $(2, 2)$; $(2, 2)$, $(2, 0)$ and $(2, 0)$; $(2, 2)$, $(2, 3)$ and $(2, 3)$; $(3, 3)$, $(3, 3)$ and $(3, 3)$.

## Exercise 1.5.2

Denote by $\mathcal{J}$ the set of closed intervals in the real numbers, and define a relation $S$ on $\mathcal{J}$ by $[a, b]S[c, d]$ if and only if $[a, b] = [c, d]$ or $b < c$. Show that $S$ is a partial ordering but not a linear ordering on $\mathcal{J}$.

Reflexivity holds by definition. For antisymmetry, let $[a, b]S[c, d]$ and $[c, d]S[a, b]$. If $[a, b] = [c, d]$, then we are done. If $b < c$, then we should also have $c < d$ (since the possibility $[c, d] = [a, b]$ has been excluded), but that is a contradiction. For transitivity, let $[a, b]S[c, d]$ and $[c, d]S[e, f]$. If $[a, b] = [c, d]$ and $[c, d] = [e, f]$, then $[a, b] = [e, f]$ and $[a, b]S[e, f]$. If $[a, b] = [c, d]$ and $d < e$, then $b = d < e$ and $[a, b]S[e, f]$. If $b < c$ and $[c, d] = [e, f]$, then $b < c = e$ and $[a, b]S[e, f]$. If $b < c$ and $d < e$, then $b < c \leqslant d < e$ and $[a, b]S[e, f]$.

## Exercise 1.5.3

Which of these relations on $\{0, 1, 2, 3\}$ are partial orderings? Determine the properties of a partial ordering that the others lack.

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

   Reflexivity is absent as $(1, 1)$ is not in the set.

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

   Transitivity is not satisfied as $(3,1)$ and $(1,2)$ are in the set whereas $(3,2)$ is not.

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

   Transitivity does not hold as $(1,2)$ and $(2,0)$ are present, but $(1,0)$ is not.

## Exercise 1.6.1

Determine whether these posets are lattices.

1. $(\{-1,2,3,7\},\leqslant)$;
2. $(\mathbb{N},\leqslant)$;
3. $(\mathbb{Z},\geqslant)$;
4. $(\mathcal{P}(S),\supseteq)$.

The first three are chains and therefore lattices. For the latter, take any two subsets $A, B$ of $S$, then $\sup\{A,B\} = A \cap B$ and $\inf\{A,B\} = A \cup B$.

## Exercise 1.6.2

Which of these posets are lattices?

1. $(\{1,3,6,9,12\},|)$;

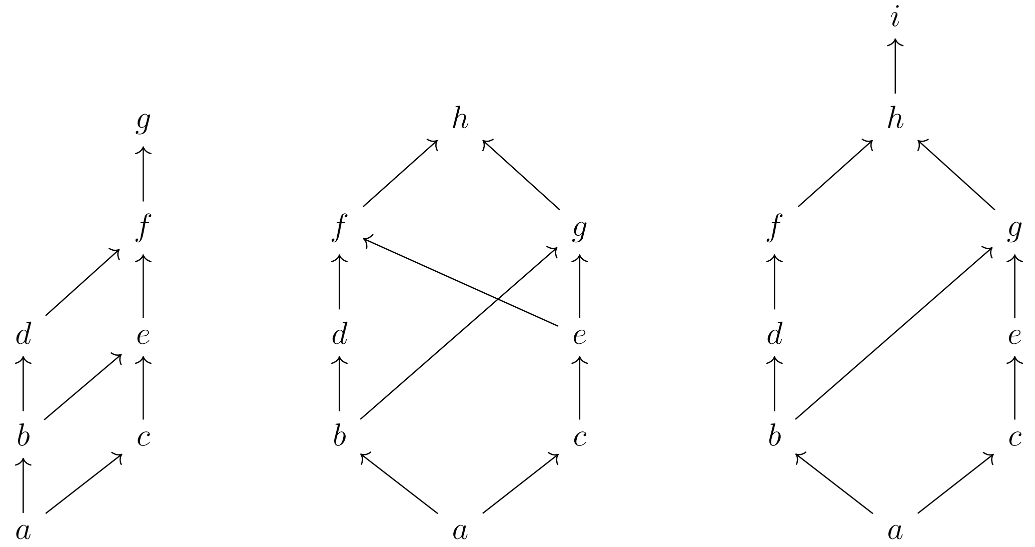
   Assume some $a \in \{1,3,6,9,12\}$ is an upper bound of 9 and 12, then $a \geqslant 36$, but none of the elements in the set are $\geqslant 36$, so there is no upper bound and hence no supremum for 9 and 12, meaning the poset is not a lattice.

2. $(\{1, 5, 25, 125\}, |)$.

This poset is a totally ordered and therefore a lattice.

## Exercise 1.6.3

Which of these posets with the Hasse diagrams in the figure below are lattices?



The first poset is a lattice. Take any two elements from $\{a, b, c, d, e, f, g\}$. If they are comparable, then we are done, so consider the incomparable ones. The only pairs of incomparable elements are $(b, c)$ and $(d, e)$. The supremum and infimum of $\{b, c\}$ are $e$ and $a$, the supremum and infimum of $\{d, e\}$ are $f$ and $b$.

The second poset is not a lattice as there is no supremum for $\{b, e\}$.

For the third poset, once again consider incomparable elements from $\{a, b, c, d, e, f, g, h, i\}$. For $\{b, c\}$ and $\{b, e\}$ the supremum and infimum are $g$ and $a$. For $\{d, c\}$, $\{d, e\}$, $\{f, c\}$ and $\{f, e\}$ the supremum and infimum are $h$ and $a$.

## 2.2 Schaum's Outline of Abstract Algebra, Chapter 2

### Exercise 2.14

Which of the following are equivalence relations?

1. "Is similar to" for the set $T$ of all triangles in a plane.

   Any triangle is similar to itself (with similarity coefficient of 1), so the relation is reflexive. If triangle 1 is similar to triangle 2 with coefficient $k_1$, then triangle 2 is similar to triangle 1 with coefficient $\frac{1}{k_1}$, so the relation is symmetric. If, ont top of that, triangle 2 is similar to triangle 3 with coefficient $k_2$, then triangle 1 is similar to triangle 3 with coefficient $k_1 k_2$, so the relation is transitive and therefore an equivalence relation.

2. "Has the same radius as" for the set of all circles in a plane.

   A circle has the same radius as itself, so the relation is reflexive. If circle 1 has the same radius as circle 2, then circle 2 has the same radius as circle 1, so the relation is symmetric. If, on top of that, circle 3 has the same radius as circle 2, then circle 1 has the same radius as circle 3, so the relation is transitive and therefore an equivalence relation.

3. "Is the square of" for the set $\mathbb{N}$.

   2 is not the square of itself, so $nRn$ is not necessarily true for all $n \in \mathbb{N}$. So the relation is not an equivalence relation.

4. "Has the same number of vertices as" for the set of all polygons in a plane.

   A polygon has the same number of vertices as itself, so the relation is reflexive. If polygon 1 has the same number of vertices as polygon 2, then polygon 2 has the same number of vertices as polygon 1, so the relation is symmetric. If, on top of that, polygon 2 has the same number of vertices as polygon 3, then polygon 1 has the same number of vertices as polygon 3, so the relation is transitive and therefore an equivalence relation.

5. "$\subseteq$" for the set of sets $S = \{A, B, C, \dots\}$.

   The relation is not necessarily symmetric as $A \subseteq B$ may not imply $B \subseteq A$ (e.g., $\{1\} \subseteq \{1, 2\}$ but $\{1, 2\} \nsubseteq \{1\}$). The only case when the relation is an equivalence relation is when $S$ contains just one set. Also, notice how $\subseteq$ is a partial order on $S$.

6. "$\leqslant$" for the set $\mathbb{R}$.

   The relation is not symmetric as $x \leqslant y$ may not imply $y \leqslant x$ (e.g., $1 \leqslant 2$ but $2 \nleqslant 1$). Notice how $\leqslant$ is a total order on $S$.

## Exercise 2.15

1. Show that "is a factor of" on $\mathbb{N}$ is reflexive and transitive but is not symmetric.

   For any $n \in \mathbb{N}$ we have $n = n \cdot 1$, meaning $n$ is a factor of itself, so the relation is reflexive. The relation is transitive as shown below:

$$\begin{cases} n_1 \text{ is a factor of } n_2 \\ n_2 \text{ is a factor of } n_3 \end{cases} \iff \begin{cases} \exists k_1 \in \mathbb{N},\ n_2 = n_1 \cdot k_1 \\ \exists k_2 \in \mathbb{N},\ n_3 = n_2 \cdot k_2 \end{cases} \implies$$

$$\implies n_3 = n_2 \cdot k_2 = n_1 \cdot k_1 \cdot k_2 \implies n_1 \text{ is a factor of } n_3$$

However, the relation is not symmetric as $n_1$ being a factor of $n_2$ may not necessarily imply $n_2$ to be a factor of $n_1$ (e.g., $2 = 1 \cdot 2$ but $\nexists k \in \mathbb{N},\ 1 = 2 \cdot k$). Notice how the relation is a partial order.

2. Show that "costs within one dollar of" for men's shoes is reflexive and symmetric but not transitive.

   A pair of men's shoes costs within one dollar of itself, so the relation is reflexive. If a pair 1 of men's shoes costs within one dollar of another pair 2 of men's shoes, then the pair 2 of men's shoes costs within one dollar of pair 1 of men's shoes. However, if we were to have pair 2 of men's shoes costing within one dollar of pair 3 of men's shoes, then it is not necessarily implied that pair 1 of men's shoes costs within one dollar of pair 3 of men's shoes (e.g., if pair 1 costs 200 dollars, pair 2 costs 200.9 dollars and pair 3 costs 201.8 dollars, we have a counterexample).

3. Give an example of a relation which is symmetric and transitive but not reflexive.

   The empty relation.

4. Conclude from (a), (b), (c) that no two of the properties reflexive, symmetric, transitive of a binary relation implies the other.

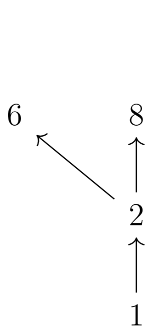
   Concluded.

## Exercise 2.16

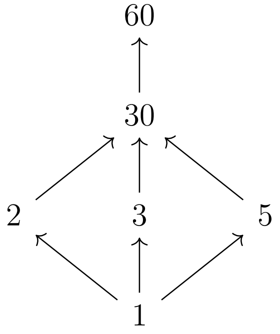
Diagram the partial ordering of

1. $A = \{1, 2, 8, 6\}$
2. $B = \{1, 2, 3, 5, 30, 60\}$
3. $C = \{1, 3, 5, 15, 30, 45\}$

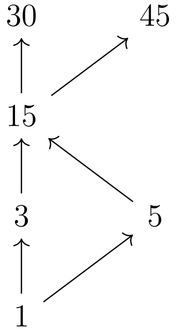
effected on each by the relation $(|)$.



$A$



$B$



$C$

## Exercise 2.17

Let $S = \{a, b, c, d, e, f\}$ be ordered by the relation $R$ as shown in Fig. 2-9.

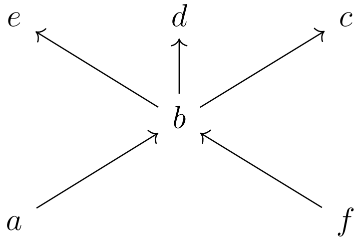


Fig. 2-9

1. List all pairs $x, y \in S$ for which $x \not R y$.

$a \not R f$, $b \not R a$, $b \not R f$, $c \not R a$, $c \not R b$, $c \not R d$, $c \not R e$, $c \not R f$, $d \not R a$, $d \not R b$, $d \not R c$, $d \not R e$, $d \not R f$, $e \not R a$, $e \not R b$, $e \not R c$, $e \not R d$, $e \not R f$, $f \not R a$.

2. List all subsets of three elements each of which are totally ordered.

$\{a, b, c\}$, $\{a, b, d\}$, $\{a, b, e\}$, $\{f, b, c\}$, $\{f, b, d\}$, $\{f, b, e\}$.

## Exercise 2.18

Verify:

1. The ordered set of subsets of $S$ in Problem 2.7 (a) has $\varnothing$ as first element (also, as minimal element) and $S$ as last element (also, as maximal element).

$\varnothing \subseteq A$ for any $A$, so it is a first element. Also, $A \subseteq \varnothing$ implies $A = \varnothing$, so $\varnothing$ is also the minimal element. $A \subseteq S$ for any $A$ (since every $A$ is a subset of $S$ by definition), so $S$ is a last element. Also, $S \subseteq A$ implies $A = S$, so $S$ is also the maximal element.

2. The ordered set $B$ of Problem 2.7 (b) has neither a first nor last element. What are its minimal and maximal elements?

By contradiction, assume it has a first element, name it $n$. Then $n \mid 2$ and $n \mid 5$, implying $n = 1$, which is not in the set. Now assume it has a last element, name it $m$. Then $60 \mid m$ and $8 \mid m$, implying $m \geqslant 120$, but none of the elements in $B$ are $\geqslant 120$. The minimal elements of $B$ are 2 and 5 (since there is no other element dividing each), whereas the maximal elements of $B$ are 8, 60 and 45 (since they divide only themselves in the set).

3. The subset $C = \{2, 4, 5, 15, 60\}$ of $B$ of Problem 2.7 (b) has a last element but no first element. What are its minimal and maximal elements?

   By contradiction, assume it has a first element, name it $k$. Then $k \mid 4$ and $k \mid 15$, implying $k \geqslant 60$ and $k = 60$ since 60 is the only element in $C$ that is $\geqslant 60$. But both $k \mid 4$ and $k \mid 15$ stop being true then. The last element of $C$ is 60 as every number in $C$ divides 60. The minimal elements of $C$ are 2 and 5, whereas the maximal element of $C$ is 60.

## Exercise 2.19

Show:

1. Multiplication is a binary operation on on $S = \{1, -1\}$, but not on $T = \{1, 2\}$.

   $1 \cdot 1 = 1 \in S$, $1 \cdot (-1) = -1 \in S$, $(-1) \cdot 1 = -1 \in S$, $(-1) \cdot (-1) = 1 \in S$, hence $\cdot$ is a binary operation on $S$. $2 \cdot 2 = 4 \notin T$, so $\cdot$ is not a binary operation on $T$.

2. Addition is a binary operation on $S = \{x : x \in \mathbb{Z}, x < 0\}$ but multiplication is not.

   Note that $x_1, x_2 \in \mathbb{Z}$ means that $x_1 + x_2 = -((-x_1) + (-x_2))$. $-x_1$ and $-x_2$ are natural numbers and, since naturals are closed under addition, we have $(-x_1) + (-x_2) \in \mathbb{Z}$ and $-((-x_1) + (-x_2)) \in S$. Hence $+$ is a binary operation on $S$ whereas $\cdot$ is not since $(-1) \cdot (-1) = 1 \notin S$.

## Exercise 2.20

Let $S = \{A, B, C, D\}$ where $A = \varnothing$, $B = \{a, b\}$, $C = \{a, c\}$, $D = \{a, b, c\}$. Construct tables to show that $\cup$ is a binary relation on $S$ but $\cap$ is not.

| $\cup$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $B$ | $C$ | $D$ |
| $B$ | $B$ | $B$ | $D$ | $D$ |
| $C$ | $C$ | $D$ | $C$ | $D$ |
| $D$ | $D$ | $D$ | $D$ | $D$ |

| $\cap$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $A$ | $A$ | $A$ |
| $B$ | $A$ | $B$ | $\{a\}$ | $B$ |
| $C$ | $A$ | $\{a\}$ | $C$ | $C$ |
| $D$ | $A$ | $B$ | $C$ | $D$ |

## Exercise 2.21

For the binary operations $\circ$ and $\Box$ defined on $S = \{a, b, c, d, e\}$ by Tables 2-9 and 2-10, assume associativity and investigate for all other properties.

| $\circ$ | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|
| $a$ | $a$ | $d$ | $a$ | $d$ | $e$ |
| $b$ | $d$ | $b$ | $b$ | $d$ | $e$ |
| $c$ | $a$ | $b$ | $c$ | $d$ | $e$ |
| $d$ | $d$ | $d$ | $d$ | $d$ | $e$ |
| $e$ | $e$ | $e$ | $e$ | $e$ | $e$ |

| $\Box$ | $a$ | $b$ | $c$ | $d$ | $e$ |
|---|---|---|---|---|---|
| $a$ | $a$ | $c$ | $c$ | $a$ | $a$ |
| $b$ | $c$ | $c$ | $c$ | $b$ | $b$ |
| $c$ | $c$ | $c$ | $c$ | $c$ | $c$ |
| $d$ | $a$ | $b$ | $c$ | $d$ | $d$ |
| $e$ | $a$ | $b$ | $c$ | $d$ | $e$ |

Both operations are commutative due to the symmetry along the diagonal. $\circ$ does not distribute over $\Box$ as $a \circ (b\Box b) = a \circ c = a \neq d = d\Box d = (a \circ b)\Box(a \circ b)$. $\Box$ does not distribute over $\circ$ since $b\Box(a \circ b) = b\Box d = b \neq c = c \circ c = (b\Box a) \circ (b\Box b)$. The identity of $\Box$ is $e$.

## Exercise 2.22

Let $S = \{A, B, C, D\}$ where $A = \varnothing$, $B = \{a\}$, $C = \{a, b\}$, $D = \{a, b, c\}$.

1. Construct tables to show that $\cup$ and $\cap$ are binary operations on $S$.

| $\cup$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $B$ | $C$ | $D$ |
| $B$ | $B$ | $B$ | $C$ | $D$ |
| $C$ | $C$ | $C$ | $C$ | $D$ |
| $D$ | $D$ | $D$ | $D$ | $D$ |

| $\cap$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|
| $A$ | $A$ | $A$ | $A$ | $A$ |
| $B$ | $A$ | $B$ | $B$ | $B$ |
| $C$ | $A$ | $B$ | $C$ | $C$ |
| $D$ | $A$ | $B$ | $C$ | $D$ |

2. Assume associativity for each operation and investigate all other properties.

   Each operation is commutative and distributive over the other. The identity of $\cup$ is $A$ and the identity of $\cap$ is $D$.

## Exercise 2.23

For the binary operation on $S = \{a, b, c, d, e, f, g, h\}$ defined by Table 2-11, assume associativity and investigate all other properties.

| $\circ$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
|---|---|---|---|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ |
| $b$ | $b$ | $c$ | $d$ | $a$ | $h$ | $g$ | $e$ | $f$ |
| $c$ | $c$ | $d$ | $a$ | $b$ | $f$ | $e$ | $h$ | $g$ |
| $d$ | $d$ | $a$ | $b$ | $c$ | $g$ | $h$ | $f$ | $e$ |
| $e$ | $e$ | $g$ | $f$ | $h$ | $a$ | $c$ | $b$ | $d$ |
| $f$ | $f$ | $h$ | $e$ | $g$ | $c$ | $a$ | $d$ | $b$ |
| $g$ | $g$ | $f$ | $h$ | $e$ | $d$ | $b$ | $a$ | $c$ |
| $h$ | $h$ | $e$ | $g$ | $f$ | $b$ | $d$ | $c$ | $a$ |

$\circ$ is not commutative (e.g., $b \circ e = h \neq g = e \circ b$). $a$ is the identity and every element has an inverse.

## Exercise 2.24

Show that $\circ$ defined in Problem 2.23 is a binary operation on the subsets $S_0 = \{a\}$, $S_1 = \{a, c\}$, $S_2 = \{a, e\}$, $S_3 = \{a, f\}$, $S_4 = \{a, g\}$, $S_5 = \{a, h\}$, $S_6 = \{a, b, c, d\}$, $S_7 = \{a, c, e, f\}$, $S_8 = \{a, c, g, h\}$ but not on the subsets $T_1 = \{a, b\}$ and $T_2 = \{a, f, g\}$ of $S$.

$S_0$ is closed under $\circ$ since $a \circ a = a \in S_0$.

$S_1$ is closed under $\circ$ since $a \circ a = a \in S_1$, $a \circ c = c \in S_1$, $c \circ a = c \in S_1$, $c \circ c = a \in S_1$.

$S_2$ is closed under $\circ$ since $a \circ a = a \in S_2$, $a \circ e = e \in S_2$, $e \circ a = e \in S_2$, $e \circ e = a \in S_2$.

$S_3$ is closed under $\circ$ since $a \circ a = a \in S_3$, $a \circ f = f \in S_3$, $f \circ a = f \in S_3$, $f \circ f = a \in S_3$.

$S_4$ is closed under $\circ$ since $a \circ a = a \in S_4$, $a \circ g = g \in S_4$, $g \circ a = g \in S_4$, $g \circ g = a \in S_4$.

$S_5$ is closed under $\circ$ since $a \circ a = a \in S_5$, $a \circ h = h \in S_5$, $h \circ a = h \in S_5$.

$S_6$ is closed under $\circ$ since $a \circ a = a \in S_6$, $b \circ b = c \in S_6$, $c \circ c = a \in S_6$, $d \circ d = c \in S_6$, $a \circ b = b \circ a = b \in S_6$, $a \circ c = c \circ a = c \in S_6$, $a \circ d = d \circ a = d \in S_6$, $b \circ c = c \circ b = d \in S_6$, $b \circ d = d \circ b = a \in S_6$, $c \circ d = d \circ c = b \in S_6$.

$S_7$ is closed under $\circ$ since $a \circ a = a \in S_7$, $c \circ c = a \in S_7$, $e \circ e = a \in S_7$, $f \circ f = a \in S_7$, $a \circ c = c \circ a = c \in S_7$, $a \circ e = e \circ a = e \in S_7$, $a \circ f = f \circ a = f \in S_7$, $c \circ e = e \circ c = f \in S_7$, $c \circ f = f \circ c = e \in S_7$, $e \circ f = f \circ e = e \in S_7$.

$S_8$ is closed under $\circ$ since $a \circ a = a \in S_8$, $c \circ c = a \in S_8$, $g \circ g = a \in S_8$, $h \circ h = a \in S_8$, $a \circ c = c \circ a = c \in S_8$, $a \circ g = g \circ a = g \in S_8$, $a \circ h = h \circ a = h \in S_8$, $c \circ g = g \circ c = h \in S_8$, $c \circ h = h \circ c = g \in S_8$, $g \circ h = h \circ g = c \in S_8$.

$T_1$ is not closed under $\circ$ since $b \circ b = c \notin T_1$.

$T_2$ is not closed under $\circ$ since $f \circ g = d \notin T_2$.

### Exercise 2.25

Prove Theorem IV. Hint: Assume $y$ and $z$ to be inverses of $x$ and consider $z \circ (x \circ y)$

Theorem IV is false. Its statement would be correct if $\circ$ was associative.

## 2.3 Undergraduate Algebra by Serge Lang, Section 1.5

### Exercise 1

Let $n, d$ be positive integers and assume $1 < d < n$. Show that $n$ can be written in the form

$$n = c_0 + c_1 d + \cdots + c_k d^k$$

with integers $c_i$ such that $0 \leqslant c_i < d$, and that these integers $c_i$ are uniquely determined. [Hint: For the existence, write $n = qd + c_0$ by the Euclidean algorithm, and then use induction. For the uniqueness, use induction, assuming $c_0, \ldots, c_r$ are uniquely determined; Show that $c_{r+1}$ is then uniquely determined.]

We shall use strong induction on $n$. For base case, let $n = 3$ so that $d = 2$ is forced. We hence have $n = 1 + 1 \cdot d$. For inductive step, assume that the statement is true for any natural number less than or equal to $n$. If $d = n$, then, obviously, $n + 1 = 1 + 1 \cdot d$. If, however, $d < n$, then we resort to the Euclidean algorithm, which suggests that $n + 1 = qd + r$ for some unique $0 \leq r < n + 1$ and $q \geq 0$. If $q < d$, then we are done. If $q = d$, then

$n+1=d^2+r$ and we are also done. If $q>d$, then we may apply inductive hypothesis and say $q=c_0+c_1d+\cdots+c_kd^k$ with unique integers $0\leq c_i<d$ for all $i\in\{0,\dots,k\}$. Thus $n=r+c_0d+c_1d^2+\cdots+c_kd^{k+1}$. Uniqueness is guaranteed why Euclidean algorithm.

## Exercise 2

Let $m,n$ be non-zero integers written in the form

$$m=p_1^{i_1}\cdots p_r^{i_r} \quad \text{and} \quad n=p_1^{j_1}\cdots p_r^{j_r}$$

where $i_v$, $j_v$ are integers $\geqslant 0$ and $p_1,\dots,p_r$ are distinct prime numbers.

1. Show that g.c.d. of $m$, $n$ can be expressed as a product $p_1^{k_1}\cdots p_r^{k_r}$ where $k_1,\dots,k_r$ are integers $\geqslant 0$. Express $k_v$ in terms of $i_v$, $j_v$.

   Our claim is that $p_1^{\min(i_1,j_1)}\cdots p_r^{\min(i_r,j_r)}$ is the g.c.d. of $m$ and $n$ where $\min:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ is defined as follows:

   $$\min(a,b)=\begin{cases}a, & a\leq b\\ b, & b<a\end{cases}$$

   We first need to show that it divides both of integers.

   $$m=p_1^{\min(i_1,j_1)}\cdots p_r^{\min(i_r,j_r)}\cdot p_1^{i_1-\min(i_1,j_1)}\cdots p_r^{i_r-\min(i_r,j_r)}$$

   $$n=p_1^{\min(i_1,j_1)}\cdots p_r^{\min(i_r,j_r)}\cdot p_1^{j_1-\min(i_1,j_1)}\cdots p_r^{j_r-\min(i_r,j_r)}$$

   Notice how both $a-\min(a,b)$ and $b-\min(a,b)$ are ensured to be nonnegative integers given that $a,b$ also are.

   Before we continue, we shall show that if a prime $p$ is present in the prime factorisation of a divisor of $a$ and $b$ but absent in the prime factorisations of $a$ and $b$, then its power must be 0. Let some multiple $p\cdot l$ divide $a$ and $b$, this means that $p\mid a$ and $p\mid b$, which is a contradiction. This shows that every common divisor should be of the form $p_1^{k_1}\cdots p_r^{k_r}$ with each $k\geqslant 0$. For that to be greater than $p_1^{\min(i_1,j_1)}\cdots p_r^{\min(i_r,j_r)}$, we would need to have some $k_m>\min(i_m,j_m)$. Without the loss of generality, let $\min(i_m, j_m) = i_m$. But that means that any integer multiple of our "new" gcd will have $p_m$ with a power greater than the one present in $a$, meaning it cannot divide $a$, which is a contradiction.

2. Define the notion of least common multiple, and express the least common multiple of $m, n$ as a product $p_1^{k_1} \cdots p_r^{k_r}$ with integers $k_v \geqslant 0$. Express $k_v$ in terms of $i_v$ and $j_v$.

   We define the least common multiple of $a$ and $b$ to be the lowest natural number divisible by both $a$ and $b$. With analogous reasoning, we get that the least common multiple of $m$ and $n$ which are mentioned in the previous part of this exercise is $p_1^{\max(i_1,j_1)} \cdots p_r^{\max(i_r,j_r)}$. Where $\max : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is defined as follows:

$$\max(a,b) = \begin{cases} a, & a \geqslant b \\ b, & a < b \end{cases}$$

## Exercise 3

Find the g.c.d. and l.c.m. of the following pairs of positive integers:

1. $5^3 2^6 3$ and 225.

   $\gcd(5^3 2^6 3, 225) = 75$, $\operatorname{lcm}(5^3 2^6 3, 225) = 72000$.

2. 248 and 48.

   $\gcd(248, 48) = 8$, $\operatorname{lcm}(248, 48) = 1488$.

## Exercise 4

Let $n$ be an integer $\geqslant 2$.

1. Show that any integer $x$ is congruent mod $n$ to a unique integer $m$ such that $0 \leqslant m < n$.

By contradiction let $x$ be congruent to $m_1, m_2$ with $0 \leqslant m_1 < m_2 < n$. By symmetry and transitivity we have that $m_1$ and $m_2$ are congruent, i.e., $m_2 - m_1$ divides $n$. But $0 \leqslant m_2 - m_1 < n$ and there is only one multiple of $n$ satisfying that double inequality, namely, 0. But $m_2 - m_1 = 0$ contradicts the definitions of $m_1$ and $m_2$. Hence such $m$ is unique.

## 2.4 Algebra by Waerden, Chapter 9

### Exercise 9.1

For the set of pairs of natural numbers $(a, b)$ define an order relation as follows: $(a, b) < (a', b')$ if either $a < a'$ or $a = a'$ and $b < b'$. Prove that this defines a well-ordering.

We start by proving that $<$ is a total ordering for pairs of natural numbers.

We first show that if $(a, b) \neq (a', b')$, i.e., $a \neq a'$ or $b \neq b'$, then we have either $(a, b) < (a', b')$ or $(a', b') < (a, b)$ by considering 3 cases. In the first case, $a < a'$, which immediately implies $(a, b) < (a', b')$. In the second case $a' < a$, which immediately implies $(a', b') < (a, b)$. In the third case, $a = a'$. We then introduce 2 subcases: $b < b'$ or $b' < b$. In the first subcase, $(a, b) < (a', b')$ and in the second subcase $(a', b') < (a, b)$. Hence in every case we have either $(a, b) = (a', b')$, $(a, b) < (a', b')$ or $(a', b') < (a, b)$.

We now show that the statements $(a, b) < (a', b')$, $(a, b) = (a', b')$ and $(a', b') < (a, b)$ are mutually exclusive (i.e., any pair of these cannot occur simultaneously). If $(a, b) = (a', b')$ and $(a, b) < (a', b')$, then we have $a = a'$ and $b = b'$ implied by $(a, b) = (a', b')$, but at the same time $(a, b) < (a', b')$ implies that either $a < a'$ or $a = a'$ and $b < b'$. Since $a < a'$ is not true, we have $b < b'$, which contradicts $b = b'$. Hence $(a, b) = (a', b')$ and $(a, b) < (a', b')$ cannot happen at the same time. Due to symmetry, we also can't have $(a, b) = (a', b')$ and $(a', b') < (a, b)$ at the same time. Finally, let $(a, b) < (a', b')$ and $(a', b') < (a, b)$. If $a < a'$, then we can't have $(a', b') < (a, b)$ and, similarly, if $a' < a$, then we can't have $(a, b) < (a', b')$. Therefore we must have $a = a'$. According to $(a, b) < (a', b')$, $b < b'$, whereas $b' < b$ according to $(a', b') < (a, b)$, which is a contradiction. Hence all of these are mutually exclusive.

To end the proof of total order, we show transitivity. Assume $(a, b) < (c, d)$ and $(c, d) < (e, f)$. If either $a < c$ or $c < e$ is true, then $a < e$ and $(a, b) < (e, f)$. If $a = c$ and $c = e$, then we must have $b < d$ and $d < f$, meaning $b < f$ and $(a, b) < (e, f)$. In either case, transitivity is present.

Now that we have shown $<$ to be a total ordering on the set of pairs of natural numbers, the rest is to prove it is a well-ordering. Take an arbitrary subset $\{(a_1, b_1), \ldots, (a_k, b_k)\}$ of the set of pairs of natural numbers. Let $a_i$ be the first element of $\{a_1, \ldots, a_k\}$ and take every pair whose first entry is $a$. Let $b_i$ be the first element of the set of second entries of the pairs with first entry $a$. (Notice that each $b_i$ is distinct.) Our claim is that $(a_i, b_i)$ is the first element of $\{(a_1, b_1), \ldots, (a_k, b_k)\}$. Take any $1 \leqslant j \leqslant k$ with $j \neq i$, then we have two cases: $a_i < a_j$ or $a_i = a_j$. In the first case we immediately have $(a_i, b_i) < (a_j, b_j)$. In the second case, we have $b_i < b_j$ and $(a_i, b_i) < (a_j < b_j)$ still. Hence the first element exists for evert nonempty subset, meaning the set of pairs of natural numbers is well-ordered with $<$.

## Exercise 9.2

In a well-ordered set, show that each element $a$ (with exception of the last element of the set if such is present) has an "immediate successor" $b > a$, so that there is no $x$ between $b$ and $a$ (that is, no $x$ such that $b > x > a$). Does each element with exception of the first also have an immediate predecessor?

Take the subset containing every element $b_i$ that's $> a$. (We are sure that this subset is nonempty since $a$ is not the last element.) Due to the set being well-ordered, there is a first element $b$ of that set. We claim $b$ to be the immediate successor of $a$. By contradiction, assume there existed $b > x > a$, but then the definition of $b$ would be violated, meaning there is no such $x$, therefore $b$ is an immediate successor of $a$.

Existence of immediate predecessors for each element is not necessarily true since existence of the last element in each nonempty subset is not guaranteed. (As a counterexample consider the set of natural numbers with partial order $<$ defined as follows: If $a, b$ have the same parity, then compare them with usual $<$ already defined for natural numbers, but if $a$ is odd and $b$ is even, then $a < b$ and vice versa. 2 does not have a predecessor in this case.)

## 2.5 Definitions

**Definition 1** (Relation). *A binary relation $R$ on a set $X$ is a subset of $X \times X$. $(x, y) \in R$ may be written as $xRy$.*

**Definition 2** (Diagonal relation). *The diagonal relation defined on a set $X$ and denoted by $\Delta_X$ is the set $\{(x, x) : x \in X\}$.*

**Definition 3** (Reflexivity). *A relation $R$ on $X$ is reflexive iff $\Delta_X \subseteq R$, i.e., $xRx$ for all $x \in X$.*

**Definition 4** (Antisymmetry). *A relation $R$ on $X$ is antisymmetric iff $x = y$ given $xRy$ and $yRx$ for all $x, y \in X$.*

**Definition 5** (Transitivity). *A relation $R$ on $X$ is transitive iff $xRz$ given $xRy$ and $yRz$ for all $x, y, z \in X$.*

**Definition 6** (Partial ordering, partially ordered set). *A relation $R$ on $X$ satisfying reflexivity, antisymmetry and transitivity is called a partial ordering on $X$ and $X$ considered with that relation, which we may denote as $(X, R)$, is called a partially ordered set or poset for short.*

**Definition 7** (Comparability). *Two elements $a, b \in X$ are comparable under a relation $R$ defined on $X$ iff $aRb$ or $bRa$.*

**Definition 8** (Chain). *A subset $A$ of a partially ordered set $X$ is a chain iff any two elements from $A$ are comparable.*

**Definition 9** (Chain width). *The chain width of a partially ordered set $X$ is the minimum number of blocks in a partition consisting of chains.*

**Definition 10** (Anti-chain). *A subset $A$ of a partially ordered set $X$ is an anti-chain iff none of the elements from $A$ are comparable.*

**Definition 11** (Anti-chain width). *The anti-chain width of a partially ordered set $X$ is the minimum number of blocks in a partition consisting of anti-chains.*

**Definition 12** (Total ordering, totally ordered set). *$X$ is totally ordered by $R$ and $R$ is a total ordering on $X$ iff $X$ is a chain.*

**Definition 13** (Neighbours). *Let $P$ be a poset. $x \in P$ is called a lower neighbour of $y \in P$ and $y$ is an upper neighbour of $x$ iff $x < y$ and there is no $z \in P$ with $x < z < y$.*

**Definition 14** (Upper/Lower bound). *An element $c \in X$ is called an upper bound of a subset $A$ of $(X, \leq)$ iff $a \leq c$ for all $a \in A$.*

*$c \in X$ is called a lower bound of $A$ iff $c \leq a$ for all $a \in A$.*

**Definition 15.** *First/maximal and last/minimal elements of a poset are respectively the unique lower and upper bounds of the entire set.*

**Definition 16** (Supremum/Infimum). *$\sup A$ with $A \subseteq (X, \leqslant)$ is an element which is simultaneously an upper bound of $A$ and a lower bound of the set containing the upper bounds of $A$.*

*$\inf A$ is an element which is simultaneously an lower bound of $A$ and an upper bound of the set containing the lower bounds of $A$.*

Some authors use the terms least upper bound and greatest lower bound to refer to supremum and infimum respectively.

**Definition 17** (Lattice). *$(X, \leqslant)$ is a lattice iff $\sup\{a, b\}$ and $\inf\{a, b\}$ exist for any $a, b \in X$.*

**Definition 18** (Bounded lattice). *A lattice is bounded iff it has the first element and the last element.*

**Definition 19** (Complete lattice). *A lattice is complete iff every its subset has a supremum and an infimum.*

**Definition 20** (Filters). *A filter $F$ of a poset $(X, \leqslant)$ is a nonempty set such that if $x \in F$ and $y \leqslant x$, then $y \in F$.*

**Definition 21** (Order functions). *Let $(X_1, \leq_1)$ and $(X_2, \leq_2)$ be posets and $f : X_1 \to X_2$ be a function.*

*$f$ is order preserving iff $x \leq_1 y$ implies $f(x) \leq_2 f(y)$ for all $x, y \in X_1$.*

*$f$ is order reflecting iff $f(x) \leq_2 f(y)$ implies $x \leq_1 y$ for all $x, y \in X_1$.*

*$f$ is order embedding iff it is order preserving and order embedding*

*$f$ is an order isomorphism iff it is order embedding and bijective. $(X_1, \leq_1)$ and $(X_2, \leq_2)$ are isomorphic posets if such $f$ exists.*

**Definition 22** (Rank function). *A function $r : P \to \mathbb{N}$ where $P$ is a poset is called a rank function on $P$ if it is order-preserving and $r(y) = r(x) + 1$ where $y \in P$ is an upper-neighbour of $x \in P$.*

**Definition 23** (Graded poset). *A poset with a rank function is called a graded poset.*

**Definition 24** (Local finiteness). *A poset $(P, \leq)$ is locally finite iff for all $x, y \in P$ with $x \leq y$ there exist finitely many $z \in P$ with $x \leq z \leq y$.*

**Definition 25** (Differential poset). *A poset $P$ is $r$-differential iff it is graded, locally finite, for all $x, y \in P$ the amounts of upper neighbours and lower neighbours of both $x$ and $y$ are the same and any element has $r$ more upper neighbours than lower neighbours.*

**Definition 26** (Differential lattice). *A poset is a differential lattice iff it is a differential poset and a lattice at the same time.*

# Chapter 3

# Boolean algebra

## 3.1 Week 3 Central Exercises

### Exercise 1.1

Fill in the following table for $x, y \in \{0, 1\}$.

| $x$ | $y$ | $xy$ | $x \oplus y$ | $x + y$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 |

### Exercise 1.2

Write down the complete truth table for the functions:

1. $f(x, y, z) = (x \oplus (\neg y \oplus z)) \wedge ((x \vee \neg z) \wedge y)$

| $x$ | $y$ | $z$ | $f(x, y, z)$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 |

2. $f(x, y, z) = (\neg x \vee (y \wedge \neg z)) \oplus ((x \oplus z) \wedge \neg y)$

| $x$ | $y$ | $z$ | $f(x, y, z)$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 |

## Exercise 1.3

Calculate the following in $\mathbb{Z}_2$.

1. $[0] + [3] \cdot [5] = [0] + [1] \cdot [1] = [0] + [1 \cdot 1] = [0] + [1] = [0 + 1] = [1]$

2. $[1]+[141]\cdot[1501] = [1]+[1]\cdot[1] = [1]+[1\cdot1] = [1]+[1] = [1+1] = [2] = [0]$

3. $[501] + [-7] \cdot [10^{41}] = [1] + [1] \cdot [0] = [1] + [1 \cdot 0] = [1] + [0] = [1 + 0] = [1]$

4. $[1717]^3 + [-6] \cdot [1567] = [1]^3 + [0] \cdot [1] = [1 \cdot 1 \cdot 1] + [0 \cdot 1] = [1] + [0] = [1 + 0] = [1]$

   [We haven't really defined exponentiation of equivalence classes, so I have assumed it is short for repetitive multiplication.]

## Exercise 1.4

Solve the following in $\mathbb{Z}_2$.

1. $x + [19] = [1]$ Say $x = [a]$ for some $a \in \mathbb{Z}$, then we have

$$\begin{aligned} [a] + [19] &= [1] \\ [a] + [1] &= [1] \\ [a+1] &= [1] \\ a + 1 &\equiv 1 \mod 2 \\ a &\equiv 0 \mod 2 \\ x &= [0] \end{aligned}$$

2. $[1] - x = [12]$

   We haven't really defined subtraction of congruence classes, so I will assume $-[a] = [-a]$.

   Let $x = [a]$ for some $a \in \mathbb{Z}$, then

$$\begin{aligned} [1] - [a] &= [12] \\ [1] + [-a] &= [0] \\ [1-a] &= [0] \\ 1 - a &\equiv 0 \mod 2 \\ a &\equiv 1 \mod 2 \\ x &= [1] \end{aligned}$$

3. $x \cdot [9] = [10]$ Let $x = [a]$ for some $a \in \mathbb{Z}$, then

$$\begin{aligned} [a] \cdot [9] &= [10] \\ [a] \cdot [1] &= [0] \\ [a \cdot 1] &= [0] \\ x = [a] &= [0] \end{aligned}$$

4. $[3] \cdot x = [13]$ Let $x = [a]$ for some $a \in \mathbb{Z}$, then

$$\begin{aligned}
[3] \cdot [a] &= [13] \\
[1] \cdot [a] &= [1] \\
[1 \cdot a] &= [1] \\
x = [a] &= [1]
\end{aligned}$$

5. $x^3 + [3] \cdot x^2 + [4] = [126]$ Let $x = [a]$ for some $a \in \mathbb{Z}$, then

$$\begin{aligned}
[a]^3 + [3] \cdot [a]^2 + [4] &= [126] \\
[a^3] + [1] \cdot [a^2] + [0] &= [0] \\
[a^3 + a^2] &= [0] \\
[a]^2 \cdot [a+1] &= [0]
\end{aligned}$$

   Note that both $a \equiv 0 \mod 2$ and $a \equiv 1 \mod 2$ work, so any $x \in \mathbb{Z}_2$ is a solution.

6. $[2] \cdot x^7 + x^2 + [4] = [4567]$ Let $x = [a]$ for some $a \in \mathbb{Z}$, then

$$\begin{aligned}
[2] \cdot [a]^7 + [a]^2 + [4] &= [4567] \\
[0] \cdot [a^7] + [a^2] + [0] &= [1] \\
[0 \cdot a^7] + [a^2 + 0] &= [1] \\
[0] + [a^2] &= [1] \\
[0 + a^2] &= [1] \\
[a^2] &= [1]
\end{aligned}$$

   Here comes the fact that you may yourself verify that $a^2 \equiv a \mod 2$, so we have $x = [a] = [a^2] = [1]$.

## Exercise 2.1

Find corresponding $A_x$ for

1. $x = (1, 0, 0)$, $A_x = \{1\}$

2. $x = (1, 1, 1)$, $A_x = \{1, 2, 3\}$

3. $x = (1, 0, 1)$, $A_x = \{1, 3\}$

4. $x = (1, 1, 1, 1)$, $A_x = \{1, 2, 3, 4\}$

5. $x = (1, 0, 0, 1, 1, 0)$, $A_x = \{1, 4, 5\}$

6. $x = (0, 1, 0, 1, 1)$, $A_x = \{2, 4, 5\}$

## Exercise 2.2

Verify the usual rules for $(B(n), +, \cdot)$ such as commutativity, associativity, and distributivity and show furthermore that

1. $x + \overline{x} = 1$

2. $x + x = x$

3. $x \cdot \overline{x} = 0$

4. $x \cdot x = x$

5. $x + xy = x(x + y) = x$

See Exercise 11.1 of the next section (Aigner, Chapter 11).

## Exercise 3.1

For a Boolean algebra $\mathcal{P}(S)$, what is the unit element, zero element, complement of the unit element and a complement of the zero element?

Which operations are addition and multiplication hasn't been specified, although the identity elements of $\cup$ and $\cap$ are $\varnothing$ and $S$ respectively with them being the complements of one another.

### Exercise 4.1

Find the Hamming distance between

1. $(1, 0, 0, 0)$ and $(0, 0, 0, 0)$

   The Hamming distance here is 1.

2. $(1, 0, 0, 1, 1, 0)$ and $(0, 1, 0, 1, 1, 0)$

   The Hamming distance here is 2.

### Exercise 4.2

The Hamming weight of $x \in B(n)$ is defined as $\Delta(x, 0)$, where 0 denotes the zero word. Show that for any two words $a, b \in B(n)$, Hamming weight of $a \oplus b$ is equal to $\Delta(a, b)$.

Let $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ with $a_1, \dots, a_n, b_1, \dots, b_n \in \{0, 1\}$, then

$$a \oplus b = (a_1 \oplus b_1, \dots, a_n \oplus b_n)$$

The Hamming weight of $a \oplus b$ is thus the amount of $k \in \{1, \dots, n\}$ such that $a_k \oplus b_k \neq 0$, i.e., $a_k \oplus b_k = 1$. Note that this happens if and only if $a_k = 1$ and $b_k = 0$ or $b_k = 0$ and $a_k = 1$, which is equivalent to saying $a_k \neq b_k$. The amount of such $k$ is precisely defined to be $\Delta(a, b)$.

## 3.2 Week 4 Central Exercises

### Exercise 1

Interpret the following Boolean functions with two variables as logical expressions.

| $x$ | $y$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ | $f_9$ | $f_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |

See Exercise 11.7 of the following section. (Discrete Mathematics by Martin Aigner, Chapter 11)

## Exercise 2

Write down the complete truth table for the functions:

1. $f(x, y, z) = (x \to y) \wedge ((y \wedge \neg z) \to (x \vee z))$;

| $x$ | $y$ | $z$ | $f(x, y, z)$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 |

2. $f(x, y, z) = ((\neg x \oplus \neg y) \wedge z) \vee ((x \oplus z) \to y)$;

| $x$ | $y$ | $z$ | $f(x, y, z)$ |
|---|---|---|---|
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 |

3. $f(x, y, z) = ((\neg y \to x) \vee \neg z) \to ((y \oplus z) \wedge \neg x)$;

| $x$ | $y$ | $z$ | $f(x,y,z)$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 0 |

4. $f(x,y,z) = ((\neg x \oplus z) \to \neg y) \to ((x \vee y) \wedge \neg z)$.

| $x$ | $y$ | $z$ | $f(x,y,z)$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 |

## Exercise 3.1

Let $f : B(3) \to \{0,1\}$ be defined by

1. $f(0,0,0) = f(0,1,1) = 0$ and 1 otherwise;
2. $f(1,1,1) = f(1,0,1) = 0$ and 1 otherwise;
3. $f(1,0,1) = f(0,1,1) = 0$ and 1 otherwise;
4. $f(1,0,1) = f(0,0,1) = 0$ and 1 otherwise.

Determine the disjunctive normal form (DNF) and conjunctive normal form (CNF) and find a simpler representation.

For (1), we have DNF as

$$f(x,y,z) = xyz + xy\overline{z} + x\overline{y}z + x\overline{y}\,\overline{z} + \overline{x}y\overline{z} + \overline{x}\,\overline{y}z$$

And CNF as

$$f(x,y,z) = (x+y+z)(x+\overline{y}+\overline{z})$$

From CNF, it follows that

$$f(x,y,z) = x + (y+z)(\overline{y}+\overline{z}) = x + y\overline{y} + y\overline{z} + \overline{y}z + z\overline{z} =$$

$$= x + y\overline{z} + \overline{y}z = x + y \oplus z$$

Which is the simplest form of this $f$.

For (2), we have DNF as

$$f(x,y,z) = xy\overline{z} + x\overline{y}\,\overline{z} + \overline{x}yz + \overline{x}y\overline{z} + \overline{x}\,\overline{y}z + \overline{x}\,\overline{y}\,\overline{z}$$

And CNF as

$$f(x,y,z) = (\overline{x}+y+\overline{z})(\overline{x}+\overline{y}+\overline{z})$$

From CNF, it follows that

$$f(x,y,z) = \overline{x} + \overline{z} + y\overline{y} = \overline{x} + \overline{z} = \overline{xz}$$

Which is the simplest form of this $f$.

For (3), we have DNF as

$$f(x,y,z) = xyz + xy\overline{z} + x\overline{y}\,\overline{z} + \overline{x}y\overline{z} + \overline{x}\,\overline{y}z + \overline{x}\,\overline{y}\,\overline{z}$$

And CNF as

$$f(x,y,z) = (x+\overline{y}+\overline{z})(\overline{x}+y+\overline{z})$$

From CNF, it follows that

$$f(x,y,z) = (x+\overline{y})(\overline{x}+y) + \overline{z} = x\overline{x} + xy + \overline{xy} + y\overline{y} + \overline{z} =$$

$$= \overline{x \oplus y} + \overline{z} = \overline{(x \oplus y) \cdot z}$$

Which is the simplest form of this $f$.

For (4), we have DNF as

$$f(x, y, z) = xyz + xy\overline{z} + x\overline{y}\,\overline{z} + \overline{x}yz + \overline{x}y\overline{z} + \overline{x}\,\overline{y}\,\overline{z}$$

And CNF as

$$f(x, y, z) = (x + y + \overline{z})(\overline{x} + y + \overline{z})$$

From CNF, it follows that

$$f(x, y, z) = x\overline{x} + y + \overline{z} = y + \overline{z}$$

## Exercise 3.2

Determine DNF and CNF of a function $f : B(3) \to \{0, 1\}$ defined by $f(1, 1, 1) = f(0, 0, 0) = f(1, 1, 0) = f(0, 1, 0) = 0$ and 1 otherwise.

For DNF, we have

$$f(x, y, z) = x\overline{y}z + x\overline{y}\,\overline{z} + \overline{x}yz + \overline{x}\,\overline{y}z$$

For CNF, we have

$$f(x, y, z) = (x + y + z)(x + \overline{y} + z)(\overline{x} + \overline{y} + z)(\overline{x} + \overline{y} + \overline{z})$$

## Exercise 4

Recall that we defined a relation $\leq$ on $B(n)$ by the following rule: for $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ we set

$$x \leq y \iff x_i \leq y_i \text{ for all } i$$

1. Show that the relation $\leq$ is indeed a partial order.

Reflexivity holds as $x_i \leq x_i$ for any $i \in \{1, \ldots, n\}$ and $x_i \in \{0, 1\}$, so $x \leq x$ for any $x \in B(n)$. (We can say the reflexivity is inherited from $\leq$ defined on $\{0, 1\}$.)

For antisymmetry, let $x \leq y$ and $y \leq x$, then we have $x_i \leq y_i$ and $y_i \leq x_i$ for all $i$, but that means that $x_i = y_i$ via antisymmetry of $\leq$ defined on $\{0, 1\}$ and therefore $x = y$.

For transitivity, let $x \leq y$ and $y \leq z$, then $x_i \leq y_i$ and $y_i \leq z_i$ for all $i$, therefore $x_i \leq z_i$ for all $i$ via transitivity of $\leq$ defined on $\{0, 1\}$ and thus $x \leq z$.

Find a supremum and an infimum for the following sets. [See the end of this exercise for the method of calculating the supremums and infimums.]

2. $\{(1, 0, 1), (1, 0, 0), (0, 1, 0)\}$ in $B(3)$;

$$\sup\{(1, 0, 1), (1, 0, 0), (0, 1, 0)\} = (1, 1, 1)$$
$$\inf\{(1, 0, 1), (1, 0, 0), (0, 1, 0)\} = (0, 0, 0)$$

3. $\{(1, 0, 0, 1), (1, 1, 0, 0), (0, 0, 0, 0)\}$ in $B(4)$;

$$\sup\{(1, 0, 0, 1), (1, 1, 0, 0), (0, 0, 0, 0)\} = (1, 1, 0, 1)$$
$$\inf\{(1, 0, 0, 1), (1, 1, 0, 0), (0, 0, 0, 0)\} = (0, 0, 0, 0)$$

4. $\{(1, 0, 0, 1, 1), (1, 1, 0, 0, 1), (1, 1, 1, 1, 1)\}$ in $B(5)$.

$$\sup\{(1, 0, 0, 1, 1), (1, 1, 0, 0, 1), (1, 1, 1, 1, 1)\} = (1, 1, 1, 1, 1)$$
$$\inf\{(1, 0, 0, 1, 1), (1, 1, 0, 0, 1), (1, 1, 1, 1, 1)\} = (1, 0, 0, 0, 1)$$

Can we find an infimum and supremum for any non-empty subset $S \subseteq B(n)$? Why? And if yes, how?

We have shown that $x \leq y$ if and only if $A_x \subseteq A_y$ and since the mapping $B(n) \to B(S)$ given by $x \mapsto A_x$ is a bijection, we have that the posets $(B(n), \leq)$ and $(B(S), \subseteq)$ are isomorphic. Since the latter is a lattice, we have that every finite subset of $B(n)$ has a supremum and infimum in $B(n)$. There are no infinite subsets in $B(n)$, so we are done.

Since supremum and infimum of $A, B \in B(S)$ are $A \cap B$ and $A \cup B$, we have that supremum and infimum of $\{x, y\} \subseteq B(n)$ are $xy$ and $x + y$. The final result is yielded via induction.

## Exercise 5

By using the equivalence transformations show, that the following equations are the same:

1. $(x \oplus y) \vee ((\neg x \wedge z) \to (y \vee \neg x)) = 1$

$$\begin{aligned}
(x \oplus y) \vee ((\neg x \wedge z) \to (y \vee \neg x)) &= (x \oplus y) \vee (\neg(\neg x \wedge z) \vee (y \vee \neg x)) \\
&= (x \oplus y) \vee x \vee \neg z \vee y \vee \neg x \\
&= (x \oplus y) \vee \neg z \vee x \vee y \vee \neg x \\
&= (x \oplus y) \vee \neg z \vee y \vee x \vee \neg x \\
&= (x \oplus y) \vee \neg z \vee y \vee 1 \\
&= 1
\end{aligned}$$

2. $(x \wedge y) \vee x \wedge (\neg y \to z) \vee y \wedge (y \vee z) = y \vee (x \wedge z)$

$$\begin{aligned}
(x \wedge y) \vee x \wedge (\neg y \rightarrow z) \vee y \wedge (y \vee z) &= (x \wedge y) \vee x \wedge (y \vee z) \vee y \wedge (y \vee z) \\
&= (x \wedge y) \vee x \wedge (y \vee z) \vee y \\
&= x \wedge (y \vee z) \vee y \\
&= (x \vee y) \wedge ((y \vee z) \vee y) \\
&= (x \vee y) \wedge ((z \vee y) \vee y) \\
&= (x \vee y) \wedge (z \vee (y \vee y)) \\
&= (x \vee y) \wedge (z \vee y) \\
&= (x \wedge z) \vee y \\
&= y \vee (x \wedge z)
\end{aligned}$$

3. $((x \wedge \neg y) \wedge (\neg z \rightarrow (y \wedge t)) \vee (\neg x \wedge \neg y)) \wedge z = \neg y \wedge z$

$$\begin{aligned}
&((x \wedge \neg y) \wedge (\neg z \rightarrow (y \wedge t)) \vee (\neg x \wedge \neg y)) \vee z \\
=&((x \wedge \neg y) \wedge (\neg\neg z \vee (y \wedge t)) \vee (\neg x \wedge \neg y)) \wedge z \\
=&((x \wedge \neg y) \wedge (z \vee (y \wedge t)) \vee (\neg x \wedge \neg y)) \wedge z \\
=&((((x \wedge \neg y) \vee (\neg x \wedge \neg y)) \wedge ((z \vee (y \wedge t)) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&((((x \vee \neg x) \wedge \neg y) \wedge ((z \vee (y \wedge t)) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&(((1 \wedge \neg y) \wedge ((z \vee (y \wedge t)) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&((\neg y \wedge ((z \vee (y \wedge t)) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&((((\neg y \wedge (z \vee (y \wedge t))) \vee (\neg y \wedge (\neg x \wedge \neg y))))) \wedge z \\
=&((((\neg y \wedge (z \vee (y \wedge t))) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&((((((\neg y \wedge z) \vee (\neg y \wedge y \wedge t))) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&((((((\neg y \wedge z) \vee (0 \wedge t))) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&((((((\neg y \wedge z) \vee 0)) \vee (\neg x \wedge \neg y)))) \wedge z \\
=&(((\neg y \wedge z)) \vee (\neg x \wedge \neg y)) \wedge z \\
=&(((z \wedge \neg y)) \vee (\neg x \wedge \neg y)) \wedge z \\
=&(z \vee \neg x) \wedge \neg y \wedge z \\
=&\neg y \wedge (z \vee \neg x) \wedge z \\
=&\neg y \wedge z
\end{aligned}$$

## 3.3 Discrete Mathematics by Martin Aigner, Chapter 11

### Exercise 11.1

Verify the usual rules for $(\mathcal{B}(n), +, \cdot)$ such as commutativity, associativity, and distributivity and show furthermore that $\mathbf{x}+\overline{\mathbf{x}} = \mathbf{1}$, $\mathbf{x}+\mathbf{x} = \mathbf{x}$, $\mathbf{x}\cdot\overline{\mathbf{x}} = 0$, $\mathbf{x}\cdot\mathbf{x} = \mathbf{x}$, $\mathbf{x}+\mathbf{x}\mathbf{y} = \mathbf{x}(\mathbf{x}+\mathbf{y}) = \mathbf{x}$.

We first show that associativity, commutativity of $+$ and $\cdot$ and distrbutivity of $\cdot$ over $+$ holds for $x, y \in \{0, 1\}$. Commutativity follows from the symmetry in the tables defining the operations, and associativity is demonstrated below: If $x = 0$, then $(x+y)+z = (0+y)+z = y+z+0+(y+z) = x+(y+z)$. If $y = 0$, then $(x+y)+z = (x+0)+z = x+z = x+(0+z) = x+(y+z)$. If $z = 0$, then $(x+y)+z = (x+y)+0 = x+y = x+(y+0) = x+(y+z)$. Finally, if $x, y, z = 1$, then $(1+1)+1 = 1+1 = 1+(1+1)$.

For associativity of multiplication, we do the same. If $x = 0$, then $(0\cdot y)\cdot z = 0\cdot z = 0 = 0\cdot(y\cdot z) = x\cdot(y\cdot z)$. If $y = 0$, then $(x\cdot y)\cdot z = (x\cdot 0)\cdot z = 0\cdot z = 0 = x\cdot 0 = x\cdot(0\cdot z) = x\cdot(y\cdot z)$. If $z = 0$, then $(x\cdot y)\cdot z = (x\cdot y)\cdot 0 = 0 = x\cdot 0 = x\cdot(y\cdot 0) = x\cdot(y\cdot z)$. Finally, if $x, y, z = 1$, then $(1\cdot 1)\cdot 1 = 1\cdot 1 = 1\cdot(1\cdot 1)$.

For distributivity, consider the following cases: $x = 0$ or $x = 1$

In the first case, $x\cdot(y+z) = 0\cdot(y+z) = 0 = 0+0 = 0\cdot y+0\cdot z = x\cdot y+x\cdot z$

In the second case, $x\cdot(y+z) = 1\cdot(y+z) = y+z = 1\cdot y+1\cdot z = x\cdot y+x\cdot z$

(Commutativity of $\cdot$ takes care of the right-distributivity.)

Now we show the same properties but for vectors taken from $\mathcal{B}(n)$ for a fixed $n \in \mathbb{Z}_{>0}$. Let $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$ and $\mathbf{z} = (z_1, \ldots, z_n)$

with $x_1, \ldots, x_k, y_1, \ldots, y_n, z_1, \ldots, z_n \in \{0,1\}$. Then we have

$$\begin{aligned}
\mathbf{x}+\mathbf{y} &= (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1+y_1, \ldots, x_k+y_n) = \\
&= (y_1+x_1, \ldots, y_n+x_n) = (y_1, \ldots, y_n) + (x_1, \ldots, x_n) = \mathbf{y}+\mathbf{x} \\
(\mathbf{x}+\mathbf{y})+\mathbf{z} &= ((x_1, \ldots, x_n) + (y_1, \ldots, y_n)) + (z_1, \ldots, z_n) = \\
&= (x_1+y_1, \ldots, x_n+y_n) + (z_1, \ldots, z_n) = \\
&= ((x_1+y_1)+z_1, \ldots, (x_n+y_n)+z_n) = \\
&= (x_1+(y_1+z_1), \ldots, x_n+(y_n+z_n)) = \\
&= (x_1, \ldots, x_n) + (y_1+z_1, \ldots y_n+z_n) = \\
&= (x_1, \ldots, x_n) + ((y_1, \ldots, y_k) + (z_1, \ldots, z_k)) = \mathbf{x}+(\mathbf{y}+\mathbf{z}) \\
\mathbf{xy} &= (x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n) = \\
&= (y_1x_1, \ldots, y_nx_n) = (y_1, \ldots, y_n)(x_1, \ldots, x_n) = \mathbf{yx} \\
\mathbf{x}(\mathbf{y}+\mathbf{z}) &= (x_1, \ldots, x_n)(y_1+z_1, \ldots, y_n+z_n) = \\
&= (x_1(y_1+z_1), \ldots, x_n(y_n+z_n)) = \\
&= (x_1y_1+x_1z_1, \ldots, x_ny_n+x_nz_n) = \mathbf{xy}+\mathbf{xz}
\end{aligned}$$

(Commutativity of multiplication forces right-distributivity once again.)

For the other properties, consider

$$\begin{aligned}
&0+\overline{0} = 0+1 = 1 \\
&1+\overline{1} = 1+0 = 1 \\
&\mathbf{x}+\overline{\mathbf{x}} = (x_1, \ldots, x_n) + (\overline{x_1}, \ldots, \overline{x_n}) = (x_1+\overline{x_1}, \ldots, x_n+\overline{x_n}) = (1, \ldots, 1) = \mathbf{1}
\end{aligned}$$

$$\begin{aligned}
&0+0 = 0 \\
&1+1 = 1 \\
&\mathbf{x}+\mathbf{x} = (x_1+x_1, \ldots, x_n+x_n) = (x_1, \ldots, x_n) = \mathbf{x}
\end{aligned}$$

$$\begin{aligned}
&0 \cdot \overline{0} = 0 \cdot 1 = 0 \\
&1 \cdot \overline{1} = 1 \cdot 0 = 0 \\
&\mathbf{x} \cdot \overline{\mathbf{x}} = (x_1 \cdot \overline{x_1}, \ldots, x_n \cdot \overline{x_n}) = (0, \ldots, 0) = \mathbf{0}
\end{aligned}$$

$$
\begin{aligned}
0 \cdot 0 &= 0 \\
1 \cdot 1 &= 1 \\
\mathbf{x} \cdot \mathbf{x} &= (x_1 \cdot x_1, \ldots, x_n \cdot x_n) = (x_1, \ldots, x_n) = \mathbf{x}
\end{aligned}
$$

$$
\begin{aligned}
x + xy &= xx + xy = x(x + y) \\
x + x \cdot 0 &= x + 0 = x \\
x + x \cdot 1 &= x + x = x \\
\mathbf{x} + \mathbf{x}\mathbf{y} &= (x_1 + x_1 y_1, \ldots, x_n + x_n y_n) = (x_1(x_1 + y_1), \ldots, x_n(x_n + y_n)) = \mathbf{x}(\mathbf{x} + \mathbf{y}) \\
\mathbf{x} + \mathbf{x}\mathbf{y} &= (x_1 + x_1 y_1, \ldots, x_n + x_n y_n) = (x_1, \ldots, x_n) = \mathbf{x}
\end{aligned}
$$

## Exercise 11.2

Are the following statements consistent or inconsistent? [The author has not defined consistency, so I have assumed it means that the conjunction is satisfiable.]

1. $A_1 = \{(x \to y) \to z, (\neg x \vee y) \to (y \wedge z), z \to (\neg x \to y)\}$

   As shown below, all of the statements are satisfied when $x = 1$, $y = 0$ and $z = 0$:

$$
\begin{aligned}
(x \to y) \to z &= (1 \to 0) \to z = 0 \to z = 1 \\
(\neg x \vee y) \to (y \wedge z) &= (\neg 1 \vee 0) \to (0 \wedge z) = (0 \vee 0) \to 0 = 0 \to 0 = 1 \\
z \to (\neg x \to y) &= z \to (\neg 1 \to 0) = z \to 1 = 1
\end{aligned}
$$

2. $A_1 \cup \{\neg(y \to z)\}$

   The example provided in part 1 does not work here as $y \to z$ would be $0 \to 0$, which is 1 and $\neg 1 = 0$. Therefore, if we were to assume that this new set is consistent, then $(x, y, z)$ which satisfies it should be different from $(1, 0, 0)$, i.e., one of $x = 0$ or $y = 1$ or $z = 1$ is required for such $(x, y, z)$.

Let $x = 0$, then $(x \to y) \to z = (0 \to y) \to z = 1 \to z = z$, so we want $z = 1$. Since $z$ implies $\neg x \to y$, it should also be true, i.e., $\neg x \to y = 1 \to y = y = 1$. But then $\neg(y \to z) = \neg(1 \to 1) = \neg 1 = 0$, which is a contradiction.

Let $y = 1$, then $\neg(y \to z) = y \wedge \neg z = 1 \wedge \neg z = \neg z = 1$ and $z = 0$. We also have $(\neg x \vee y) \to (y \wedge z) = (x \vee 1) \to (1 \wedge 0) = 1 \to 0 = 0$, which is a contradiction.

Let $z = 1$, then $\neg(y \to z) = \neg(y \to 1) = \neg 1 = 0$, which is a contradiction.

Hence this system is inconsistent.

3. $A_1 \cup \{y \to z\}$

   The example from part 1 satisfies this system as $y \to z = 0 \to 0 = 1$.

## Exercise 11.3

Suppose the Boolean functions $f, g \in \mathcal{B}(n)$ are monotonic, $s = x_1 \wedge \cdots \wedge x_n$, $t = x_1 \vee \cdots \vee x_n$. Show that:

1. $s \leqslant f \vee g \implies s \leqslant f$ or $s \leqslant g$.

   If $x_k = 0$ for some $k \in \{1, \ldots, n\}$, then $s = 0$, meaning each inequality is true and so is the implication.

   If $x_k = 1$ for all $k \in \{1, \ldots, n\}$, then $s = 1$ and $f \vee g = 1$, meaning $f = 1$ or $g = 1$ and $s \leqslant f$ or $s \leqslant g$ respectively.

2. $f \wedge g \leqslant t \implies f \leqslant t$ or $g \leqslant t$

   If $x_k = 1$ for some $k \in \{1, \ldots, n\}$, then $t = 1$, meaning each inequality is true and so is the implication.

If $x_k = 0$ for all $k \in \{1, \dots, n\}$, then $t = 0$ and $f \wedge g = 0$, meaning $f = 0$ or $g = 0$ and $f \leqslant t$ or $g \leqslant t$ respectively.

## Exercise 11.4

Show that CNF follows from DNF by applying de Morgan's laws.

Before we do so we shall show that $\overline{a^b} = a^{\overline{b}}$.
If $b = 0$, then $\overline{a^b} = \overline{a^0} = \overline{\overline{a}} = a$ via involution law and $a^{\overline{b}} = a^{\overline{0}} = a^1 = a$.
If $b = 1$, then $\overline{a^b} = \overline{a^1} = \overline{a}$ and $a^{\overline{b}} = a^{\overline{1}} = a^0 = \overline{a}$.
We now consider the following:

$$\sum_{c:f(c)=1} \prod_{k=1}^{n} x_k^{c_k} = f(x) = \overline{\overline{f(x)}} = \overline{\sum_{c:\overline{f(c)}=1} \prod_{k=1}^{n} x_k^{c_k}} = \overline{\sum_{c:f(c)=0} \prod_{k=1}^{n} x_k^{c_k}} =$$

$$= \prod_{c:f(c)=0} \overline{\prod_{k=1}^{n} x_k^{c_k}} = \prod_{c:f(c)=0} \sum_{k=1}^{n} \overline{x_k^{c_k}} = \prod_{c:f(c)=0} \sum_{k=1}^{n} x_k^{\overline{c_k}}$$

## Exercise 11.5

Show that every $f \in \mathcal{B}(n)$ can be written in the form

$$f(x_1, \dots, x_n) = x_1 f(1, x_2, \dots, x_n) + \overline{x_1} f(0, x_2, \dots, x_n)$$

and apply this principle to $f = x_1\overline{x_2} + x_2x_3 + x_2\overline{x_3}x_4$ to obtain DNF.

If $x_1 = 0$, then

$$x_1 f(1, x_2, \dots, x_n) + \overline{x_1} f(0, x_2, \dots, x_n) = 0 \cdot f(1, x_2, \dots, x_n) + 1 \cdot f(0, x_2, \dots, x_n) =$$

$$= f(0, x_2, \dots, x_n) = f(x_1, \dots, x_n)$$

If $x_1 = 1$, then

$$x_1 f(1, x_2, \dots, x_n) + \overline{x_1} f(0, x_2, \dots, x_n) = 1 \cdot f(1, x_2, \dots, x_n) + 0 \cdot f(0, x_2, \dots, x_n) =$$

$$= f(1, x_2, \ldots, x_n) = f(x_1, \ldots, x_n)$$

This, of course, can be generalised.

Applying this principle to the Boolean function $f = x_1\overline{x_2} + x_2x_3 + x_2\overline{x_3}x_4$, we see that

$$\begin{aligned}
x_1\overline{x_2} &= x_3 \cdot x_1\overline{x_2} + \overline{x_3} \cdot x_1\overline{x_2} = x_1\overline{x_2}x_3 + x_1\overline{x_2}\,\overline{x_3} \\
&= x_4 \cdot (x_1\overline{x_2}x_3 + x_1\overline{x_2}\,\overline{x_3}) + \overline{x_4} \cdot (x_1\overline{x_2}x_3 + x_1\overline{x_2}\,\overline{x_3}) \\
&= x_1\overline{x_2}x_3x_4 + x_1\overline{x_2}\,\overline{x_3}x_4 + x_1\overline{x_2}x_3\overline{x_4} + x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4} \\
x_2x_3 &= x_1x_2x_3 + \overline{x_1}x_2x_3 \\
&= x_4(x_1x_2x_3 + \overline{x_1}x_2x_3) + \overline{x_4}(x_1x_2x_3 + \overline{x_1}x_2x_3) \\
&= x_1x_2x_3x_4 + \overline{x_1}x_2x_3x_4 + x_1x_2x_3\overline{x_4} + \overline{x_1}x_2x_3\overline{x_4} \\
x_2\overline{x_3}x_4 &= x_1x_2\overline{x_3}x_4 + \overline{x_1}x_2\overline{x_3}x_4
\end{aligned}$$

Meaning that the DNF of $f = x_1\overline{x_2} + x_2x_3 + x_2\overline{x_3}x_4$ is

$$x_1\overline{x_2}x_3x_4 + x_1\overline{x_2}\,\overline{x_3}x_4 + x_1\overline{x_2}x_3\overline{x_4} + x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4} + x_1x_2x_3x_4 +$$

$$+\overline{x_1}x_2x_3x_4 + x_1x_2x_3\overline{x_4} + \overline{x_1}x_2x_3\overline{x_4} + x_1x_2\overline{x_3}x_4 + \overline{x_1}x_2\overline{x_3}x_4$$

## Exercise 11.6

Let $f : \mathcal{B}(3) \to \{0, 1\}$ be defined by $f(0, 0, 0) = f(0, 1, 1) = 0$ and 1 otherwise. Determine the DNF and CNF and find a simpler representation with three summands in which the variables appear five times in all.

For DNF, since the solutions to $f(c) = 0$ are $(0, 0, 1)$, $(0, 1, 0)$, $(1, 0, 0)$, $(1, 0, 1)$, $(1, 1, 0)$ and $(1, 1, 1)$, we have

$$f = x_1x_2x_3 + x_1x_2\overline{x_3} + x_1\overline{x_2}x_3 + x_1\overline{x_2x_3} + \overline{x_1}x_2\overline{x_3} + \overline{x_1}\,\overline{x_2}x_3$$

For CNF, since the solutions to $f(c) = 0$ are just $c = (0, 0, 0)$ and $c = (0, 1, 1)$, we have

$$f = (x_1 + x_2 + x_3) \cdot (x_1 + \overline{x_2} + \overline{x_3})$$

Via the identity $(x + y)(x + z) = x + yz$, we also have

$$f = x_1 + (x_2 + x_3)(\overline{x_2} + \overline{x_3}) = x_1 + x_2\overline{x_2} + x_2\overline{x_3} + x_3\overline{x_2} + x_3\overline{x_3} =$$

$$= x_1 + x_2\overline{x_3} + \overline{x_2}x_3 = x_1 + x_3^{\overline{x_2}}$$

## Exercise 11.7

Interpret all 16 Boolean functions $f$ with two variables as logical expressions and as operations on sets.

| $x$ | $y$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ | $f_9$ | $f_{10}$ | $f_{11}$ | $f_{12}$ | $f_{13}$ | $f_{14}$ | $f_{15}$ | $f_{16}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

$$\begin{array}{llll}
f_1 = 0 & f_2 = x \wedge y & f_3 = \neg(x \to y) & f_4 = x \\
f_5 = \neg(y \to x) & f_6 = y & f_7 = \neg(x \leftrightarrow y) & f_8 = x \vee y \\
f_9 = \neg(x \vee y) & f_{10} = x \leftrightarrow y & f_{11} = \neg y & f_{12} = y \to x \\
f_{13} = \neg x & f_{14} = x \to y & f_{15} = \neg(x \wedge y) & f_{16} = 1
\end{array}$$

$$\begin{array}{llll}
f_1 = \varnothing & f_2 = A_x \cap A_y & f_3 = A_x \cap \overline{A_y} & f_4 = A_x \\
f_5 = \overline{A_x} \cap A_y & f_6 = A_y & f_7 = A_x \Delta A_y & f_8 = A_x \cup A_y \\
f_9 = \overline{A_x} \cap \overline{A_y} & f_{10} = (A_x \cap A_y) \cup (\overline{A_x} \cap \overline{A_y}) & f_{11} = \overline{A_y} & f_{12} = A_x \cup \overline{A_y} \\
f_{13} = \overline{A_x} & f_{14} = \overline{A_x} \cup A_y & f_{15} = \overline{A_x} \cup \overline{A_y} & f_{16} = S
\end{array}$$

Where $\Delta$ is the symmetric difference and $S = \{1, \ldots, n\}$.

## Exercise 11.8

Show that $\Omega = \{\oplus, \cdot\}$ is no longer a basis if the constants 0 and 1 are not given.

By contradiction, assume $\Omega = \{\oplus, \cdot\}$ to be a basis without constants functions 0 and 1 given. Then there should exist nonconstant Boolean functions $f, g$ such that $\neg x = f(x) \oplus g(x)$ or $\neg x = f(x) \cdot g(x)$. We, obviously, require

$f(x)$ and $g(x)$ to be different from $\neg x$. But, since $f$ are nonconstant, we have $f(0) \neq f(1)$, meaning $f(0) = 0$ and $f(1) = 1$ or $f(0) = 1$ or $f(1) = 0$. The latter makes $f(x) = \neg x$, so we $f(x) = x$ is forced. (Same conclusion for $g(x)$). But then neither $f(x) \oplus g(x) = \neg x$ nor $f(x) \cdot g(x)$ as $x \oplus x = 0$ and $x \cdot x = x$. Neither the functions 0, $x$ are equal to $\neg x$, hence $\neg x$ can't be expressed with basis $\Omega$ unless the constants (specifically, the constant 1) is given.

### Exercise 11.9

With each order $P$ we associate a graph $G(P)$ as follows: The vertices of $G(P)$ are the elements of $P$, and $xy \in K(G(P))$ if and only if $x < y$ or $y < x$ in $P$. The graph $G(P)$ is called the comparability graph of $P$. Think about what Dilworth's theorem means for $G(P)$.

...

## 3.4 Definitions

**Definition 27** (0,1 words)**.** *The elements of $B(n) = \{0,1\}^n$ are $0,1$ words. For all $x \in B(n)$, we define $x_i$ to be the $i$th component of $x$.*

*A $0,1$ word $x \in B(n)$ is a zero word if and only if $x_i = 0$ for all $i \in \{1,\ldots,n\}$.*

*A $0,1$ word $x \in B(n)$ is a unit word if and only if $x_i = 1$ for all $i \in \{1,\ldots,n\}$.*

**Definition 28** (Binary representation)**.** *The binary representation of a $0,1$ word is $\sum\limits_{k=1}^{n} x_k 2^{k-1}$.*

**Definition 29** (Operations on $0,1$ words)**.** *In $B(1)$, we define the operations $+$, $\cdot$, $\oplus$ and $\rightarrow$ using the truth table below.*

| $x$ | $y$ | $x+y$ | $x \cdot y$ | $x \oplus y$ | $x \rightarrow y$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 |

*In $B(n)$ with $n > 1$, the same operations except for $\rightarrow$ are defined element-wise, i.e., $(x+y)_i = x_i+y_i$, $(x\cdot y)_i = x_i\cdot y_i$, $(x\oplus y)_i = x_i\oplus y_i$ for all $x, y \in B(n)$ and $i \in \{1, \ldots, n\}$.*

*For $0, 1$ words we also may replace $+$ and $\cdot$ with $\vee$ and $\wedge$ respectively.*

**Definition 30** (Standard order on $B(n)$)**.** *In $B(1)$, we define the standard order $\leq$ by $x \leq y$ if and only if $x \rightarrow y$ for all $x, y \in B(1)$.*

*In $B(n)$, we define the standard order $\leq$ element-wise, i.e., $x \leq y$ if and only if $x_i \leq y_i$ for all $x, y \in B(n)$ and $i \in \{1, \ldots, n\}$.*

**Definition 31** (Boolean function)**.** *A function is Boolean if and only if its domain and codomain are $B(n)$ for some positive integer $n$ and $B(1)$ respectively.*

**Definition 32** (Hamming distance/weight)**.** *For $0, 1$ words $x, y \in B(n)$ with some positive integer $n$, the Hamming distance between $x$ and $y$ denoted by $\Delta(x, y)$ is $|\{j \in \{1, \ldots, n\} \mid x_j \neq y_j\}|$. The Hamming weight of $x$ is the Hamming distance between $x$ and the zero word of $B(n)$.*

# Chapter 4

# Counting

## 4.1 Week 5 Central Exercises

### Exercise 1

Suppose we are given $n$ disjoint sets $S_i$. Let the first have $a_1$ elements, the second $a_2$, and so on. Show that the number of sets that contain at most one element from each $S_i$ is equal to $(a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$.

Apply this result to the following number-theoretic problem: Let $n = p_1^{a_1} p_2^{a_2}$ be the prime decomposition of $n$. Then $n$ has exactly $t(n) = \prod(a_i + 1)$ divisors. Conclude that $n$ is a square if and only if $t(n)$ is odd.

See Exercise 1.2 of the following section. (Discrete Mathematics by Martin Aigner, Sections 1.1-1.2).

### Exercise 2

Recall that in the exercises for week 1 you were tasked to find functions from $A = \{1, 2\}$ to $B = \{3, 4, 5\}$. Now, try to answer the following questions using what you learned in lecture 5.

1. How many functions are there from $A$ to $B$?

Cardinalities of $A$ and $B$ are 2 and 3 respectively. Thus, the amount of functions $A \to B$ is $3^2 = 9$.

2. How many injections?

   There are $3 \cdot 2 = 6$ injections $A \to B$.

3. How many surjections?

   There are no surjections as $|A| < |B|$.

How many bijections are there from some $n$ element set to another $n$ element set?

Since the cardinalities of domain and codomain are equal, injectivity implies bijectivity and therefore we simply need to count the injections, which there are $n^{\underline{n}}$ of, which is the same as $n!$.

## Exercise 3

Consider a panel with 5 light bulbs, each of which can be either on or off.

1. How many different states are there in total?

   Since there are 5 light bulbs and each has 2 possible states, via product rule, we get $2^5 = 32$ different states in total.

2. How many states are there where two lights are on.

   Each such state can be identified with a subset with 2 elements of the set of light bulbs and we already know that $\binom{5}{2} = 10$.

3. How many states are there where $k$ lights are on?

   Generalising our previous argument, we get $\binom{5}{k}$

4. Now suppose that there are $n$ lights on the panel. Answer the previous questions again.

   Further generalising our argument, weget $\binom{n}{k}$.

## Exercise 4

Let $N = \{1, 2, \ldots, 100\}$ and let $A$ be a subset of $N$ with $|A| = 55$. Show that $A$ contains two numbers $a$ and $b$ such that $|a - b| = 9$. Does this hold for $|A| = 54$?

See Exercise 1.3 of the following section. (Discrete Mathematics by Martin Aigner, Sections 1.1-1.2.)

## Exercise 5

In the parliament of country $X$ there are 111 seats and three political parties. How many ways $(i, j, k)$ are there of dividing up the seats such that no party has an absolute majority?

Since $\left\lfloor \frac{111}{2} \right\rfloor = 55$, we shall count the number of $(i, j, k) \in \{1, \ldots, 55\}^3$ with $i + j + k = 111$.

Fix $i \in \{1, \ldots, 55\}$. Define $A_i = \{56 - i, \ldots, 55\}$ and $S_i = \{(j, k) \in A_i^2 : i + j + k = 111\}$.

$\{i\} \times S_i$ is the set of all solutions $(i, j, k)$ as $j < 56 - i$ (resp. $k < 56 - i$) implies $111 = i+j+k < i+56-i+k = k+56 \leq 111$ (resp. $111 = i+j+k < i + j + 56 - i = j + 56 \leq 111$). Our goal is therefore to evalute $\left|\bigcup_{i=1}^{55} S_i\right|$. The latter, since $S_i \cap S_j = \varnothing$ given $i \neq j$, is equal to $\sum\limits_{i=1}^{55} |S_i|$.

Consider the mapping $f : A_i \to S_i$ given by $j \mapsto (j, 111 - (i + j))$. Indeed, since $56 - i \leq 111 - (i + j) \leq 55$ given $56 - i \leq j \leq 55$ and $i + j + 111 - (i + j) = 111$, we have $(j, 111 - (i + j)) \in S$ for all $j \in A_i$, meaning $f$ is well-defined.

Our claim is that $f$ is also a bijection. The mapping $f^{-1} : S_i \to A_i$ given by $(j, k) \mapsto j$ satisfies the following.

$$\begin{aligned}
(f \circ f^{-1})(j, k) &= f(j) = (j, 111 - (i + j)) = (j, k) \\
(f^{-1} \circ f)(j) \quad &= f^{-1}(j, 111 - (i + j)) = j
\end{aligned}$$

Where $(i, j) \in S_i$. The last equation of the first line is justified as $(i, j) \in S_i$ means $i + j + k = 111$, which implies $k = 111 - (i + j)$. We hence have $f \circ f^{-1} = \mathrm{id}_{S_i}$ and $f^{-1} \circ f = \mathrm{id}_{A_i}$. Since $f$ is invertible, it is a bijection. Thus $|A_i| = |S_i|$. Clearly, $|A_i| = 55 - (56 - i) + 1 = i$.

Finally, we have $\sum\limits_{i=1}^{55} A_i = \sum\limits_{i=1}^{55} i = \frac{55 \cdot 56}{2} = 55 \cdot 28 = 1540$.

## Exercise 6

Consider

$$(x + y)^n = \underbrace{(x + y)(x + y) \cdots (x + y)}_{n \text{ times}} = \sum_{k=0}^{n} c_k x^k y^{n-k}$$

and determine what is the coefficient of $c_k$ in front of $x^k y^{n-k}$.

...

### Exercise 7

Show that $1! + 2! + \cdots + n!$ for $n > 3$ is never a square.

Since $n \geq 4$, we have $1! + 2! + \cdots + n! \equiv 1! + 2! + 3! + 4! \equiv 3 \mod 5$. However, 3 is not a square residue modulo 5 since $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 4$ and $4^2 \equiv 1$ all $\mod 5$.

## 4.2 Discrete Mathematics by Martin Aigner, Sections 1.1-1.2

### Exercise 1.1

Suppose that Dean B of County College determines that every student must enroll in exactly four courses in the history of mathematics from among the seven that are offered. The professors of the various courses specify the maximum enrollments in their courses as 51, 30, 30, 20, 25, 12, 18. What can one conclude from this?

That average enrollment in a course is approximately 26.5714285714.

### Exercise 1.2

Suppose we are given $n$ disjoint sets $S_i$. Let the first have $a_1$ elements, the second $a_2$, and so on. Show that the number of sets that contain at most one element from each $S_i$ is $(a_1 + 1)(a_2 + 1) \cdots (a_n + 1)$. Apply this result to the following number-theoretic problem: Let $n = p_1^{a_1} p_2^{a_2} \cdots$ be the prime decomposition of $n$. Then $n$ has exactly $t(n) = \prod(a_i + 1)$ divisors. Conclude that $n$ is a square if and only if $t(n)$ is odd.

For each $i$ and such set $A$ there are two cases; $A$ contains no element from $S_i$ or $A$ contains exactly one element from $S_i$. In total there hence are $a_i + 1$ possibilities for $A \cap S_i$ for each $i$. To each $A$ we assign $(A \cap S_1, \ldots, A \cap S_n)$. This is clearly a bijection as the inverse is the assignment of $(X_1, \dots, X_n)$ to $\bigcup\limits_{i=1}^{n} X_i$. Via product rule, the amount of such sets $A$ is $(a_1+1)(a_2+1)\cdots(a_n+1)$.

Let $f_i(d)$ denote the power of $p_i$ in the prime decomposition of $d$. If $d \mid n$, then, clearly, we can't have $f_i(d) > a_i$, so $f_i(d) \le a_i$ for all $i$. For each $i$ define $S_i = \{p_i, p_i^2, \dots\}$ so that $|S_i| = a_i$. Each $d$ can be identified with the set $\{p_1^{f_1(d)}, \dots\}$. Clearly, that set has to contain at most one element from each $S_i$ since $f_i(d) \le a_i$ for all $i$. Therefore there are $\prod(a_i+1)$ divisors of $n$.

If $n$ is a square, then every $a_i$ is even and every $(a_i+1)$ is odd. A product of odd numbers is also odd. Conversely, let $n$ not be a square, meaning there is at least one odd $a_i$, then $(a_i+1)$ is even for that $i$, making the whole product even.

## Exercise 1.3

Let $N = \{1, 2, \dots, 100\}$ and let $A$ be a subset of $N$ with $|A| = 55$. Show that $A$ contains two numbers $a$ and $b$ such that $a - b = 9$. Does this hold as well for $|A| = 54$?

$N$ clearly has 9 congruence classes modulo 9, each of which contains less than or equal to of 12 elements. Pigeonhole principle tells us that there should be $\lfloor \frac{55}{9} \rfloor + 1 = 7$ elements from $A$ that are from the same congruence class. Each congruence class has 12 pairs of the form $\{n, n+9\}$ and another application of pigeonhole principle tells us that at least two of those 7 elements must be in the same pair, i.e., there is a pair of integers from $A$ with difference 9.

However, for the case $|A| = 54$, we have $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 19, 20, 21, 22, 23, 24, 25, 26, 27, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 58, 59, 60, 61, 62, 63, 64, 65, 66, 76, 77, 78, 79, 80, 81, 82, 83, 84, 94, 95, 96, 97, 98, 99, 100\}$

# Chapter 5

# Sums and discrete calculus

## 5.1 Week 6 Central Exercises

### Exercise 1.1

Compute the following

1. $\sum_{i=1}^{5} i(i+1)$

$$\sum_{i=1}^{5} i(i+1) = 1\cdot(1+1)+2\cdot(2+1)+3\cdot(3+1)+4\cdot(4+1)+5\cdot(5+1) =$$

$$= 2+6+12+20+30 = 70$$

2. $\sum_{k=3}^{6} \frac{4k}{k+2}$

$$\sum i = 3^6 \frac{4k}{k+2} = \frac{4\cdot 3}{3+2} + \frac{4\cdot 4}{4+2} + \frac{4\cdot 5}{5+2} + \frac{4\cdot 6}{6+2} = \frac{12}{5} + \frac{8}{3} + \frac{20}{7} + 3 =$$

$$\frac{12\cdot 21 + 8\cdot 35 + 20\cdot 15 + 3\cdot 105}{105} = \frac{1147}{105}$$

3. $\sum_{0<j<7} 14(j-1)^2$

$$\sum_{0<j<7} 14(j-1)^2 = 14(1-1)^2+14(2-1)^2+14(3-1)^2+14(4-1)^2+14(5-1)^2+14(6-1)^2 =$$

$$= 14(0+1+4+9+16+25) = 14 \cdot 55 = 770$$

4. $\sum\limits_{0\leq j,k<4} j^2k$

$$\sum_{0\leq j,k<4} j^2k = \sum_{1\leq j,k\leq 3} j^2k = 1^2{\cdot}1+1^2{\cdot}2+1^2{\cdot}3+2^2{\cdot}1+2^2{\cdot}2+2^2{\cdot}3+3^2{\cdot}1+3^2{\cdot}2+3^2{\cdot}3 =$$

$$= 1+2+3+4+8+12+9+9+18+27 = 93$$

5. $\sum\limits_{0\leq j\leq k<4} j^2k$

$$\sum_{1\leq j\leq k\leq 3} j^2k = 1^2\cdot 1 + 2^2\cdot 1 + 2^2\cdot 2 + 3^2\cdot 1 + 3^2\cdot 2 + 3^2\cdot 3$$

$$= 1+4+8+9+18+27 = 67$$

6. $\sum\limits_{i=1}^{3}\sum\limits_{j=3}^{4}\frac{ij}{j+4}$

$$\sum_{i=1}^{3}\sum_{j=3}^{4}\frac{ij}{j+4} = \sum_{i=1}^{3}\left(\frac{3i}{7}+\frac{i}{2}\right) = \left(\frac{3}{7}+\frac{1}{2}\right)+\left(\frac{6}{7}+1\right)+\left(\frac{9}{7}+\frac{9}{2}\right) =$$

$$= \frac{18}{7}+6 = \frac{18+6\cdot 7}{7} = \frac{60}{7}$$

7. $\sum\limits_{\substack{0\leq a,b\leq 9\\ a+b=18}} (a-b)^{15}$

$$\sum_{\substack{0\leq a,b\leq 9\\ a+b=18}} (a-b)^{15} = (9-9)^{15} = 0^{15} = 0$$

8. $\prod\limits_{k=2}^{5}(1+k)$

$$\prod_{k=2}^{5}(1+k) = (1+2)(1+3)(1+4)(1+5) = 3\cdot 4\cdot 5\cdot 6 = 360$$

9. $\prod\limits_{\substack{u\in\mathbb{Z}\\|u|\leq 3}} \frac{u}{u+4}$

$$\prod_{\substack{u\in\mathbb{Z}\\|u|\leq 3}} \frac{u}{u+4} = \frac{0}{0+4} \cdot \prod_{\substack{u\in\mathbb{Z}\\0\neq|u|\leq 3}} = 0$$

10. $\prod\limits_{\substack{u\in\mathbb{N}\\u|10}} \sum\limits_{\substack{0\leq v\leq 4\\v\neq 2}} (u+v)$

$$\prod_{\substack{u\in\mathbb{N}\\u|10}} \sum_{\substack{0\leq v\leq 4\\v\neq 2}} (u+v) = \prod_{\substack{u\in\mathbb{N}\\u|10}} (u+0+u+1+u+3+u+4)$$

$$= \prod_{\substack{u\in\mathbb{N}\\u|10}} (4u+8) = (4\cdot 1+8)(4\cdot 2+8)(4\cdot 5+8)(4\cdot 10+8) =$$

$$12\cdot 16\cdot 28\cdot 48 = 258048$$

## Exercise 1.2

Use capital Sigma and Pi notations to write

1. $20+25+30+35+\cdots+100$;

$$\sum_{i=4}^{20} 5i$$

2. $\pi(0.1)+\pi(0.01)+\pi(0.001)+\ldots$;

$$\sum_{i=1}^{\infty} \pi 10^{-i}$$

3. $-4+16-25+36-\ldots$;

$$-4+\sum_{i=4}^{\infty}(-1)^i i^2$$

4. $20 \cdot 25 \cdot 30 \cdot 35 \cdots 100$;

$$\prod_{i=4}^{20} 5i$$

5. $1 \cdot 2 \cdot 3 \cdot 4 \cdots 10 + 2 \cdot 4 \cdot 6 \cdots 20 + 3 \cdot 6 \cdot 9 \cdots 30 + \cdots + 10 \cdot 20 \cdot 30 \cdots 100$;

$$\sum_{j=1}^{10} \prod_{i=1}^{10} ij$$

6. $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$.

$$\sum_{k=0}^{n} a_k x^k$$

## Exercise 1.3

Show that the following equations are true

1. $\sum\limits_{k=1}^{n}(2k-1) = n^2$;

$$\sum_{k=1}^{n}(2k-1) = 2\sum_{k=1}^{n} k - \sum_{k=1}^{n} 1 = 2 \cdot \frac{n(n+1)}{2} - n = n^2 + n - n = n^2$$

2. $\sum\limits_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n}\left(\frac{1}{k} - \frac{1}{k+1}\right) = \sum_{k=1}^{n}\frac{1}{k} - \sum_{k=1}^{n}\frac{1}{k+1} = \sum_{k=1}^{n}\frac{1}{k} - \sum_{k=2}^{n+1}\frac{1}{k} =$$

$$= 1 + \sum_{k=2}^{n}\frac{1}{k} - \sum_{k=2}^{n}\frac{1}{k} - \frac{1}{n+1} = 1 - \frac{1}{n+1} = \frac{n}{n+1}$$

## Exercise 2.1

Calculate the following

1. $\Delta(2x^3 - x^2)$;

$$\Delta(2x^3 - x^2) = 2\Delta(x^3) - \Delta(x^2) = 2(3x^2 + 3x + 1) - (2x + 1) = \\ = 6x^2 + 6x + 2 - 2x - 1 = 6x^2 + 4x + 1$$

2. $\nabla(2x^3 - x^2)$;

$$\nabla(2x^3 - x^2) = 2\nabla(x^3) - \nabla(x^2) = 2(3x^2 - 3x + 1) - (2x - 1) = \\ = 6x^2 - 6x + 2 - 2x + 1 = 6x^2 - 8x + 3$$

3. $\Delta(e^x)$;

$$\Delta(e^x) = e^{x+1} - e^x = e \cdot e^x - e^x = (e - 1)e^x$$

4. $\nabla(e^x)$;

$$\nabla(e^x) = e^x - e^{x-1} = e^x - e^x \cdot e^{-1} = e^x \left(1 - \frac{1}{e}\right)$$

5. $\Delta^2(e^x)$;

$$\Delta^2(e^x) = \Delta(\Delta(e^x)) = \Delta((e - 1)e^x) = (e - 1)\Delta(e^x) = \\ = (e - 1)(e - 1)e^x = (e - 1)^2 e^x$$

6. $\Delta^4(2x^4)_{x=0}$.

$$\Delta^4(2x^4)_{x=0} = 2\Delta^4(x^4)_{x=0} = \sum_{k=0}^{4} (-1)^k \binom{4}{k} k^4 = \\ = \binom{4}{0} 0^4 - \binom{4}{1} 1^4 + \binom{4}{2} 2^4 - \binom{4}{3} 3^4 + \binom{4}{4} 4^4 = \\ = -4 + 96 - 324 + 256 = 24$$

## Exercise 2.2

Show that $\sum\limits_{k=1}^{10}(s(k+1)-s(k)) = s(11)-s(1)$ for any function $s:\mathbb{Z}\to\mathbb{R}$.

$$\sum_{k=1}^{10}(s(k+1)-s(k)) = \sum_{k=1}^{10} s(k+1) - \sum_{k=1}^{10} s(k) = \sum_{k=2}^{11} s(k) - \sum_{k=1}^{10} s(k) =$$

$$= s(11) + \sum_{k=2}^{10} s(k) - \sum_{k=2}^{10} s(k) - s(1) = s(11) - s(1)$$

## Exercise 2.3

Compute $\sum_{k=0}^{n} k3^k$. Hint: Take a look at lecture slides.

$\frac{3}{4}(3^n(2n-1)+1)$ [See Exercise 2.2 of the following section.]

## Exercise 2.4

Find the discrete analogue of the logarithm function, that is, a function $\alpha$ such that $\alpha(x) = \sum x^{\underline{-1}}$

Since $x^{\underline{-1}} = \frac{1}{x+1}$, we have $\Delta\alpha(x) = \frac{1}{x+1}$ and we can solve for $\alpha$ we follows.

$$\alpha(x+1) - \alpha(x) = \frac{1}{x+1}$$

$$\alpha(x+1) = \alpha(x) + \frac{1}{x+1}$$

$$\alpha(x) = \sum_{i=1}^{x} \frac{1}{i} = H_x$$

Hence the discrete analogue of the logarithm function is the harmonic function. (assuming the initial condition is $\alpha(1) = 1$)

### Exercise 2.5

Find the discrete analogue of $e^x$ function, that is, a function $\beta$ such that $\beta(x) = \Delta\beta(x)$.

Using the definition of $\Delta$, we get a recursive formula for $\beta(x)$ like previously.

$$\beta(x) = \beta(x+1) - \beta(x)$$
$$\beta(x+1) = 2\beta(x)$$
$$\beta(x) = \beta_0 \cdot 2^x$$

The author, however, seems to have forgotten to mention the initial condition, so we shall point out that for $\beta(0) = 1$ we have the solution $\beta(x) = 2^x$.

### Exercise 3

How many integers in $\{1, \ldots, 100\}$ are not divisible by 2, 3 or 5.

Let $S = \{1, \ldots, 100\}$, $A = \{2 \mid k \text{ and } k \in S\}$, $B = \{3 \mid k \text{ and } k \in S\}$, $B = \{5 \mid k \text{ and } k \in S\}$, then, via inclusion-exclusion principle, we have

$$|S \setminus (A \cup B \cup C)| = |S| - |A| - |B| - |C| + |A \cap B| + |B \cap C| + |A \cap C| - |A \cap B \cap C|$$

$$|S \setminus (A \cup B \cup C)| = 100 - \left\lfloor \frac{100}{2} \right\rfloor - \left\lfloor \frac{100}{3} \right\rfloor - \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{6} \right\rfloor + \left\lfloor \frac{100}{10} \right\rfloor + \left\lfloor \frac{100}{15} \right\rfloor - \left\lfloor \frac{100}{30} \right\rfloor$$
$$|S \setminus (A \cup B \cup C)| = 100 - 50 - 33 - 20 + 16 + 10 + 6 - 3 = 26$$

## 5.2 Discrete Mathematics by Martin Aigner, Chapter 2

### Exercise 2.1

With the help of the summation factor, solve the recurrence $T_0 = 3$, $2T_n = nT_{n-1} + 3 \cdot n!$ $(n > 0)$.

First we define $s_n = \frac{2^n}{n!}$ so that $2s_{n-1} = s_n n$ and $S_n = 2s_nT_n$. Observe that

$$S_n = 2s_nT_n = s_n(nT_{n-1}+3) = s_nnT_{n-1}+3s_n = 2s_{n-1}T_{n-1}+3s_n = S_{n-1}+3s_n$$

Meaning that

$$S_n = 2s_0T_0 + 3\sum_{i=1}^{n} s_i = 6 + 3\sum_{k=1}^{n}\frac{2^k}{k!}$$

$$T_n = \frac{n!}{2^{n+1}}\left(6 + 3\sum_{k=1}^{n}\frac{2^k}{k!}\right) = \frac{3n!}{2^{n+1}}\left(1 + \sum_{k=0}^{n}\frac{2^k}{k!}\right)$$

## Exercise 2.2

Compute $\sum\limits_{k=0}^{n} kx^k$ $(x \neq 1)$: (a) Using the method of isolation of terms. (b) Using the double sum $\sum\limits_{1\le j\le k\le n} x^k$. (c) By differentiating $\sum_{k=0}^{n} x^k$.

For part a, we have the following

$$\sum_{k=1}^{n+1} kx^k = \sum_{k=1}^{n} kx^k + (n+1)x^{n+1}$$

$$\sum_{k=1}^{n+1} kx^k = x + \sum_{k=2}^{n+1} kx^k = x + \sum_{k=1}^{n}(k+1)x^{k+1} = x + x\sum_{k=1}^{n}(k+1)x^k =$$

$$= x+x\sum_{k=1}^{n}(kx^k+x^k) = x+x\left(\sum_{k=1}^{n} kx^k + \sum_{k=1}^{n} x^k\right) = x+x\left(\sum_{k=1}^{n} kx^k + x\sum_{k=1}^{n} x^{k-1}\right) =$$

$$x+x\left(\sum_{k=1}^{n} kx^k + x\sum_{k=0}^{n-1} x^k\right) = x+x\left(\sum_{k=1}^{n} kx^k + x\frac{x^n-1}{x-1}\right) = x+x\sum_{k=1}^{n} kx^k+x^2\frac{x^n-1}{x-1}$$

Via symmetry and transitivity of =, we have

$$\sum_{k=1}^{n} kx^k + (n+1)x^{n+1} = x + x\sum_{k=1}^{n} kx^k + x^2\frac{x^n-1}{x-1}$$

Isolating the sum that we are interesting in yields

$$\sum_{k=1}^{n} kx^k = x \cdot \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}$$

And finally

$$\sum_{k=0}^{n} kx^k = x \cdot \frac{x^n((x-1)n-1)+1}{(x-1)^2}$$

For part b, we have

$$\sum_{k=0}^{n} kx^k = \sum_{k=1}^{n} kx^k = \sum_{k=1}^{n}\sum_{j=1}^{k} 1 \cdot x^k = \sum_{1 \leq j \leq k \leq n} x^k = \sum_{j=1}^{n}\sum_{k=j}^{n} x^k =$$

$$= \sum_{j=1}^{n} x^j \sum_{k=j}^{n} x^{k-j} = \sum_{j=1}^{n} x^j \sum_{k=0}^{n-j} x^k = \sum_{j=1}^{n} x^j \frac{x^{n-j+1}}{x-1} =$$

$$= \frac{1}{x-1}\sum_{j=1}^{n}(x^{n+1} - x^j) = \frac{1}{x-1}\left(nx^{n+1} - x\sum_{j=1}^{n} x^{j=1}\right) =$$

$$= \frac{1}{x-1}\left(nx^{n+1} - x\sum_{j=0}^{n-1} x^j\right) = \frac{1}{x-1}\left(nx^{n+1} - x\frac{x^n-1}{x-1}\right) =$$

$$= \frac{1}{(x-1)^2}(nx^{n+1}(x-1) - x^{n+1} + x) = \frac{x}{(x-1)^2}(x^n((x-1)n-1)+1)$$

For part c, ...

## Exercise 2.3

Calculate $\sum_k [1 \leq j \leq k \leq n]$ as a function of $j$ and $n$.

$$\sum_k [1 \leq j \leq k \leq n] = \begin{cases} 0, & j \leq 0 \\ 0, & n \leq 0 \\ 0, & j > n \\ n-j+1, & \text{otherwise} \end{cases}$$

## Exercise 2.4

Write down the number 1 and subtract 1. Multiply the result by 2 and add 1. Multiply the result by 3 and subtract 1. Multiply by 4 and add 1, and so on. Finally, multiply the result by $n$ and add $(-1)^n$. Show that the result is $D_n$. For example $4(3(2(1-1)+1)-1)+1 = D_4$.

This is a simple consequence of the fact that $D_0 = 1$ and $D_{n+1} = nD_n + (-1)^n$, which is already proven in the book. (via induction.)

## Exercise 2.5

In an array with three rows and $n$ columns there appear, in some order, $n$ red, $n$ white and $n$ green stones. Show that regardless of the arrangement, one can rearrange the stones in each row in such a way that the stones in each column are all of different colours.

...

## Exercise 2.6

Compute $\sum_{k=1}^{n-1} \frac{H_k}{(k+1)(k+2)}$ using partial summation.

Let $u = H_x$ and $v = -\frac{1}{x+1}$ so that $\Delta v = \frac{1}{(x+1)(x+2)}$ and via partial summation we have

$$\sum_{k=0}^{n-1} \frac{H_k}{(k+1)(k+2)} = \sum_1^n \frac{H_x}{(x+1)(x+2)} = -\frac{H_x}{x+1}\bigg|_1^n + \sum_1^n \frac{1}{(x+1)(x+2)} =$$

$$= \frac{1}{2} - \frac{H_n}{n+1} + \sum_1^n x^{\underline{-2}} = \frac{1}{2} - \frac{H_n}{n+1} - x^{\underline{-1}}\bigg|_1^n =$$

$$= \frac{1}{2} - \frac{H_n}{n+1} - \frac{1}{x+1}\bigg|_1^n = \frac{1}{2} - \frac{H_n}{n+1} - \frac{1}{n+1} + \frac{1}{2} =$$

$$= 1 - \frac{H_n+1}{n+1} = \frac{n-H_n}{n+1}$$

## Exercise 2.7

Compute $\sum\limits_{k=1}^{n} \frac{2k+1}{k(k+1)}$ in two different ways: (a) By partial fraction decomposition $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$. (b) By partial summation.

For part a, we have

$$\sum_{k=1}^{n} \frac{2k+1}{k(k+1)} = \sum_{k=1}^{n} \frac{k+k+1}{k(k+1)} = \sum_{k=1}^{n} \left( \frac{1}{k+1} + \frac{1}{k} \right) =$$

$$= \sum_{k=1}^{n} \frac{1}{k+1} + \sum_{k=1}^{n} \frac{1}{k} = \sum_{k=2}^{n+1} \frac{1}{k} + \sum_{k=1}^{n} \frac{1}{k} =$$

$$= \sum_{k=1}^{n} \frac{1}{n} + \frac{1}{n+1} - 1 + \sum_{k=1}^{n} \frac{1}{k} = 2H_n - \frac{n}{n+1}$$

For part b, we have

$$\sum_{k=1}^{n} \frac{2k+1}{k(k+1)} = \sum_{k=0}^{n-1} \frac{2k+3}{(k+1)(k+2)} = \sum_{0}^{n} \frac{2x+3}{(x+1)(x+2)} =$$

$$= \sum_{0}^{n} (2x+3)x^{\underline{-2}} = \sum_{0}^{n} x^{\underline{-2}} \Delta(x^2+2x) =$$

$$= x^{\underline{-2}}(x^2+2x) \Big|_{0}^{n} - \sum_{0}^{n} ((x+1)^2+2(x+1))\Delta(x^{\underline{-2}}) = \frac{x(x+2)}{(x+1)(x+2)} \Big|_{0}^{n} + 2\sum_{0}^{n} (x+1)(x+3)x^{\underline{-3}} =$$

$$= \frac{n}{n+1} + 2\sum_{0}^{n} \frac{(x+1)(x+3)}{(x+1)(x+2)(x+3)} = \frac{n}{n+1} + 2\sum_{0}^{n} \frac{1}{x+2} =$$

$$= \frac{n}{n+1} + 2\sum_{k=0}^{n-1} \frac{1}{k+2} = \frac{n}{n+1} + 2\sum_{k=2}^{n+1} \frac{1}{k} = \frac{n}{n+1} + 2\left( \sum_{k=1}^{n} \frac{1}{k} + \frac{1}{n+1} - 1 \right) =$$

$$= \frac{n}{n+1} + 2\left( H_n - \frac{n}{n+1} \right) = 2H_n - \frac{n}{n+1}$$

## Exercise 2.8

Prove the following analogue of the binomial theorem:

$$(x+y)^{\underline{n}} = \sum_{k=0}^{n} \binom{n}{k} x^{\underline{k}} y^{\underline{n-k}} \quad (x+y)^{\overline{n}} = \sum_{k=0}^{n} \binom{n}{k} x^{\overline{k}} y^{\overline{n-k}}$$

# Chapter 6

# Asymptotic analysis

## 6.1 Week 7 Central Exercises

### Exercise 1.1

Rank the following functions from the slowest growing to the fastest growing.

1. $n$, $(5/3)^n$, $n^4$, $3$, $n^3$, $2n$;

   $3 \prec n \asymp 2n \prec n^3 \prec n^4 \prec (5/3)^n$

2. $7n^2$, $56$, $4n^3$, $3n$, $n \log_2 n$, $\log_8 n$, $n \log_5 n$, $\log_2 n$, $7^{2n}$;

   $56 \prec \log_2 n \asymp \log_8 n \prec 3n \prec n \log_2 n \asymp n \log_5 n \prec 7n^2 \prec 4n^3 \prec 7^{2n}$

### Exercise 1.2

Show the following

1. $n^2 + 0.5n = O(n^2)$;

   For $n \geq 1$ we have $|n^2 + 0.5n| \leq |n^2| + 0.5|n| \leq |n^2| + 0.5|n^2| = 1.5|n^2|$.

2. $3x^5 - 4x^3 + 4 = O(x^5)$;

   For $x \geq 1$ we have $|3x^5 - 4x^3 + 4| \leq 3|x^5| + 4|x^3| + 4 \leq 3|x^5| + 4|x^5| + 4|x^5| = 11|x^5|$.

3. $3x^5 - 4x^3 + 4 = o(x^6)$;

   For any $\varepsilon > 0$ choose $x_0 = \frac{11}{\varepsilon}$ so that for $x \geq x_0$ we have $11 \leq \varepsilon|x|$, $11|x^5| \leq \varepsilon|x^6|$ and, finally, $|3x^5 - 4x^3 + 4| \leq 11|x^5| \leq \varepsilon|x^6|$.

4. $3x^5 - 4x^3 + 4 = \Omega(x^5)$.

   For $x \geq \lceil\sqrt{2}\rceil$ we have $2x^5 - 4x^3 = 2x^3(x^2 - 2) > 0$ and so $2x^5 - 4x^3 > 0$ and $3x^5 - 4x^3 + 4 > x^5$, meaning $|3x^5 - 4x^3 + 4| > |x^5|$ since both sides are positive anyway.

5. $3x^5 - 4x^3 + 4 = \Theta(x^5)$;

   This follows from (2) and (4).

6. $|3x^5 - 4x^3 + x^2 + 4| = \Theta(x^5)$;

   We once again observe that for $x \geq 1$ we have $|3x^5 - 4x^3 + x^2 + 4| \leq 3|x^5| + 4|x^3| + |x^2| + 4 \leq 3|x^5| + 4|x^5| + |x^5| + 4|x^5| = 12|x^5|$, so $3x^5 - 4x^3 + x^2 + 4 \in O(x^5)$.

   If we again let $x \geq \lceil\sqrt{2}\rceil$, then we arrive at $3x^5 - 2x^3 + 4 > x^5$ and $3x^5 - 2x^3 + x^2 + 4 > x^5 + x^2 > x^5$, meaning $|3x^5 - 2x^3 + x^2 + 4| > |x^5|$ and $3x^5 - 4x^3 + 2x^2 + 4 \in \Omega(x^5)$.

Finally, we have $3x^5 - 4x^3 + 2x^2 + 4 \in \Theta(x^5)$.

7. $\sin x = O(1)$;

For any $x$, we have $|\sin x| \leq 1$.

8. $(x^2+1)^{-1} + 2\cos 3x^3 = O(1)$;

Let $x \geq 0$, then $x^2 + 1 \geq 1$ and $(x^2+1)^{-1} \leq 1$, meaning we have $|(x^2+1)^{-1} + 2\cos 3x^3| \leq |(x^2+1)^{-1}| + 2|\cos 3x^3| \leq 1 + 2 = 3$.

9. $\frac{x+1}{x^2-3x} = o(1)$;

For every $\varepsilon > 0$, let $x_0 = \left\lceil 4 + \frac{1}{\varepsilon} \right\rceil$, so that for every $x \geq x_0$, we have the following sequence of inequalities.

$$\begin{aligned}
x &\geq 4 + \frac{1}{\varepsilon} \\
(x+1) - 5 &\geq \frac{1}{\varepsilon} \\
(x+1) - 5 + \frac{4}{x+1} &\geq \frac{1}{\varepsilon} \\
(x+1)^2 - 5(x+1) + 14 &\geq \frac{x+1}{\varepsilon} \\
x^2 - 3x &\geq \frac{x+1}{\varepsilon} \\
\varepsilon(x^2 - 3x) &\geq x + 1 \\
\left| \frac{x+1}{x^2-3x} \right| &\leq \varepsilon
\end{aligned}$$

10. $\sin x \cos x + x^2 = o(x^3)$;

For every $\varepsilon > 0$, let $x_0 = \left\lceil \frac{3}{2\varepsilon} \right\rceil$, so that for $x \geq x_0$, we have the following sequence of inequalities.

$$\begin{aligned}
x &\geq \frac{3}{2\varepsilon} \\
\frac{3}{2} &\leq \varepsilon x^3 \\
\frac{3x^2}{2} &\leq \varepsilon x^3 \\
\frac{1}{2}x^2 + x^2 &\leq \varepsilon x^3 \\
\frac{1}{2} + x^2 &\leq \varepsilon x^3 \\
\frac{|\sin(2x)|}{2} + \left|x^2\right| &\leq \varepsilon \left|x^3\right| \\
\left|\frac{\sin(2x)}{2} + x^2\right| &\leq \varepsilon \left|x^3\right| \\
\left|\sin(x)\cos(x) + x^2\right| &\leq \varepsilon \left|x^3\right|
\end{aligned}$$

11. $n + 30 = \Theta(3n + 1)$;

We first show that $n + 30 \in O(3n + 1)$ via the observation that for $n \geq \left\lceil \frac{27}{8} \right\rceil$, we have $27 \leq 8n$ and $n + 30 \leq 3(3n + 1)$. Both sides are positive, so we say $|n + 30| \leq C(3n + 1)$ for $C = 3$ and $n \geq n_0 = \left\lceil \frac{27}{8} \right\rceil$.

Now, we show that $3n + 1 \in O(n + 30)$. This time we, for any $n$, have $1 \leq 90$, meaning $3n + 1 \leq 3(n + 30)$. Let $n \geq 0$, so that both sides are positive and we have $|3n + 1| \leq C(n + 30)$ for $C = 3$ and $n \geq n_0 = 1$.

Finally, we get $n + 30 \in O(3n + 1)$ and $n + 30 \in \Omega(3n + 1)$, meaning $n + 30 \in \Theta(3n + 1)$.

12. $\log_2 x = \Theta(\log_2 2x)$.

    For any $x > 0$ we have $\log_2 x < \log_2 x + 1$ and $\log_2 x < \log_2 2x$. Let $x > 1$, so that both sides are positive and we have $|\log_2 x| < C|\log_2 2x|$ for $C = 1$ and $x \geq x_0 = 1$. This shows $\log_2 x \in O(\log_2 2x)$.

    For any $x > 2$ we also have $\log_2 x > 1$, meaning $\log_2 x + 1 < \log_2 x + \log_2 x = 2\log_2 x$. Both sides are positive, so we have $|\log_2 2x| = |\log_2 x + 1| \leq 2|\log_2 x|$. This shows $\log_2 2x \in O(\log_2 x)$.

    Finally, we get $\log_2 x \in O(\log_2 2x)$ and $\log_2 x \in \Omega(\log_2 2x)$, meaning $\log_2 x \in \Theta(\log_2 2x)$.

## Exercise 1.3

What is the asymptotic relationship between the functions

1. $n^k$ and $c^n$; Assuming $k \geq 1$ and $c > 1$.

   We observe that $\frac{n^k}{c^n}$ is decreasing for sufficiently large $n$. Namely, for $n > \frac{1}{\sqrt[k]{c}-1}$ we have the following sequence of inequalities.

$$
\begin{aligned}
n &> \frac{1}{\sqrt[k]{c}-1} \\
\frac{1}{n} &< \sqrt[k]{c} - 1 \\
n + 1 &< n\sqrt[k]{c} \\
(n+1)^k &< n^k \cdot C \\
\frac{(n+1)^k}{C^{n+1}} &< \frac{n^k}{C^n}
\end{aligned}
$$

   We also notice that $\frac{n^k}{c^n} < \varepsilon$ for $n = \sqrt[k]{\varepsilon}$. This shows that we have $\frac{n^k}{c^n} < \varepsilon$ for $n > \left\lceil \max(\sqrt[k]{\varepsilon}, \frac{1}{\sqrt[k]{c}-1}) \right\rceil$ we have $\frac{n^k}{c^n} < \varepsilon$, which can be rewritten as $\left|n^k\right| < \varepsilon|c^n|$. Meaning we have $n^k \prec c^n$.

2. $\log_3 n$ and $\log_7 n$;

   Via change of base formula for logarithms we obtain $\log_7 n = \frac{\log_3 n}{\log_3 7}$ and, clearly, $\log_3 7 > 1$. Meaning, for $n > 1$, we have $\log_7 n < \log_3 n$ and $|\log_7 n| \leq |\log_3 n|$. We also have $\log_3 n < (\log_3 7 + 1)\log_7 n$ and $|\log_3 n| \leq (\log_3 7 + 1)|\log_7 n|$. This shows that $\log_3 n \in O(\log_7 n)$ and $\log_7 n \in O(\log_3 n)$, so $\log_3 n \asymp \log_7 n$.

3. $2^n$ and $8^n$;

   Let $n \geq \left\lceil \log_4\left(\frac{1}{\varepsilon}\right)\right\rceil$, so that $\frac{1}{\varepsilon} \leq 4^n$, $\frac{2^n}{8^n} = \frac{1}{4^n} \leq \varepsilon$ and $|2^n| \leq \varepsilon|8^n|$. Hence $2^n \prec 8^n$.

4. $\log_2 n^{\log_2 12}$ and $\log_2 12^{\log_2 n}$.

   Assuming that the author meant $\log_2\left(n^{\log_2 12}\right)$ and $\log_2\left(12^{\log_2 n}\right)$, these functions are the same, so, obviously, $\log_2\left(n^{\log_2 12}\right) \sim \log_2\left(12^{\log_2 n}\right)$.

## Exercise 1.4

In general, prove the validity of the following equations

1. $O(f(n))O(g(n)) = O(f(n)g(n))$;
2. $O(f(n)g(n)) = f(n)O(g(n))$;
3. $O(f(n)) + O(g(n)) = O(|f(n)| + |g(n)|)$.

See Problem 5.1 of the following section.

## Exercise 1.5

Is the following assertion correct?

From $f_1(n) \prec g_1(n)$, $f_2(n) \prec g_2(n)$ it follows that $f_1(n) + f_2(n) \prec g_1(n) + g_2(n)$.

See Problem 5.2 of the following section.

## Exercise 2

Minimize the total cost of visiting all cities $c_2$, $c_3$, $c_4$ for the travelling salesmen starting from the first city $c_1$. Travel costs are given in the array below (example: $c_{1,3} = 3$ is a cost to travel from $c_1$ to $c_3$).

| | $c_1$ | $c_2$ | $c_3$ | $c_4$ |
|---|---|---|---|---|
| $c_1$ | 0 | 2 | 3 | 4 |
| $c_2$ | 1 | 0 | 3 | 4 |
| $c_3$ | 2 | 2 | 0 | 4 |
| $c_4$ | 1 | 2 | 0 | 0 |

We shall consider each route. (Unfortunately, it is not always true that the cheapest route has an instance of travelling from a city to another city without spending anything.)

For the route $c_1 \to c_2 \to c_3 \to c_4$, the overall cost is 9.

For the route $c_1 \to c_2 \to c_4 \to c_3$, the overall cost is 6.

For the route $c_1 \to c_3 \to c_2 \to c_4$, the overall cost is 9.

For the route $c_1 \to c_3 \to c_4 \to c_2$, the overall cost is 9.

For the route $c_1 \to c_4 \to c_2 \to c_3$, the overall cost is 9.

For the route $c_1 \to c_4 \to c_3 \to c_2$, the overall cost is 5.

Clearly, the optimal route is $c_1 \to c_4 \to c_3 \to c_2$.

## Exercise 3.1

Show that for $f \prec h$ there is always $g$ such that $f \prec g \prec h$. Hint: Consider the absolute value of the geometric mean.

See Problem 5.4 of the following section.

### Exercise 3.2

An addition chain for $n$ is a sequence $1 = a_1, a_2, \ldots, a_m = n$ such that for every $k$, we have $a_k = a_i + a_j$ for some $i, j < k$. Example: $n = 19$, $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 8 = 4 + 4$, $a_5 = 9 = 8 + 1$, $a_6 = 17 = 9 + 8$, $a_7 = 19 = 17 + 2$. Let $l(n)$ be the minimal length of an addition chain for $n$. Show that $\lg n < l(n) < 2 \lg n$. Are there integers $n$ for which $l(n) = \lg n$?

See Exercise 5.10 of the following section.

## 6.2 Discrete Mathematics by Martin Aigner, Chapter 5

### Exercise 5.1

Prove the validity of the following equations: [Note: Multiplication of sets and of an element and a set is assumed to be defined element-wise.]

1. $O(f(n))O(g(n)) = O(f(n)g(n))$,

   Let $a(n) \in O(f(n))$ and $b(n) \in O(g(n))$, i.e., there exist $C_1, C_2, n_1, n_2 > 0$ such that $|a(n)| \leq C_1|f(n)|$ for $n \geq n_1$ and $|b(n)| \leq C_2|g(n)|$ for all $n \geq n_2$. Then we have $a(n) \cdot b(n) \leq C_1|f(n)| \cdot C_2|g(n)| = C_1C_2|f(n)g(n)|$ for $n \geq \max(n_1, n_2)$. This proves $O(f(n))O(g(n)) \subseteq O(f(n)g(n))$.

   Conversely, let $c(n) \in O(f(n)g(n))$, i.e., there exists $C, n_0 > 0$ such that $|c(n)| \leq C|f(n)g(n)|$ for all $n \geq n_0$. Our goal is to show that $c(n)$ is a product of a function from $O(f(n))$ and another function from $O(g(n))$. Rewriting the equation yields $|f(n)| \cdot \left|\frac{c(n)}{f(n)}\right| \leq C|f(n)||g(n)|$ and $\left|\frac{c(n)}{f(n)}\right| \leq C|g(n)|$ for $n \geq n_0$, meaning $|c(n)|f(n) \in O(g(n))$ and, trivially, $f(n) \in O(f(n))$. This proves $O(f(n)g(n)) \subseteq O(f(n))O(g(n))$.

   Finally, we get $O(f(n))O(g(n)) = O(f(n)g(n))$.

2. $O(f(n)g(n)) = f(n)O(g(n))$.

   We have already proven $O(f(n)g(n)) \subseteq f(n)O(g(n))$.

   For converse, let $a(n) \in O(g(n))$, i.e., there exist $C, n_0 > 0$ such that $|a(n)| \leq C|g(n)|$ for all $n \geq n_0$, meaning $|f(n)| \cdot |a(n)| \leq |f(n)| \cdot C|g(n)|$ and $|f(n)g(n)| \leq C|f(n)g(n)|$ for all $n \geq n_0$, so $f(n)a(n) \in O(f(n)g(n)$. This proves $f(n)O(g(n)) \subseteq O(f(n)g(n))$.

   Finally, we get $O(f(n)g(n)) = f(n)O(g(n))$.

3. $O(f(n)) + O(g(n)) = O(|f(n)| + |g(n)|)$.

   Let $a(n) \in O(f(n))$ and $b(n) \in O(g(n))$, i.e., there exist $C_1, C_2, n_1, n_2 > 0$ such that $|a(n)| \leq C_1|f(n)|$ for all $n \geq n_1$ and $|b(n)| \leq C_2|g(n)|$ for all $n \geq n_2$. Adding the equations up yields the following

$$|a(n) + b(n)| \leq |a(n)| + |b(n)| \leq C_1|f(n)| + C_2|g(n)| \leq$$

$$\leq \max(C_1, C_2)|f(n)| + \max(C_1, C_2)|g(n)| =$$

$$= \max(C_1, C_2)(|f(n)| + |g(n)|) = \max(C_1, C_2)||f(n)| + |g(n)||$$

   For all $n \geq \max(n_1, n_2)$. This shows $a(n) + b(n) \in O(|f(n)| + |g(n)|)$ and $O(f(n)) + O(g(n)) \subseteq O(|f(n)| + |g(n)|)$.

   Now let $c(n) \in O(|f(n)| + |g(n)|)$, i.e., there exist $C > 0$ and $n_0$ such that $|c(n)| \leq C||f(n)| + |g(n)|| = C|f(n)| + C|g(n)|$ for all $n \geq n_0$. Then $|Cf(n) + c(n) - Cf(n)| \leq C|f(n)| + C|g(n)|$ and, via the triangle inequality, $C|f(n)| + |c(n) - Cf(n)| \leq C|f(n)| + C|g(n)|$, meaning $|c(n) - Cf(n)| \leq C|g(n)|$ and $c(n) - Cf(n) \in O(g(n))$. Thus $c(n)$ can be written as a sum of a function from $O(f(n))$ and $O(g(n))$. This proves $O(|f(n)| + |g(n)|) \subseteq O(f(n)) + O(g(n))$.

   Finally, we have $O(f(n)) + O(g(n)) = O(|f(n)| + |g(n)|)$.

## Exercise 5.2

Is the following assertion correct? From $f_1(n) \prec g_1(n)$, $f_2(n) \prec g_2(n)$ it follows that $f_1(n) + f_2(n) \prec g_1(n) + g_2(n)$?

Let $f_1(n) = f_2(n) = 1$ and $g_1(n) = n = 1 - g_2(n)$, then $f_1(n) \prec g_1(n)$ and $f_2(n) \prec g_2(n)$, but $f_1(n) + f_2(n) \not\prec g_1(n) + g_2(n)$. The assertion is hence false.

## Exercise 5.3

Let $f(n) = n^2$ ($n$ even) and $f(n) = 2n$ ($n$ odd). Show that $f(n) = O(n^2)$, but not $f(n) = o(n^2)$ and not $n^2 = O(f(n))$.

For all $n \geq 2$ we have $|f(n)| \leq 1 \cdot |n^2|$ since by considering cases we have $n^2 \leq n^2$ for even $n$ and $2n \leq n^2$ for odd $n$, so $f(n) \in O(n^2)$.

Let $\epsilon = \frac{1}{2}$, then for any $n_0$ we will have $|f(n)| > \epsilon|n^2|$ where $n$ is the smallest even number not less than $n_0$. This contradicts the definition of $o(n^2)$, hence $f(n) \notin o(n^2)$. Since $n^2$ has finitely many zeroes, we could also use the calculus definition of $o(n^2)$ and show that $\lim\limits_{n\to\infty} \frac{f(n)}{n^2} \neq 0$. In fact, the limit does not exist as it is different along the sequences $n_k = 2k$ and $n_k = 2k + 1$.

For all $C > 0$ and $n_0$ we have $|n^2| > C|f(n)|$ where $n$ is the smallest odd number larger than $2C$. This contradicts the definition of $O(f(n))$, hence $n^2 \notin O(f(n))$.

## Exercise 5.4

Show that for $f \prec h$ there is always $g$ such that $f \prec g \prec h$.

Let $f \prec h$, i.e., for all $\varepsilon > 0$ there is $n_0$ such that for all $n \geq n_0$ we have $|f(n)| \leq \varepsilon|h(n)|$. Now pick any $\varepsilon' > 0$ and choose $\varepsilon = (\varepsilon')^2$. We then have the following sequence of inequalities for $n \geq n_0$.

$$\begin{aligned}|f(n)| &\leq \varepsilon |h(n)| \\ |f(n)| &\leq (\varepsilon')^2 |h(n)| \\ |f(n)|^2 &\leq (\varepsilon')^2 |f(n)h(n)| \\ |f(n)| &\leq \varepsilon' \sqrt{|f(n)h(n)|}\end{aligned}$$

Meaning $f \prec \sqrt{|f(n)h(n)|}$.

We similarly arrive at $\sqrt{|f(n)h(n)|} \leq \varepsilon' |h(n)|$, meaning $\sqrt{|f(n)h(n)|} \prec h$.

Finally, we get that $f \prec g \prec h$ for $g = \sqrt{|f(n)g(n)|}$.

## Exercise 5.5

In each case below, find a function $g(n) \neq \Theta(f(n))$ of the form $g : \mathbb{N} \to \mathbb{R}$ such that $f(n) = O(g(n))$ holds for the following function $f$:

1. $f(n) = \binom{n}{2}$,

   We can simplify $f(n)$ to $n^2 - n$ and pick $g(n) = n^3$. For $n \geq 1$ we have $|f(n)| = |n^2 - n| \geq |n^2| + |n| \geq 2n^2 < n^3 = 1 \cdot |g(n)|$, meaning $f(n) \in O(g(n))$.

   If $g(n) \in \Theta(f(n))$ was true, then we would have $g(n) \in O(f(n))$, but for all $C > 0$ and $n_0$ there exists $n \geq n_0$ such that $|n^3| > C|n^2 - n|$, namely, for $n = \max(n_0, \lceil 2C \rceil$ we have $n^3 \geq 2Cn^2 = Cn^2 + Cn^2 > C|n^2| + C|-n| \geq C|n^2 - n|$, which contradicts $g(n) \in O(f(n))$.

2. $f(n) = \frac{5n^3+1}{n+3}$,

   This time let $g(n) = 5n^3 + 1$, so that $\left|\frac{5n^3+1}{n+3}\right| \leq |5n^3 + 1|$ for $n \geq -2$ since $|n + 3| \geq 1$, meaning $f(n) \in O(g(n))$.

Like previously, our claim is that $g(n) \notin O(f(n))$. For all $C > 0$ and $n_0$, if we let $n = \max(n_0, \lceil C-3 \rceil)$, then $|n+3| > C$, meaning $|5n^3+1| > C\left|\frac{5n^3+1}{n+3}\right|$, which contradicts $g(n) \in O(f(n))$.

3. $f(n) = \frac{n^2 3^n}{2^n}$,

   Let $g(n) = n^3\left(\frac{3}{2}\right)^n$ so that $|f(n)| \leq |g(n)|$ for $n \geq 1$, meaning $f(n) \in O(g(n))$.

   For all $C > 0$ and $n_0$ we have $n^3\left(\frac{3}{2}\right)^n > Cn^2\left(\frac{3}{2}\right)^n$, so $g(n) \notin O(f(n))$.

4. $f(n) = n!$.

   We already know that $n! \prec n^n$, i.e., $n! \in o(n^n)$ and, trivially, $o(h(n)) \subseteq O(h(n))$ for any function $h(n)$, so $n! \in O(n^n)$.

   To prove that $n^n \notin O(n!)$, we need to show that for all $C > 0$ and $n_0$ there is $n \geq n_0$ with $\frac{n^n}{n!} > C$. Clearly, it is sufficient to show that there are infinitely many such positive $n$. Since $n! \in o(n^n)$, we can choose $\varepsilon = \frac{1}{C}$ so that $n! \leq \varepsilon n^n$ and $\frac{n^n}{n!} \geq C$ for sufficiently large $n$. The only thing to show now is that there are only finitely many $n$ with $\frac{n^n}{n!} = C$ for any $C > 0$ via the claim that $\frac{n^n}{n!}$ is increasing.

   $$\frac{(n+1)^{n+1}}{(n+1)!} = \frac{(n+1)\cdot(n+1)^n}{(n+1)\cdot n!} = \frac{(n+1)^n}{n!} > \frac{n^n}{n!}$$

   Which finishes the proof.

## Exercise 5.6

What is wrong with the following argument? Let $T(n) = 2T\left(\left\lfloor\frac{n}{2}\right\rfloor\right) + n$, $T(1) = 0$. We assume $T\left(\left\lfloor\frac{n}{2}\right\rfloor\right) = O\left(\left\lfloor\frac{n}{2}\right\rfloor\right)$ inductively with $T\left(\frac{n}{2}\right) < c\frac{n}{2}$. It follows that $T(n) \leq 2c\left\lfloor\frac{n}{2}\right\rfloor + n \leq (c+1)n = O(n)$.

Being an element of $O(h(n))$ can't be shown directly via induction, so here the assumption must have been that $T\left(\frac{n}{2}\right) < c\frac{n}{2}$, but the same has not been proven about $T(n)$, only that $T(n) < (c+1)n$.

## Exercise 5.7

Let $T(n) = 2T(\lfloor\sqrt{n}\rfloor) + \lg n$. Using the substitution $n = 2^m$, show that $T(n) = O(\lg n \lg\lg n)$.

## Exercise 5.8

Determine the order of magnitude of $T(n)$ in the following cases: [The author has not specified the initial conditions, for convenience, $T(0)$ is assumed to be 0.]

1. $T(n) = 3T(n-1) + n^2 2^n$,

   Our claim is that $T(n) \in O(n3^n)$. By induction we shall show that $T(n) \leq 2n3^n$. The base case holds, so, for inductive step, assume that $T(n) \leq 2n3^n$ for some $n$. We thus have the following inequalities:

$$n^2\left(\frac{2}{3}\right)^n \leq 6$$

$$n^2 2^n \leq 6 \cdot 3^n$$

$$6n3^n + n^2 2^n \leq 6n3^n + 6 \cdot 3^n$$

$$6n3^n + n^2 2^n \leq 2n3^{n+1} + 2 \cdot 3^{n+1}$$

$$T(n+1) = 3T(n) + n^2 2^n \leq 6n3^n + n^2 2^n \leq 2(n+1)3^{n+1}$$

   To prove the first inequality, we look for the largest values of $n^2\left(\frac{2}{3}\right)^n$ by first observing that it is decreasing for $n \geq 5$.

$$(n-2)^2 \geq (5-2)^2 = 3^2 = 9 \geq 6$$

$$n^2 - 4n + 4 \geq 6$$

$$n^2 \geq 4n + 2$$

$$3n^2 \geq 2n^2 + 4n + 2 = 2(n^2 + 2n + 1) = 2(n+1)^2$$
$$3n^2 \left(\frac{2}{3}\right)^n \geq 2(n+1)^2 \left(\frac{2}{3}\right)^n$$
$$n^2 \left(\frac{2}{3}\right)^n \geq (n+1)^2 \left(\frac{2}{3}\right)^{n+1}$$

Meaning that we need to compare the values at $n = 0, 1, 2, 3, 4$ and 5.

For $n = 0$, $n^2 \left(\frac{2}{3}\right)^n = 0$.

For $n = 1$, $n^2 \left(\frac{2}{3}\right)^n = \frac{2}{3}$.

For $n = 2$, $n^2 \left(\frac{2}{3}\right)^n = \frac{8}{9}$.

For $n = 3$, $n^2 \left(\frac{2}{3}\right)^n = \frac{8}{3}$.

For $n = 4$, $n^2 \left(\frac{2}{3}\right)^n = \frac{256}{81}$.

For $n = 5$, $n^2 \left(\frac{2}{3}\right)^n = \frac{800}{243}$.

Clearly, we thus have $n^2 \left(\frac{2}{3}\right)^n \leq 6$. This finishes the proof. (One may as well verify that $T(n) = 30(3^n - 2^n) - n(n+6)2^{n+1}$.)

2. $T(n) = 3T(n-1) + \frac{n+1}{n+2}3^n$,

Our claim is that $T(n) \in O(3^n(n + \lg n))$. By induction we shall show that $T(n) \leq 3^n(n + \lg n)$ for $n \geq 1$. The base case, $n = 1$, clearly holds since $T(1) = 3T(0) + 2 = 2 \leq 3 = 3^1(1 + \log 1)$. For inductive step, assume that $T(n) \leq 3^n(n + \lg n)$ for some $n$. We thus have the following inequalities:

$$\frac{n+1}{n+2} \leq \frac{n+2}{n+2} = 1 \leq 3$$
$$\frac{n+1}{n+2}3^n \leq 3^{n+1}$$
$$3^{n+1}(n + \lg n) + \frac{n+1}{n+2}3^n \leq 3^{n+1}(n + \lg n) + 3^{n+1}$$
$$T(n+1) = 3T(n) + \frac{n+1}{n+2}3^n \leq 3 \cdot 3^n(n + \lg n) + \frac{n+1}{n+2}3^n \leq$$

$$\leq 3^{n+1}(n+1+\lg n) \leq 3^{n+1}(n+1+\lg(n+1))$$

This finishes the proof. (One may as well verify that $T(n) = 3^n(n + H_{n+2} - \frac{3}{2})$.)

3. $T(n) = 2T(n-1) + \frac{1+n^2}{3+n^2}2^{n-1}$,

Our claim is that $T(n) \in O(n2^n)$. By induction we shall show that $T(n) \leq 2^n$. The base case clearly holds. For inductive step, assume that $T(n) \leq n2^n$ for some $n$. We thus have the following inequalities:

$$\frac{1}{4} \leq 1 = C$$
$$2^{-2} \leq C$$
$$2^{n-1} \leq C2^{n+1}$$
$$Cn2^{n+1} + 2^{n-1} \leq Cn2^{n+1} + C2^{n+1}$$
$$T(n+1) = 2T(n) + \frac{1+n^2}{3+n^2}2^{n-1} \leq 2Cn2^n + \frac{1+n^2}{3+n^2}2^{n-1} \leq$$
$$\leq Cn2^{n+1} + 2^{n-1} \leq C(n+1)2^{n+1}$$

This finishes the proof. (One may as well verify that $T(n) = 2^{n-1}\left(\sum\limits_{i=0}^{n} \frac{1+i^2}{3+i^2} - \frac{1}{3}\right)$.)

4. $T(n) = 2T(n/3) + n\sqrt{n}$.

...

## Exercise 5.9

Suppose we have an algorithm that for an input of length $n$, executes $n$ steps, where the $i$th step requires $i^2$ operations. Show that the running time of the algorithm is $O(n^3)$.

Let $T(n)$ be the running time of the algorithm so that $T(n) = \sum\limits_{i=0}^{n} i^2$, meaning $T(0) = 0$ and $T(n+1) = T(n) + (n+1)^2$. By induction we shall show that $T(n) \leq n^3$. The base case clearly holds. For inductive step, assume that $T(n) \leq n^3$ for some $n$. We thus have the following inequalities.

$$\begin{gathered} 0 \leq n(2n+1) \\ 0 \leq 2n^2 + n \\ n^2 + 2n \leq 3n^2 + 3n \\ n^3 + n^2 + 2n + 1 \leq n^3 + 3n^2 + 3n + 1 \\ T(n+1) = T(n) + (n+1)^2 \leq n^3 + n^2 + 2n + 1 \leq (n+1)^3 \end{gathered}$$

## Exercise 5.10

An addition chain for $n$ is a sequence $1 = a_1, a_2, \ldots, a_m = n$ such that for every $k$, we have $a_k = a_i + a_j$ for some $i, j < k$. Example: $n = 19$, $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 8$, $a_5 = 9 = 8 + 1$, $a_6 = 17 = 9 + 8$, $a_7 = 19 = 17 + 2$. Let $\ell(n)$ be the minimal length of an addition chain for $n$. Show that $\lg n \leq \ell(n) \leq 2 \lg n$. Are there integers $n$ for which $\ell(n) = \lg n$?

We begin by proving that an addition chain for $n$ with minimal length is $1, 2, 4, \ldots, 2^k$ when $n = 2^k$ via induction on $k$. The base case $k = 0$ is trivial. For inductive step assume the hypothesis is true and claim it to be true for $2^{k+1}$. Since an addition chain for $2^k$ with minimal length is $1, 2, 4, \ldots, 2^k$, an addition chain for $2^{k+1}$ with minimal length is $1, 2, 4, \ldots, 2^k, 2^{k+1}$. (If it was shorter, then it would contradict the minimality of the sequence $1, 2, 4, \ldots, 2^k$.) This shows that $l(2^k) = k + 1$.

Via repeated Euclidean algorithm we obtain $n = \sum\limits_{i \in A} 2^i$ for some $A \subseteq \{0, \ldots, \lfloor \lg n \rfloor\}$. Let $A$ be ordered so that $a_k$ denotes the $k$-th least element in

$A$. Our claim is that it follows that the addition chain $\{x_k\}_{k=1}^{l(n)}$ is of minimal length where $x_k$ is defined as follows.

$$x_k = \begin{cases} 2^{k-1}, & 1 \leq k \leq \lfloor \lg n \rfloor + 1 \\ \sum\limits_{\substack{j \in A \\ j \leq a_k}} 2^j, & \lfloor \lg n \rfloor + 1 < k \leq l(n) \end{cases}$$

Which implies $\lfloor \lg n \rfloor + 1 \leq l(n) \leq 2 \lfloor \lg n \rfloor + 1$. $\lg n < l(n)$ is clearly implied. We now consider two cases on $A$. If $A \subset \{0, \ldots, \lfloor \lg n \rfloor\}$. Then $l(n) \leq 2 \lfloor \lg n \rfloor \leq 2 \lg n$. If however, $A = \{1, \ldots, \lfloor \lg n \rfloor\}$, then $n = \sum\limits_{0 \leq i \leq \lfloor \lg n \rfloor} 2^i = 2^{\lfloor \lg n \rfloor + 1} - 1$ and we have hence

$$1 < (2 - \sqrt{2}) 2^{\lfloor \lg n \rfloor}$$

$$2^{\lfloor \lg n \rfloor} \sqrt{2} < 2 \cdot 2^{\lfloor \lg n \rfloor} - 1$$

$$\lfloor \lg n \rfloor + \frac{1}{2} < \lg(2^{\lfloor \lg n \rfloor + 1} - 1)$$

$$2 \lfloor \lg n \rfloor + 1 < 2 \lg(2^{\lfloor \lg n \rfloor + 1} - 1)$$

$$2 \lfloor \lg n \rfloor + 1 < 2 \lg n$$

Finally, if we let $l(n) = \lg n$. Then $\lg n$ must be an integer, i.e., $n = 2^k$ for some natural $k$, but then $l(n) = k + 1$ as we have already shown, hence $l(n) \neq \lg n$ for all $n$.

## Exercise 5.11

Show that every permutation $a_1 a_2 \ldots a_n$ can be brought via successive exchanges of neighbouring elements into the form $12 \ldots n$. Example: 3124 → 3214 → 2314 → 2134 → 1234. What is the minimal number of exchanges?

...

### Exercise 5.12

Carefully verify whether the following equation is correct: $\sum\limits_{k=0}^{n}(k^2 + O(k)) = \frac{n^3}{3} + O(n^2)$. Note that this is a set comparison (from left to right).

Define a sequence of functions $f_0, \ldots, f_k : \mathbb{Z} \to \mathbb{R}$ with $f_k \in O(k)$ for all $i \in \{0, \ldots, n\}$, i.e., there exist $C_k > 0$ and $n_k$ with $|f_k| \leq C_k k$ for all $n \geq n_k$. Let $n \leq \max\{n_k \mid k \in \{0, \ldots, n\}\}$ and $C = \max\{C_k \mid k \in \{0, \ldots, n\}\}$. We hence have

$$\sum_{i=0}^{n}(k^2+f_k) \leq \sum_{k=0}^{n}(k^2+C_k k) \leq \sum_{k=0}^{n} k^2+C\sum_{k=0}^{n} k = O(n^3)+O(Cn^2) = O(\frac{n^3}{3})+O(n^2) = O(\frac{n^3}{3}+n^2) =$$

Via transitivity of $O$, we get $\sum\limits_{k=0}^{n}(k^2 + f_k) \in \frac{n^3}{3} + O(n^2)$.

### Exercise 5.13

Show that $O(x + y)^2 = O(x^2) + O(y^2)$ for real numbers $x, y$.

...

## 6.3 Definitions

In this section by "function" we shall mean a function with domain a subset of $\mathbb{R}$ containing $\mathbb{N}$ and codomain $\mathbb{R}$.

**Definition 33** (Big O/Small o)**.** *For functions $f, g$ with same domain we say $f \in O(g)$ or $f(x) \in O(g(x))$ if and only if there exists $C > 0$ and $x_0$ such that $|f(x)| \leq C|g(x)|$ given $x \geq x_0$. One may write $f = O(g)$ or $f(x) = O(g(x))$ instead.*

*We also say $f \in o(g)$ or $f(x) \in o(g(x))$ if and only if for all $\varepsilon > 0$ there exists $x_0$ such that $|f(x)| \leq \varepsilon|g(x)|$ given $x \geq x_0$. One may write $f = o(g)$, $f(x) = o(g(x))$, $f \prec g$ or $f(x) \prec g(x)$ instead.*

**Definition 34** (Big $\Omega$/Small $\omega$)**.** *For functions $f, g$ with same domain we say $f \in \Omega(g)$ or $f(x) \in \Omega(g(x))$ if and only if $g \in O(f)$. One may write $f = \Omega(g)$ or $f(x) = \Omega(g(x))$ instead.*

*We also say $f \in \omega(g)$ or $f(x) \in \omega(g(x))$ if and only if $g \in o(f)$.One may write $f = \omega(g)$ or $f(x) = \omega(g(x))$ instead.*

**Definition 35** (Big $\Theta$)**.** *For function $g$ we define $\Theta(g) = O(g) \cap \Omega(g)$. One may write $f = \Theta(g)$ or $f(x) = \Theta(g(x))$ instead of $f \in \Theta(g)$ with $f$ a function with same domain as $g$.*

# Chapter 7

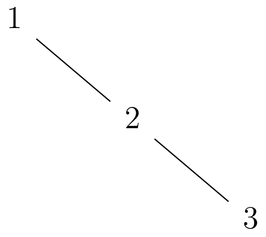
# Graph theory

## 7.1 Week 8 Central Exercises

### Exercise 1

Choose some labeling and indicate the set of vertices and edges for graphs on Figure 1; determine circuits if any. Write down adjacency and incidence matrices for your labeling and determine the corresponding bandwidth.

1.



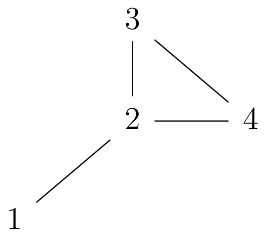
For the given graph, the set of vertices $V = \{1, 2, 3\}$ and the set of edges $E = \{\{1, 2\}, \{2, 3\}\}$. There are no non-trivial circuits. Let the labelling on the edges be $e_1 = \{1, 2\}$ and $e_2 = \{2, 3\}$. The adjacency and incidence matrices, respectively, are hence written as follows:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

The bandwidth, given this labelling, is 1.

2.



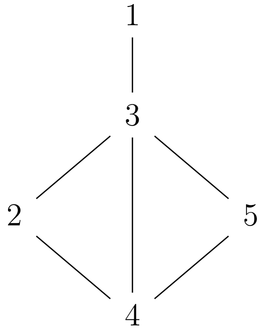
For the given graph, the set of vertices $V = \{1, 2, 3, 4\}$ and the set of edges $E = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$. Besides the trivial circuits there is one given by the sequence $2, 3, 4$. Let the labelling on the edges be $e_1 = \{1, 2\}$, $e_2 = \{2, 3\}$, $e_3 = \{2, 4\}$ and $e_4 = \{3, 4\}$. The adjacency and incidence matrices, respectively, are hence written as follows:

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

The bandwidth, given this labelling, is 2.

3.



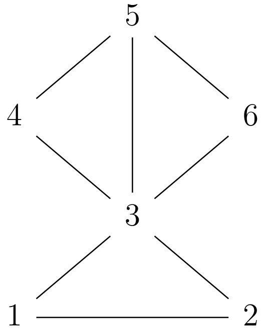
For the given graph, the set of vertices $V = \{1, 2, 3, 4, 5\}$ and the set of edges $E = \{\{1, 3\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\}$. Besides the trivial circuits there is three given by the sequences $2, 3, 5, 4$ and $2, 3, 4$ and $3, 4, 5$. Let the labelling on the edges be $e_1 = \{1, 3\}$, $e_2 = \{2, 3\}$, $e_3 = \{2, 4\}$, $e_4 = \{3, 4\}$, $e_5 = \{3, 5\}$, $e_6 = \{4, 5\}$. The adjacency and incidence matrices, respectively, are hence written as follows:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

The bandwidth, given this labelling, is 2.

4.



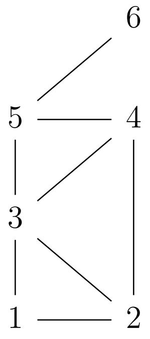
For the given graph, the set of vertices $V = \{1,2,3,4,5,6\}$ and the set of edges $E = \{\{1,2\},\{1,3\},\{2,3\},\{3,4\},\{3,5\},\{3,6\},\{4,5\},\{5,6\}\}$. Besides the trivial circuits there are four given by the sequences $1,2,3$ and $3,4,5$ and $3,5,6$ and $3,4,5,6$. Let the labelling on the edges be $e_1 = \{1,2\}$, $e_2 = \{1,3\}$, $e_3 = \{2,3\}$, $e_4 = \{3,4\}$, $e_5 = \{3,5\}$, $e_6 = \{3,6\}$, $e_7 = \{4,5\}$ and $e_8 = \{5,6\}$. The adjacency and incidence matrices, respectively, are hence written as follows:

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

The bandwidth, given this labelling, is 3.

5.



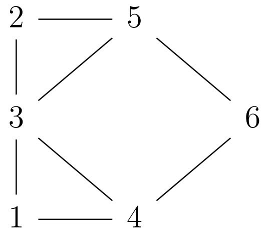
For the given graph, the set of vertices $V = \{1, 2, 3, 4, 5, 6\}$ and the set of edges $E = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{3, 5\}, \{4, 5\}, \{5, 6\}\}$. Besides the trivial circuits there are six given by the sequences $1, 2, 3$ and $3, 4, 5$ and $2, 3, 4$ and $1, 3, 4, 2$ and $2, 3, 5, 4$ and $1, 2, 4, 5$. Let the labelling on the edges be $e_1 = \{1, 2\}$, $e_2 = \{1, 3\}$, $e_3 = \{2, 3\}$, $e_4 = \{2, 4\}$, $e_5 = \{3, 4\}$, $e_6 = \{3, 5\}$, $e_7 = \{4, 5\}$ and $e_8 = \{5, 6\}$. The adjacency and incidence matrices, respectively, are hence written as follows:

$$\begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The bandwidth, given this labelling, is 2.

6.



For the given graph, the set of vertices $V = \{1, 2, 3, 4, 5, 6\}$ and the set of edges $E = \{\{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 5\}, \{3, 4\}, \{3, 5\}, \{4, 6\}, \{5, 6\}\}$. Besides the trivial circuits there are six given by the sequences $1, 3, 4$ and $2, 3, 5$ and $3, 4, 6, 5$ and $1, 3, 5, 6, 4$ and $2, 3, 4, 6, 5$ and $1, 3, 2, 5, 6, 4$. Let the labelling on the edges be $e_1 = \{1, 3\}$, $e_2 = \{1, 4\}$, $e_3 = \{2, 3\}$, $e_4 = \{2, 5\}$, $e_5 = \{3, 4\}$, $e_6 = \{3, 5\}$, $e_7 = \{4, 6\}$ and $e_8 = \{5, 6\}$. The adjacency and incidence matrices, respectively, are hence written as follows:

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

The bandwidth, given this labelling, is 3.

## Exercise 2

Let $G$ be a graph with at least two vertices. Show that $G$ always has two vertices of the same degree.

See Exercise 6.1 of the following section.

## Exercise 3

Determine the graphs with $n \geq 2$ vertices that have $n-1$ different degrees.

See Exercise 6.2 of the following section.

## Exercise 4

Prove the remark from the lecture: an edge is a cut edge if and only if it is not contained in any circuit.

See Exercise 6.14 of the following section.

## Exercise 5

1. Show that the relation $\sim$ given by $G \sim G'$ if and only if there is an isomorphism $f : G \to G'$ is an equivalence relation. What are the corresponding equivalence classes?

   We first prove reflexivity. Consider the identity mapping of $V$. It is clearly a bijection, so we just show that the isomorphism property holds. If $\{u, v\} \in E$ for some $u, v \in V$ where $G = (V, E)$ is a graph, then $\{\mathcal{I}_V(u), \mathcal{I}_V(v)\} = \{u, v\} \in E$ where $\mathcal{I}_V$ is the identity map of $V$. Conversely, let $\{\mathcal{I}_V(v), \mathcal{I}_V(u)\} \in E$, then $\{u, v\} = \{\mathcal{I}_V(v), \mathcal{I}_V(u)\} \in E$. Hence $G \sim G$.

   For symmetry, assume $G \sim G'$ for some graphs $G = (V, E)$ and $G' = (V', E')$, i.e., there is an isomorphism $\varphi : G \to G'$ and consider the mapping $\varphi^{-1} : G' \to G$. $\varphi$ is a bijection, so is $\varphi^{-1}$. Since $\{u, v\} \in E$ if and only if $\{\varphi(u), \varphi(v)\} \in E'$, we can pick $x, y \in V'$ such that $\varphi^{-1}(x) = u$ and $\varphi^{-1}(y) = v$. Rewriting the isomorphism property of $\varphi$ in terms of $x$ and $y$ yields $\{\varphi^{-1}(x), \varphi^{-1}(y)\} \in E$ if and only if $\{x, y\} \in E'$, which makes $\varphi^{-1}$ also an isomorphism, meaning $G' \sim G$

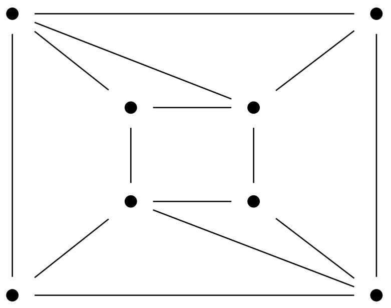
For transitivity, assume that $G_1 \sim G_2$ and $G_2 \sim G_3$ for some graphs $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ and $G_3 = (V_3, E_3)$, i.e., there exist isomorphisms $\varphi : G_1 \to G_2$ and $\varphi' : G_2 \to G_3$. Our claim is that $\varphi' \circ \varphi$ is an isomorphism. Composition of bijections is always a bijection and we also have $\{u, v\} \in E_1$ for some $u, v$ if and only if $\{\varphi(u), \varphi(v)\} \in E_2$, which itself happens if and only if $\{\varphi'(\varphi(u)), \varphi'(\varphi(v))\} \in E_3$. We got that $\{u, v\} \in E_1$ if and only if $\{(\varphi' \circ \varphi)(u), (\varphi' \circ \varphi)(v)\} \in E_3$, hence $\varphi' \circ \varphi$ is also an isomorphism, i.e., $G_1 \sim G_3$.

Since $\sim$ is reflexive, symmetric and transitive, it is also an equivalence relation where equivalence classes contain isomorphic graphs.

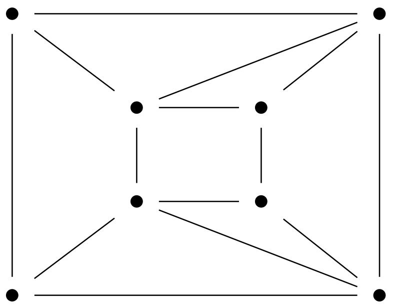
2. Are any of the graphs on Figure 1 (the ones from Exercise 1 of this section) isomorphic?

(1) is the only graph with 3 vertices, (2) is the only graph with 4 vertices, (3) is the only graph with 5 vertices, (4) is the only graph with a vertex of degree 5, (5) is the only graph with 6 vertices and a vertex of degree 1, (6) is the only graph with 6 vertices, no vertex of degree 1 or 5. Hence none of the graphs are isomorphic.

3. Are graphs pictured in Figure 2 (the ones below) isomorphic?



*G*



*H*

No, since in $H$ there is a circuit of 4 vertices with degree 4 each, in $G$, however, there is no such circuit.

## Exercise 6

Show that a graph with $n$ vertices and $q$ edges has at least $n-q$ components.

See Exercise 6.8 of the following section.

## Exercise 7

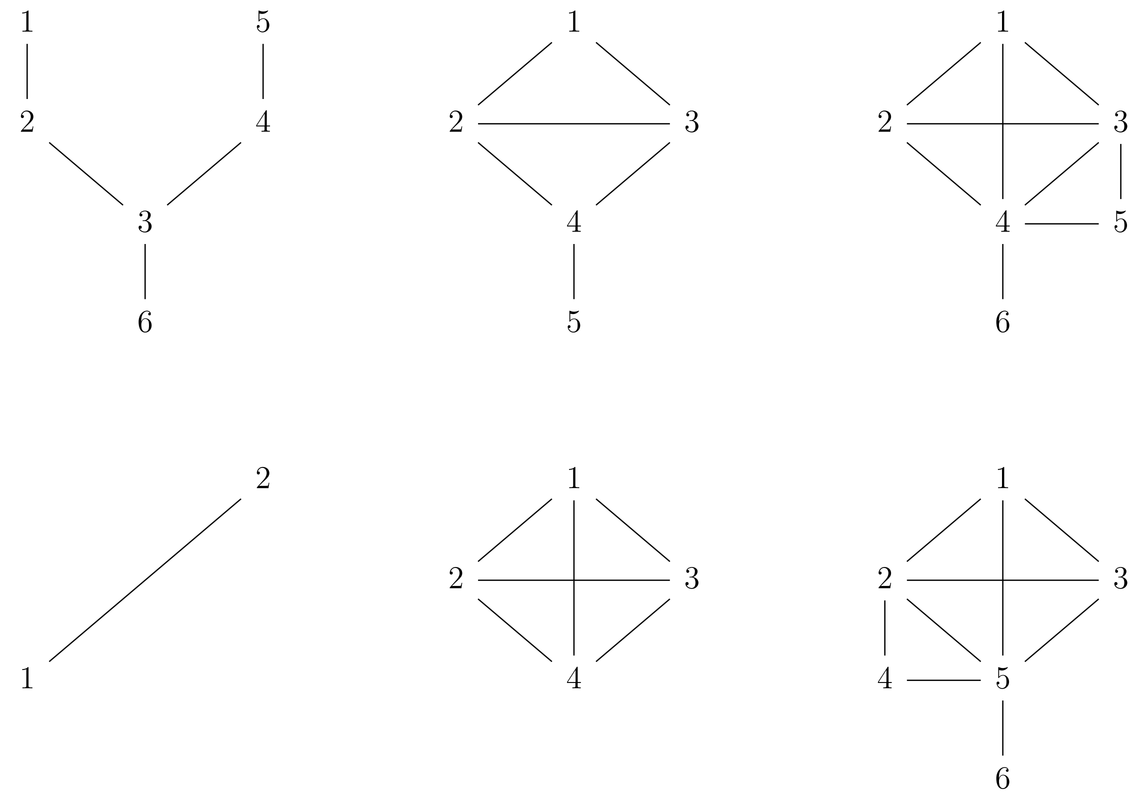
Suppose a graph $G = (V, E)$ with $|E| \geq 3$ and without isolated vertices has no induced subgraphs with exactly two vertices. Show that $G = K_n$, $n \geq 4$.

See Exercise 6.15 of the following section.

## 7.2 Week 9 Central Exercises

### Exercise 1

Which of the graphs depicted on Figure 1 are bipartite, trees, paths and/or a complete graphs. [For convenience, I have labelled the nodes for each graph.]



The fist graph is a bipartite graph with parts $\{1, 3, 5\}$ and $\{2, 4, 6\}$ since the edges $\{1, 3\}$, $\{1, 5\}$, $\{3, 5\}$, $\{2, 4\}$, $\{2, 6\}$ and $\{4, 6\}$ are absent. It is also a tree since it is connected and has no circuits. It is not a path as a path with 6 vertices would have 5 edges. It is not complete since the edge $\{1, 3\}$ is absent.

The second graph is not bipartite since, clearly, there can't be a part formed with 1 or $\geq 3$ vertices and choosing $\{1, 4\}$ as a part is invalid since then the $\{2, 3\}$ is present in the other part. It is not a tree since there is a circuit given by the sequence $1, 2, 3$. It is not a path as a path with 5 vertices would have 4 edges. It is not complete as the edge $\{1, 4\}$ is absent.

The third graph is not bipartite as the vertex 4 is a neighbour of every other vertex, meaning, if there was a part containing 4, then it must be $\{4\}$ itself (as otherwise we would have an edge in that part), but then the edge $\{1, 2\}$ is present in the other part. It is not a tree as there is a circuit given by the sequence $1, 2, 3$. It is not a path as a path with 6 vertices would have 5 edges. It is not complete as the edge $\{1, 5\}$ is absent.

The fourth graph is a bipartite graph with parts $\{1\}$ and $\{2\}$. It is a tree as it is connected and has no circuits. It is the path given by the sequence $1, 2$ since the edge $\{1, 2\}$ is present. It is also complete.

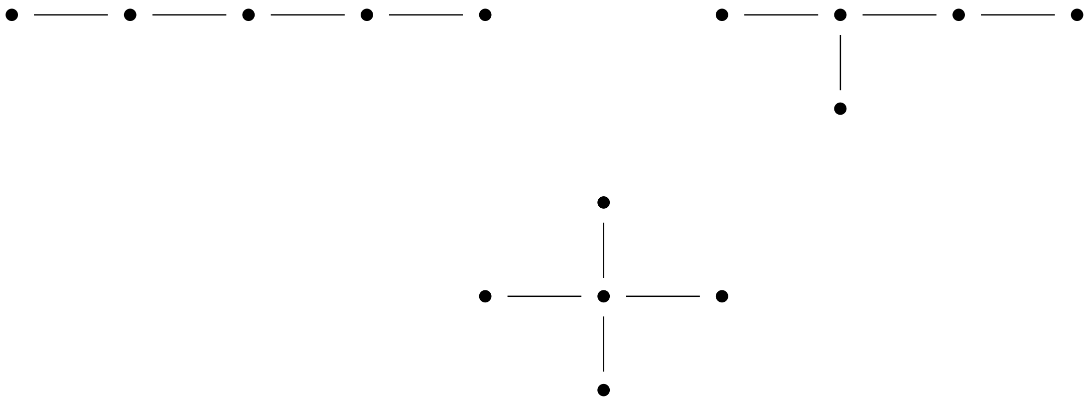
The fifth graph is not a bipartite graph as the vertex 1 is a neighbour of every other vertex, meaning, if there was a part containing 1, then it must be $\{1\}$ (as otherwise we would have an edge present in that part), but then the edge $\{2, 3\}$ is present in the other part. It is not a tree as there is a circuit given by the sequence $1, 2, 3$. It is not a path as a path with 4 vertices would have 3 edges. It is complete.

The sixth graph is isomorphic to the third graph, so it not bipartite, not a tree, not a path and not complete.

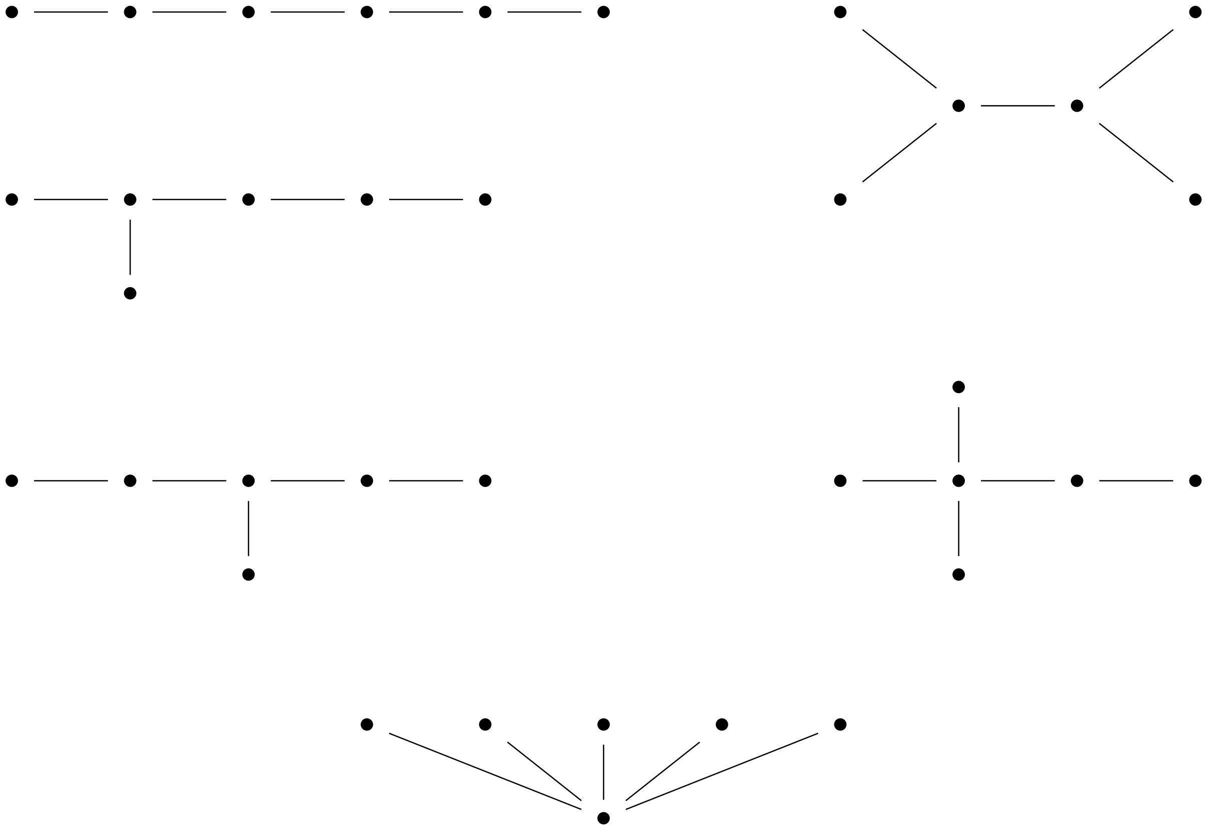
## Exercise 2

Draw all non-isomorphic trees with 5, 6 and 7 vertices. *Hint*: There are 3, 6 and 11 trees respectively.

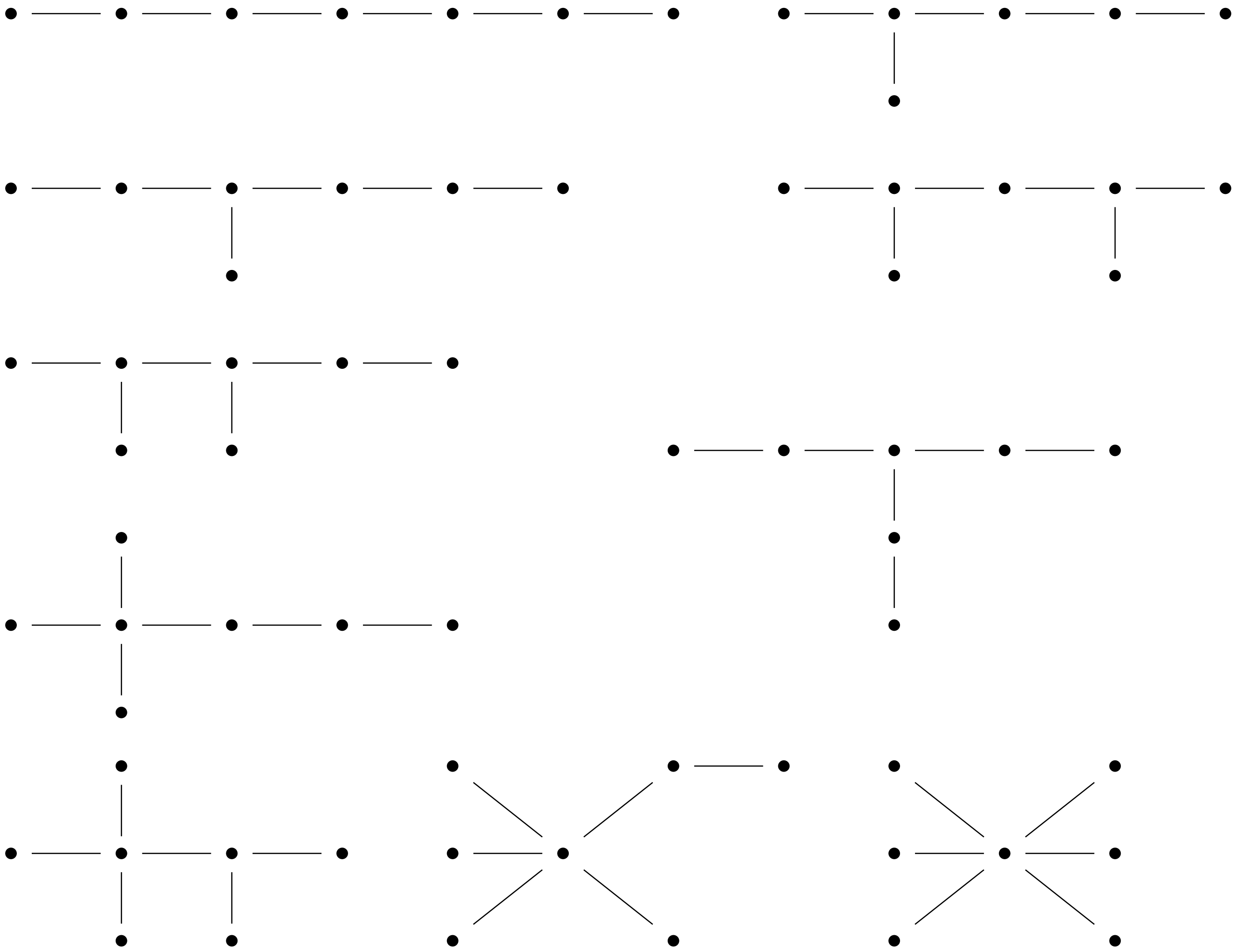
Here are all non-isomorphic trees with 5 vertices:



Here are all non-isomorphic trees with 6 vertices:



Here are all non-isomorphic trees with 7 vertices:

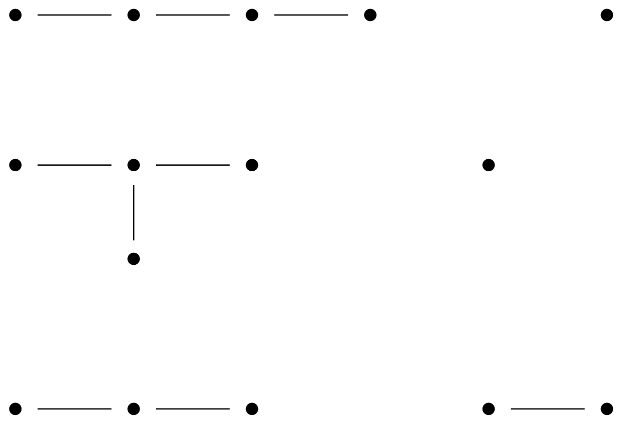


### Exercise 3

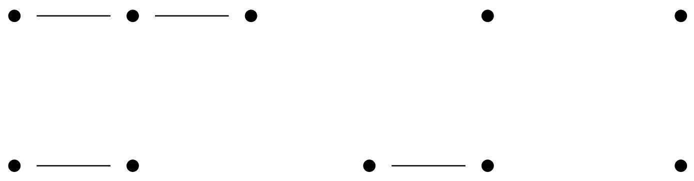
Draw all non-isomorphic forests with 5 vertices and two or more components.

Since there are 5 vertices and each component should consist of at least 1 vertex, we have four cases, namely, the graph has either 2, 3, 4 or 5 components.

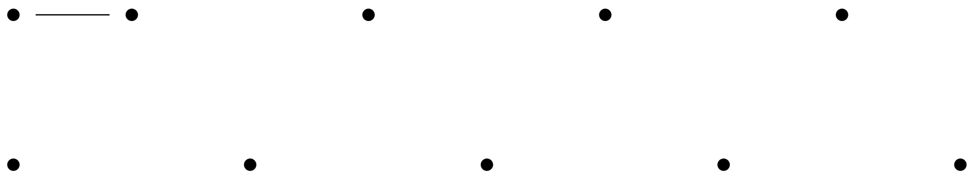
Let us consider the first case. There are two components and, obviously, the number of vertices of each shall add up to 5. We hence have 2 subcases, namely, the components contain 1 and 4 vertices respectively, or 2 and 3. We thus arrive at the following forests: [To avoid confusion, there is one tree per each row]



Similarly, for the second case, there are three subcases, namely, the three components that the forest is supposed to have either contain contain 1, 1 and 3 vertices respectively 1, 2 and 2. We thus arrive at the following forests:

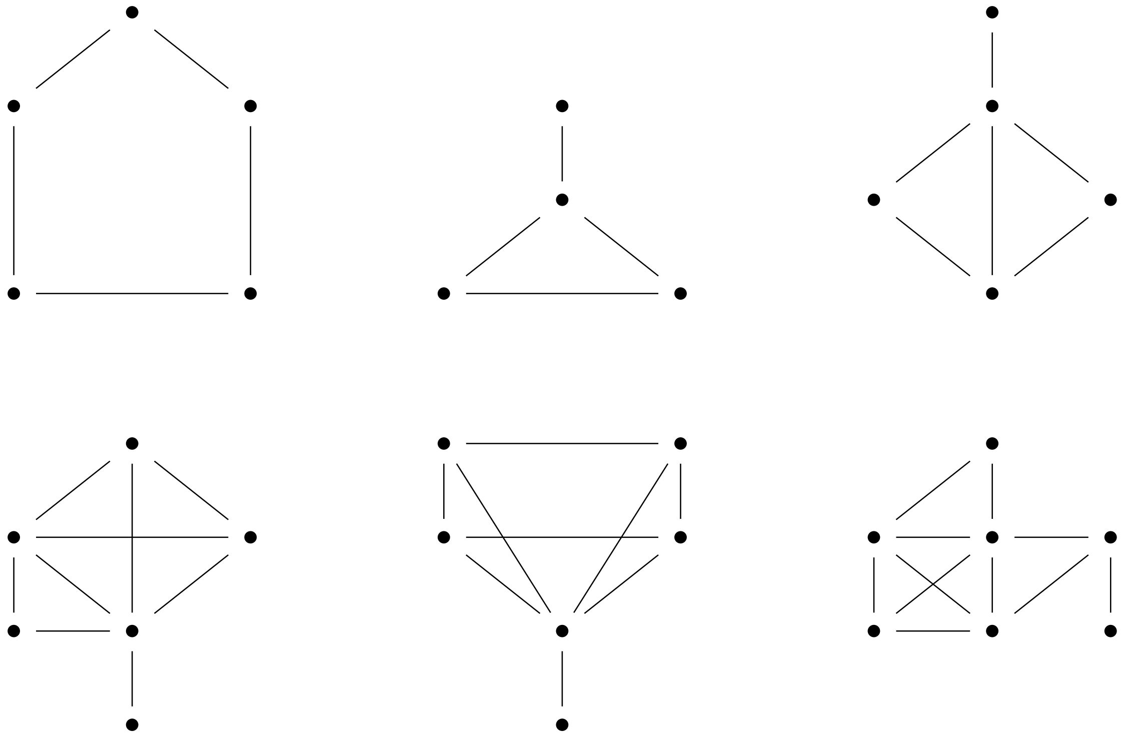


And for the other cases we simply get the following forests:

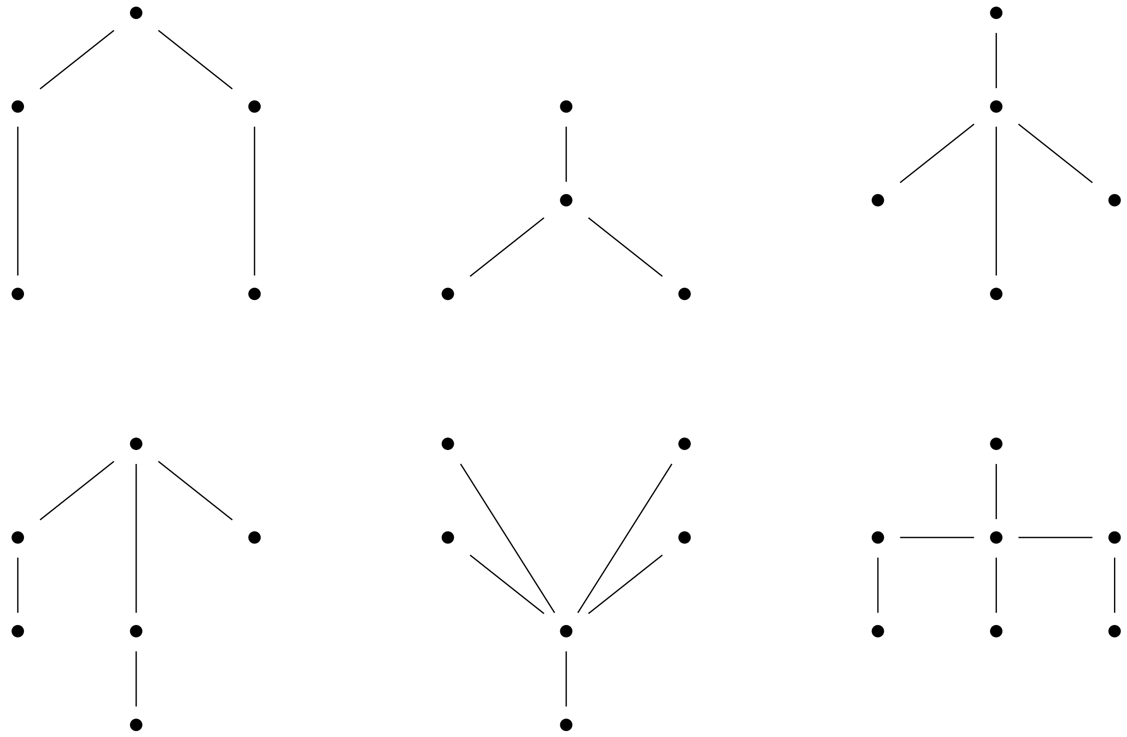


## Exercise 4

Determine the spanning trees for all graphs on Figure 2.



The most straightforward way of getting a spanning tree given a connected graph is by finding a circuit, removing one of its edges and repeating this step until there is no circuit. (If the graph already has no circuits to begin with, we do not have to do anything.) Do note that the final result may depend on the choice of the edges being removed, so this "algorithm" is non-deterministic. For the given graphs, one may obtain the following spanning trees:



## Exercise 5

Show that $G$ is a tree if and only if $G$ is connected and every edge is a cut edge.

Let $G = (V, E)$ be a tree. $G$ is immediately connected. Now, consider an edge $e = \{u, v\} \in E$ for some $u, v \in V$. Since removing an edge cannot decrease the amount of components in a graph, we have two cases for the amount of components in $G \setminus \{e\}$, namely, it either increased or stayed the same. If it increased, then $\{u, v\}$ is a cut edge by definition and we are done. If it stayed the same, then it would mean that $u$ is reachable from $v$, which would mean that there is a path $P$ from $v$ to $u$. The latter is a contradiction as $P$ would form a circuit in $G$ due to the edge $\{u, v\}$, but $G$ supposedly has no circuits.

Conversely, let $G$ be a connected graph such that every edge in it is a cut edge and assume that there is a circuit $C$ containing some vertices edge $e = \{u, v\} \in E$ where $u, v \in V$. According to the definition of a cut edge, $u$ is not reachable from $v$ in $G \setminus \{e\}$ (otherwise it would mean that the amount of components has not increased). The latter is a contradiction as $C$ forms a path in $G \setminus \{e\}$ from $v$ to $u$, which would mean that $u$ is reachable from $v$. By contradiction, we get that $G$ must contain no circuits and, along with the fact that it is connected, we conclude that $G$ is a tree.

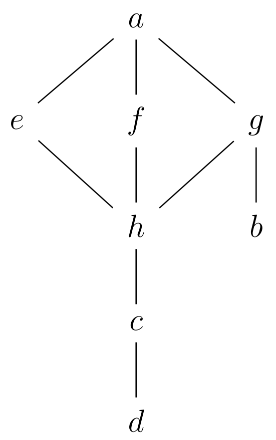
## Exercise 6

(1) Perform a breadth-first and depth-first searches on graphs given by the adjacency matrices

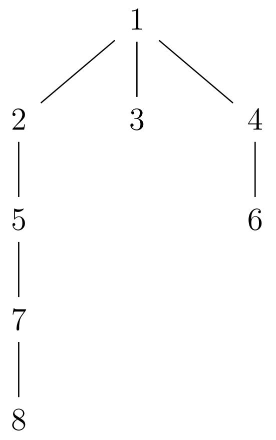
$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

And sketch the corresponding spanning trees.

For convenience, we shall draw the graph and name the vertices.

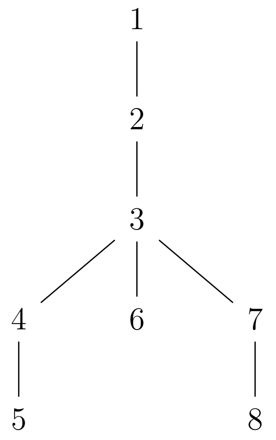


Let $a$ be the initial vertex during performance of each of the algorithms. Using breadth-first search, one may arrive at the following spanning tree:



Where the vertices $a$, $b$, $c$, $d$, $e$, $f$ and $g$ have been relabelled as 1, 6, 7, 8, 2, 3 and 4 respectively.

Using depth-first search, one may arrive at the following spanning tree:



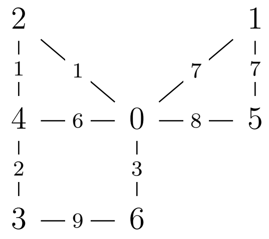
Where the vertices $a$, $b$, $c$, $d$, $e$, $f$ and $g$ have been relabelled as 1, 8, 4, 5, 2, 6 and 7.

(2) Show that if $G$ is not connected, breadth-first search algorithm halts with the assertion that the graph is not connected.

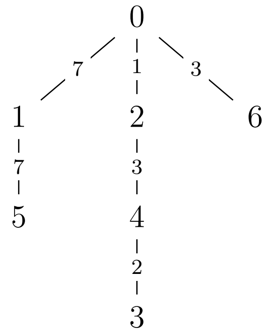
We shall prove the contrapositive of this statement, namely, that if the algorithm halts with the assertion that the graph is connected, then $G$ is indeed connected. Recall that the algorithm halts with the assertion that the graph is connected if and only if iterated over every vertex in the graph. We shall show that every vertex that the algorithm considers is reachable from the starting point by strong induction on the label $i$. We start with the base case $i = 2$ (if $G$ has only one vertex, then the assertion is immediately true), then the vertex $i$ is a neighbour of 1. Now, assume that every vertex with label $< i$ is reachable from the initial vertex. The vertex $i$ must have a neighbour whose number is lower, meaning that neighbour is reachable from the initial vertex and thus the vertex $i$ also is. Hence $G$ is connected.

## Exercise 7

Apply the greedy algorithm to find a minimal spanning tree for the weighted graph given on Figure 3 (Here, you should write down an ordered sequence of edges produced by the greedy algorithm).



If we choose 0 as out starting point and get the following minimal spanning tree:

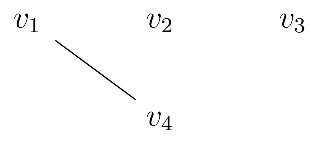


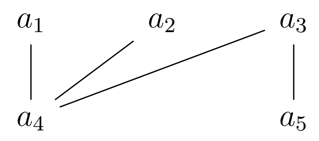
With ordered sequence of edges $(\{0,2\},\{2,4\},\{4,3\},\{0,6\},\{0,1\},\{1,5\})$.

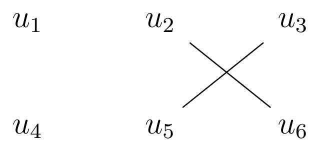
## 7.3 Week 10 Central Exercises

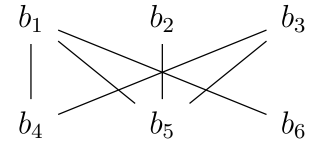
### Exercise 1

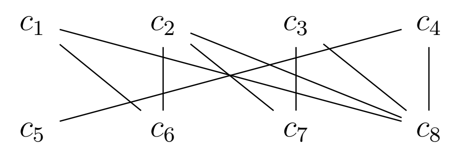
Determine maximum matching and a corresponding matching number for six graphs on Figure 1.

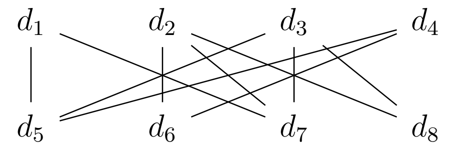












For the first and third graphs, the maximum matching is the set of edges itself. Hence for the first graph the matching number is 1 and 2 for the third graph.

For the second graph, there is a matching $\{\{a_1, a_4\}, \{a_3, a_5\}\}$ and it is maximal since it covers every vertex. Hence the matching number is 2.

For the fourth graph, there is a matching $\{\{b_1, b_6\}, \{b_2, b_5\}, \{b_3, b_4\}\}$ and it is maximal since it covers every vertex. Hence the matching number is 3.

For the fifth graph, there is a matching $\{\{c_1, c_6\}, \{c_2, c_7\}, \{c_3, c_8\}, \{c_4, c_5\}\}$ and it is maximal since it covers every vertex. Hence the matching number is 4.

For the sixth graph, there is a matching $\{\{d_1, d_7\}, \{d_2, d_8\}, \{d_3, d_5\}, \{d_4, d_6\}\}$ and it is maximal since it covers every vertex. Hence the matching number is 4.

## Exercise 2

Show that the bipartite graph $G = (S \cup T, E)$ given by a matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

does not have a matching $M$ with $|M| = 5$.

We look for a subset $A$ of $T$ such that $|A| > |N(A)|$. Assuming that the neighbours of vertices of $T$ are represented in the rows, the third and fourth vertex in $T$ have only one neighbour. Via marriage theorem, there is no matching $M$ with $|M| = |T| = 5$.

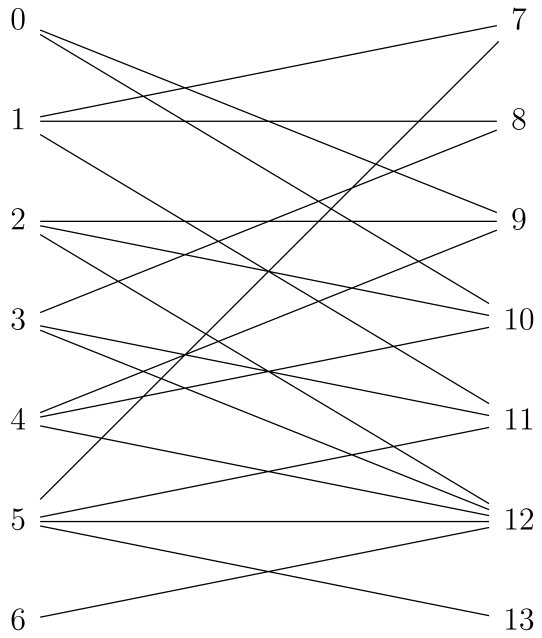
## Exercise 3

Recall the "equilibrium theorem" proved in the lecture.

1. Find the minimum vertex covers for bipartite graphs on Figure 1.

2. Find the minimum vertex covers for the graph from Exercise 2.

3. The set $\{1, 3, 5, 9, 10, 12\}$ is a minimum vertex cover for the left graph on Figure 2. Find a maximum matching.



For part 1, the minimum vertex covers for the first graph on Figure 1 are $\{v_1\}$ and $\{v_4\}$. For the second graph, the minimum vertex covers are $\{a_3, a_4\}$ and $\{a_4, a_5\}$. For the third graph, the minimum vertex covers are $\{u_2, u_3\}$, $\{u_3, u_6\}$, $\{u_2, u_5\}$ and $\{u_5, u_6\}$. For the fourth graph, the minimum vertex covers are $\{b_1, b_2, b_3\}$, $\{b_1, b_3, b_5\}$, $\{b_1, b_4, b_5\}$ and $\{b_2, b_4, b_6\}$. For the fifth graph, the minimum vertex covers are $\{c_1, c_2, c_3, c_4\}$, $\{c_3, c_4, c_6, c_8\}$, $\{c_3, c_5, c_6, c_8\}$, $\{c_4, c_6, c_7, c_8\}$ and $\{c_5, c_6, c_7, c_8\}$. For the sixth graph, the minimum vertex covers are $\{b_1, b_2, b_3, b_4\}$, $\{d_2, d_3, d_5, d_7\}$ and $\{d_5, d_6, d_7, d_8\}$.

For part 2, according to our result from Exercise 2, there is no matching with $|M| = 5$, meaning $|M| \leq 4$ for all matchings $M$. This shows that if there is a minimum vertex cover with 4 vertices, then it must be minimal. There indeed are vertex covers with 4 vertices, namely, $\{s_1, s_2, t_2, t_5\}$ and $\{s_2, t_1, t_2, t_5\}$.

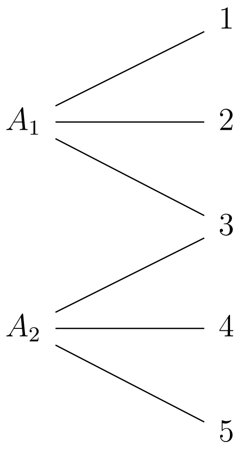
For part 3, according to equilibrium theorem, the maximal matching would have 6 edges. There indeed is a matching with 6 edges, namely, $\{\{0, 9\}, \{1, 7\}, \{3, 8\}, \{4, 10\}, \{5, 13\}, \{6, 12\}\}$. One may even verify by exhaustion that $\{1, 3, 5, 9, 10, 12\}$ is in fact the only minimum vertex cover.

## Exercise 4

Draw appropriate bipartite graphs and find a transversal (if it exists) for following family of sets: [The universal set is assumed to be the union of the sets.]

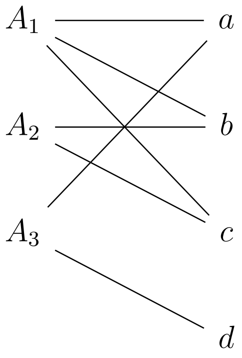
1. $A_1 = \{1, 2, 3\}$, $A_2 = \{3, 4, 5\}$;
2. $A_1 = \{a, b, c\}$, $A_2 = \{b, c\}$, $A_3 = \{a, d\}$;
3. $A_1 = \{a, b, c\}$, $A_2 = \{b, c\}$, $A_3 = \{c\}$, $A_4 = \{a, b, c, d\}$;
4. $A_1 = \{1, 2, 3\}$, $A_2 = \{1, 2, 3, 4\}$, $A_3 = \{1\}$, $A_4 = \{2\}$, $A_5 = \{4\}$.

For part 1, the appropriate bipartite graph looks as follows.



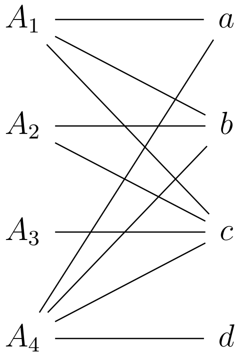
For a transversal, we may consider the injection $f : \{A_1, A_2\} \to \{1, 2, 3, 4, 5\}$ given by $f(A_1) = 1$ and $f(A_2) = 3$. The corresponding transversal is thus $\{1, 3\}$.

For part 2, the appropriate bipartite graph looks as follows.



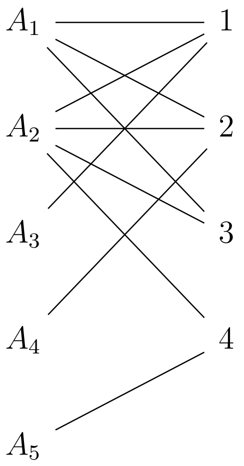
For a transversal, we may consider the injection $f : \{A_1, A_2, A_3\} \to \{a, b, c, d\}$ given by $f(A_1) = a$, $f(A_2) = b$ and $f(A_3) = d$. The corresponding transversal is thus $\{a, b, d\}$.

For part 3, the appropriate bipartite graph looks as follows.



For a transversal, we may consider the injection $f : \{A_1, A_2, A_3, A_4\} \to \{a, b, c, d\}$ given by $f(A_1) = a$, $f(A_2) = b$, $f(A_3) = c$ and $f(A_4) = d$. (In fact, we must consider that particular function since, as one may verify, that is the only selection function in this case.) The corresponding transversal is thus $\{a, b, c, d\}$.

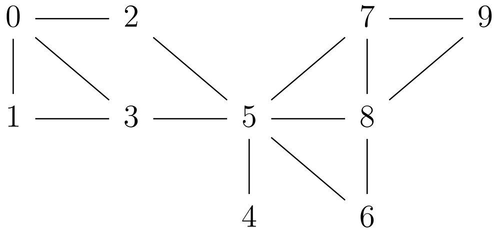
For part 3, the appropriate bipartite graph looks as follows.



There, however, is no selection function as the number of given set is 5, whereas the universal set has 4 elements and $5 > 4$, meaning there is no injective function.

## Exercise 5

Is the matching $M = \{\{0,2\},\{3,5\},\{7,8\}\}$ a maximum matching for a graph on Figure 3?



No, as there is a matching with larger cardinality, namely, $\{\{0,2\},\{1,3\},\{4,5\},\{6,8\},\{7,9\}\}$. (One may verify that this is in fact the only maximum matching.)

## Exercise 6

Alice, Bob, Camilla and Daniel are applying for jobs at company $X$. Alice applied for network architect and software tester, Bob for web developer and software tester, Camilla only for web development and Daniel for web developer, network architect and data scientist.

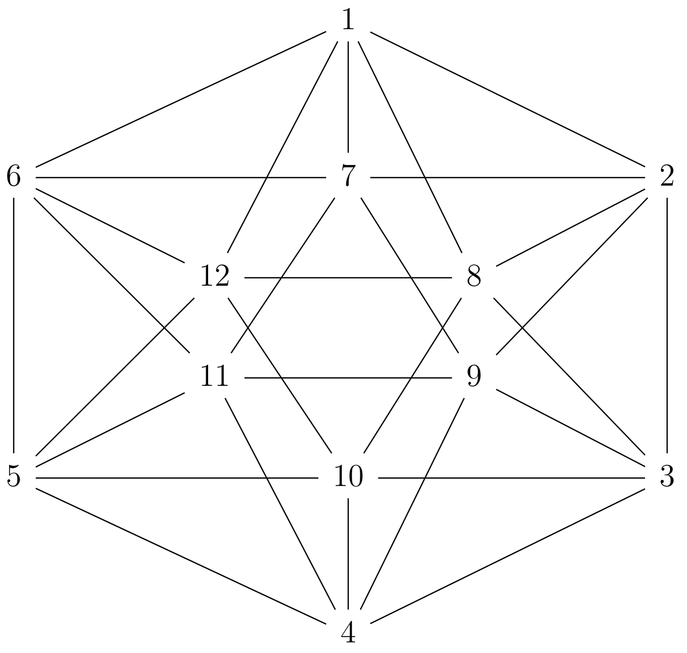
Company $X$ assigned a value coefficient to each applicant: $(1.5, 3, 5, 2)$ to Alice, Bob, Camilla and Daniel respectively.

Find a matching for a company that maximizes the value assigned. Which algorithm should we use? Why?

The problem can be translated into a problem of graph theory. Let $G$ be a bipartite graph where one part is the set containing Alice, Bob, Camilla and Daniel whereas the other part is the set of jobs mentions (network architect, software tester, web developer, data scientist) and let an edge connect a person and a job if and only if that person has applied for that job. Define the weight function $w$ on $G$ so that every edge incident to the vertices of Alice, Bob, Camilla and Daniel have weights 1.5, 3, 5, 2 respectively. The matching in $G$ with maximal weight gives the solution. Since transversals form a matroid, the greedy algorithm can work. In this case, though, each person can be given a job at the company $X$. Hire Alice as the network architect, Bob as the software tester, Camilla as the web developer and Daniel as the data scientist. This yields the value of 11.5 which is indeed maximal.

## Exercise 7

(1) Every platonic solid, considered as a graph, is Hamiltonian. Try to find one of 512 Hamiltonian circuits of the icosahedral graph on Figure 4. (2) Show that all hypercubes $Q_n$, $n \geq 2$ are Hamiltonian.



For part 1, there is a Hamiltonian circuit given by the sequence, 1, 2, 8, 12, 10, 4, 3, 9, 7, 11, 5, 6. For part 2, see Exercise 8.15 of the following section.

## Exercise 8

The cost matrix given by the following table of distances (in kilometers) between cities in Georgia.

| | Tb | K | B | P | Te |
|---|---|---|---|---|---|
| Tbilisi | - | 228 | 373 | 323 | 95 |
| Kutaisi | 228 | - | 151 | 100 | 315 |
| Batumi | 373 | 151 | - | 75 | 463 |
| Poti | 323 | 100 | 75 | - | 411 |
| Telavi | 95 | 315 | 463 | 411 | - |

Use the "nearest neighbour" and "double nearest-neighbour" algorithms to find shortest trips through all 5 cities starting in Kutaisi.

To apply the "nearest neighbour" algorithm, we start at Kutaisi and at each iteration pick the unvisited city with lowest cost available from the current city (if there are several such options, we pick any). We hence obtain the path

$$\text{Kutaisi} \xrightarrow{100} \text{Poti} \xrightarrow{75} \text{Batumi} \xrightarrow{373} \text{Tbilisi} \xrightarrow{95} \text{Telavi} \quad \text{(Total: 643)}$$

To apply the "double nearest neighbour" algorithm, however, we need to contemplate the weights of edges not only at the current node, but also at the starting node. We hence obtain the path

$$\text{Telavi} \xrightarrow{95} \text{Tbilisi} \xrightarrow{228} \text{Kutaisi} \xrightarrow{100} \text{Poti} \xrightarrow{75} \text{Batumi} \xrightarrow{463} \text{Telavi}$$

As expected, though, this path doesn't start at Kutaisi, so we may "shift" it to instead get the path

$$\text{Kutaisi} \xrightarrow{100} \text{Poti} \xrightarrow{75} \text{Batumi} \xrightarrow{463} \text{Telavi} \xrightarrow{95} \text{Tbilisi} \quad \text{(Total: 733)}$$

## 7.4 Discrete Mathematics by Martin Aigner, Chapter 6

### Exercise 6.1

Let $G$ be a graph with at least two vertices. Show that $G$ always has two vertices of the same degree.

Let $G$ have $n$ vertices. If each vertex had a different degree, then the function $V \to \{0, \dots, n-1\}$ which maps each vertex to its degree would be injective. But $|V| = n = |\{0, \dots, n-1\}|$, meaning the function is also surjective. We hence have vertices $u, v \in V$ where $u$ has degree 0, which means that $u$ has no neighbours, and $v$ has degree $n-1$, which would mean that $v$ should be a neighbour of every other vertex including $u$, which is a contradiction.

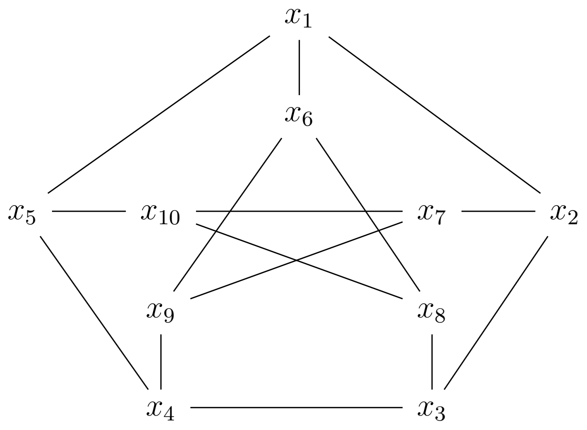
## Exercise 6.2

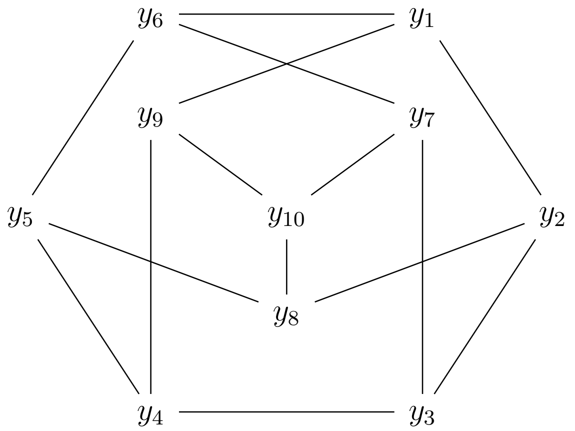
Determine the graphs with $n \geq 2$ vertices that have $n-1$ different degrees.

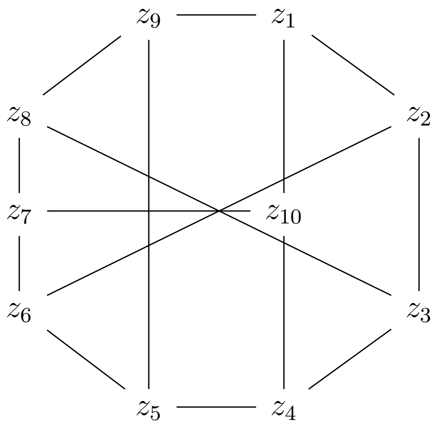
...

## Exercise 6.3

Which of the three pictured graphs are isomorphic?







All of them are isomorphic. The two mappings $f_1$ and $f_2$ as defined in the table below are isomorphisms from the first graph to the second and third graphs respectively.

| $x_i$ | $f_1(x_i)$ | $f_2(x_i)$ |
|---|---|---|
| $x_1$ | $y_1$ | $z_1$ |
| $x_2$ | $y_2$ | $z_2$ |
| $x_3$ | $y_3$ | $z_3$ |
| $x_4$ | $y_7$ | $z_8$ |
| $x_5$ | $y_6$ | $z_9$ |
| $x_6$ | $y_9$ | $z_{10}$ |
| $x_7$ | $y_8$ | $z_6$ |
| $x_8$ | $y_4$ | $z_4$ |
| $x_9$ | $y_{10}$ | $z_7$ |
| $x_{10}$ | $y_5$ | $z_5$ |

To show that these indeed are isomorphisms, let $E_1$, $E_2$ and $E_3$ be the sets of edges in the first, second and third graphs respectively. As demonstrated below, the mappings are indeed graph homomorphisms. (Since each graph is 3-regular, it is sufficient to show that edges are preserved.)

| | | |
|---|---|---|
| $\{x_1, x_2\} \in E_1$ | $\{f_1(x_1), f_1(x_2)\} = \{y_1, y_2\} \in E_2$ | $\{f_2(x_1), f_2(x_2)\} = \{z_1, z_2\} \in E_3$ |
| $\{x_1, x_5\} \in E_1$ | $\{f_1(x_1), f_1(x_5)\} = \{y_1, y_6\} \in E_2$ | $\{f_2(x_1), f_2(x_5)\} = \{z_1, z_9\} \in E_3$ |
| $\{x_1, x_6\} \in E_1$ | $\{f_1(x_1), f_1(x_6)\} = \{y_1, y_9\} \in E_2$ | $\{f_2(x_1), f_2(x_6)\} = \{z_1, z_{10}\} \in E_3$ |
| $\{x_2, x_3\} \in E_1$ | $\{f_1(x_2), f_1(x_3)\} = \{y_2, y_3\} \in E_2$ | $\{f_2(x_2), f_2(x_3)\} = \{z_2, z_3\} \in E_3$ |
| $\{x_2, x_7\} \in E_1$ | $\{f_1(x_2), f_1(x_7)\} = \{y_2, y_8\} \in E_2$ | $\{f_2(x_2), f_2(x_7)\} = \{z_2, z_6\} \in E_3$ |
| $\{x_3, x_4\} \in E_1$ | $\{f_1(x_3), f_1(x_4)\} = \{y_3, y_7\} \in E_2$ | $\{f_2(x_3), f_2(x_4)\} = \{z_3, z_8\} \in E_3$ |
| $\{x_3, x_8\} \in E_1$ | $\{f_1(x_3), f_1(x_8)\} = \{y_3, y_4\} \in E_2$ | $\{f_2(x_3), f_2(x_8)\} = \{z_3, z_4\} \in E_3$ |
| $\{x_4, x_5\} \in E_1$ | $\{f_1(x_4), f_1(x_5)\} = \{y_7, y_6\} \in E_2$ | $\{f_2(x_4), f_2(x_5)\} = \{z_8, z_9\} \in E_3$ |
| $\{x_4, x_9\} \in E_1$ | $\{f_1(x_4), f_1(x_9)\} = \{y_7, y_{10}\} \in E_2$ | $\{f_2(x_4), f_2(x_9)\} = \{z_8, z_7\} \in E_3$ |
| $\{x_5, x_{10}\} \in E_1$ | $\{f_1(x_5), f_1(x_{10})\} = \{y_6, y_5\} \in E_2$ | $\{f_2(x_5), f_2(x_{10})\} = \{z_9, z_5\} \in E_3$ |
| $\{x_6, x_8\} \in E_1$ | $\{f_1(x_6), f_1(x_8)\} = \{y_9, y_4\} \in E_2$ | $\{f_2(x_6), f_2(x_8)\} = \{z_{10}, z_4\} \in E_3$ |
| $\{x_6, x_9\} \in E_1$ | $\{f_1(x_6), f_1(x_9)\} = \{y_9, y_{10}\} \in E_2$ | $\{f_2(x_6), f_2(x_9)\} = \{z_{10}, z_7\} \in E_3$ |
| $\{x_7, x_9\} \in E_1$ | $\{f_1(x_7), f_1(x_9)\} = \{y_8, y_{10}\} \in E_2$ | $\{f_2(x_7), f_2(x_9)\} = \{z_6, z_7\} \in E_3$ |
| $\{x_7, x_{10}\} \in E_1$ | $\{f_1(x_7), f_1(x_{10})\} = \{y_8, y_5\} \in E_2$ | $\{f_2(x_7), f_2(x_{10})\} = \{z_6, z_5\} \in E_3$ |
| $\{x_8, x_{10}\} \in E_1$ | $\{f_1(x_8), f_1(x_{10})\} = \{y_4, y_5\} \in E_2$ | $\{f_2(x_8), f_2(x_{10})\} = \{z_4, z_5\} \in E_3$ |

## Exercise 6.4

Determine the automorphism groups for $P_n$, $C_n$, and $K_n$.

Let $V = \{v_1, \dots, v_n\}$ and define $E$ such that $e \in E$ if and only if $e = \{v_i, v_{i+1}\}$ for some $i \in \{1, \dots, n-1\}$ so that $(V, E)$ is a path of $n$ vertices. Let $\varphi$ be an automorphism of $P_n = (V, E)$. Since there are only vertices with degree 1 are $v_1$ and $v_n$, we have two cases: $\varphi(v_1) = v_1$ or $\varphi(v_n) = v_n$.

In the first case, since $\{v_1, v_2\} \in E$, we should have $\{v_1, \varphi(v_2)\} \in E$. But the only neighbour of $v_1$ is $v_2$, so $\varphi(v_2) = v_2$. Similarly, for $v_2$ the only two neighbours are $v_1$ and $v_3$ and $\varphi(v_3)$ should be a neighbour of $\varphi(v_2) = v_2$, so $\varphi(v_3) = v_1$ or $\varphi(v_3) = v_3$. The former can't happen as $\varphi$ would no longer be injective, so $\varphi(v_3) = v_3$. We continue and arrive at $\varphi(v_i) = v_i$ for all $i \in \{1, \dots, n\}$.

In the second case, since $\{v_1, v_2\} \in E$, we should have $\{v_n, \varphi(v_2)\} \in E$. But the only neighbour of $v_n$ is $v_{n-1}$, so $\varphi(v_2) = v_{n-1}$. Similarly, for $v_{n-1}$ the only two neighbours are $v_{n-2}$ and $v_n$, so $\varphi(v_3)$ should be a neighbour of $\varphi(v_2) = v_{n-1}$, so $\varphi(v_3) = v_{n-2}$ or $\varphi(v_3) = v_n$. The former can't happen as $\varphi$ would no longer be injective, so $\varphi(v_3) = v_{n-1}$. We continue and arrive at $\varphi(v_i) = v_{n-i+1}$ for all $i \in \{1, \dots, n\}$.

We hence have two automorphisms for $P_n$, namely, the identity map $\mathcal{I}$ and $\varphi : V \to V$ given by $\varphi(v_i) = v_{n-i+1}$ for all $i \in \{1, \dots, n\}$. Clearly, $\varphi \circ \varphi = \mathcal{I}$. So the automorphism group of $P_n$ is isomorphic to the additive group $\mathbb{Z}_2$.

The automorphism group of $C_n$ is the dihedral group of $n$ elements.

For $K_n$ any permutation of $\{v_1, \dots, v_n\}$ is an automorphism. Hence the automorphism group of $K_n$ is the symmetric group of $n$ elements.

## Exercise 6.5

Show that for every even $n \geq 4$ there is a 3-regular graph with $n$ vertices.

We shall induct on $k \geq 2$ where $n = 2k$. For $k = 2$, we have the graph $K_n = K_4$, which is 3-regular. For induction step, assume there is a 3-regular graph $G = (V, E)$ of $2k$ vertices for some $k \geq 2$. Pick four vertices $v_1, v_2, v_3, v_4 \in V$ such that $\{v_1, v_2\}, \{v_3, v_4\} \in E$ and introduce new vertices $u_1, u_2$. Now $G' = (V \cup \{u_1, u_2\}, (E \cup \{\{v_1, u_1\}, \{v_2, u_1\}, \{v_3, u_2\}, \{v_4, u_2\}\}) \setminus \{\{v_1, v_2\}, \{v_3, v_4\}\})$ is a 3-regular graph of $2k + 2 = 2(k + 1)$ vertices.

## Exercise 6.6

Show that in a connected graph, every pair of paths of maximal length has a common vertex.

By contradiction, assume there is a connected graph $G = (V, E)$ with a pair of paths $x_1, \dots, x_n$ and $y_1, \dots, y_n$ of maximal length where $x_i \neq y_j$ for all $i, j \in \{1, \dots, n\}$. Since $G$ is connected, $y_n$ should be reachable from $x_1$, i.e., there exists a path $\{v_k\}_{k=1}^{m}$ from $x_1$ to $y_n$ for some $m$. Let $x_i = \max\{k \mid x_k \in p\}$ and $y_j = \min\{k \mid y_k \in p\}$ (Existence is guaranteed since $x_1 = v_1 \in p$ and $y_n = v_m \in p$). Define $p' = \{v_k\}_{k=a}^{b}$ where $v_a = x_i$ and

$v_b = y_j$ and notice that its length $l$ should be $\geq 1$ as otherwise we would have $x_i = y_j$. Out of the paths from $x_1$ to $x_i$ and from $x_n$ to $x_i$, pick the longest one (if both have the same length, pick either), concatenate it with the path from $x_i$ to $y_j$ and next with the path from $y_j$ to either $y_1$ or $y_n$ again depending on which one is longer (if both have the same length, pick either). We hence get a path of length $\max\{i-1, n-i\} + \max\{j-1, n-j\} + l$. But $\max\{i-1, n-i\} + \max\{j-1, n-j\} + l \geq \frac{(i-1)+(n-i)}{2} + \frac{(j-1)+(n-j)}{2} + 1 = n$, we, however, assumed $n-1$ to be the maximal length of a path in $G$, so this is a contradiction.

## Exercise 6.7

Suppose the graph $G$ has the degree sequence $d_1 \leq \cdots \leq d_n$. Show that for the bandwidth, we have $b(G) \geq \max_j \max\left(d_j - \left\lfloor\frac{j-1}{2}\right\rfloor, \frac{d_j}{2}\right)$.

...

## Exercise 6.8

Show that a graph with $n$ vertices and $q$ edges has at least $n-q$ components.

In the case $n = 1$, we have only 1 component and $1 \geq 1 - 0$.

For inductive step, assume that any graph with $n$ vertices has at least $n - q$ components where $q$ is the number of edges in that graph. For any graph $G' = (V', E')$ with $|V'| = n + 1$ pick a vertex $v \in V'$ so that the graph $G = G' \setminus \{v\}$ has $n$ vertices. Call the number of its edges $q$. Via inductive hypothesis we say that $G'$ has at least $n - q$ components. The vertex $v$ is connected to some number of vertices from $G$, let $i$ be the number of components of $G'$ from where, in $G$, the vertex $v$ is reachable. , Now $G$ will have $n - q - i + 1$ components, $n + 1$ vertices and $q + i$ edges. $n - q - i + 1 \geq (n + 1) - (q + i)$ is indeed true.

## Exercise 6.14

Show that an edge $k$ is a cut edge if and only if it is contained in no circuits. What graphs have only cut circuits show further that $G$ has no cut edges if all its degrees are even.

Let $k = \{u, v\} \in E$ be a cut edge in a graph $G = (V, E)$, i.e., $G \setminus \{k\}$ has at least two components $C_1, C_2 \subseteq V$. Assume that there existed a circuit with $k$ as one of its edges, i.e., it had $u, v$ as its vertices. In $G \setminus \{k\}$, that circuit becomes a path starting from $u$ to $v$ (or vice versa). This gives a contradiction as that makes $u$ and $v$ reachable from one another meanwhile they should be in different components, i.e., they should not be reachable.

Conversely, assume that no path with $k$ as one of its edges can be extended to a circuit. Let $C_1$ be a set of vertices reachable from $u$ in $G \setminus \{k\}$ and $C_2$ be the set of vertices reachable from $v$ in $G \setminus \{k\}$. If there existed a path from $c_1 \in C_1$ to $c_2 \in C_2$, then we could concatenate it with the path from $c_1$ to $c_2$ in $G$ with $k$ as one of its edges and get a circuit, which would be a contradiction. So $C_1$ and $C_2$ are distinct components, meaning $k$ has been a cut edge.

A graph with only cut edges has components that also have only cut edges. A component itself is connected, so the components of such graph are trees. The graph is hence a forest.

## Exercise 6.15

Suppose a graph $G = (V, E)$ with $|E| \geq 3$ and without isolated vertices has no induced subgraphs with exactly two edges. Show that $G = K_n$, $n \geq 3$.

We shall prove a more general version of this theorem. Let $G = (V, E)$ have no isolated vertices and no induced subgraphs with exactly two edges. Our claim is that $G$ is a complete graph.

Let $|V| = n$. We can't have $n = 1$ as we would have an isolated point, so $n \geq 2$. Let $v, w \in V$ be distinct vertices and assume that $\{v, w\} \notin V$. $v$ and $w$ must not be isolated, so let $u \in V$ be a neighbour of $v$ (obviously, distinct from $w$) and $z \in V$ be a neighbour of $w$ (obviously, distinct from $v$). Note that we can't have $\{u, w\} \in E$ as then the subgraph $(\{u, v, w\}, \{\{u, v\}, \{u, w\}\})$ is induced and has exactly two edges. Now, if $\{u, z\} \notin E$, then the subgraph $(\{u, v, w, z\}, \{\{u, v\}, \{w, z\}\})$ is induced and has exactly two edges, so $\{u, z\} \in E$. But that's a contradiction, as then the subgraph $(\{u, z, w\}, \{\{u, z\}, \{w, z\}\})$ is induced and has exactly two edges.

Hence $\{v, w\} \in V$, meaning any two vertex of $G$ are connected by an edge, i.e., $G$ is complete.

## 7.5 Discrete Mathematics by Martin Aigner, Chapter 7

### Exercise 7.1

Prove the following characterizations of trees: Let $G$ be a graph on $n$ vertices and $q$ edges. Then $G$ is a tree if and only if the following conditions are satsfied: (a) $G$ has no circuits and $q = n - 1$. (b) $G$ has no circuits and if any pair of nonneighbouring vertices are joined by an edge, then the resulting graph has precisely one circuit. (c) $G$ is connected ($G \neq K_n$ if $n \geq 3$), and if any two nonneighbouring vertices are joined by an edge, then the resulting graph has exactly one circuit.

First we show that if a tree has no circuits and the amount of edges in it is one less than the amount of vertices. The former is immediately true. The latter can be proven by induction on the amount of vertices $n$. For base case, $n = 1$, the only tree is $(\{v\}, \varnothing)$, meaning the amount of edges $q$ is 1 and $n = q - 1$ indeed holds. Now, assume that $n = q - 1$ for any tree with $n$ vertices and let $G = (V, E)$ be a tree of $n + 1$ vertices. Every tree has a vertex of degree 1, pick $v \in V$ to be such. Then $G \setminus \{v\}$ is a tree of $n$ vertices and, according to the inductive hypothesis, $n + 1$ edges, meaning $G$ has $n + 1$ vertices and $n + 2$ edges, so the equation still holds for any tree of $n + 1$ vertices.

Conversely, let the graph $G = (V, E)$ have no circuits and let $n = q - 1$ with $n = |V|$ and $q = |E|$. Let $t$ also denote the number of components of $G$. Since the components of $G$ also have no circuits and are, by definition, connected, they are trees. Let $n_i$ and $q_i$ be the number of vertices and edges in the $i$th component and note that $\sum_{i=1}^{t} n_i = n$ and $\sum_{i=1}^{n} q_i = q$. According to our previous result, we have $n_i = q_i - 1$ for all $i$ and hence $q - 1 = n = \sum_{i=1}^{t} n_i = \sum_{i=1}^{t} (q_i - 1) = \sum_{i=1}^{t} q_i - \sum_{i=1}^{t} 1 = q - t$. We immediately get $t = 1$, meaning $G$ is itself tree.

Now we show that if $G = (V, E)$ is a tree, then $G$ has no circuits and if any pair of nonneighbouring vertices are joined by an edge, then the resulting graph has precisely one circuit. Let $u, v \in V$ be nonneighbouring, i.e., $\{u, v\} \notin E$ and consider the graph $(V, E \cup \{u, v\})$. Since $G$ is a graph, there exists exactly one path from $u$ to $v$, which forms a circuit in $(V, E \cup \{u, v\})$. If any other circuit was formed, then it would mean that there is another path from $u$ to $v$, which would contradict $G$ being a tree.

Conversely, let $G = (V, E)$ be a graph with no circuits where if any pair of nonneighbouring vertices are joined by an edge, then the resulting graph has precisely one circuit. Let $u, v \in V$ be distinct vertices. If $\{u, v\} \in E$, then there is exactly one path from $u$ to $v$. (If there were any other paths, we would have a circuit formed.) If $\{u, v\} \notin E$, then the graph $(V, E \cup \{\{u, v\}\})$ has exactly one circuit which contains $\{u, v\}$. Removing the edge $\{u, v\}$ gives the unique path from $u$ to $v$ in $G$. (If it was not unique, then we would have more than 1 circuits.) Hence $G$ has no circuits and is connected, i.e., $G$ is indeed a tree.

Now we show that if $G$ is a tree, then $G$ is connected, not complete in case $|V| \geq 3$ and if any pair of two nonneighbouring vertices are joined by an edge, the resulting graph has exactly one circuit. Let $G$ be a tree, i.e., let $G = (V, E)$ be connected and have no circuits. Then $G$ is immediately connected, not complete for $|V| \geq 3$ as otherwise $G$ would have a circuit and, as we have already shown, if any pair of two nonneighbouring vertices are joined by an edge, the resulting graph has exactly one circuit.

Conversely, let $G$ be connected, not complete in case $|V| \geq 3$ and if any pair of nonneighbouring vertices are joined by an edge, then the resulting graph has precisely one circuit. If $|V| < 3$, then $G$ is immediately a tree since it has to be connected. If $|V| \geq 3$, then $G$ is not complete, i.e., there are $u, v \in V$ with $\{u, v\} \notin E$. Assume that $G$ has a circuit, then the graph $(V, E \cup \{\{u, v\}\})$ has exactly one circuit, which would mean that there was no path from $u$ to $v$ (if there was, then we would have more than 2 circuits), meaning $v$ is not reachable from $u$, contradicting the fact that $G$ is connected. Hence $G$ is connected and has no circuits, i.e., $G$ is indeed a tree.

## Exercise 7.2

Show that a connected graph with an even number of vertices always has a spanning subgraph in which all vertices have odd degree. Does this hold for disconnected subgraphs?

...

## 7.6 Discrete Mathematics by Martin Aigner, chapter 8

### Exercise 8.1

Suppose the bipartite graph $G = (S + T, E)$ is $k$-regular, $k \geq 1$. Show that $|S| = |T|$ and $G$ always contains a matching $M$ with $|M| = |S| = |T|$.

We begin by claiming that $|E| = \sum\limits_{v \in S} d(v)$ for any bipartite graph $G$ with parts $S$, $T$ and set of edges $E$. For all $v \in S$, define $E_v = \{e \in E \mid v \in e\}$. Clearly, each $E_v$ is disjoint, (if there existed $e \in E$ with $u, v \in e$ for some $u, v \in S$, then $G$ would not be bipartite.), and $E = \bigcup_{v \in S} E_v$, meaning $|E| = \sum\limits_{v \in S} |E_v|$. Now we shall prove that $|E_v| = d(v)$. Since $G$ is bipartite, for all $e \in E_v$ with $v \in S$ there exists $u \in T$ with $e = \{u, v\}$ (in fact, we have $u \in N(v)$.), let $f : E_v \to N(v)$ be given by $e \mapsto u$ where $u$ is defined as mentioned for $e \in E_v$. For injectivity, let $e_1, e_2 \in E_v$ be distinct, i.e., $e_1 = \{v, u_1\}$ and $e_2 = \{v, u_2\}$ for some $u_1, u_2 \in N(v)$. If $u_1 = u_2$, we would have $e_1 = e_2$, so $u_1 \neq u_2$ and $f(e_1) \neq f(e_2)$. For surjectivity, let $u \in N(v)$. By definition, we have $\{u, v\} \in E$ and, since $v \in \{u, v\}$, we have $f(\{u, v\}) = u$. $f$ is bijective, meaning $|E_v| = |N(v)| = d(v)$. Finally, we obtain $|E| = \sum\limits_{v \in S} |E_v| = \sum\limits_{v \in S} d(v)$.

So, if $G$ is $k$-regular with $k \geq 1$, i.e., $d(v) = k$ for all $v \in S \cup T$, we have $|E| = \sum\limits_{v \in S} d(v) = \sum\limits_{v \in S} k = k \sum\limits_{v \in S} = k|S|$ and, similarly, $|E| = k|T|$. By symmetry and transitivity of $=$ we get $k|S| = k|T|$ and $|S| = |T|$.

Let $A \subseteq S$ and consider the induced graph $G'$ of $G$ generated by $A \cup N(A)$ which is clearly also bipartite. Let $E'$ be the set of edges in $G'$ and $d'(v)$ denote the degree of $v$ in $G'$ assuming $v \in A \cup N(A)$. According to our recent result, we would have $|E'| = \sum\limits_{v \in A} d'(v) = \sum\limits_{v \in A} k = k \sum\limits_{v \in A} = k|A|$. At the same time, however, we have $|E'| = \sum\limits_{v \in N(A)} d'(v) \leq \sum\limits_{v \in N(A)} k = k \sum\limits_{v \in N(A)} = k|N(A)|$ since $d'(v) \leq d(v)$ for all $v \in N(A)$. Hence $k|A| \leq k|N(A)|$ and $|A| \leq |N(A)|$.

According to the marriage theorem, there exists a matching $M$ (which is maximal) with $|M| = |S|$. Since $|S| = |T|$, we also have $|M| = |S| = |T|$.

## Exercise 8.2

A 1-factor in an arbitrary graph $G = (V, E)$ is a matching $M$ that contains all vertices; hence $|M| = \frac{|V|}{2}$. The graph $G$ is said to be 1-factorable if $E$ can be decomposed into disjoint 1-factors. Use the previous exercise to conclude that a $k$-regular bipartite graph, $k \geq 1$, is 1-factorizable.

We shall furthermore show that $G$ (defined as above) can be decomposed into $k$ disjoint 1-factors.

Let $G$ be a bipartite graph with parts $S$ and $T$ and the set of edges $E$. We have established that $|S| = |T|$, so let $n$ denote $|S|$. We shall prove by induction on $k$. For base case, $k = 1$, according to our previous result, we have a matching with $|M| = n$ . We also have $|E| = kn = n$, $|M| = |E|$ and $M = E$ since $M \subseteq E$. $M$ is clearly 1-factorable since it has $n$ edges, each of which cover disjoint sets of 2 vertices (as otherwise a pair of edges would be incident, making $M$ not a matching), meaning $M$ covers $2n$ vertices and $G$ contains exactly that many vertices.

For inductive step, assume that any $k$-regular bipartite graph with no isolated edges is 1-factorable, i.e., its set of edges can be decomposed into disjoint 1-factors. We may also assume that $k < n$ so that $k + 1 \leq n$ as otherwise the implication is vacuously true. Let $G$ be a $(k + 1)$-regular bipartite graph with parts $S$ and $T$ and the set of edges $E$. According to our previous result, there exists a 1-factor $M$. Consider the graph $G' = (S \cup T, E \setminus M)$. Clearly, it is still bipartite with no isolated vertices. It is also clearly $k$-regular since each vertex in $G'$ has 1 less neighbours than in $G$. The inductive hypothesis suggests that $E \setminus M$ has a partition $F$ with $k$ 1-factors. Clearly, $F \cup \{M\}$ is a partition of $E$ with $k + 1$ disjoint 1-factors, meaning $G$ is 1-factorizable.

## Exercise 8.3

Show that a bipartite graph $G = (S + T, E)$ with $|S| = |T| = n$ and $|E| > (m - 1)n$ contains a matching of size $m$. Is $m$ the best possible?

...

## Exercise 8.4

How many distinct transversals does the family of sets $\mathcal{A} = \{\{1,2\},\{2,3\},\{3,4\},\ldots,\{n-1,n\},\{n,1\}\}$ possess? [The universal set is assumed to be the union of the given family of sets.]

Note that $|\mathcal{A}| = |\{1,\ldots,n\}|$, meaning that if there is at least one injection from $\mathcal{A}$ to $\{1,\ldots,n\}$, then its image is automatically $\{1,\ldots,n\}$. Consider the bipartite graph with the set of vertices $\mathcal{A} \cup \{1,\ldots,n\}$ and connect a set $S \in \mathcal{A}$ to an element $i \in \{1,\ldots,n\}$ if and only if $i \in S$. The resulting graph is 2-regular, since every set has exactly two elements and every element is contained in exactly two sets. According to our recent result (See Exercise 8.1) there is a matching with 5 edges. That matching corresponds to a selection function. Hence there is only one transversal, namely, $\{1,\ldots,n\}$.

## Exercise 8.5

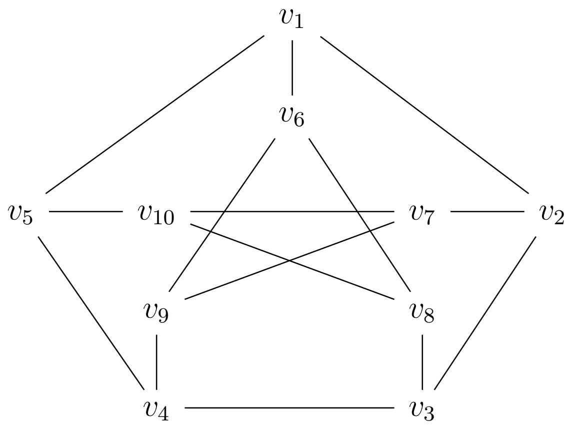
Show that a tree possesses at most one 1-factor.

We shall induct on the number of vertices. For base cases, the only trees are $K_1$ and $K_2$. The former has no 1-factors and the latter has one exactly 1-factor. For inductive step, assume that any tree with $n$ vertices has at most one 1-factor and consider a tree $G = (V,E)$ with $n+2$ vertices. Assume that $G$ has at least two 1-factors, let $M$ and $M'$ be some distinct ones. Pick a vertex $v \in V$ with degree 1 and a neighbour $u$ (existence is guaranteed by $G$ being a tree). Clearly, $\{u,v\} \in M$ and $\{u,v\} \in M'$ as $v$ has no other neighbour. Now, if $M$ and $M'$ are distinct, then so are $M \setminus \{u,v\}$ and $M' \setminus \{u,v\}$, they, however, are 1-factors in the graph $G \setminus \{u,v\}$, which is a tree with $n$ vertices. This contradicts the inductive hypothesis, so $G$ has at most one 1-factor.

## Exercise 8.6

Show that the Peterson graph is not 1-factorizable.

Let $G$ be the Peterson graph illustrated below.



Assume that $G$ is 1-factorizable. Let $M$ be the 1-factor containing the edge $\{v_1, v_2\}$ (existence is trivial). We have two cases, $\{v_5, v_{10}\} \in M$ or $\{v_4, v_5\} \in M$. If $\{v_4, v_5\} \in M$, then $\{v_3, v_8\} \in M$ is forced as the other edges containing $v_3$ are already incident to some edge in $M$. And, finally, we also have $\{v_7, v_{10}\}, \{v_6, v_9\} \in M$ forced. Now let $M'$ be the 1-factor containing the edge $\{v_1, v_5\}$ (existence is trivial). Then $\{v_8, v_{10}\} \in M'$ is forced. Now, none of the edges incident to $v_6$ should belong to $M'$. (We can't have $\{v_6, v_9\} \in M'$ as $\{v_6, v_9\} \in M$ and every 1-factor in the decomposition should be disjoint; we can't have $\{v_6, v_8\} \in M'$ as $\{v_6, v_8\}$ is incident to $\{v_8, v_{10}\}$ and $\{v_8, v_{10}\} \in M'$; we similarly can't have $\{v_1, v_6\} \in M'$ as $\{v_1, v_6\}$ is incident to $\{v_1, v_5\}$ and $\{v_1, v_5\} \in M'$.) The latter is a contradiction. If, however, $\{v_3, v_4\} \in M$, then $\{v_5, v_{10}\} \in M$ is forced and the same argument follows due to symmetry. Hence $G$ is not 1-factorizable.

## Exercise 8.7

Let $G$ be a graph on $n$ vertices, $n$ even, in which $d(u) + d(v) \geq n - 1$ for every pair of vertices $u, v$. Show that $G$ possesses a 1-factor.

...

## Exercise 8.14

Show that the Peterson graph is not Hamiltonian.

If it were Hamiltonian, we would be able to produce two disjoint 1-factors in the Peterson graph. We, however, have already shown that the Peterson graph can't have two disjoint 1-factors. (See Exercise 8.6)

## Exercise 8.15

Show that all hypercubes $Q_n$, $n \geq 2$, are Hamiltonian.

We shall induct on $n$. For base case, $n = 2$, so $Q_n = Q_2$ is indeed Hamiltonian as it contains a Hamiltonian circuit given by the sequence $(0,0), (0,1), (1,1), (1,0)$. For induction step, assume that every hypercube $Q_n$ contains a Hamiltonian circuit for some $n$ and consider the hypercube $Q_{n+1}$. Since, according to the inductive hypothesis, there is a path from the zero word of length $n$ to $\mathbf{x} \in B(n)$ with weight 1, define $x_1, \ldots, x_n \in \{0,1\}$ so that $(x_1, \ldots, x_n) = \mathbf{x}$. Now there exists a path from the zero word of length $n + 1$ to the 0,1-word $(0, x_1, \ldots, x_n)$. Since $\{(0, x_1, \ldots, x_n), (1, x_1, \ldots, x_n)\}$ is an edge in $Q_n$ and since similarly there exists a path from $(1, x_1, \ldots, x_n)$ to $(1, \underbrace{0, \ldots, 0}_{n})$, we may concatenate these paths and obtain a Hamiltonian circuit from the zero word of length $n+1$ to $(1, \underbrace{0, \ldots, 0}_{n})$. Hence $Q_{n+1}$ is also Hamiltonian.

### Exercise 8.16

Construct a non-Hamiltonian graph on 10 vertices for which $d(u) + d(v) \geq 9$ for each pair of nonneighbouring vertices.

...

## 7.7 Definitions

**Definition 36** (Graphs). *Let $E \subseteq \{e \mid e \subseteq V \text{ and } |e| = 2\}$. $G = (V, E)$ is a graph.*

**Definition 37** (Complete graphs). *A graph $G = (V, E)$ is complete if and only if $\{e \mid e \subseteq V \text{ and } |e| = 2\} \subseteq E$.*

**Definition 38** (Paths). *Let $G = (V, E)$ be a graph. A sequence $\{u_i\}_{i=1}^k$ of distinct vertices such that $\{u_i, u_{i+1}\} \in E$ for all $i \in \{1, \ldots, k-1\}$ is a path of length $(k-1)$ and of $k$ vertices. The vertices $v_1$ and $v_k$ are called first and last vertices of $P$ respectively.*

**Definition 39** (Cycles/Circuits). *Let $G = (V, E)$ be a graph. A path $\{u_i\}_{i=1}^k$ is a cycle/circuit if and only if $\{u_k, u_1\} \in E$ and $k \geq 3$.*

**Definition 40** (Hamiltonian circuits). *A circuit in a graph $G = (V, E)$ is called Hamiltonian if it consists of every vertex in $G$. The graph $G$ is then also called a Hamiltonian graph.*

**Definition 41** (Neighbours and degree). *Let $G = (V, E)$ be a graph. $u$ and $v$ are neighbours and are neighbouring vertices if and only if $\{u, v\} \in E$. $N(u)$ denotes the set of all neighbours of $u$.*

*Degree of $u$ is $|N(u)|$.*

**Definition 42** (Regular graph). *A graph $G = (V, E)$ is $r$-regular if and only if $|N_G(v)| = r$ for all $v \in V$.*

**Definition 43** (Isolated vertices). *Let $G = (V, E)$ be a graph. A vertex $v \in V$ is isolated if and only if its degree is 0.*

**Definition 44** (Order and size of a graph). *Let $G = (V, E)$ be a graph. $|V|$ and $|E|$ are order and size of $G$ respectively.*

**Definition 45** (Incident edges)**.** *Let $G = (V, E)$ be a graph. A set of edges $\{e_1, \dots, e_n\} \subseteq E$ is incident if and only if $\bigcap\limits_{i=1}^{n} e_i \neq \varnothing$.*

**Definition 46** ($k$-partite graphs)**.** *A graph $G = (V, E)$ is a k-partite graph if and only if there exists a k-paritition $\{V_1, \dots, V_k\}$ of $V$ such that $e \not\subseteq V_i$ for all $i \in \{1, \dots, k\}$ and $e \in E$.*

*The sets $V_1, \dots, V_k$ are parts of the bipartite graph $G$.*

*A k-partite graph is a complete k-partite graph if and only if for all $x \in V_i$ and $y \in V_j$ where $i, j \in \{1, \dots, k\}$ are distinct, we have $\{x, y\} \in E$.*

*In cases $k = 2$ and $k = 3$, $G$ may be referred to as a bipartite graph and a tripartite graph respectively.*

**Definition 47** (Hypercube)**.** *A graph $G = (V, E)$ is a hypercube of dimension $n$ if and only if $V = \mathcal{B}(n)$ and $\{x, y\} \in \mathcal{E}$ if and only if $\delta(x, y) = 1$ where $\delta$ is the Hamming distance.*

**Definition 48** (Graph isomorphisms)**.** *Graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic and a mapping $f : V_1 \to V_2$ is a graph isomorphism if and only if $f$ is a bijection such that $\{u, v\} \in E \iff \{f(u), f(v)\} \in E$ for any $u, v \in V_1$.*

**Definition 49** (Reachability)**.** *Let $G = (V, E)$ be a graph. A vertex $v \in V$ is reachable from $u \in V$ if and only if there is a path containing both vertices.*

*A component of $G$ is a quotient set of $V$ by the equivalence relation of reachability.*

**Definition 50** (Connected graphs)**.** *A graph is connected if and only if it has only one component. A graph is disconnected otherwise.*

**Definition 51** (Bridges/Cut edges)**.** *Let $G = (V, E)$ be a graph. An edge $e \in E$ is a bridge/cut edge if and only if the graph $(V, E \setminus \{e\})$ has more components than $G$.*

*$G$ is bridgeless if no such $e$ exists.*

**Definition 52** (Distance)**.** *Let $G = (V, E)$ be graph. The distance function $d_G : V \times V \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ of $G$ is the function defined by setting $d_G(u, v)$ to the minimal length of a path containing both $u$ and $v$ if $u$ is reachable from $v$ and to $\infty$ otherwise.*

**Definition 53** (Diameter)**.** *Let $G = (V, E)$ be a graph. Diameter of $G$ is* $\max\{d_G(u, v) \mid u, v \in V\}$.

**Definition 54** (Radius and centers). *Let $G = (V, E)$ be a graph and $r(v) = \max\{d_G(u, v) \mid u \in V\}$ where $d_G$ is a distance function on $G$. Then $\min\{r(v) \mid v \in V\}$ is the radius of $G$.*

*A vertex $v \in V$ is a center of $G$ if and only if $r(v)$ is equal to the radius of $G$.*

**Definition 55** (Independence). *A set of vertices $A \subseteq V$ in a graph $G = (V, E)$ is independent if and only if $\{u, v\} \notin E$ for all $u, v \in A$.*

**Definition 56** (Trees and forests). *A graph is a tree if and only if it is connected and does not contain any cycles.*

*A graph is a forest if and only if every its component is a tree.*

**Definition 57** (Stars). *A complete bipartite graph is a star if and only if one of the parts has only one vertex.*

**Definition 58** (Weight). *A weighted graph is a graph $G = (V, E)$ with a weight function $w : E \to \mathbb{R}_{\geq 0}$.*

*The weight of $G$, denoted by $w(G)$, is $\sum\limits_{e \in E} w(e)$.*

**Definition 59** (Matchings). *A set $M$ is a matching in a graph $G = (V, E)$ if and only if $M \subseteq E$ and $e_1 \cap e_2 = \varnothing$ for all distinct $e_1, e_2 \in E$.*

*The matching number $m(G)$ of the graph $G$ is $\max\{|M| : M \text{ is a matching}\}$. A matching $M$ is maximal if and only if $|M| = m(G)$.*

**Definition 60** ($k$-factors). *A matching $M$ in a graph $G = (V, E)$ is a 1-factor if and only if for all $v \in V$ there exists $e \in M$ with $v \in e$.*

*A subgraph of a graph $G$ is a $k$-factor of $G$ if and only if it is a spanning subgraph and also $k$-regular.*

*The graph $G$ is $k$-factorizable if and only if there is a set of $k$-factors forming a partition of $E$.*

**Definition 61** (Saturation). *In a graph $G = (V, E)$ with a matching $M$, a vertex $v \in V$ is $M$-saturated if and only if there is $e \in M$ with $v \in e$. Otherwise $v$ is $M$-unsaturated.*

**Definition 62** (Alternating paths). *A path $P$ in a graph $G = (V, E)$ with a matching $M$ is $M$-alternating if and only if the first and last vertices in $P$ are $M$-unsaturated and $\{v_{n-1}, v_n\} \in M \iff \{v_n, v_{n+1} \notin M\}$ for all suitable $n$ with $v_i \in P$ for all suitable $i$.*

# Chapter 8

# Abstract algebra

## 8.1 Week 11 Central Exercises

### Exercise 1

Determine if the following operations $*: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ are associative and/or commutative and whether they possess a neutral element. [For commutative operations, I have shown existence of the neutral element using existence of a left neutral element]

1. $a * b := kab$ for some $k \in \mathbb{R} \setminus \{0\}$;

   The operation is assocative as $a*(b*c) - a*(kbc) = kakbc = kkabc = (kab)*c = (a*b)*c$, commutative as $a*b = kab = kba = b*a$. It also has a neutral element, namely, $\frac{1}{k}$ as $\frac{1}{k} * a = k\frac{1}{k}a = 1a = a$.

2. $a * b := a^2 b$;

   The operation is not associative as $(2*2)*3 = (2^2 \cdot 2)*3 = 8*3 = 8^2 \cdot 3 = 192 \neq = 48 = 2^2 \cdot 12 = 2*12 = 2*(2^2 \cdot 3) = 2*(2*3)$; not commutative as $1*2 = 1^2 \cdot 2 = 2 \neq 4 = 2^2 \cdot 1 = 2*1$. Despite possessing a left neutral element, namely, 1 since $1 * b = 1^2 b = b$ for all real $b$, there is no right neutral element (if it had one, it would be 1, however, $(-1) * 1 = (-1)^2 * 1 = 1 \neq -1$), hence no neutral element.

3. $a * b := a - b$;

   The operation is not associative as $0 * (0 * 1) = 0 * (0 - 1) = 0 * (-1) = 0 - (-1) = 1 \neq -1 = 0 - 1 = 0 * 1 = (0 - 0) * 1 = (0 * 0) * 1$. It is neither commutative as $1 * 2 = 1 - 2 = -1 \neq 1 = 2 - 1 = 2 * 1$. Despite possessing a right neutral element, namely, 0 since $a * 0 = a - 0 = a$ for all real $a$, there is no left neutral element (if there was one, it would be 0, however, $0 * (-1) = 0 - (-1) = 1 \neq 0$), hence no neutral element.

4. $a * b := k(a + b)$ for some $k \in \mathbb{R} \setminus \{0\}$;

   The operation is not associative as $a * (b * c) = a * (k(b + c)) = k(a + kb + kc) \neq k(ka + kb + c) = (k(a + b)) * c = (a * b) * c$ unless $k = 1$ (since otherwise the coefficients of the polynomials in $a, b$ and $c$ are not equal, meaning the polynomials themselves are not equal). The operation is commutative as $a * b = k(a + b) = k(b + a) = b * a$. For $k = 1$, the neutral element is 0 as we already know. If, however, $k \neq 1$, then, by contradiction, assume there is a neutral element and name it $e$, then $0 = e * 0 = k(e + 0) = ke$, which would mean that $e = 0$, but $1 = 1 * e = 1 * 0 = k(1 + 0) = k \cdot 1 = k$ which would mean that $k = 1$, but the latter is a contradiction. Hence no neutral element.

5. $a * b := a|b|$;

   The operation is associative as $a * (b * c) = a * b|c| = a|b|c|| = a|b||c| = a|b| * c = (a * b) * c$. It is not commutative as $1 * (-1) = 1|-1| = 1 \neq$

$-1 = -1 \cdot |1| = (-1) * 1$. Despite having right elements, namely $-1$ and 1, there is no left neutral element (if there was one, we would have a unique neutral element, but $1 \neq -1$.), hence no neutral element.

6. $a * b := a/b$;

   Assuming the author meant "$a$ divided by $b$", this is not an operation on $\mathbb{R}$; Let us instead consider the domain to be $R\backslash\{0\}$. The operation is not associative as $1*(1*2) = 1*\frac{1}{2} = \frac{1}{\frac{1}{2}} = 2 \neq \frac{1}{2} = 1*2 = \frac{1}{1}*2 = (1*1)*2$. It is neither commutative as $1 * 2 = \frac{1}{2} \neq 2 = 2 * 1$. Despite having a right identity, namely 1 since $a * 1 = \frac{a}{1} = a$ for all real $a$, there is no left identity (if there was one, it would have 1, however, $1 * 2 = \frac{1}{2} \neq 2$), hence no neutral element.

7. $a * b := \max(a, b)$;

   The operation is commutative as $a * b = \max(a, b) = \max(b, a) = b * a$. Before we discuss associativity, we need to show that $\max(a, \max(b, c))$ for $a, b, c$ elements of any totally ordered set. We shall consider cases; If $a \geq b \geq c$, then $\max(a, \max(b, c)) = \max(a, b) = a = \max(a, b, c)$; If $b \geq a \geq c$, then $\max(a, \max(b, c)) = \max(a, b) = b = \max(a, b, c)$. Symmetry and commutativity take care of the other cases. The operation is hence associative as $a*(b*c) = a*\max(b, c) = \max(a, \max(b, c)) = \max(a, b, c) = \max(\max(a, b), c) = \max(a, b) * c = (a * b) * c$. By contradiction, assume there is a netural element $e$ and pick a real number $r < e$, then $\max(r, e) = e \neq r$. Thus there is no neutral element.

8. $a * b := 2a + b$;

   The operation is not associative as $1 * (0 * 0) = 1 * (2 \cdot 0 + 0) = 1 * 0 = 2 \cdot 1 + 0 = 2 \neq 4 = 2 \cdot 2 + 0 = 2 * 0 = (2 \cdot 1 + 0) * 0 = (1 * 0) * 0$. It is neither commutative as $1 * 2 = 2 \cdot 1 + 2 = 2 + 2 = 4 \neq 5 = 4 + 1 = 2 \cdot 2 + 1 = 2 * 1$. Despite having a left neutral element, namely, 0 since $0 * b = 2 \cdot 0 + b = 0 + b = b$ for all real $b$, there is no right neutral element (if there was one, it would be 0, however, $1 * 0 = 2 \cdot 1 + 0 = 2 \neq 1$), hence no neutral element.

9. $a * b :=$ average$(a, b)$; [The "average" of $a$ and $b$ in this context is assumed to be the arthmetic mean $\frac{a+b}{2}$ as the geometric mean is not an operation on $\mathbb{R}$. (Neither is the harmonic mean.)]

   Then the operation is not associative as $1 * (1 * 2) = 1 * \frac{3}{2} = \frac{5}{4} \neq \frac{3}{2} = 1 * 2 = \frac{2}{2} * 2 = (1 * 1) * 2$. The operation is commutative as $a * b = \frac{a+b}{2} = \frac{b+a}{2} = b * a$. By contradiction, assume there is a neutral element $e$, meaning $\frac{x+e}{2} = x$ for all real $x$. The polynomials $\frac{x}{2} + \frac{e}{2}$ and $x$, however, can never be equal, as we would require the coefficients to be equal, but $\frac{1}{2} \neq 1$. Thus there is no neutral element.

10. $a * b = a^b$.

    This is not an operation on $\mathbb{R}$, let us instead consider the domain to be $\mathbb{R}_{>0}$. The operation is not associative as $2 * (3 * 2) = 2 * 3^2 = 2 * 9 = 2^9 = 512 \neq 64 = 8^2 = 8 * 2 = 2^3 * 2 = (2 * 3) * 2$. The operation is neither commutative as $1 * 2 = 1^2 = 1 \neq 2 = 2^1 = 2 * 1$. Despite the operation possessing a right neutral element, namely 1, there is no left neutral element (by contradiction, assume there is, then it must be 1, but $1 * 2 = 1^2 = 1 \neq 2$.), hence no neutral element.

Is $* : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ defined by $A * B := A \setminus B$ associative and/or commutative for some set $X$?

If $X$ is empty, then both properties hold. If $X$ is nonempty, then it is not associative as $X * (\varnothing * X) = X * (\varnothing \setminus X) = X * \varnothing = X \setminus \varnothing = X \neq \varnothing = X \setminus X = (X \setminus \varnothing) \setminus X = (X * \varnothing) * X$ commutative as $X \setminus \varnothing = X \neq \varnothing = \varnothing \setminus X$.

## Exercise 2

Determine the set of invertible elements for the following operations.

1. $* : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ where $a * b := a + b$;

   0 is the neutral element and therefore invertible. For any elements $a, a' \in \mathbb{N}_0$ with nonzero $a$ consider the sum $a + a'$. Since $a$ is nonzero, we have $a > 0$ and $a + a' > 0 + a' = a' \geq 0$, meaning $a + a' \neq 0$ for any $a'$, meaning $a$ is not invertible. Thus the set of invertible elements is $\{0\}$.

2. $* : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ where $a * b := a + b$;

   The neutral element is 0. For any $q \in \mathbb{Q}$, let $a, b$ be integers with $q = \frac{a}{b}$, then $q' = \frac{-a}{b} \in \mathbb{Q}$ is the inverse of $q$ as $q+q' = \frac{a}{b} = \frac{-a}{b} = \frac{a+(-a)}{b} = \frac{0}{b} = 0$. Thus the set of invertible elements is $\mathbb{Q}$.

3. $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ where $a * b := ab$.

   The neutral element is 1. The only non-invertible element is 0, so the set of invertible elements is $\mathbb{R} \setminus \{0\}$. (The proof is not provided as one would require the definition/construction of $\mathbb{R}$.)

4. $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ where $a * b := kab$ for some $k \in \mathbb{R} \setminus 0$;

   The neutral element is $\frac{1}{k}$. For every nonzero $r \in \mathbb{R}$, take the product of the multiplicative products of $k$ and $a$ (with regular multiplication) and name it $r'$. Then $r * r' = krr' = 1$. So, the set of invertible elements is again $\mathbb{R} \setminus \{0\}$.

5. $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ where $a * b := \max(a, b)$;

The neutral element is 1 as $1 \leq n$ for all $n \in \mathbb{N}$, meaning $\max(1, n) = \max(n, 1) = n$. 1 is trivially invertible. Any $n \in \mathbb{N}$ besides 1 is not invertible as we have $n > 1$, meaning $\max(n, n') > 1$ with any $n' \in \mathbb{N}$, i.e., $\max(n, n') = 1$ never holds for $n$ different from 1. Thus the set of invertible elements is $\{1\}$.

## Exercise 3

The dihedral group $D_3$ is the symmetry group of an equilateral triangle, that is, it is the set of all transformations such as reflection, rotation and combinations of these, that leave the shape and position of this triangle fixed.

(1) Write down a complete composition table (Cayley table) for $D_3$;

(2) is $D_3$ abelian?

(3) Find all six subgroups of $D_3$ and determine whether they are abelian.

For part (1), we first need to name the elements of $D_3$. Let the triangle have vertices $a$, $b$ and $c$. Let $e$ be the identity transformation, $r_1$ counterclockwise rotation by 120 degrees, $r_2$ counterclockwise rotation by 240 degrees, $d_1$, $d_2$ and $d_3$ be the reflections about the lines crossing the center of the triangle and $a$, $b$ or $c$ respectively. We obtain the following Cayley table.

| $\circ$ | $e$ | $r_1$ | $r_2$ | $d_1$ | $d_2$ | $d_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r_1$ | $r_2$ | $d_1$ | $d_2$ | $d_3$ |
| $r_1$ | $r_1$ | $r_2$ | $e$ | $d_3$ | $d_1$ | $d_2$ |
| $r_2$ | $r_2$ | $e$ | $r_1$ | $d_2$ | $d_3$ | $d_1$ |
| $d_1$ | $d_1$ | $d_2$ | $d_3$ | $e$ | $r_2$ | $r_1$ |
| $d_2$ | $d_2$ | $d_3$ | $d_1$ | $r_1$ | $e$ | $r_2$ |
| $d_3$ | $d_3$ | $d_1$ | $d_2$ | $r_2$ | $r_1$ | $e$ |

For part (2), from the Cayley table it is clear that the group is not Abelian; E.g., $d_1r_1 = d_2 \neq d_3 = r_1d_1$. (In fact, there is only one pair of commuting nonneutral elements, namely $r_1$ and $r_2$.)

For part (3), the subgroups of $D_3$ are $\{e\}, \{e, r_1, r_2\}$, $\{e, d_1\}$, $\{e, d_2\}$, $\{e, d_3\}$ and $D_3$ itself. All of them, except $D_3$, are Abelian groups.

## Exercise 4.1

Show that $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with $a + b := a + b \mod 4$ and $ab := ab \mod 4$ forms a ring.

(a) Determine the group of units $E(\mathbb{Z}_4)$. Is $\mathbb{Z}_4$ a field?

(b) Is $\mathbb{Z}_6$, with multiplication and addition defined as multiplication and addition modulo 6 a field? What is $E(\mathbb{Z}_6)$?

$(\mathbb{Z}_4, +)$ forms an Abelian group as the neutral element, associativity and commutativity are inherited from the integers. Associativity of multiplication is also inherited, so $(\mathbb{Z}_4, \cdot)$ forms a semi-group and thus $(\mathbb{Z}_4, +, \cdot)$ is a ring.

For part (a), 1 is the multiplicative neutral element and therefore is invertible. 3 is also invertible as $3 \cdot 3 = 9 \equiv 1 \mod 4$. 0 is trivially not invertible and 2 is also not invertible as every its multiple of either congruent to 0 or 2 modulo 4, but never 1. Hence $E(\mathbb{Z}_4) = \{1, 3\}$. $\mathbb{Z}_4$ is not a field as $E(\mathbb{Z}_4) = \{1, 3\} \neq \{1, 2, 3\} = \mathbb{Z}_4 \setminus \{0\}$.

For part (b), $\mathbb{Z}_6$ is not a field as $3 \cdot n$ is either congruent to 0 or 3 modulo 6, but never 1, which is the multiplicative neutral element, meaning 3 is not invertible; Thus $3 \notin E(\mathbb{Z}_6)$ and $3 \in \mathbb{Z}_6 \setminus \{0\}$, meaning $E(\mathbb{Z}_6) \neq \mathbb{Z}_6 \setminus \{0\}$.

## Exercise 4.2

Let $X$ be a set. Can you think of a ring structure on a set $\text{map}(X, \mathbb{R})$ of all functions $X$ to the set of real numbers?

(a) What are unity and zero of this ring?

(b) Determine the group of units $E(\text{map}(X, \mathbb{R}))$.

Consider the set $\max(X, \mathbb{R})$ with addition and multiplication of functions. (I.e., given functions $f, g : X \to \mathbb{R}$, define the functions $f + g, f \cdot g : X \to \mathbb{R}$ given by $f + g : x \mapsto f(x) + g(x)$ and $f \cdot g : x \mapsto f(x)g(x)$.)

To prove that the functions $f + (g + h)$ and $(f + g) + h$ are the same for all $f, g, h \in \operatorname{map}(X, \mathbb{R})$, we show that they are equal when evaluated at the same points. Let $x \in X$, then $(f + (g + h))(x) = f(x) + (g + h)(x) = f(x) + (g(x) + h(x)) = (f(x) + g(x)) + h(x) = (f + g)(x) + h(x) = ((f + g) + h)(x)$, so $(\operatorname{map}(X, \mathbb{R}), +)$ is a semi-group. Define $e : X \to \mathbb{R}$ given by $e(x) = 0$ for all $x \in X$ so that $e \in \operatorname{map}(X, \mathbb{R})$ and, with any $f \in \operatorname{map}(X, \mathbb{R})$, we have $(f + e)(x) = f(x) + e(x) = f(x) + 0 = f(x) = 0 + f(x) = e(x) + f(x) = (e + f)(x)$, i.e., the functions $f + e$ and $e + f$ are both equal to the function $f$, i.e., $e$ is the neutral element in $(\operatorname{map}(X, \mathbb{R}), +)$. So the latter is a monoid. Now, for all $f \in \operatorname{map}(X, \mathbb{R})$ define $-f : X \to \mathbb{R}$ given by $(-f)(x) = -f(x)$ so that $-f \in \operatorname{map}(X, \mathbb{R})$ and $(f + (-f))(x) = f(x) + (-f)(x) = f(x) + (-f(x)) = 0 = e(x) = 0 = (-f)(x) + f(x) = ((-f) + f)(x)$, i.e., $f + (-f)$ and $(-f) + f$ are both equal to the function $e$, which is the additive neutral element, i.e., $-f$ is the additive inverse of $f$. So, $(\max(X, \mathbb{R}), +)$ is a group. Finally, we prove that the functions $f + g$ and $g + f$ are the same for all $f, g \in \operatorname{map}(X, \mathbb{R})$: $(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$. Hence $(\max(X, \mathbb{R}), +)$ is an Abelian group.

Now, for all functions $f, g, h \in \operatorname{map}(X, \mathbb{R})$ and $x \in \mathbb{R}$ we have $(f \cdot (g \cdot h))(x) = f(x) \cdot (g \cdot h)(x) = f(x) \cdot (g(x) \cdot h(x)) = (f(x) \cdot g(x)) \cdot h(x) = (f \cdot g)(x) \cdot h(x) = ((f \cdot g) \cdot h)(x)$, meaning the functions $f \cdot (g \cdot h)$ and $(f \cdot g) \cdot h$ are equal, so associativity holds and $(\operatorname{map}(X, \mathbb{R}), \cdot)$ is a semi-group.

Finally, $(\max(X, \mathbb{R}), +, \cdot)$ thus forms a (as one may verify, commutative) ring. [Remark: The set of reals could be replaced with any ring and the assertion would still be true.]

For part (a), like already mentioned, the zero of this ring is the function $e$. Define $u : X \to \mathbb{R}$ given by $u(x) = 1$ for all $x \in X$ so that $u \in \operatorname{map}(X, \mathbb{R})$ and, for all $f \in \operatorname{map}(X, \mathbb{R})$, we have $(f \cdot u)(x) = f(x) \cdot u(x) = f(x) \cdot 1 = f(x) = 1 \cdot f(x) = u(x) \cdot f(x) = (u \cdot f)(x)$, i.e., the functions $u \cdot f$ and $f \cdot u$ are both equal to $f$, i.e., $u$ is the unit element of the ring.

For part (b), let $f \in \operatorname{map}(X, \mathbb{R})$. If $f(x) \neq 0$ for all $x \in X$, then define $g : X \to \mathbb{R}$ given by $g(x) = (g(x))^{-1}$ so that $g^{-1} \in \operatorname{map}(X, \mathbb{R})$ and $(f \cdot g)(x) = f(x) \cdot g(x) = f(x) \cdot (f(x))^{-1} = 1 = u(x) = 1 = (f(x))^{-1} \cdot f(x) = g(x) \cdot f(x) = (gf)(x)$, i.e., the functions $fg$ and $gf$ are both equal to the function $u$, which is the multiplicative neutral element, meaning $g$ is the multiplicative inverse of $f$. If, however, there exists $c \in X$ with $f(c) = 0$, then, for all functions $h \in \text{map}(X, \mathbb{R})$, we have $(f \cdot h)(c) = f(c) \cdot h(c) = 0 \cdot h(c) = 0 \neq 1 = u(x)$, meaning $f \cdot h$ is never equal to the unit element, therefore $f$ has no inverse. Hence $E(\max(X, \mathbb{R}))$ is the set of functions from $X$ to $\mathbb{R}$ that have no roots.

## Exercise 5

A lattice $(P, \leq)$ is said to be distributive if the laws $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ and $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ hold. For example, the Boolean lattice is distributive. Show that in a lattice, the first law implies the second, and conversely.

We start by proving that $\wedge$ and $\vee$ are associative operations on $P$ and the absorption laws.

Let $a, b, c \in P$, our claim is that $\sup\{a, \sup\{b, c\}\} = \sup\{a, b, c\}$. First, $a \leq \sup\{a, \sup\{b, c\}\}$ and $\sup\{b, c\} \leq \sup\{a, \sup\{b, c\}\}$ according to the definition, but we also have $b \leq \sup\{b, c\}$ and $c \leq \sup\{b, c\}$. Via transitivity we also obtain $b \leq \sup\{a, \sup\{b, c\}\}$ and $c \leq \sup\{a, \sup\{b, c\}\}$. This shows that $\sup\{a, \sup\{b, c\}\}$ is an upper bound of $\{a, b, c\}$. Now let $u \in P$ be an upper bound of $\{a, b, c\}$ (existence is trivial), then $u$ is also an upper bound of $\{b, c\}$, meaning $\sup\{b, c\} \leq u$ and we also have $a \leq u$. The latter two imply that $\sup\{a, \sup\{b, c\}\} \leq u$. Therefore $\sup\{a, \sup\{b, c\}\}$ is the least upper bound, i.e., the supremum, of $\{a, b, c\}$. We thus obtain $\sup\{a, \sup\{b, c\}\} = \sup\{a, b, c\} = \sup\{c, a, b\} = \sup\{c, \sup\{a, b\}\} = \sup\{\sup\{a, b\}, c\}$, or, written with $\vee$, $a \vee (b \vee c) = (a \vee b) \vee c$. Thus $\vee$ associative. Associativity is proven likewise.

Let $a, b \in P$, then, obviously, $\inf\{a, b\} \leq a \leq \sup\{a, b\}$, meaning we have $\inf\{a, \sup\{a, b\}\} = a$ and $\sup\{a, \inf\{a, b\}\} = a$, or, written with $\vee$ and $\wedge$, $a \vee (a \wedge b) = a$ and $a \wedge (a \vee b)$.

Assume distributivity of $\wedge$ over $\vee$ and consider the following.

$$(x \vee y) \wedge (x \vee z) = ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) = x \vee ((x \wedge z) \vee (y \wedge z)) =$$
$$(x \vee (x \wedge z)) \vee (y \wedge z) = x \vee (y \wedge z)$$

Conversely, assume distributivity of $\vee$ over $\wedge$ and consider the following.

$$(x \wedge y) \vee (x \wedge z) = ((x \wedge y) \vee x) \wedge ((x \wedge y) \vee z) = x \wedge ((x \vee z) \wedge (y \vee z)) =$$
$$(x \wedge (x \vee z)) \wedge (y \vee z) = x \wedge (y \vee z)$$

## 8.2 Week 12 Central Exercises

### Exercise 1

Show that a semi-group with left unity and right inverses is not a group: *Hint*: Consider the operation $a * b := |a|b$ on $\mathbb{R} \setminus \{0\}$.

I assume the author meant to say "Show that a semi-group with left unity and right inverses may not be a group" as there definitely are semigroups with left unity and right inverses that are groups. (Just consider any group.) In the previous central exercises we have shown that the operation on $\mathbb{R} \setminus \{0\}$ defined by $a * b := |a|b$ has a left unity (in fact, two of them, namely, 1 and $-1$), but it has no right unity, already making this set not a group. We now need to show that there are right inverses. For all $x \in \mathbb{R} \setminus \{0\}$ its right inverses are $\frac{1}{|x|}$ and $\frac{1}{|x|}$ respectively as $x * \frac{1}{|x|} = |x| \cdot \frac{1}{|x|} = 1$ and $x * \left(-\frac{1}{|x|}\right) = |x| \cdot \left(-\frac{1}{|x|}\right) = -1$.

### Exercise 2

(1) Write down a composition table (Cayley table) for rotations of a regular pentagon in the plane.

(2) Fill in the following composition table (Cayley table) for a group $G$ with neutral element $e$.

|  | $e$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| $e$ | $e$ |  |  |  |  |
| $a$ |  | $b$ |  |  | $e$ |
| $b$ |  | $c$ | $d$ | $e$ |  |
| $c$ |  | $d$ |  | $a$ | $b$ |
| $d$ |  |  |  |  |  |

For part (a), let $e$, $r$ and $d$ be the action of doing nothing, counterclockwise rotation by 72 degrees and reflection around a line crossing the center of the pentagon and some fixed vertex. With composition as our operation and consider the facts that $a^5 = e$, $d^2 = e$ and $dr = r^4d$, we thus obtain the following Cayley table:

| $\circ$ | $e$ | $r$ | $r^2$ | $r^3$ | $r^4$ | $d$ | $rd$ | $r^2d$ | $r^3d$ | $r^4d$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $r$ | $r^2$ | $r^3$ | $r^4$ | $d$ | $rd$ | $r^2d$ | $r^3d$ | $r^4d$ |
| $r$ | $r$ | $r^2$ | $r^3$ | $r^4$ | $e$ | $rd$ | $r^2d$ | $r^3d$ | $r^4d$ | $d$ |
| $r^2$ | $r^2$ | $r^3$ | $r^4$ | $e$ | $r$ | $r^2d$ | $r^3d$ | $r^4d$ | $d$ | $rd$ |
| $r^3$ | $r^3$ | $r^4$ | $e$ | $r$ | $r^2$ | $r^3d$ | $r^4d$ | $d$ | $rd$ | $r^2d$ |
| $r^4$ | $r^4$ | $e$ | $r$ | $r^2$ | $r^3$ | $r^4d$ | $d$ | $rd$ | $r^2d$ | $r^3d$ |
| $d$ | $d$ | $r^4d$ | $r^3d$ | $r^2d$ | $rd$ | $e$ | $r^4$ | $r^3$ | $r^2$ | $r$ |
| $rd$ | $rd$ | $d$ | $r^4d$ | $r^3d$ | $r^2d$ | $r$ | $e$ | $r^4$ | $r^3$ | $r^2$ |
| $r^2d$ | $r^2d$ | $rd$ | $d$ | $r^4d$ | $r^3d$ | $r^2$ | $r$ | $e$ | $r^4$ | $r^3$ |
| $r^3d$ | $r^3d$ | $r^2d$ | $rd$ | $d$ | $r^4d$ | $r^3$ | $r^2$ | $r$ | $e$ | $r^4$ |
| $r^4d$ | $r^4d$ | $r^3d$ | $r^2d$ | $rd$ | $d$ | $r^4$ | $r^3$ | $r^2$ | $r$ | $e$ |

For part (b), we begin by acknowledging that, since $e$ is the neutral element, its row and column are simply copies of the first row and the first column respectively. We notice that the column of $a$ can be completed; The elements $a$, $b$, $c$ and $d$ appear it in, so, clearly, the unknown entry should have $e$ in it. We similarly see that the unknown entry in the row of $b$ should be $a$. Continuing in such manner, we obtain the complete Cayley table of the original group: [One may notice that this group is isomorphic to the additive group of integers modulo 5.]

| | $e$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ |
| $b$ | $b$ | $c$ | $d$ | $e$ | $a$ |
| $c$ | $c$ | $d$ | $e$ | $a$ | $b$ |
| $d$ | $d$ | $e$ | $a$ | $b$ | $c$ |

## Exercise 3

Recall that order of a subgroup is a number of its elements.

(1) Find a subgroup of $D_8$ which has order 4 and is abelian.

(2) Find another subgroup of $D_8$ of order 4.

(3) The center of a group $G$ is defined to be

$$Z(G) := \{a \in G : ab = ba \text{ for all } b \in G\}.$$

Find $Z(D_8)$ and list all its elements.

For part (a), we may consider the subgroup generated by the rotation by 90 degrees since it has order is 4 and so will the subgroup generated by it. It will also be Abelian as every cyclic group is Abelian.

For part (b), we may consider the subgroup generated by rotation by 180 degrees and reflection around an axis of symmetry.

For part (c), finding centers can be simplified to observing whose elements have symmetric rows and columns in the Cayley table. In this case, the center is the trivial group.

## Exercise 4

(1) Describe the subgroup of $\mathbb{Z}$ generated by $-12$.

(2) Describe the subgroup of $\mathbb{Z}$ generated by $-12$ and 4.

(3) Describe the subgroup of $\mathbb{Z}$ generated by elements $-12$, 4 and 5.

(4) Show that $\mathbb{Z}$ has no non-trivial finite subgroups.

(5) Show that every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ or some $n \in \mathbb{Z}$.

For part (1), the subgroup is the set of integers of the form $-12k$ for some $k \in \mathbb{Z}$, or, alternatively, of the form $12m$ for some $m \in \mathbb{Z}$.

For part (2), the subgroup is the set of integers of the form $-12a + 4b$ for some $a, b \in \mathbb{Z}$, or, alternatively, of the form $4k$ for some $k \in \mathbb{Z}$.

For part (3), the subgroup is the set of integers of the form $-12a+4b+5c$ for some $a, b, c \in \mathbb{Z}$, or, alternatively, it's the entire group $\mathbb{Z}$ since it contains $1 = -12 \cdot 0 + 4 \cdot (-1) + 5 \cdot 1$ meanwhile 1 generated $\mathbb{Z}$.

For part (4), let $H$ be a non-trivial subgroup of $\mathbb{Z}$, then it contains some nonzero integer $n \in \mathbb{Z}$ and should also contain the subgroup generated by $n$, which is not finite (since the order of every nonzero integer is infinite).

For part (5), let $H$ again be a non-trivial subgroup of $\mathbb{Z}$. Pick some $n \in H$. If $n > 0$, then $H$ has a positive integer. If $n < 0$, then its inverse, $-n$, should be in $H$ meanwhile $-n > 0$. This shows that $H$ contains at least one positive integer. Let $n_0$ be the smallest positive integer in $H$. Our claim is that $H$ is generated by $n_0$. Let $n$ be an arbitrary element of $H$. Via Euclidean algorithm, we obtain $n = qn_0 + r$ for some unique $q, r \in \mathbb{Z}$ with $0 \leq r < n_0$. Clearly, $r = n - qn_0$ should be contained in $H$. We can't have $0 < r < n_0$ since it would contradict the minimality of $n_0$, so $r = 0$ and $n = qn_0$, i.e., every element in $H$ is an integer multiple of $n_0$ as desired.

## Exercise 5

(1) Show that the order of any element $a$ of a finite group divides the order of that group.

(2) A simple Abelian group is a nontrivial Abelian group whose only subgroups are the trivial group and the group itself. Show that any group of prime order is cyclic and simple.

For part (1), we consider the subgroup generated by $a$. The subgroup should have order equal to the order of $a$. Via Lagrange theorem, the order of $a$ divides the order of the group.

For part (2), let $G$ be a group of prime order. Clearly, $|G| \leq 2$, so there exists a nonneutral element, call it $x$. According to part (a), the order of $x$ divides the order of the group. Since the order of $x$ is not 1 and the order of the group is prime, the order of the subgroup should be equal to the order of the group, meaning $x$ generated $G$, meaning $G$ is cyclic. Now, consider any subgroup $H$ of $G$. The order of $H$ should divide the order of $G$ which is prime, so we have $|H| = 1$ or $H = G$. The former is equivalent to saying $H$ is the trivial group. Therefore all subgroups of $G$ are either the trivial group of $G$ itself, i.e., $G$ is simple.

## Exercise 6

(1) Let $G$ be a group and $1 \neq a \in G$ with $O(a) = 30$. Find $O(a^3)$, $O(a^{10})$, $O(a^{25})$ and $O(a^{16})$.

(2) Let $G$ be a group and suppose $O(a) \leq 2$ for every $a \in G$. Prove that $G$ is abelian.

(3) Show that a finite group of even order has an odd number of elements of order 2.

For part (1), using the formula $O(a^n) = \frac{O(a)}{\gcd(n,O(a))}$, we obtain $O(a^3) = \frac{30}{\gcd(3,30)} = \frac{30}{3} = 10$, $O(a^{10}) = \frac{30}{\gcd(10,30)} = \frac{30}{10} = 3$, $O(a^{25}) = \frac{30}{\gcd(25,30)} = \frac{30}{5} = 6$ and $O(a^{16}) = \frac{30}{\gcd(16,30)} = \frac{30}{2} = 15$.

For part (2), all elements have order equal to 1 or 2, i.e., every element $a$ has either property $a^2 = 1$ or $a = 1$ where 1 is the neutral element of $G$. Now consider $(ab)^2$ for all $a, b \in G$. We have $(ab)^2 = 1$ whether or not the order of $ab$ is 1 or 2 and, by multiplying both sides by $a$ on the left and by $b$ on the right, we obtain $ab = ba$, i.e., every pair of elements commute. Thus the group is Abelian.

For part (3), let $G$ be a group with even order and $k$ be the number of elements with order 2. Consider the bijection $\varphi$ from $G$ to $G$ given by $g \mapsto g^{-1}$. The number of elements fixed by $\varphi$ is $k + 1$ (Since the neutral element gets mapped to itself and so do the elements of order 2 since $a^2 = 1$ implies $a = a^{-1}$ for all $a \in G$ with $O(a) = 2$.), we now shall count the elements not fixed by $\varphi$. Note that $\varphi$ is some permutation on the elements of $G$, namely, it is a product of disjoint transpositions since $\varphi^2$ is the identity map. The number of elements permuted, i.e., not fixed, is hence double the number of transpositions, meaning the number of elements in $G$ not fixed by $\varphi$ is even, call that number $m$. Finally, we have that $|G| = k + 1 + m$ and $k = |G| - m - 1$. The latter is odd and so is $k$. (In fact, this can be generalized into saying that the number of elements of order 2 is always of different parity than the order of the group.)

## 8.3 Week 13 Central Exercises

### Exercise 1

Show that for any abelian group $(G, +)$ and a subgroup $H \subseteq G$, the congruence

$$a \approx b \iff a - b \in H$$

is compatible.

In this case, instead of $G/\approx$ one simply writes $G/H$ as a factor group of $G$ by a subgroup $H$. Determine the factor groups $G/G$ and $G/\{0\}$.

Let $a \approx b$ for some $a, b \in G$, i.e., $a - b \in H$. Pick any $c \in G$. We have $(a + c) - (b + c) = a + c - c - b = a + 0 - b = a - b \in H$, meaning we have $a + c \approx b + c$, i.e., the congruence is indeed compatible. (Commutativity takes care of the rest.)

The factor group $G/G$ will contain all elements $a, b \in G$ such that $a - b \in G$, but that holds for all elements of $G$, meaning $G/G$ consists of only one congruence class, i.e., is the trivial group. The factor group $G/\{0\}$, each congruence class will contain elements $a, b \in G$ such that $a - b \in \{0\}$, i.e., $a - b = 0$ and $a = b$ via the uniqueness of inverses. But that means that the congruence classes are simply singletons containing each element of $G$, meaning $G/\{0\}$ is isomorphic to $G$ itself.

### Exercise 2.1

Calculate the following in $\mathbb{Z}_6$, $\mathbb{Z}_7$ and then in $\mathbb{Z}_8$.

(1) $2 - 5 + 3 \cdot 5$;

(2) $1 \cdot 5 + 6 \cdot 5$;

(3) $6 - 5 \cdot 5^4$;

(4) $3^3 - 6 \cdot 2^7$.

For (1), we have $2 - 5 + 3 \cdot 5 = 12$. The latter is congruent to 0 modulo 6, to 5 modulo 7 and to 4 modulo 8.

For (2), we have $1 \cdot 5 + 6 \cdot 5 = 7 \cdot 5$. The latter is congruent to $1 \cdot 5 = 5$ modulo 6, to $0 \cdot 5$ modulo 7 and to $(-1) \cdot 5 = -5 = 3$ modulo 8.

For (3), we have $6 - 5 \cdot 5^4 = 0 - (-1) \cdot (-1)^4 = 1$ modulo 6, $6 - 5 \cdot 5^4 = (-1) - (-2) \cdot (-2)^4 = -1 + 32 = 31 = 3$ modulo 7 and $6 - 5 \cdot 5^4 = (-2) - (-3) \cdot 25^2 = -2 + 3 \cdot 1^2 = 1$ modulo 8.

For (4), we have $3^3 - 6 \cdot 2^7 = 27 - 0 \cdot 2^7 = 3$ modulo 6, $3^3 - 6 \cdot 2^7 = 9 \cdot 3 - (-1) \cdot 2^3 \cdot 2^3 \cdot 2 = 2 \cdot 3 + 8 \cdot 8 \cdot 2 = 6 + 1 \cdot 1 \cdot 2 = 8 = 1$ modulo 7 and $3^3 - 6 \cdot 2^7 = 9 \cdot 3 - 6 \cdot 2^3 \cdot 2^4 = 1 \cdot 3 - 6 \cdot 0 \cdot 2^4 = 3$ modulo 8.

## Exercise 2.2

Try to solve the following equations in $\mathbb{Z}_6$, $\mathbb{Z}_7$ and then in $\mathbb{Z}_8$. Indicate if the (unique) solution does not exist and explain why is this the case.

(1) $x + 3 = -1$;

(2) $5 \cdot x = 1$;

(3) $3 \cdot x = 0$;

(4) $4 \cdot x + 2 = -6$.

For the first equation, we have $x = -4$ and, if we were to write the solution as a remainder, we would have $x = 2$, $x = 3$ and $x = 4$ in $\mathbb{Z}_6$, $\mathbb{Z}_7$ and $\mathbb{Z}_8$ respectively.

For the second equation, the inverse of 5 modulo 6 is itself (since $5 \cdot 5 = 25$ leaves the remainder of 1), so we obtain $5 \cdot 5 \cdot x = 5 \cdot 1$ and $x = 5$ modulo 6. The inverse of 5 modulo 7, however, is 3 (since $5 \cdot 3 = 15$ leaves the remainder of 1), so we obtain $3 \cdot 5 \cdot x = 3 \cdot 1$ and $x = 3$ modulo 7. The inverse of 5 modulo 8 is again itself (since $5 \cdot 5 = 25$ leaves the remainder of 1), so we obtain $x = 5$ modulo 8 as before.

For the third equation, in $\mathbb{Z}_6$, we know that $3 \cdot x$ should be divisible by 6. $3 \cdot x$ is already divisible by 3, so we require $x$ to be even, i.e., the obtain the solutions $x = 0$, $x = 2$ and $x = 4$ modulo 6. In $\mathbb{Z}_7$, since 7 is prime, $\mathbb{Z}_7$ is an integran domain, meaning $3 \cdot x = 0$ (as $3 \neq 0$ modulo 7) implies $x = 0$ modulo 7. In $\mathbb{Z}_8$, 3 is also invertible (since it is coprime to 8), so we get $x = 0$ modulo 8.

We may start solving the last equation by rewriting it as $4 \cdot (x + 2) = 0$. In $\mathbb{Z}_6$, using the same reasoning as before, we therefore require $x + 2$ to be divisible by 3, i.e., we obtain $x + 2 = 0$ or $x + 2 = 3$ modulo 6 and, finally, $x = 4$ or $x = 1$ modulo 6. In $\mathbb{Z}_7$, however, $4 \cdot (x + 2) = 0$ (as $4 \neq 0$ modulo 7) implies $x + 2 = 0$ and $x = 5$ modulo 7. In $\mathbb{Z}_8$, $4 \cdot (x + 2) = 0$ implies $x + 2$ is even, i.e., $x + 2$ is 0, 2, 4 or 6 modulo 8, which yields the solutions $x = 6$, $x = 0$, $x = 2$ and $x = 4$ modulo 8.

## Exercise 3

Calculate the following.

(1) $\varphi(47)$;

(2) $\varphi(46)$;

(3) The order of the group of primitive residue classes $\mod 900$;

(4) The order of the group of primitive residue classes $\mod 326$.

Since 47 is prime, we have $\varphi(47) = 47 - 1 = 46$ recall that ($\varphi(p) = p - 1$ for primes $p$.). Since $46 = 2 \cdot 23$ , we have $\varphi(46) = \varphi(2)\varphi(23) = 1 \cdot 22 = 22$ (recall that $\varphi(ab) = \varphi(a)\varphi(b)$ given $a, b$ are coprime.). The order of the group of primitive residue classes $\mod n$, in general, is $\varphi(n)$, so we get that the order of the group of primitive residue classes $\mod 900$ and $\mod 326$ are $\varphi(900) = \varphi(2^2 \cdot 3^2 \cdot 5^2) = \varphi(2^2)\varphi(3^2)\varphi(5^2) = 2^1(2-1)3^1(3-1)5^1(5-1) = 2 \cdot 3 \cdot 2 \cdot 5 \cdot 4 = 240$ and $\varphi(326) = \varphi(2 \cdot 163) = \varphi(2)\varphi(163) = 162$ respectively.

## Exercise 4

First, show that if $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

For each pair of integers $(a, b)$, use the Euclidean algorithm to find their gcd. Then reverse the steps of the algorithm to find the integers $x$ and $y$ such that $xa + yb = \gcd(a, b)$.

(1) $a = 254, b = 32$;

(2) $a = 74, b = 383$;

(3) $a = 7544, b = 115$;

(4) $a = 687, b = 24$.

What is the inverse of $74 \mod 383$?

By definition, we have $\gcd(a, b)$ divides $b$. Also, $r = a - bq$. The right hand side of the latter is a multiple of $\gcd(a, b)$, meaning $\gcd(a, b)$ also divides $r$. Hence $\gcd(a, b)$ is a common divisor of $b$ and $r$; We now show that it is also their greatest common divisor. Let $d$ be a divisor of $b$ and $r$, our goal is to show that $d$ divides $\gcd(a, b)$. Since $d$ is a divisor of $b$ and $r$, we have $b = b'd$ and $r = r'd$ for some integers $b'$ and $r'$. We then have $a = b'dq + r'd$. The right hand side of the latter is a multiple of $d$, meaning $d$ should also divide $a$. Since $d$ is consequently a common divisor of $a$ and $b$, it also divides $\gcd(a, b)$, which finishes the proof.

For part (1), we begin as follows.

$$\begin{aligned} 254 &= 32 \cdot 7 + 30 \\ 32 &= 30 \cdot 1 + 2 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Reversing the steps of the algorithm, we get

$$254 = 32 \cdot 7 + 30 = 32 \cdot 7 + (32 - 2) = 32 \cdot 8 - 2$$
$$2 = 32 \cdot 8 - 254 \cdot 1$$

For part (2), we begin as follows.

$$\begin{aligned} 383 &= 74 \cdot 5 + 13 \\ 74 &= 13 \cdot 5 + 9 \\ 13 &= 9 \cdot 1 + 4 \\ 9 &= 4 \cdot 2 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

Reversing the steps of the algorithm, we get

$$1 = 9 - 4 \cdot 2 = 9 - (13 - 9 \cdot 1) \cdot 2 = 9 \cdot 3 - 13 \cdot 2 = (74 - 13 \cdot 5) \cdot 3 - 13 \cdot 2 =$$

$$= 74 \cdot 3 - 13 \cdot 17 = 74 \cdot 3 - (383 - 74 \cdot 5) \cdot 17 = 74 \cdot 88 - 383 \cdot 17$$

For part (3), we begin as follows.

$$\begin{aligned} 7544 &= 115 \cdot 65 + 69 \\ 115 &= 69 \cdot 1 + 46 \\ 69 &= 46 \cdot 1 + 23 \\ 46 &= 23 \cdot 2 + 0 \end{aligned}$$

Reversing the steps of the algorithm, we get

$$23 = 69{-}46 = 69{-}(115{-}69) = 69{\cdot}2{-}115 = (7544{-}115{\cdot}65){\cdot}2{-}115 = 7544{\cdot}2{-}115{\cdot}131$$

For part (4), we begin as follows.

$$\begin{aligned} 687 &= 24 \cdot 28 + 15 \\ 24 &= 15 \cdot 1 + 9 \\ 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Reversing the steps of the algorithm, we get

$$3 = 9{-}6 = 9{-}(15{-}9) = 9{\cdot}2{-}15 = (24{-}15){\cdot}2{-}15 = 24{\cdot}2{-}15{\cdot}3 = 24{\cdot}2{-}(687{-}24{\cdot}28){\cdot}3 = 24{\cdot}86{-}687$$

Finally, the inverse of 74 mod 383 is 88 is suggested by our result for part (3).

## Exercise 5

Compose the following in $S_5$.

(1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$;

(2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix}$;

(3) $(3, 4) \circ (1, 2, 4)$;

(4) $(4, 1, 2, 3) \circ (5, 1, 2)$.

(5) Find inverses of the following permutations in $S_5$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \quad \text{and} \quad (4, 1, 6, 2).$$

(6) Decompose four permutations in (1) and (2) into a product of disjoint cycles and then into transpositions. Determine whether the permutations are odd or even. [The author is assumed to mean the permutations whose products are being taken in (1) and (2).]

(7) Solve $\sigma x = \mu$ in $S_9$ for

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 3 & 4 & 5 & 6 & 1 & 8 \end{pmatrix}$$

and

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 8 & 9 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}.$$

For (1), we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

For (2), we have

$$\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5\\1&3&5&4&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&5&3&4&1\end{pmatrix}$$

For (3), we have

$$(3,4)\circ(1,2,4)=(1,2,3,4)$$

For (4), we have

$$(4,1,2,3)\circ(5,1,2)=\begin{pmatrix}1&2&3&4&5\\3&5&4&1&2\end{pmatrix}$$

For (5), we have

$$\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3&4&5\\3&5&2&1&4\end{pmatrix}$$
$$(4,1,6,2)^{-1}=(1,4,2,6)$$

For (6), we have

$$\begin{pmatrix}1&2&3&4&5\\4&3&5&1&2\end{pmatrix}=(1,4)(2,3,5)=(1,4)(2,3)(3,5)$$
$$\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}=(3,4)$$
$$\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}=(1,2)(3,5)$$
$$\begin{pmatrix}1&2&3&4&5\\1&3&5&4&2\end{pmatrix}=(2,3,5)=(2,3)(3,5)$$

The permutations are hence odd, odd, even and even respectively.
For (7), we have

$$x=\sigma^{-1}\mu$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 3 & 4 & 5 & 6 & 1 & 8 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 8 & 9 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 4 & 5 & 6 & 7 & 2 & 9 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 8 & 9 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 9 & 3 & 4 & 5 & 6 & 1 & 8 \end{pmatrix}$$

## 8.4 Week 14 Central Exercises

### Exercise 1

Let $R$ be a ring and $a, b, c, d \in R$.

(a) Evaluate $(a + b)(c + d)$.

(b) Prove that $(a + b)^2 = a^2 + ab + ba + b^2$ where by $x^2$ we mean $xx$.

(c) If in a ring $R$ every $x \in R$ satisfies $x^2 = x$, prove that $R$ must be commutative.

For part (a), applying the distributivity laws yields the following

$$(a + b)(c + d) = a(c + d) + b(c + d) = ac + ad + bc + bd$$

For part (b), we apply our result from part (a) while letting $a = c$ and $b = d$, so that we obtain

$$(a + b)(a + b) = aa + ab + ba + bb$$

Which, written using the notation of squaring, is the same as

$$(a + b)^2 = a^2 + ab + ba + b^2$$

For part (c), we take any $x, y \in R$ and consider the square of their sum. Using part (b), we get

$$(x + y)^2 = x^2 + xy + yx + y^2$$

But, the definition of $R$ allows us to rewrite that as

$$x + y = x + xy + yx + y$$

Cancelling both sides by $x$ and $y$, we obtain $xy + yx$, i.e., $xy = -yx$. At the same time, $-1 = (-1)^2 = 1$ and $-yx = (-1)yx$, so $xy = yx$, i.e., all elements commute. Thus $R$ is commutative.

## Exercise 2.1

Recall that $\mathrm{map}(X, \mathbb{R})$ denotes the ring of all real valued functions from a set $X$, endowed with pointwise multiplication and addition.

Let $A \subseteq X$. Show that the set

$$\mathcal{I}_A = \{f \in \mathrm{map}(X, \mathbb{R}) : f(a) = 0 \text{ for all } a \in A\}$$

is an ideal in $\mathrm{map}(X, \mathbb{R})$.

Clearly, $\mathcal{I}_A isnonempty$. Let $f_1, f_2 \in \mathcal{I}_A$ and consider the function $f_1 - f_2$ by which we mean $f_1 + (-f_2)$. For all $a \in A$, we have $(f_1 - f_2)(a) = f_1(a) - f_2(a) = 0 - 0 = 0$, i.e., $f_1 - f_2 \in A$. This shows that $(\mathcal{I}_A, +)$ is a subgroup of $(\mathrm{map}(X, \mathbb{R}), +)$. We now show that $\mathcal{I}_A$ is closed under multiplication by all ring elements. Let $f \in \mathcal{I}_A$ and $g \in \mathrm{map}(X, \mathbb{R})$ and consider their product $fg$. For all $a \in A$, we have $(fg)(a) = f(a)g(a) = 0 \cdot g(a) = 0$, meaning $fg \in \mathcal{I}_A$. (Commutativity takes care of the other condition.) Thus $\mathcal{I}_A$ is an ideal of $\mathrm{map}(X, \mathbb{R})$.

## Exercise 2.2

Let $U, V$ be ideals of a ring $R$. Define $U + V = \{u + v : u \in U, v \in V\}$. Prove that $U + V$ is also an ideal in $R$.

Let $w, w' \in U + V$. Then there exist $u, u' \in U$ and $v, v' \in V$ with $w = u + v$ and $w' = u' + v'$. This means that $w - w' = (u + v) - (u' + v') = u + v - u' - v' = (u - u') + (v - v')$. Since $U$ and $V$ are subgroups of $(R, +)$ (by definition of ideals) and $u, u'$ and $v, v'$ are their elements respectively, we have $u - u' \in U$ and $v - v' \in V$. Together with $w - w' = (u - u') + (v - v')$, this implies that $w - w' \in U + V$. This shows that $(U + V, +)$ is a subgroup of $(R, +)$. Now let $r \in R$ and consider the products $rw$ and $wr$. We have $rw = r(u + v) = ru + rv$. Since $U$ and $V$ are ideals, they are closed under multiplication by all ring elements, meaning $ru \in U$ and $rv \in V$. Together with the last equation, this implies $rw \in U + V$. We similarly show that $wr \in U + V$. Thus $U + V$ is an ideal of $R$.

## Exercise 3.1

Show that the rotation subgroup $R$ is normal in $D_3$. How many elements are there in $D_3/R$? Can you "identify" this group?

The rotation group $R$ consists of 3 elements whereas $D_3$ consists of 6, so the index of $R$ in $D_3$ is 2. Every subgroup of index 2 is normal (see Exercise 2.13 of Waerden). Lastly, there is only one group of two elements, namely, the group of integer congruence classes modulo 2 under addition.

## Exercise 3.2

Show that a subgroup generated by a single reflection is not a normal subgroup of $D_3$.

Let $r$ denote rotation by 120 degrees and $s$ be an arbitrary reflection in $D_3$. Then $r\langle s\rangle = \{r, rs\} \neq \{r, sr\} = \langle s\rangle r$ since $rs \neq sr$.

## Exercise 4

Prove that

(1) $x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$.

(2) $x^2 + 1$ is irreducible over $\mathbb{Z}_7$.

(3) $x^3 - 9$ is irreducible over $\mathbb{Z}_{31}$.

(4) $x^3 - 9$ is reducible over $\mathbb{Z}_{11}$.

*Hint:* If the polynomials above are reducible, one of the factors has to be linear.

We will use the hint without proving it (as so far there is not enough theory developed to solve this with reasonable time without extra assumptions). We also infer that a polynomial has a linear factor if and only if it has a root (via root-factor theorem). We hence prove that each of the polynomials are nonzero at every point.

For part (1), $0^2 + 0 + 1 = 1 = 2 + 1 = 1 + 1 + 1 = 1^2 + 1 + 1$ and $1 \neq 0$.

For part (2), we have $0^2 + 1 = 1$, $1^2 + 1 = 2$, $2^2 + 2 = 1$ and $3^2 + 2 = 4$ (symmetry of squaring takes care of the rest).

For parts (3) and (4), we have

$$\begin{aligned}
0^3 &= -9 & 11^3 - 9 &= 1322 & 21^3 - 9 &= 9252 \\
1^3 - 9 &= -8 & 12^3 - 9 &= 1719 & 22^3 - 9 &= 10639 \\
2^3 - 9 &= -1 & 13^3 - 9 &= 2188 & 23^3 - 9 &= 12158 \\
4^3 - 9 &= 55 & 14^3 - 9 &= 2735 & 24^3 - 9 &= 13815 \\
5^3 - 9 &= 116 & 15^3 - 9 &= 3366 & 25^3 - 9 &= 15616 \\
6^3 - 9 &= 207 & 16^3 - 9 &= 4087 & 26^3 - 9 &= 17567 \\
7^3 - 9 &= 334 & 17^3 - 9 &= 4904 & 27^3 - 9 &= 19674 \\
8^3 - 9 &= 503 & 18^3 - 9 &= 5823 & 28^3 - 9 &= 21943 \\
9^3 - 9 &= 720 & 19^3 - 9 &= 6850 & 29^3 - 9 &= 24380 \\
10^3 - 9 &= 991 & 20^3 - 9 &= 7991 & 30^3 - 9 &= 26991 \\
 & & & & 31^3 - 9 &= 29782
\end{aligned}$$

Since none of the integers in the image are divisible by 31, i.e., are nonzero modulo 31, the polynomial has no roots in $\mathbb{Z}_{31}$ whereas, when $x = 4$, we have $4^3 - 9 = 5 \cdot 11 \equiv 0 \mod 11$, meaning it is reducible over $\mathbb{Z}_{11}$.

## Exercise 5

During the lecture, we constructed finite fields as factor rings of polynomial rings with coefficients in prime fields by irreducible polynomials.

In this exercise, we will try a more hands on approach to construct Galois fields.

Since the fields are determined by the number of elements, there should really be a unique way to construct them. To demonstrate what we mean, let us adjoin a single element $a$ to $\mathbb{Z}_2$ and try to define addition and multiplication on $\mathbb{Z}_2 \cup \{a\}$. Addition must be commutative and we have

$$\begin{aligned} 0+0&=0\\ 1+0&=1\\ 0+a&=a \end{aligned}$$

Also, by distributive property, we must have $a+a = a\cdot(1+1) = a\cdot 0 = 0$.

What about $a+1$? if we put $a+1=0$ it follows that $a=1$, which we do not want. Similarly, $a+1=1$ implies $a=0$ and $a+1=a$ implies $1=0$. Therefore, we are forced to adjoin one more element, namely, $a+1$, and consider a four element set $\{0,1,a,a+1\}$.

Addition is now settled, how about commutative multiplication? Multiplication by 0 and 1 is obvious. Other than that, we need only see what $a\cdot a$, $a\cdot(a+1)$ and $(a+1)\cdot(a+1)$ are.

We can't have $a^2=a$, for then $a(a-1)=0$ and we are supposing $a \notin \{0,1\}$; similarly, $a^2 \neq 0$. If $a^2=1$, then $(a-1)^2 = a^2-1 = 0$, which is also impossible. So, we must have $a^2 = 1+a$.

Next, using this, $a\cdot(a+1) = a^2+a = 1+a+a = 1$. Finally, using that $1+1=0$, $(a+1)(a+1) = a^2+1 = a$. Multiplication is completely determined. Check that index, we have a four element field. Go through a similar process by adjoining an element to $\mathbb{Z}_3$ to construct a nine element field.

The additive neutral element of $\{0,1,a,a+1\}$ is clearly 0. The additive inverses of 1, $a$ and $a+1$ are themselves. We also defined addition to be commutative, so $(\{0,1,a,a+1\},+)$ is indeed an Abelian group. For associativity of multiplication, we skip over the trivial verifications and observe that $(a\cdot a)\cdot(a+1) = (a+1)\cdot(a+1) = a = a\cdot 1 = a\cdot(a\cdot(a+1))$ and $(a\cdot(a+1))\cdot(a+1) = 1\cdot(a+1) = a+1 = a\cdot a = a\cdot((a+1)\cdot(a+1))$ (commutativity takes care of the rest). Clearly, 1 is the multiplicative neutral element in this case. The inverses of $a$ and $a+1$ are $a+1$ and $a$ respectively. This shows that $(\{1,a,a+1\},\cdot)$ is a group. Hence $\{0,1,a,a+1\}$ is indeed a field.

Let us adjoin an element $a \notin \{0, 1, 2\}$ to $\mathbb{Z}_3$ and try to construct a field with those elements included. Per usual, we can't have $a + 1 = 0$, $a + 1 = 1$ nor $a+1 = 2$ as they would imply $a = 2$, $a = 0$ and $a = 1$ respectively. Hence we consider $a+1$ as an element separately from $0, 1, 2, a$. Also, distributivity suggests that $a + (a + a) = 0$, i.e., $a + a$ is the additive inverse of $a$. Hence we can't have $a + a = 0$, $a + a = 1$ nor $a + a = 2$ as they would imply $a = 0$, $a = 2$ and $a = 1$. $a+a = a$ and $a+a = a+1$ are impossible as well for similar reasons. Hence $a + a$ shall be another element separate from $0, 1, 2, a, a + 1$. Now we determine $a + 2$. We can't have $a + 2 = 0$, $a + 2 = 1$, $a + 2 = 2$, $a + 2 = a$, , $a + 2 = a + 1$ nor $a + 2 = a + a$ as they would imply $a = 1$, $a = 2$, $a = 0$, $2 = 0$, $2 = 1$ and $a = 2$ respectively, meaning $a + 2$ is another element to be considered separately. We can't have $a + a + 1 = 0$, 1, 2, $a$, $a+1$ nor $a+2$ as they would imply $a = 2$, 0, 2, 2, 0 and 1 respectively. Since, clearly, $a + a + 1 = a + a$ is also impossible, $a + a + 1$ will be another distinct element. Finally, we can't have $a + a + 2 = 0$, 1, 2, $a$, $a + 1$ nor $a + 2$ as they would imply $a = 1$, 2, 0, 1, 1 and 0. Since, clearly, $a + a + 2 \neq a + a$ and $a + a + 2 \neq a + a + 1$, the element $a + a + 2$ is to be considered separate from others. Addition has been settled as one may complete its Cayley table and obtain

| $+$ | $0$ | $1$ | $2$ | $a$ | $a+1$ | $a+2$ | $2a$ | $2a+1$ | $2a+2$ |
|---|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $1$ | $2$ | $a$ | $a+1$ | $a+2$ | $2a$ | $2a+1$ | $2a+2$ |
| $1$ | $1$ | $2$ | $0$ | $a+1$ | $a+2$ | $a$ | $2a+1$ | $2a+2$ | $2a$ |
| $2$ | $2$ | $0$ | $1$ | $a+2$ | $a$ | $a+1$ | $2a+2$ | $2a$ | $2a+1$ |
| $a$ | $a$ | $a+1$ | $a+2$ | $2a$ | $2a+1$ | $2a+2$ | $0$ | $1$ | $2$ |
| $a+1$ | $a+1$ | $a+2$ | $a$ | $2a+1$ | $2a+2$ | $2a$ | $1$ | $2$ | $0$ |
| $a+2$ | $a+2$ | $a$ | $a+1$ | $2a+2$ | $2a$ | $2a+1$ | $2$ | $0$ | $1$ |
| $2a$ | $2a$ | $2a+1$ | $2a+2$ | $0$ | $1$ | $2$ | $a$ | $a+1$ | $a+2$ |
| $2a+1$ | $2a+1$ | $2a+2$ | $2a$ | $1$ | $2$ | $0$ | $a+1$ | $a+2$ | $a$ |
| $2a+2$ | $2a+2$ | $2a$ | $2a+1$ | $2$ | $0$ | $1$ | $a+2$ | $a$ | $a+1$ |

For multiplication, we can determine $a^2$ and then complete the rest of the Cayley table per usual. Due to the implications listed below, we have only three cases.

$$\begin{aligned}
a^2 = 0 &\implies a = 0\\
a^2 = 1 &\implies a = a - 1 + 1 = (a-1)^2(a-1)^{-1} + 1 = (a^2 - 2a + 1)(a-1)^{-1} + 1\\
&\quad = (2 - 2a)(a-1)^{-1} + 1 = (a-1)(a-1)^{-1} + 1 = 1 + 1 = 2\\
a^2 = 2 &\implies a =\\
a^2 = a &\implies a = a^2a^{-1} = aa^{-1} = 1\\
a^2 = a + 2 &\implies a = a - 2 + 2 = (a-2)^2(a-2)^{-1} + 2 = (a^2 - 4a + 4)(a-2)^{-1} + 2\\
&\quad = (a + 2 - a + 1)(a-2)^{-1} + 2 = 0 \cdot (a-2)^{-1} + 2 = 0 + 2 = 2\\
a^2 = 2a &\implies a = a^2a^{-1} = 2aa^{-1} = 2 \cdot 1 = 2\\
a^2 = 2a + 2 &\implies a = a - 2 + 2 = (a-2)^2(a-2)^{-1} + 2\\
&\quad = (a-2)(a-2)(a-2)^{-1} + 2 = (a-2)(a+1)(a-2)^{-1} + 2\\
&\quad = (a^2 + a - 2 = a^2 - 2a - 2)(a-2)^{-1} + 2 = (a^2 - (2a+2))(a-2)^{-1} + 2\\
&\quad = ((2a+2) - (2a+2))(a-2)^{-1} + 2 = 0 \cdot (a-2)^{-1} + 2 = 0 + 2 = 2
\end{aligned}$$

Namely, we have either $a^2 = 2$, $a^2 = a + 1$ or $a^2 = 2a + 1$. We may choose $a^2 = 2$. The Cayley table for multiplication thus becomes

| $\cdot$ | $0$ | $1$ | $2$ | $a$ | $a+1$ | $a+2$ | $2a$ | $2a+1$ | $2a+2$ |
|---|---|---|---|---|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $2$ | $a$ | $a+1$ | $a+2$ | $2a$ | $2a+1$ | $2a+2$ |
| $2$ | $0$ | $2$ | $1$ | $2a$ | $2a+2$ | $2a+1$ | $a$ | $a+2$ | $a+1$ |
| $a$ | $0$ | $a$ | $2a$ | $2$ | $a+2$ | $2a+2$ | $1$ | $a+1$ | $2a+1$ |
| $a+1$ | $0$ | $a+1$ | $2a+2$ | $a+2$ | $2a$ | $1$ | $2a+1$ | $2$ | $a$ |
| $a+2$ | $0$ | $a+2$ | $2a+1$ | $2a+2$ | $1$ | $a$ | $a+1$ | $2a$ | $2$ |
| $2a$ | $0$ | $2a$ | $a$ | $1$ | $2a+1$ | $a+1$ | $2$ | $2a+2$ | $a+2$ |
| $2a+1$ | $0$ | $2a+1$ | $a+2$ | $a+1$ | $2$ | $2a$ | $2a+2$ | $a$ | $1$ |
| $2a+2$ | $0$ | $2a+2$ | $a+1$ | $2a+1$ | $a$ | $2$ | $a+2$ | $1$ | $2a$ |

One may verify that this is indeed a field.

## 8.5 Algebra by Waerden, Chapter 2

### Exercise 2.1

A nonempty set $\mathfrak{G}$ of transformations of a set $\mathfrak{M}$ is a group if it contains (a) the product of any two transformations and (b) the inverse of each transformation.

Closure under multiplication is given and composition of transformations is associative in general, so $\mathfrak{G}$ is a semi-group. Let $a$ be a transformation of $\mathfrak{M}$ and $a^{-1}$ be its inverse. Since $a, a^{-1} \in \mathfrak{G}$, closure under multiplication suggests that $e = aa^{-1} \in \mathfrak{G}$, meaning $\mathfrak{G}$ has a neutral element. Since $\mathfrak{G}$ is also closed under inversion, it is a group.

### Exercise 2.2

The rotations of a plane about a fixed point $P$ form an Abelian group. If the reflections across the lines through $P$ are also included, a non-Abelian group is obtained. [The binary operation is assumed to be composition.]

A composition of two rotations is also a rotation, so closure holds. (Namely, the resulting rotation rotates about $\alpha+\beta$ angle where $\alpha$ and $\beta$ are the angles around which the given rotations rotate.) Composition is in general associative. The identity element is the rotation with the 0 angle. For a rotation $r$ with angle $\alpha$, there is the rotation $r^{-1}$ with angle $2\pi - \alpha$ (or simply $-\alpha$ if we allow negative angles) such that $r^{-1}r = I$ where $I$ is the neutral element. This proves that rotations form a group. For commutativity, we have that $r_1r_2$ is the rotation about $\alpha + \beta$ angle if $r_1$ and $r_2$ are the rotaions about $\alpha$ and $\beta$ angles respectively, but $\alpha + \beta = \beta + \alpha$, so $r_1r_2$ does the same effect as $r_2r_1$ to every point, hence rotations form an Abelian group.

Let reflections $r_1$ and $r_2$ about some lines $l_1$ and $l_2$ respecitvely be given. If $r_1 = r_2$, then their composition is the neutral element. Otherwise, their composition is reflection about double the angle between $l_1$ and $l_2$. Now let $r$ be the reflection about a line $l$ and $R$ be a rotation about $\alpha$ angles. The composition $rR$ is the reflection about the line $l$ rotated counterclockwise by $\frac{\alpha}{2}$ degrees wherees $Rr$ is the same but with $l$ rotated clockwise. This shows closure. Composition is associative in general. We have already shown the neutral element. Finally, the inverse of a reflection is itself. Thus reflections and rotations form a group. The group is non-Abelian since, for example, rotating the point $(1, 1)$ counterclockwise with 45 degrees and reflecting it around the $y$-axis yields $(0, \sqrt{2})$, where as reflecting it around the $y$-axis and then rotating counterclockwise with 45 degrees yields $(-\sqrt{2}, 0)$.

## Exercise 2.3

Prove that the elements $e$, $a$ with the composition law

$$ee = e \quad ea = a \quad ae = e \quad aa = e$$

form a (Abelian group).

Let $S = \{e, a\}$. $S$ is closed under the defined composition since $ee = e \in S$, $ea = a \in S$, $ae = a \in S$ and $aa = e \in S$. Associativity also holds as shown below.

$$e(ee) = ee = (ee)e$$

$$e(ea) = ea = (ee)a$$

$$e(ae) = ea = a = ae = (ea)e$$

$$e(aa) = ee = e = aa = (ea)a$$

$$a(ee) = ae = (ae)e$$

$$a(ea) = aa = (ae)a$$

$$a(ae) = aa = e = ee = (aa)e$$

$$a(aa) = ae = a = ea = (aa)a$$

Finally, the inverse of $e$ is $e$ since $ee = ee = e$ and the inverse of $a$ is $a$ since $aa = aa = a$. For commutativity, we have $ae = a = ea$. (Other cases are trivial.) Hence $(S, \circ)$ is an Abelian group where $\cdot$ is the defined composition.

## Exercise 2.4

Form the group table for the group of permutations of three numbers.

Let the permutations of $\{1, 2, 3\}$ be defined as below.

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

We thus have the following table for the group $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$.

| $\circ$ | $\sigma_0$ | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ | $\sigma_4$ | $\sigma_5$ |
|---|---|---|---|---|---|---|
| $\sigma_0$ | $\sigma_0$ | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ | $\sigma_4$ | $\sigma_5$ |
| $\sigma_1$ | $\sigma_1$ | $\sigma_0$ | $\sigma_4$ | $\sigma_5$ | $\sigma_2$ | $\sigma_3$ |
| $\sigma_2$ | $\sigma_2$ | $\sigma_3$ | $\sigma_0$ | $\sigma_1$ | $\sigma_5$ | $\sigma_4$ |
| $\sigma_3$ | $\sigma_3$ | $\sigma_2$ | $\sigma_5$ | $\sigma_4$ | $\sigma_0$ | $\sigma_1$ |
| $\sigma_4$ | $\sigma_4$ | $\sigma_5$ | $\sigma_1$ | $\sigma_0$ | $\sigma_3$ | $\sigma_2$ |
| $\sigma_5$ | $\sigma_5$ | $\sigma_4$ | $\sigma_3$ | $\sigma_2$ | $\sigma_1$ | $\sigma_0$ |

## Exercise 2.5

Prove for Abelian groups that

$$\prod_{v=1}^{n} \prod_{\mu=1}^{m} a_{\mu v} = \prod_{\mu=1}^{m} \prod_{v=1}^{n} v_{\mu v}$$

We first show that $\left(\prod\limits_{k=1}^{m} a_k\right)\left(\prod\limits_{k=1}^{m} b_k\right) = \prod\limits_{k=1}^{m} a_k b_k$ by induction on $m$. For base case, $m = 1$, so the equation becomes

$$\left(\prod_{k=1}^{m} a_k\right)\left(\prod_{k=1}^{m} b_k\right) = \left(\prod_{k=1}^{1} a_k\right)\left(\prod_{k=1}^{1} b_k\right) = a_1 b_1 = \prod_{k=1}^{1} a_k b_k = \prod_{k=1}^{m} a_k b_k$$

Which is indeed true. For inductive step, assume the equality to hold for some natural $m$. We then have

$$\left(\prod_{k=1}^{m+1} a_k\right)\left(\prod_{k=1}^{m+1} b_k\right) = \left(\prod_{k=1}^{m} a_k\right) a_{m+1} \left(\prod_{k=1}^{m} b_k\right) b_{k+1} = \left(\prod_{k=1}^{m} a_k\right)\left(\prod_{k=1}^{m} b_k\right) a_{m+1} b_{m+1} =$$

$$= \left(\prod_{k=1}^{m} a_k b_k\right) a_{m+1} b_{m+1} = \prod_{k=1}^{m+1} a_k b_k$$

Now, we shall induct on $n$. For $n = 1$, the equation becomes

$$\prod_{v=1}^{n}\prod_{\mu=1}^{m} a_{\mu v} = \prod_{v=1}^{1}\prod_{\mu=1}^{m} a_{\mu v} = \prod_{\mu=1}^{m} a_{\mu v} = \prod_{\mu=1}^{m}\prod_{v=1}^{1} a_{\mu v} = \prod_{\mu=1}^{m}\prod_{v=1}^{n} a_{\mu v}$$

Which is indeed true. For inductive step, assume the equality to hold for some natural $n$. We then have

$$\prod_{v=1}^{n+1}\prod_{\mu=1}^{m} a_{\mu v} = \left(\prod_{v=1}^{n}\prod_{\mu=1}^{m} a_{\mu v}\right)\prod_{\mu=1}^{m} a_{\mu(n+1)} = \left(\prod_{\mu=1}^{m}\prod_{v=1}^{n} a_{\mu v}\right)\prod_{\mu=1}^{m} a_{\mu(n+1)} =$$

$$= \prod_{\mu=1}^{m}\left(\left(\prod_{v=1}^{n} a_{\mu v}\right) a_{\mu(n+1)}\right) = \prod_{\mu=1}^{m}\prod_{v=1}^{n+1} a_{\mu v}$$

Where the second from last equality follows from our recent result.

## Exercise 2.6

Similarly, prove

$$\prod_{v=1}^{n}\prod_{\mu=1}^{v} a_{\mu v} = \prod_{\mu=1}^{n}\prod_{v=\mu}^{n} a_{\mu v}$$

We shall induct on $n$. For base case, $n = 1$, so the equation becomes

$$\prod_{v=1}^{n}\prod_{\mu=1}^{v} a_{\mu v} = \prod_{v=1}^{1}\prod_{\mu=1}^{v} a_{\mu v} = \prod_{\mu=1}^{1} a_{\mu 1} = a_{11} = \prod_{v=1}^{1} a_{1v} = \prod_{\mu=1}^{1}\prod_{v=\mu}^{1} a_{\mu v} = \prod_{\mu=1}^{n}\prod_{v=\mu}^{n} a_{\mu v}$$

Which is indeed true. For inductive step, assume the equality to hold for some natural $n$. We then have

$$\prod_{v=1}^{n+1}\prod_{\mu=1}^{v} a_{\mu v} = \left(\prod_{v=1}^{n}\prod_{\mu=1}^{v} a_{\mu v}\right)\prod_{\mu=1}^{n+1} a_{\mu(n+1)} = \left(\prod_{\mu=1}^{n}\prod_{v=\mu}^{n} a_{\mu v}\right)\prod_{\mu=1}^{n+1} a_{\mu(n+1)} =$$

$$= \left(\prod_{\mu=1}^{n}\prod_{v=\mu}^{n} a_{\mu v}\right)\left(\left(\prod_{\mu=1}^{n} a_{\mu(n+1)}\right) a_{(n+1)(n+1)}\right) =$$

$$= \left(\left(\prod_{\mu=1}^{n}\prod_{v=\mu}^{n} a_{\mu v}\right)\left(\prod_{\mu=1}^{n} a_{\mu(n+1)}\right)\right) a_{(n+1)(n+1)} =$$

$$= \left(\prod_{\mu=1}^{n}\left(\prod_{v=\mu}^{n} a_{\mu v}\right) a_{\mu(n+1)}\right) a_{(n+1)(n+1)} =$$

$$= \left(\prod_{\mu=1}^{n}\prod_{v=\mu}^{n+1} a_{\mu v}\right) a_{(n+1)(n+1)} =$$

$$= \left(\prod_{\mu=1}^{n}\prod_{v=\mu}^{n+1} a_{\mu v}\right)\prod_{v=n+1}^{n+1} a_{(n+1)v} = \prod_{\mu=1}^{n+1}\prod_{v=\mu}^{n+1} a_{\mu v}$$

## Exercise 2.7

The order of the symmetric $\mathfrak{S}_n$ is $n! = \prod_{1}^{n} v$.

We shall induct on $n$. For base case, $n = 1$ and indeed there is only one permutation for a singleton set (namely, the identity function). For inductive step, assume that the set $\{1, \ldots, n\}$ has $n!$ permutations and consider the mapping $\varphi : \mathfrak{S}_{n+1} \to \mathfrak{S}_n \times \{1, \ldots, n+1\}$ given by $\varphi : f \mapsto$

$(f\big|_{\{1,\ldots,n+1\}\setminus\{f^{-1}(n+1)\}}, f^{-1}(n+1))$. (Note that the mentioned restricted function $f\big|_{\{1,\ldots,n+1\}\setminus\{f^{-1}(n+1)\}}$ is also a permutation of $n$ element.) $\varphi$ is a bijection since its inverse exists, namely, $\varphi^{-1} : \mathfrak{S}_n \times \{1,\ldots,n+1\} \to \mathfrak{S}_{n+1}$ is given by $(g,k) \mapsto g'$ where $g' : \{1,\ldots,n+1\} \to \{1,\ldots,n+1\}$ is defined below.

$$g'(i) = \begin{cases} k, & i = n+1 \\ g(i), & \text{otherwise} \end{cases}$$

Hence we have $|\mathfrak{S}_{n+1}| = |\mathfrak{S}_n||\{1,\ldots,n+1\}|$ and, by inductive hypothesis, $|\mathfrak{S}_{n+1}| = n! \cdot (n+1) = (n+1)!$.

## Exercise 2.8

There are cyclic permutation groups of any given order.

Let $n$ be the given natural number a group of whose order is desired. Then the residue classes of integers modulo $n$ form an additive group addition defined with $n$ elements. Alternatively one could consider the subspace of $\mathfrak{S}_n$ generated by the cycle $(n\ (n-1)\ \ldots\ 2\ 1)$ since its order is equal to $n$. (Later we will see why these are almost the same groups.)

## Exercise 2.9

Prove by induction on $n$ that the $n-1$ transpositions $(1\ 2), (1\ 3), \ldots, (1\ n)$ for $n > 1$ generate the symmetric group $\mathfrak{S}_n$.

For $n = 2$, the group generated by $(1\ 2)$ has elements $\{(1), (1\ 2)\}$ since the order of $(1\ 2)$ is 2. (It is clearly not the neutral element and $(1\ 2)^2 = (1\ 2)(1\ 2) = (1)$.) The symmetric group $\mathfrak{S}_2$ consists of only those elements as well.

For inductive hypothesis, assume that the transpositions $(1\ 2), (1\ 3), \ldots, (1\ n)$ generate the symmetric group $\mathfrak{S}_n$ for some natural $n > 1$. Consider a permutation $\pi$ from the group $\mathfrak{S}_{n+1}$. If it fixes $n+1$, then, by inductive hypothesis, it can be expressed as a product with $(1\ 2), (1\ 3), \ldots (1\ n)$ and their inverses. If $n+1$ is not fixed by the permutation, say, some $k \in \{1,\dots,n\}$ gets mapped to $n+1$, then $(k\ n+1)\pi$ is a permutation of $\{1,\dots,n\}$, meaning it is in the group generated by $(1\ 2),(1\ 3),\dots,(1\ n)$. Clearly, we also have $\pi = (k\ n+1)(k\ n+1)\pi$, meaning we simply need to show that $(k, n+1)$ is in the group generated by $(1,2),(1,3),\dots,(1,n+1)$ and closure finishes the proof. We indeed have $(k\ n+1) = (1\ k)(1\ n+1)(1\ k)$.

## Exercise 2.10

Prove, as in 2.9, that for $n > 2$ the $n-2$ cyclic permutations on three digits $(1\ 2\ 3),(1\ 2\ 4),\dots,(1\ 2\ n)$ generate the alternating group $\mathfrak{A}_n$.

For $n = 3$, the group generated by $(1\ 2\ 3)$ has elements $\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$. The identity function is trivially even, the cycle $(1\ 2\ 3)$ is also even since $(1-2)(1-3)(2-3) = (2-3)(2-1)(3-1)$, similarly, $(1\ 2\ 3)$ is also even since $(1-2)(1-3)(2-3) = (3-1)(3-2)(1-2)$. There are no other even permutations since there must be $\frac{3!}{2} = 3$ of them and we have found that many, so the base case holds.

For inductive hypothesis, assume that any even permutation of $\{1,\dots,n\}$ is an element of the group generated by $(1\ 2\ 3),(1\ 2\ 4),\dots,(1\ 2\ n)$ for some natural $n > 2$. Consider an even permutation $\pi$ of elements $\{1,\dots,n+1\}$. If $\pi$ fixes $n+1$, then we are done as it is then an even permutation of the elements $\{1,\dots,n\}$ and, by inductive hypothesis, is in the group generated by the permutations $(1\ 2\ 3),(1\ 2\ 4),\dots,(1\ 2\ n)$ and thus should also be in the group generated by $(1\ 2\ 3),\dots,(1\ 2\ n{+}1)$. If, however, $n{+}1$ is not fixed by $\pi$, then let $k \in \{1,\dots,n\}$ be the element with $\pi(k) = n{+}1$. We clearly have $\pi = (1\ k\ n{+}1)^2(1\ k\ n{+}1)\pi$. This shows that $(1\ k\ n{+}1)$ is an even permutation (if it were odd, we would have a contradiction due to the latter equation.), and thus $(1\ k\ n{+}1)\pi$ is an even permutation of $\{1,\dots,n\}$ (note that $n{+}1$ is its fixed point.), meaning it is in the group generated by $(1\ 2\ 3),\dots,(1\ 2\ n)$ and thus also in the group generated by $(1\ 2\ 3),\dots,(1\ 2\ n+1)$. Our claim is that the same holds for $(1\ k\ n+1)^2$ and closure will finish the proof. $(1\ k\ n+1)^2 = (1\ n+1\ k) = (1\ 2\ k)(1\ 2\ k)(1\ 2\ n+1)(1\ 2\ k)$.

## Exercise 2.11

Find the right and left cosets for the subgroups of the $\mathfrak{S}_3$ group. Which of these subgroups are normal divisors?

Recall that the subgroups of $\mathfrak{S}_3$ of are $\{(1)\}$, $\{(1), (1\ 2)\}$, $\{(1), (1\ 3)\}$, $\{(1), (2\ 3)\}$, $\{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ and $\mathfrak{S}_3$ itself. Name the first ones $\mathfrak{g}_0$, $\mathfrak{g}_1$, $\mathfrak{g}_2$, $\mathfrak{g}_3$ and let $\sigma_i$ be defined for each $i \in \{0, \dots, 5\}$ as in Exercise 2.4 of this section (the second from last subgroup already has a name). Obviously, the left and right cosets of $\mathfrak{g}_0$ are the singleton complexes and the only left and right coset of $\mathfrak{G}_3$ is itself. Both of $\mathfrak{g}_0$ and $\mathfrak{G}_3$ are normal subgroups.

The left cosets of $\mathfrak{g}_1$ besides itself are

$$\begin{aligned} \sigma_1\mathfrak{g}_1 = \sigma_4\mathfrak{g}_1 &= \{(2\ 3), (1\ 3\ 2)\} \\ \sigma_3\mathfrak{g}_1 = \sigma_5\mathfrak{g}_1 &= \{(1\ 3), (1\ 2\ 3)\} \end{aligned}$$

The right cosets of $\mathfrak{g}_1$ besides itself are

$$\begin{aligned} \mathfrak{g}_1\sigma_1 = \mathfrak{g}_1\sigma_3 &= \{(2\ 3), (1\ 2\ 3)\} \\ \mathfrak{g}_1\sigma_4 = \mathfrak{g}_1\sigma_5 &= \{(1\ 3), (1\ 3\ 2)\} \end{aligned}$$

The left cosets of $\mathfrak{g}_2$ besides itself are

$$\begin{aligned} \sigma_1\mathfrak{g}_2 = \sigma_3\mathfrak{g}_2 &= \{(2\ 3), (1\ 2\ 3)\} \\ \sigma_2\mathfrak{g}_2 = \sigma_4\mathfrak{g}_2 &= \{(1\ 2), (1\ 3\ 2)\} \end{aligned}$$

The right cosets of $\mathfrak{g}_2$ besides itself are

$$\begin{aligned} \mathfrak{g}_2\sigma_1 = \mathfrak{g}_2\sigma_4 &= \{(2\ 3), (1\ 3\ 2)\} \\ \mathfrak{g}_2\sigma_2 = \mathfrak{g}_2\sigma_3 &= \{(1\ 2), (1\ 2\ 3)\} \end{aligned}$$

The left cosets of $\mathfrak{g}_3$ besides itself are

$$\begin{aligned} \sigma_2\mathfrak{g}_3 = \sigma_3\mathfrak{g}_3 &= \{(1\ 2), (1\ 2\ 3)\} \\ \sigma_4\mathfrak{g}_3 = \sigma_5\mathfrak{g}_3 &= \{(1\ 3), (1\ 3\ 2)\} \end{aligned}$$

The right cosets of $\mathfrak{g}_3$ besides itself are

$$\mathfrak{g}_3\sigma_2 = \mathfrak{g}_3\sigma_4 = \{(1\ 2), (1\ 3\ 2)\}$$
$$\mathfrak{g}_3\sigma_3 = \mathfrak{g}_3\sigma_5 = \{(1\ 3), (1\ 2\ 3)\}$$

The only left and right coset of $\mathfrak{A}_3$ besides itself is $\{(1\ 2), (1\ 3), (2\ 3)\}$.

Clearly, none of $\mathfrak{g}_1$, $\mathfrak{g}_2$ or $\mathfrak{g}_3$ are normal subgroups since $\sigma_1\mathfrak{g}_1 \neq \mathfrak{g}_1\sigma_1$, $\sigma_1\mathfrak{g}_2 \neq \mathfrak{g}_2\sigma_1$ and $\sigma_2\mathfrak{g}_3 \neq \mathfrak{g}_3\sigma_2$. However, $\mathfrak{A}_3$ is normal. (One could verify that without using the definition but rather the theorem mentioned in Exercise 2.13 of this section since its $\mathfrak{A}_3$ has 3 elements from $\mathfrak{S}_3$ which has 6.)

## Exercise 2.12

Show that for any subgroup the inverses of the elements of a left coset form a right coset. Conclude from this that the index may also be determined as the number of the right cosets.

Let $\mathfrak{g}$ be a subgroup of $\mathfrak{G}$ and $a \in$ so that $a\mathfrak{g}$ is a left coset with some $a \in \mathfrak{G}$. Let $\mathfrak{h}$ denote the set of inverses of the elements from $a\mathfrak{g}$. Let $x \in \mathfrak{G}$ so that $ax \in a\mathfrak{G}$ and consider its inverse. We have $(ax)^{-1} = x^{-1}a^{-1}$, but $x^{-1} \in \mathfrak{g}$, so we have $(ax)^{-1} \in \mathfrak{g}a^{-1}$. This shows that $\mathfrak{h} \subseteq \mathfrak{g}a^{-1}$. Conversely, we have $ya^{-1} \in \mathfrak{g}a^{-1}$ with $y \in \mathfrak{g}$ and $ya^{-1}$ is the inverse of $ay^{-1}$, but $y^{-1} \in \mathfrak{g}$, meaning $ay^{-1} \in a\mathfrak{g}$. This shows that $\mathfrak{g}a^{-1} \subseteq \mathfrak{h}$. Finally, $\mathfrak{h} = \mathfrak{g}a^{-1}$.

## Exercise 2.13

Show that any subgroup of index 2 is a normal divisor. Example: the alternating group of the symmetric group of $n$ letters.

Let $\mathfrak{g}$ be a subgroup with index 2 of some group $\mathfrak{G}$. Since $\mathfrak{g}$ has index 2, its left cosets are itself and $a\mathfrak{g}$ for some $a \in \mathfrak{G} \setminus \mathfrak{g}$, this means that $a\mathfrak{g} = \mathfrak{G} \setminus \mathfrak{g}$. Similarly, the only right cosets of $\mathfrak{g}$ are itself and $\mathfrak{g}a$, meaning $\mathfrak{g}a = \mathfrak{G} \setminus \mathfrak{g}$. Finally, $a\mathfrak{g} = \mathfrak{g}a$, meaning $\mathfrak{g}$ is normal.

The alternating group of the symmetric group of $n$ letters is hence normal as its index is 2. (the left cosets are itself and the set of odd permutations.)

## Exercise 2.14

A subgroup of an Abelian group is always a normal divisor.

Let $\mathfrak{G}$ be an Abelian group and $\mathfrak{g}$ be its subgroup. Let $a \in \mathfrak{G}$, so that $a\mathfrak{g}$ is a left coset and for all $x \in a\mathfrak{g}$ we have $x = ag$ for some $g \in \mathfrak{g}$. Since $ag = ga$, we have $x = ga$, but $ga \in \mathfrak{g}a$. This shows that $a\mathfrak{g} \subseteq \mathfrak{g}a$. Conversely, let $y \in \mathfrak{g}a$, meaning $y = g'a$ for some $g' \in \mathfrak{g}$. Since $g'a = ag'$, we have $y = ag'$, but $ag' \in a\mathfrak{g}$. This shows that $a\mathfrak{g} = \mathfrak{g}a$ for all $a \in \mathfrak{G}$, i.e., $\mathfrak{g}$ is normal.

## Exercise 2.15

If $\mathfrak{G}$ is a cyclic group generated by $a$, and $\mathfrak{g}$ a subgroup distinct from $\mathfrak{G}$ and generated by $a^m$ with the smallest $m$ (see Section 2.2), then $1, a, a^2, \ldots, a^{m-1}$ are representatives of the cosets, and $m$ is the index of $\mathfrak{g}$ in $\mathfrak{G}$.

Let $i, j \in \{0, \ldots, m-1\}$ be distinct with $i > j$, our claim is that the left cosets $a^i\mathfrak{g}$ and $a^j\mathfrak{g}$ are also distinct. By contradiction, assume that there exist $g, g' \in \mathfrak{g}$ with $a^i g = a^j g'$, then $a^{i-j} = g'g^{-1} \in \mathfrak{g}$, but $\mathfrak{g}$ is generated by $a^m$, meaning $a^{i-j} = a^{mk}$ for some integer $k \in \{0, \ldots, m-1\}$ and $a^{i-j-mk} = 1$, so $i - j - mk = mk'$ and $i - j = m(k + k')$ for some $k' \in \{0, \ldots, m-1\}$. The only multiply of $m$ that $i - j$ can be equal to is 0, but that would imply that $i = j$, which is a contradiction. This shows that $1, a, a^2, \ldots, a^{m-1}$ are repersentatives of distinct left cosets. Furthermore, let $i \geq m - 1$ and consider the left coset $a^i\mathfrak{g}$. We have $i = mq + r$ for some integer $q$ and $r$ with $0 \leq r < m$, meaning for all $x \in a^i\mathfrak{g}$ we have $x = a^i a^{mk}$ for some integer $k$ and $x = a^{mq+r}a^{mk} = a^r a^{m(k+q)} \in a^r\mathfrak{g}$, immediately showing that $a^i\mathfrak{g} = a^r\mathfrak{g}$ for some $r \in \{0, \ldots, m-1\}$. This proves that there are no other left cosets, i.e., $1, a, a^2, \ldots, a^{m-1}$ are representatives of all distinct left cosets. By counting we also get that the index of $\mathfrak{g}$ in $\mathfrak{G}$ is $m$. Since $\mathfrak{G}$ is cyclic, it is also Abelian, meaning the same holds for the right cosets.

## Exercise 2.16

If the product of any two left cosets of $\mathfrak{g}$ in $\mathfrak{G}$ is itself a left coset, $\mathfrak{g}$ is a normal subgroup in $\mathfrak{G}$.

Let $a\mathfrak{g}$ and $b\mathfrak{g}$ be the left cosets so that their product is also a left coset of $\mathfrak{g}$, i.e., let $a\mathfrak{g}b\mathfrak{g} = c\mathfrak{g}$ for any $a, b, c \in \mathfrak{G}$. Since $ab \in a\mathfrak{g}b\mathfrak{g}$, we have $ab \in c\mathfrak{g}$ and $c\mathfrak{g} = ab\mathfrak{g}$. The equation $a\mathfrak{g}b\mathfrak{g} = ab\mathfrak{g}$ suggests that for all $\mathfrak{g}_1, \mathfrak{g}_2 \in \mathfrak{g}$ there exists $\mathfrak{g}_3 \in \mathfrak{g}$ with $ag_1bg_2 = abg_3$, meaning $g_1b = bg_3g_2^{-1}$. But $bg_3g_2^{-1} \in b\mathfrak{g}$, so $g_1b \in b\mathfrak{g}$ for all $g_1 \in \mathfrak{g}$ and $\mathfrak{g}b \subseteq b\mathfrak{g}$. The latter also implies that for all $b \in \mathfrak{G}$ and $g_1 \in \mathfrak{g}$ there exists $g_2 \in \mathfrak{g}$ with $g_1b^{-1} = b^{-1}g_2$, i.e., $bg_1 = g_2b$. But $g_2b \in \mathfrak{g}b$, so $bg_1 \in \mathfrak{g}b$ for all $b \in \mathfrak{G}$ and $g_1 \in \mathfrak{g}$, meaning $b\mathfrak{g} \subseteq \mathfrak{g}b$. Finally, $b\mathfrak{g} = \mathfrak{g}b$ for all $b$, so $\mathfrak{g}$ is normal.

## Exercise 2.17

Abelian groups have no inner automorphisms except the identity automorphism.

Let $\mathfrak{G}$ be an Abelian group and $\varphi : \mathfrak{G} \to \mathfrak{G}$ be an inner automorphism, i.e., $\varphi(x) = axa^{-1}$ with a fixed $a \in \mathfrak{G}$. But, since $\mathfrak{G}$ is Abelian, we have $axa^{-1} = aa^{-1}x = x$, so $\varphi(x) = x$ for all $x \in \mathfrak{G}$, i.e., $\varphi$ is the identity automorphism (and hence there is no other inner automorphism).

## Exercise 2.18

In permutation groups the transform $aba^{-1}$ of an element $b$ can be obtained by expressing $b$ as a product of cycles (Section 2.2), and by performing the permutation $a$ on the digit of these cycles. Give the proof. Use this proposition to compute $aba^{-1}$ for

$$b = (1\ 2)(3\ 4\ 5)$$

$$a = (2\ 3\ 4\ 5)$$

Let $a, b \in \mathfrak{S}_n$ be permutations, $\pi_1 \cdots \pi_k$ be the disjoint cycle decomposition of $b$. Let $\pi_i'$ also denote $\pi$ but with the permutation $a$ on its digits applied to it for all $i \in \{1, \ldots, k\}$. Our claim is that $ab = a\pi_1 \cdots \pi_k$ and $b' = \pi_1' \cdots \pi_k' a$ are the same permutations. Let $i \in \{1, \ldots, n\}$, $a(i) = r$, $b(i) = m$. The latter implies that there exists a cycle $\pi_l$ in the decomposition of $b$ with $\pi_l(m)$ whereas every other cycle fixes $i$. We also have $\pi_l'(r) = a(m)$ whereas every other cycle in $b'$ fixes $r$. Finally, we have

$$ab(i) = a(m)$$

$$b'a(i) = b'(r) = a(m)$$

Hence $ab = b'a$ and $aba^{-1} = b'$.

The proposition suggests that $(2\ 3\ 4\ 5)(1\ 2)(3\ 4\ 5)(2\ 3\ 4\ 5)^{-1}$ is equal to $(1\ 3)(4\ 5\ 2)$. One may verify that to indeed be true.

## Exercise 2.19

Prove that the symmetric group $\mathfrak{S}_3$ has no outer, but six inner automorphisms.

Let $\varphi : \mathfrak{S}_3 \to \mathfrak{S}_3$ be an automorphism. By consider cases we will show that $\varphi$ is one of the six inner automorphisms (which we will discover along). Firstly, since the only permutations of order 3 are $(1\ 2\ 3)$ and $(1\ 3\ 2)$, we have two cases: $\varphi(1\ 2\ 3) = (1\ 2\ 3)$ or $\varphi(1\ 2\ 3) = (1\ 3\ 2)$ (recall that isomorphisms preserve order).

In the first case, clearly, we also have $\varphi(1\ 3\ 2) = (1\ 3\ 2)$. We have 3 further subcases to consider. If $\varphi(1\ 2) = (1\ 2)$, then $\varphi(1\ 3) = \varphi((1\ 2)(1\ 3\ 2)) = \varphi(1\ 2)\varphi(1\ 3\ 2) = (1\ 2)(1\ 3\ 2) = (1\ 3)$ and, similarly, $\varphi(2\ 3) = (2\ 3)$ is forced, which yields the trivial automorphism. If $\varphi(1\ 2) = (1\ 3)$, then $\varphi(1\ 3) = \varphi((1\ 2)(1\ 3\ 2)) = \varphi(1\ 2)\varphi(1\ 3\ 2) = (1\ 3)(1\ 3\ 2) = (2\ 3)$ and $\varphi(2\ 3) = (1\ 2)$ is forced. As shown below, this is indeed an inner automorphism, namely, conjugation by $(1\ 3\ 2)$.

$$\begin{aligned}
\varphi(1) &= (1\ 3\ 2)(1)(1\ 3\ 2)^{-1} = (1)\\
\varphi(1\ 2) &= (1\ 3\ 2)(1\ 2)(1\ 3\ 2)^{-1} = (1\ 3)\\
\varphi(1\ 3) &= (1\ 3\ 2)(1\ 3)(1\ 3\ 2)^{-1} = (2\ 3)\\
\varphi(2\ 3) &= (1\ 3\ 2)(2\ 3)(1\ 3\ 2)^{-1} = (1\ 2)\\
\varphi(1\ 2\ 3) &= (1\ 3\ 2)(1\ 2\ 3)(1\ 3\ 2)^{-1} = (1\ 2\ 3)\\
\varphi(1\ 3\ 2) &= (1\ 3\ 2)(1\ 3\ 2)(1\ 3\ 2)^{-1} = (1\ 3\ 2)
\end{aligned}$$

If $\varphi(1\ 2) = (2\ 3)$, then $\varphi(2\ 3) = \varphi((1\ 2)(1\ 2\ 3)) = \varphi(1\ 2)\varphi(1\ 2\ 3) = (2\ 3)(1\ 2\ 3) = (1\ 3)$ and $\varphi(1\ 3) = (1\ 2)$ is forced. As shown below, this is indeed an inner automorphism, namely, conjugation by $(1\ 2\ 3)$.

$$\begin{aligned}
\varphi(1) &= (1\ 2\ 3)(1)(1\ 2\ 3)^{-1} = (1)\\
\varphi(1\ 2) &= (1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1} = (2\ 3)\\
\varphi(1\ 3) &= (1\ 2\ 3)(1\ 3)(1\ 2\ 3)^{-1} = (1\ 2)\\
\varphi(2\ 3) &= (1\ 2\ 3)(2\ 3)(1\ 2\ 3)^{-1} = (1\ 3)\\
\varphi(1\ 2\ 3) &= (1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3)^{-1} = (1\ 2\ 3)\\
\varphi(1\ 3\ 2) &= (1\ 2\ 3)(1\ 3\ 2)(1\ 2\ 3)^{-1} = (1\ 3\ 2)
\end{aligned}$$

In the second case, clearly, we have $\varphi(1\ 3\ 2) = (1\ 2\ 3)$. Let us consider the same 3 subcases as previously. If $\varphi(1\ 2) = (1\ 2)$, then $\varphi(1\ 3) = \varphi((1\ 2)(1\ 3\ 2)) = \varphi(1\ 2)\varphi(1\ 3\ 2) = (1\ 2)(1\ 2\ 3) = (2\ 3)$ and $\varphi(2\ 3) = (1\ 3)$ is forced. As shown below, this is indeed an inner automorphism, namely, conjugation by $(1\ 2)$.

$$\begin{aligned}
\varphi(1) &= (1\ 2)(1)(1\ 2)^{-1} = (1)\\
\varphi(1\ 2) &= (1\ 2)(1\ 2)(1\ 2)^{-1} = (1\ 2)\\
\varphi(1\ 3) &= (1\ 2)(1\ 3)(1\ 2)^{-1} = (2\ 3)\\
\varphi(2\ 3) &= (1\ 2)(2\ 3)(1\ 2)^{-1} = (1\ 3)\\
\varphi(1\ 2\ 3) &= (1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (1\ 3\ 2)\\
\varphi(1\ 3\ 2) &= (1\ 2)(1\ 3\ 2)(1\ 2)^{-1} = (1\ 2\ 3)
\end{aligned}$$

If $\varphi(1\ 2) = (1\ 3)$, then $\varphi(1\ 3) = \varphi((1\ 2)(1\ 3\ 2)) = \varphi(1\ 2)\varphi(1\ 3\ 2) = (1\ 3)(1\ 2\ 3) = (1\ 2)$ and $\varphi(2\ 3) = (2\ 3)$ is forced. As shown below, this is indeed an inner automorphism, namely, conjugation by $(2\ 3)$.

$$\begin{aligned}
\varphi(1) &= (2\ 3)(1)(2\ 3)^{-1} = (1)\\
\varphi(1\ 2) &= (2\ 3)(1\ 2)(2\ 3)^{-1} = (1\ 3)\\
\varphi(1\ 3) &= (2\ 3)(1\ 3)(2\ 3)^{-1} = (1\ 2)\\
\varphi(2\ 3) &= (2\ 3)(2\ 3)(2\ 3)^{-1} = (2\ 3)\\
\varphi(1\ 2\ 3) &= (2\ 3)(1\ 2\ 3)(2\ 3)^{-1} = (1\ 3\ 2)\\
\varphi(1\ 3\ 2) &= (2\ 3)(1\ 3\ 2)(2\ 3)^{-1} = (1\ 2\ 3)
\end{aligned}$$

If $\varphi(1\ 2) = (2\ 3)$, then $\varphi(2\ 3) = \varphi((1\ 2)(1\ 2\ 3)) = \varphi(1\ 2)\varphi(1\ 2\ 3) = (2\ 3)(1\ 3\ 2) =$ $(1\ 2)$ and $\varphi(1\ 3) = (1\ 3)$ is forced. As shown below, this is indeed an inner automorphism, namely, conjugation by $(1\ 3)$.

$$\begin{aligned}
\varphi(1) &= (1\ 3)(1)(1\ 3)^{-1} = (1)\\
\varphi(1\ 2) &= (1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3)\\
\varphi(1\ 3) &= (1\ 3)(1\ 3)(1\ 3)^{-1} = (1\ 3)\\
\varphi(2\ 3) &= (1\ 3)(2\ 3)(1\ 3)^{-1} = (1\ 2)\\
\varphi(1\ 2\ 3) &= (1\ 3)(1)(1\ 3)^{-1} = (1\ 3\ 2)\\
\varphi(1\ 3\ 2) &= (1\ 3)(1)(1\ 3)^{-1} = (1\ 2\ 3)
\end{aligned}$$

Finally, this proves that $\mathfrak{S}_3$ has exactly 6 automorphisms, all of them inner automorphisms.

## Exercise 2.20

The symmetric group $\mathfrak{S}_4$ has, besides itself and the identity group, only the following normal divisors:

a. The alternating group $\mathfrak{A}_4$.

b. Klein's four-group $\mathfrak{B}_4$, consisting of the permutations

$$(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3).$$

The latter group is Abelian.

Clearly, $\mathfrak{B}_4$ is closed under inversion, so we simply need to verify its closure under multiplication.

$$(1\ 2)(3\ 4)(1\ 3)(2\ 4) = (1\ 3)(2\ 4)(1\ 2)(3\ 4) = (1\ 4)(2\ 3)$$

$$(1\ 2)(3\ 4)(1\ 4)(2\ 3) = (1\ 4)(2\ 3)(1\ 2)(3\ 4) = (1\ 3)(2\ 4)$$

$$(1\ 3)(2\ 4)(1\ 4)(2\ 3) = (1\ 4)(2\ 3)(1\ 3)(2\ 4) = (1\ 2)(3\ 4)$$

This shows that $\mathfrak{B}_4$ is a group and, clearly, also an Abelian group.

Now, let $\mathfrak{g}$ be a non-trivial proper subgroup of $\mathfrak{S}_4$. By considering cases, we shall show that $\mathfrak{g}$ is either $\mathfrak{A}_4$ or $\mathfrak{B}_4$. Assume that $\mathfrak{g}$ has a permutation that permutes only 2 elements, i.e., a transposition. Since we want $\mathfrak{g}$ to be closed under conjugation and since every other transposition is obtainable via conjugation (see Exercise 2.18 of this section), $\mathfrak{g}$ must contain every transposition. But, since every permutation can be written as a product of transpositions (see Exercise 2.9 of this section) and $\mathfrak{g}$ must be closed under multiplication, it must be equal to $\mathfrak{S}_4$. Now, assume that $\mathfrak{g}$ has an element that permutes exactly 3 elements, i.e., a cycle of length 3. Since we want $\mathfrak{g}$ to be closed under conjugation and since every other 3-cycle of the form $(1\ 2\ k)$ with $k \in \{3, 4\}$ can be obtained via conjugation, $\mathfrak{g}$ must contain the 3-cycles $(1\ 2\ 3), (1\ 2\ 4)$. But then $\mathfrak{g}$ must contain every even permutation (see Exercise 2.10 of this section), so $\mathfrak{A}_4 \subseteq \mathfrak{g}$. If $\mathfrak{g}$ contains any elements outside of $\mathfrak{A}_4$, then its order must be $> 12$ and the only divisor of $4! = 24$ greater than 12 is 24 itself, so $\mathfrak{g}$ would be $\mathfrak{S}_4$. Now, assume that $\mathfrak{g}$ has an element that permutes exactly 4 elements. We have two cases. That permutation is either a 4-cycle or a product of two transpositions. In the first case, again, $\mathfrak{g}$ must contain every 4-cycle, but then $\mathfrak{g}$ must contain 3-cycles as well since $(1\ 2\ 3\ 4)(1\ 3\ 2\ 4) = (1\ 4\ 2)$, so we consider the other case. In the other case, again, $\mathfrak{g}$ contains every product of two transpositions, namely, $(1\ 2)(3\ 4), (1\ 3)(2\ 4)$ and $(1\ 4)(2\ 3)$. We have already considered the cases of $\mathfrak{g}$ having permutations permuting less than 4 elements and at the same time we can't have permutations permuting more than 4 elements, so we eventually have $\mathfrak{g} = \mathfrak{B}_4$. Finally, normality of $\mathfrak{B}_4$ follows from the fact that no matter how you permute the digits in the members of $\mathfrak{B}_4$, it will still stay in the subgroup, i.e., it is closed under conjugation.

## Exercise 2.21

If $\mathfrak{g}$ is a normal divisor of $\mathfrak{G}$, and if $\mathfrak{H}$ is an intermediate group

$$\mathfrak{g} \subseteq \mathfrak{H} \subseteq \mathfrak{G}$$

Then $\mathfrak{g}$ is a normal divisor in $\mathfrak{H}$.

$\mathfrak{g}$ is clearly a subgroup of $\mathfrak{H}$ and, if it is closed under conjugation by every element in $\mathfrak{G}$, then it is also closed under conjugation by every element in $\mathfrak{H}$ since $\mathfrak{H} \subseteq \mathfrak{G}$, so $\mathfrak{g}$ is a normal subgroup of $\mathfrak{H}$.

## Exercise 2.22

All infinite cyclic groups are isomorphic with additive groups of integers.

Let $\mathfrak{C}$ be an infinite cyclic group generated by $a$ and consider the mapping $\varphi : \mathfrak{C} \to \mathbb{Z}$ given by $\varphi : a^k \mapsto k$. $\varphi$ is indeed well defined since if there existed distinct $k, k'$ with $a^k = a^{k'}$, then we would have $a^{k-k'} = 1$, meaning $\mathfrak{C}$ is finite, which would be a contradiction. $\varphi$ is a bijection since it has an inverse, namely, $\varphi^{-1} : \mathbb{Z} \to \mathfrak{C}$ is given by $\varphi^{-1} : n \mapsto a^n$. Finally, we also have $\varphi(a^{m_1}a^{m_2}) = \varphi(a^{m_1+m_2}) = m_1 + m_2 = \varphi(a^{m_1}) + \varphi(a^{m_2})$, so $\varphi(xy) = \varphi(x) + \varphi(y)$ for all $x, y \in \mathfrak{C}$. $\varphi$ is hence an isomorphism and $\mathfrak{C}$ is isomorphic to the additive group of integers.

## Exercise 2.23

The conjugation relation is symmetric, reflexive, and transitive. It is thus possible to partition the elements of a group into classes of conjugate elements.

Let $\mathfrak{G}$ be a group and $g_1, g_2 \in \mathfrak{G}$. Define the relation $\sim$ by $g_1 \sim g_2$ if and only if there exists $g_3 \in \mathfrak{G}$ with $g_1 = g_3 g_2 g_3^{-1}$. The relation is transitive as for all $g \in \mathfrak{G}$ there exists $g' \in \mathfrak{G}$ with $g = g'g(g')^{-1}$, namely, $g' = 1$, since $1g1^{-1} = 1$, thus $g \sim g$. The relation is symmetric since if $g_1 \sim g_2$, i.e., there exists $g_3 \in \mathfrak{G}$ with $g_1 = g_3 g_2 g_3^{-1}$, then we have $g_3^{-1} g_1 g_3 = g_2$ and $g_3^{-1} g_1 (g_3^{-1})^{-1} = g_2$, meaning there exists $g_4 \in \mathfrak{G}$ with $g_2 = g_4 g_1 g_4^{-1}$, namely, $g_4 = g_3^{-1}$, thus $g_1 \sim g_2 \implies g_2 \sim g_1$. For transitivity, assume $g_1 \sim g_2$ and $g_2 \sim g_3$, i.e., there exist $g_4, g_5 \in \mathfrak{G}$ with $g_1 = g_4 g_2 g_4^{-1}$ and $g_2 = g_5 g_3 g_5^{-1}$, by substitution, we obtain $g_1 = g_4 g_5 g_3 g_5^{-1} g_4^{-1} = (g_4 g_5) g_3 (g_4 g_5)^{-1}$, meaning there exists $g_6 \in \mathfrak{G}$ with $g_1 = g_6 g_3 g_6^{-1}$, thus $g_1 \sim g_2, g_2 \sim g_3 \implies g_1 \sim g_3$. Hence $\sim$ is an equivalence relation on the group and the conclusion follows.

## Exercise 2.24

Trivial factor groups of any group $\mathfrak{G}$ are

$$\mathfrak{G}/\mathfrak{G} \cong \mathfrak{G}; \quad \mathfrak{G}/\mathfrak{G} \cong \mathfrak{G}.$$

[What Waerden expects the reader to do here or why he wrote the same wrong equation twice is unclear, I have assumed the exercise is about proving $\mathfrak{G}/\{e\} \cong \mathfrak{G}$ and $\mathfrak{G}/\mathfrak{G} \cong \{e\}$ where $e$ is the neutral element of $\mathfrak{G}$.]

Let $\mathfrak{G}$ be a group with the identity element $e$. For any group $\mathfrak{G}$, the identity mapping is an isomorphism and thus also an homomorphism with trivial kernel. The homomorphism theorem for groups implies that $\mathfrak{G}/\{e\} \cong \mathfrak{G}$. Now consider the mapping $f : \mathfrak{G} \to \{e\}$ defined by $f : x \mapsto e$. $f$ is a surjective homomorphism since $f(xy) = e = ee = f(x)f(y)$ for all $x, y \in \mathfrak{G}$. The kernel of $f$ is the entire $\mathfrak{G}$, so, another application of the homomorphism theorem for groups shows that $\mathfrak{G}/\mathfrak{G} \cong \{e\}$.

## Exercise 2.25

The factor group of the alternating group ($\mathfrak{S}_n/\mathfrak{A}_n$) is a cyclic group of order two.

The alternating group is a normal subgroup (see Exercise 2.13 of this section), so $\mathfrak{S}_n/\mathfrak{A}_n$ is indeed a factor group. Recall that the left cosets of the alternating group are itself and $\pi\mathfrak{A}_n$ with some odd permutation $\pi \in \mathfrak{S}_n$, i.e., the set of odd permutations. Since the product of two odd permutations is always an even permutation, we have $(\pi\mathfrak{A}_n)^2 = \pi\mathfrak{A}_n\pi\mathfrak{A}_n = \pi\pi\mathfrak{A}_n = \mathfrak{A}_n$, meaning $\mathfrak{A}_n$ is a power of $\pi\mathfrak{A}_n$ and, obviously, $\pi\mathfrak{A}_n$ is a power of itself, so the factor group is a cyclic group with order two generated by the set of odd permutations.

## Exercise 2.26

The factor group $\mathfrak{S}_4/\mathfrak{B}_4$ of the four-group (Exercise 2.20) is isomorphic with $\mathfrak{S}_3$.

Denote the cosets of $\mathfrak{B}_4$ as follows.

$$\begin{aligned}
\mathfrak{c}_0 &= \mathfrak{B}_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \\
\mathfrak{c}_1 &= (1\ 2)\mathfrak{B}_4 = \{(1\ 2), (3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\} \\
\mathfrak{c}_2 &= (1\ 3)\mathfrak{B}_4 = \{(1\ 3), (2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\} \\
\mathfrak{c}_3 &= (2\ 3)\mathfrak{B}_4 = \{(1\ 4), (2\ 3), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2)\} \\
\mathfrak{c}_4 &= (1\ 2\ 3)\mathfrak{B}_4 = \{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\} \\
\mathfrak{c}_5 &= (1\ 3\ 2)\mathfrak{B}_4 = \{(1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 3), (2\ 3\ 4)\}
\end{aligned}$$

There are 4 elements in $\mathfrak{B}_4$ and 24 elements in $\mathfrak{S}_4$, so there are $\frac{24}{4} = 6$ cosets, so we have named all of them and $\mathfrak{S}_4/\mathfrak{B}_4 = \{\mathfrak{c}_0, \mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{c}_3, \mathfrak{c}_4, \mathfrak{c}_5\}$. Clearly, each $\mathfrak{c}_i$ with $i \in \{0, \ldots, 5\}$ contains exactly one element from $\mathfrak{S}_3$ and define $\varphi : \mathfrak{S}_4/\mathfrak{B}_4$ by mapping each $\mathfrak{c}_i$ to that element. Since cosets should be disjoint, this mapping is injective and consequently surjective (the domain and the codomain have the same cardinality). Finally, we have $\varphi(\mathfrak{c}_i\mathfrak{c}_j) = \varphi(\varphi(\mathfrak{c}_i)\mathfrak{B}_4\varphi(\mathfrak{c}_j)B_4) = \varphi(\varphi(\mathfrak{c}_i)\varphi(\mathfrak{c}_j)\mathfrak{B}_4) = \varphi(\mathfrak{c}_i)\varphi(\mathfrak{c}_j)$ for all $i, j \in \{0, \ldots, 5\}$, so $\varphi$ is an isomorphism and $\mathfrak{G}_4/\mathfrak{B}_4 \cong \mathfrak{S}_3$.

## Exercise 2.27

The elements $aba^{-1}b^{-1}$ of a group $\mathfrak{G}$ and their products form a group called the *commutator group* of $\mathfrak{G}$. It is a normal divisor, and its factor group is an Abelian group. Any normal divisor whose factor group is Abelian contains the commutator group.

Let $x$ be an element of the commutator group $\mathfrak{G}'$ of $\mathfrak{G}$ and $g$ be an element of $\mathfrak{G}$, then $gxg^{-1}x^{-1} \in \mathfrak{G}'$ and, via closure, $gxg^{-1}x^{-1}x \in \mathfrak{G}'$. But $gxg^{-1}x^{-1}x = gxg^{-1}$, so every conjugate of $x$ is also present in the commutator group, meaning it is normal. Since $\mathfrak{G}'$ is normal, we have $a\mathfrak{G}'b\mathfrak{G}' = ab\mathfrak{G}'$ for all $a, b \in \mathfrak{G}$. We first show that $ab\mathfrak{G}' \subseteq ba\mathfrak{G}'$. Namely, we have $abg = ba(a^{-1}b^{-1}abg)$ for all $g \in \mathfrak{G}'$ and, via symmetry, $ba\mathfrak{G}' \subseteq ab\mathfrak{G}'$. This shows that $a\mathfrak{G}'b\mathfrak{G}' = b\mathfrak{G}'a\mathfrak{G}'$, i.e., the left cosets of the commutator group commute, meaning its factor group is Abelian. For the last part, let $\mathfrak{g}$ be a normal subgroup of $\mathfrak{G}$ with all left cosets commuting. It is sufficient to show that every element of the form $aba^{-1}b^{-1}$ is present in $\mathfrak{g}$. Since $ab\mathfrak{g} = ba\mathfrak{g}$, we have

$ab \in ba\mathfrak{g}$, i.e., there exists $x \in \mathfrak{g}$ with $ab = bax$ and $bab^{-1}a^{-1} = x^{-1} \in \mathfrak{g}$ for all $a, b \in \mathfrak{G}$.

[Remark: The standard notation for a commutative group of $G$ is $[G, G]$.]

### Exercise 2.28

If $\mathfrak{G}$ is cyclic, $a$ the generating element of $\mathfrak{G}$, and $\mathfrak{g}$ a subgroup of index $m$, then $\mathfrak{G}/\mathfrak{g}$ is cyclic of order $m$.

Let $b\mathfrak{g}$ be a left coset of $\mathfrak{g}$ with $b \in \mathfrak{G}$, then $b = a^k$ for some integer $k$ and $b\mathfrak{g} = a^k\mathfrak{g} = (a\mathfrak{g})^k$, i.e., every left coset is generated by $a\mathfrak{g}$. The subgroup $\mathfrak{g}$ has $m$ left cosets, so the quotient group $\mathfrak{G}/\mathfrak{g}$ will have $m$ elements, i.e., will have order $m$.

### Exercise 2.29

Any cyclic group of order $m$ is isomorphic with the residue class module modulo an integer $m$.

Let $\mathfrak{C}$ be a cyclic group generated by $x$ of order $m$, i.e., let $\mathfrak{C}$ consist of $x^0, x^1, \ldots, x^{m-1}$ with $x^m = 1$. Our claim is that $\mathfrak{C}$ is isomorphic to the residue class module modulo $m$ via mapping each $a^i$ to $i$ for all $i \in \{0, \ldots, m-1\}$. We shall show that $a^ia^j = a^k$ if and only if $i + j \equiv k \mod m$. If $a^ia^j = a^k$, then $a^{i+j-k} = 1$, meaning $i + j - k$ is a multiple of $m$, i.e., $i + j \equiv k \mod m$. Conversely, let $i + j \equiv k \mod m$, i.e., there exists an integer $q$ with $i + j - k = mq$ and $i + j = mq + k$, then $a^ia^j = a^{i+j} = a^{mq+k} = a^{mq}a^k = (a^m)^q a^k = 1^q a^k = a^k$. Hence the mapping is indeed an isomorphism.

## 8.6 Algebra by Waerden, Chapter 3

### Exercise 3.1

The pair of integers $(a_1, a_2)$ with

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1, b_1, a_2, b_2)$$

form a ring with zero divisors.

First we verify that this is a ring. Let $a_1, a_2, b_1, b_2, c_1, c_2, x_1, x_2$ be integers. Associativity of addition indeed holds as

$$((a_1, a_2) + (b_1, b_2)) + (c_1, c_2) = (a_1 + a_2, b_1 + b_2) + (c_1, c_2) =$$
$$= ((a_1 + b_1) + c_1, (a_2 + b_2) + c_2) = (a_1 + (b_1 + c_1), a_2 + (b_2 + c_2)) =$$
$$= (a_1, a_2) + (b_1 + c_1, b_2 + c_2) = (a_1, a_2) + ((b_1, b_2) + (c_1, c_2))$$

Commutativity of addition is also inherited.

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2) = (b_1 + a_1, b_2 + a_2) = (b_1, b_2) + (a_1, a_2)$$

Solvability of the equation $(a_1, a_2) + x = (b_1, b_2)$ is also guaranteed since $x = (b_1 - a_1, b_2 - a_2)$ is a solution as shown below.

$$(a_1, a_2) + (b_1, -a_1, b_2 - a_2) = (a_1 + b_1 - a_1, a_2 + b_2 - a_2) = (b_1, b_2)$$

Commutativity of multiplication is also inherited.

$$((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2) = (a_1 b_1, a_2 b_2) \cdot (c_1, c_2) = ((a_1 b_1) c_1, (a_2 b_2) c_2) =$$
$$= (a_1 (b_1 c_1), a_2 (b_2 c_2)) = (a_1, a_2) \cdot (b_1 c_1, b_2 c_2) = (a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2))$$

Distributive laws (namely, distributivity of multiplication over addition) also hold. (Multiplication is commutative since $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) = (b_1 a_1, b_2 a_2) = (b_1, b_2)(a_1, a_2)$, so showing left distributivity suffices.)

$$(a_1, a_2) \cdot ((b_1, b_2) + (c_1, c_2)) = (a_1, a_2) \cdot (b_1 + c_1, b_2 + c_2) =$$
$$= (a_1 (b_1 + c_1), a_2 (b_2 + c_2)) = (a_1 b_1 + a_1 c_1, a_2 b_2 + a_2 c_2) =$$
$$= (a_1 b_1, a_2 b_2) + (a_1 c_1, a_2 c_2) = (a_1, a_2)(b_1, c_2) + (a_1, a_2)(c_1, c_2)$$

Hence we indeed have a ring. (In fact, a commutative ring.)

Now we show that there are zero divisors. First, we need to identify which element is the additive identity.

$$(a_1, a_2) + (0, 0) = (a_1 + 0, a_2 + 0) = (a_1, a_2)$$

Thus $(0, 0)$ is the zero element of our ring. We also have

$$(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$$

Whereas $(1, 0) \neq (0, 0)$ and $(0, 1) \neq (0, 0)$. Thus zero divisors are indeed present. (This can be generalised for any nonzero ring and Cartesian products of arbitrary length.)

## Exercise 3.2

It is permissible to cancel $a$ in an equation $ax = ay$, provided $a$ is not a left zero divisor. (In particular, it is possible to cancel any $a \neq 0$ in an integral domain.)

Let $a$ an element of a ring that is not be a left zero divisor, i.e., for all nonzero elements $b$. But, given $ax = ay$, we have $ax = ay$ and $ax - ay = 0$ and $a(x - y) = 0$, forcing $x - y$ to be zero, i.e., $x = y$. In an integral domain the only zero divisor is zero itself, so every nonzero element can be cancelled.

## Exercise 3.3

Taking as an additive group any arbitrary Abelian group, construct a ring in which the product of any two elements is equal to 0.

Let $\mathfrak{R}$ be an Abelian group with binary operation $+$ and neutral element 0. Consider the same set with the $+$ taken as addition and $\cdot : \mathfrak{R} \times \mathfrak{R} \to \mathfrak{R}$ given by $a \cdot b = 0$ as multiplication. The laws of addition immediately hold since $\mathfrak{R}$ is already an Abelian group under multiplication. Associativity of multiplication holds as $a \cdot bc = a \cdot 0 = 0 = 0 \cdot c = ab \cdot c$ for all $a, b, c \in \mathfrak{R}$. Similarly, distributive laws (namely, distibutivity of multiplication over addition) are also satisfied as $a(b+c) = 0 = 0+0 = ab+ac$ and $(a+b)c = 0 = 0 + 0 = ac + bc$. Thus $\mathfrak{R}$ is a ring. (One may verify that it is a commutative ring.)

## Exercise 3.4

A left zero divisor has no left inverse; a right zero divisor has no right inverse. In particular, the zero element has neither a right nor a left inverse. A trivial exception is the ring consisting of but one element 0, which, simultaneously, is the identity and its own inverse.

Let $\mathfrak{R}$ and $l \in \mathfrak{R}$ be a left zero divisor, i.e., $l$ is nonzero and there exists a nonzero $r \in \mathfrak{R}$ with $lr = 0$. Then, for all $l' \in \mathfrak{R}$, we have $l'lr = l'0 = 0 \neq r$, i.e., $l'lr \neq r$. If $l$ had a left inverse, it would contradict the latter

Similarly, let $r \in \mathfrak{R}$ be a right zero divisor, i.e., $r$ is nonzero and there exists a nonzero $l \in \mathfrak{R}$ with $lr = 0$. Then, for all $r' \in \mathfrak{R}$, we have $lrr' = 0r' = 0 \neq l$, i.e., $lrr' \neq l$. If $r$ had a right inverse, it would contradict the latter.

The zero element itself had neither a right nor a left inverse in a nonzero ring as any product involving it is itself and, in a nonzero ring, the zero and the unit elements are distinct.

The case with the zero ring is an exception for third assertion as, in that case, $0 = 1$, meaning the left inverse of 0 is itself $(0 \cdot 0 = 0 = 1)$ and the right inverse of 0 is itself $(0 \cdot 0 = 0 = 1)$. (The first two implications, though, remain true, in this case, vacuously.)

## Exercise 3.5

Prove for arbitrary commutative rings the *binomial theorem*:

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + b^n,$$

by induction on $n$. Here $\binom{n}{k}$ denotes the integer

$$\frac{n(n-1)\dots(n-k+1)}{1 \cdot 2 \dots k} = \frac{n!}{(n-k)!k!}.$$

[For the sake of clarity and in order to avoid exponentiation to the 0th power (as some commutative rings are non-unital), the right hand side has been rewritten as $a^n + \sum_{v=1}^{n-1} \binom{n}{v} a^v b^{n-v} + b^n$.]

We first show that $\binom{n}{v-1} + \binom{n}{v} = \binom{n+1}{v}$ and that $\binom{n}{n-1} = \binom{n}{1} = n$.

$$\binom{n}{v-1} + \binom{n}{v} = \frac{n!}{(n-(v-1)!)(v-1)!} + \frac{n!}{(n-k)!k!} =$$

$$= \frac{n! \cdot v}{(n-v+1)!(v-1)! \cdot v} + \frac{n! \cdot (n-v+1)}{(n-v)!v! \cdot (n-v+1)} = \frac{n!v + n!(n-v+1)}{(n-v+1)1v!} =$$

$$\frac{n!(n+1)}{(n+1-v)!v!} = \binom{n+1}{v}$$

$$\binom{n}{1} = \frac{n!}{(n-1)!1!} = \frac{(n-1)!n}{(n-1)!} = n$$

$$\binom{n}{n-1} = \frac{n!}{(n-(n-1))!(n-1)!} = \frac{n1}{(n-1)!1!} = \binom{n}{1}$$

For base case, $n = 1$, so we have

$$(a+b)^n = (a+b)^1 = a + b = a + 0 + b = a + \sum_{v=1}^{0} \binom{1}{v} a^v b^{1-v} + b =$$

$$= a^1 + \sum_{v=1}^{1-1} \binom{1}{v} a^v b^{1-v} + b^1 = a^n + \sum_{v=1}^{n-1} \binom{n}{v} a^v b^{1-v} + b^n$$

For inductive step, assume that the equality is true for some natural $n$. We then have

$$(a+b)^{n+1} = (a+b)^n(a+b) = (a+b)(a+b)^n = (a+b)\left(a^n + \sum_{v=1}^{n-1} \binom{n}{v} a^v b^{n-v} + b^n\right)$$

$$(a+b)^{n+1} = aa^n + a\sum_{v=1}^{n-1} \binom{n}{v} a^v b^{n-v} + ab^n + ba^n + b\sum_{v=1}^{n-1} \binom{n}{v} a^v b^{n-v} + bb^n$$

$$(a+b)^{n+1} = a^{n+1} + a^n b + \sum_{v=1}^{n-1} \binom{n}{v} aa^v b^{n-v} + \sum_{v=1}^{n-1} \binom{n}{v} ba^v b^{n-v} + ab^n + b^{n+1}$$

$$(a+b)^{n+1} = a^{n+1} + a^n b + \sum_{v=1}^{n-1} \binom{n}{v} a^{v+1} b^{n-v} + \sum_{v=1}^{n-1} \binom{n}{v} a^v b^{n-v+1} + ab^n + b^{n+1}$$

We now show that $a^n b + \sum\limits_{v=1}^{n-1} \binom{n}{v} a^{v+1} b^{n-v} + \sum\limits_{v=1}^{n-1} \binom{n}{v} a^v b^{n-v+1} + ab^n$ and $\sum_{v=1}^{n} \binom{n+1}{v} a^v b^{n-v+1}$ are equal, which will finish the proof.

$$a^n b + \binom{n}{n-1} a^{n-1+1} b^{n-(n-1)} + \sum_{v=1}^{n-2} \binom{n}{v} a^{v+1} b^{n-v} +$$

$$+ \sum_{v=2}^{n-1} \binom{n}{v} a^v b^{n-v+1} + \binom{n}{1} ab^n + ab^n$$

$$= a^n b + na^n b^1 + \sum_{v=2}^{n-1} \binom{n}{v-1} a^{v-1+1} b^{n-(v-1)} + \sum_{v=2}^{n-1} \binom{n}{v} a^v b^{n-v+1} + nab^n + ab^n$$

$$= (n+1)a^n b + \sum_{v=2}^{n-1} \left( \binom{n}{v-1} + \binom{n}{v} \right) a^v b^{n-v+1} + (n+1)ab^n$$

$$= (n+1)a^n b + \sum_{v=2}^{n-1} \binom{n+1}{v} a^v b^{n+1-v} + (n+1)ab^n$$

$$= \sum_{v=1}^{n} \binom{n}{v} a^v b^{n+1-v}$$

## Exercise 3.6

In a ring with exactly $n$ elements we have for every $a$:

$$n \cdot a = 0$$

[Cf. Section 2.3, where $a^n = e$ was proved.]

The additive group of a ring also has exactly $n$ elements meaning the $n$th "power" of $a$ for any element $a$, i.e., $n \cdot a$ (since we are dealing with addition), is equal to the neutral element of the additive group, i.e., 0. Shortly, $n \cdot a = 0$.

## Exercise 3.7

If $a$ commutes with $b$, that is, $ab = ba$, then $a$ also commutes with $-b$, with $nb$, and with $b^{-1}$. If $a$ commutes with $b$ and $c$, then $a$ also commutes with $b + c$ and $bc$.

We first shall show that $x \cdot (-y) = -xy$ for elements $x, y$ of a ring. Definition of $-y$ suggests that $y + (-y) = 0$, so $x(y + (-y)) = 0$ and $xy + x(-y) = 0$. Due to uniqueness of additive inverses, we have $x(-y) = -xy$.

Let $a$ and $b$ be a pair commuting elements of a ring, i.e., $ab = ba$, and $n$ be an integer. If $n$ is nonnegative, then we have $a \cdot nb = a \sum_{v=1}^{n} b = \sum_{v=1}^{n} ab =$

$\sum\limits_{v=1}^{n} ba = \left(\sum\limits_{v=1}^{n} b\right) a = nb \cdot a$. If $n$ is negative, then $a \cdot nb = a \cdot (-(-n)b) = -(a\cdot(-n)b) = -((-n)b\cdot a) = (-(-n)b)\cdot a = nb\cdot a$. In both cases, $a$ commutes with $nb$ and plugging $n = 1$ in shows that $a$ commutes with $-b$. Assume that $b$ has an inverse $b^{-1}$, then $ab = ba$ can be rewritten as $b^{-1}a = ab^{-1}$, meaning $a$ commutes with $b^{-1}$. Now let $c$ be another ring element commuting with $a$, then $a(b+c) = ab + ac = ba + ca = (b+c)a$ and $abc = bac = bca$, so $a$ commutes with $b + c$ and $bc$.

## Exercise 3.8

Carry out the proof of the above. [For context, what is asked to be proven here is that solvability of $ax = b$ and $ya = b$ with $a, b, x, y$ elements of a skew field and $a$ nonzero follows from existence of inverses (of nonzero elements) and identity.]

Let $a, b, x, y$ be elements of a skew field with identity $e$ with $a$ nonzero. The solutions for $x$ and $y$ to $ax = b$ and $ya = b$ are hence $a^{-1}b$ and $ba^{-1}$ respectively as shown below.

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$
$$(ya^{-1})a = y(a^{-1}a) = ye = y$$

## Exercise 3.9

Construct a field of three elements. (First discuss what structures the additive and the multiplicative groups have.)

Let addition and multiplication for the integers 1, 2 and 3 be defined via the following tables.

| $+$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| $\cdot$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

Clearly, the set $\{0, 1, 2\}$ forms an additive Abelian group with neutral element 0 and where the inverses of 0 and 1 are 0 and 2 respectively. $\{1, 2\}$ also forms an Abelian multiplicative group with neutral element 1 and where the inverses of 1 and 2 are themselves. The latter guaranteed solvability of the equations $ax = b$ and $ya = b$ for all $a, b, x, y \in \{0, 1, 2\}$ with $a \neq 0$. Hence $\{0, 1, 2\}$ forms a field.

## Exercise 3.10

An integral domain with a finite number of elements is a field. (Compare the corresponding result for groups in Section 2.1)

Let $\mathfrak{F}$ be an integral domain, i.e., a commutative ring without zero divisors and consider solving for $x$ in $ax = b$ with $a, b, x \in \mathfrak{F}$ and $a \neq 0$. If $b = 0$, then $x = 0$ is a solution. If $b \neq 0$, then, since the multiplicative group of $\mathfrak{F}$ is also finite, we have $a^n = 1$ for some positive integer $n$, meaning $x = a^{n-1}b$ is a solution since $a(a^{n-1}b) = (aa^{n-1})b = a^n b = 1b = b$. Commutativity suggests that the equation $xa = b$ is also solvable. Finally, absence of zero divisors guarantees at least one element besides 0 and thus $\mathfrak{F}$ is a skew field and also a field due to commutativity.

## Exercise 3.11

Show that any commutative ring $\mathfrak{R}$ (with or without a zero divisor) can be embedded in a "quotient ring" consisting of all quotients $a/b$, with $b$ not a divisor of zero. More generally, $b$ may range over any set $\mathfrak{M}$ of nondivisors of zero which is closed under multiplication (that is, $b_1 b_2$ is in $\mathfrak{M}$ whenever $b_1$ and $b_2$ are). The result is a quotient ring $\mathfrak{R}_{\mathfrak{M}}$. [The ring $\mathfrak{R}$ is assumed to have at least one nondivisor of zero as otherwise the assertion is false.]

The proof is the same as in the book.

## Exercise 3.12

If $x, y, \ldots$ are an infinite number of symbols, we may consider the totality of all $\mathfrak{R}$-polynomials in these indeterminates. Every polynomial, however, must contain only a finite number of these terms. Prove that the domain thus defined is, respectively, a ring or integral domain whenever $\mathfrak{R}$ is a ring or an integral domain.

Each law can be verified by letting $A_1, \dots A_n$ be the sets of intermediates of whatever polynomials $p_1, \dots, p_n$ are being considered and using the already derived results for $\mathfrak{R}[\bigcup_{v=1}^{n} A_v]$.

## Exercise 3.13

Show that in the ring of integers the residue class modulo an ideal $(m)$ $(m > 0)$ may be represented by the number $0, 1, \dots, m-1$ and may thus be denoted as $\mathfrak{R}_0, \mathfrak{R}_1, \dots, R_{m-1}$.

By definition, we simply need to count the cosets of the subgroup consisting of multiples of $m$ within the additive group of integers, which there are $m$ of [See exercise 2.15 of the previous section]. The conclusion follows naturally.

## Exercise 3.14

What ideal is generated by the numbers 10 and 13 together in the ring of integers?

The ideal generated by 10 and 13 in the ring of integers is the set of integers of the form $10a + 13b$ with $a, b \in \mathbb{Z}$.

## Exercise 3.15

What does $a \equiv b \ (0)$ mean?

For $a \equiv b \ (0)$ to hold, we would require $a - b \in (0)$, but the principle ideal $(0)$ consists of only 0, so that is equivalent to saying $a - b = 0$. I.e., $a \equiv b \ (0)$ if and only if $a = b$.

## Exercise 3.16

All multiples $ra$ of an element $a$ form an ideal $\mathfrak{o}a$. Considering the ring of the even integers, make clear to yourself that this ideal is not necessarily identical with the principal ideal $(a)$. [What Waerden refers to by $\mathfrak{o}$ is unclear here, we simply show that all multiples $ra$ form some ideal.]

Let $a$ be an element of a ring $\mathfrak{R}$ and $\mathfrak{o} = \{ra \mid r \in \mathfrak{R}\}$. The set $\mathfrak{o}$ is closed under subtraction, as $ra - r'a = (r - r')a$ for $r, r' \in \mathfrak{R}$ and, since $r - r' \in \mathfrak{R}$, we have $(r - r')a \in \mathfrak{R}$ and $ra - r'a \in \mathfrak{R}$. $\mathfrak{o}$ is also closed under multiplication by any ring element as $r'(ra) = (r'r)a \in \mathfrak{o}$ for all $r, r' \in \mathfrak{R}$.

Now consider $\mathfrak{R} = 2\mathbb{Z}$ with the usual addition and $a = 2$. Then the principle ideal $(2)$ contains 6 since $6 = 0 \cdot 2 + 3 \cdot 2$, however, $2\mathfrak{R} = 4\mathbb{Z}$ does not.

## Exercise 3.17

The residue class ring $\mathfrak{o}/\mathfrak{m}$ may have divisors of zero, even though $\mathfrak{o}$ does not have any. Give examples in the ring of integers.

Let $\mathfrak{o} = \mathbb{Z}$ with usual addition and $\mathfrak{m} = (4)$. The residue classes are then the sets of integers of the forms $4k$, $4k + 1$, $4k + 2$ and $4k + 3$. The latter is the zero element of the residue class ring whereas multiplying the second from last residue class by itself yields the zero residue class, so $\mathfrak{o}/\mathfrak{m}$ has zero divisors despite $\mathfrak{o}$ being a ring without zero divisors.

## Exercise 3.18

The homomorphism $\mathfrak{o} \sim \overline{\mathfrak{o}}$ is an isomorphism if and only if $\mathfrak{n} = (0)$. [For context, $\mathfrak{n}$ is the kernel of the homomorphism in question.]

Every coset of $(0)$ has the same amount of elements, i.e., every preimage of the homomorphism has upmost 1 element. This shows that the homomorphism is injective and, with addition to surjectivity, this makes it an isomorphism.

## Exercise 3.19

In a field there are no ideals except for the null ideal and the unit ideal. Furnish the proof. What does this imply for the possible homomorphic mappings of a field?

Let $\mathfrak{m}$ be an ideal in a field $\mathfrak{F}$. If $\mathfrak{m}$ contains no other elements besides 0, then it is the null ideal. Otherwise it contains at least one nonzero element, name it $a$ and let $b \in \mathfrak{F}$ be arbitrary. Since $\mathfrak{F}$ is a field, there is a solution for $x$ in $ax = b$ within the field. Since $a \in \mathfrak{m}$, we have $b = ax \in \mathfrak{m}$, i.e., every element is contain in $\mathfrak{m}$. Thus every ideal of a field is either the null ideal or the unit ideal, meaning there are no other ideals. [Conversely, one could show that every commutative ring with only two ideals is a field.]

This implies that every homomorphism from a field is either a zero map onto the zero ring or is an isomorphism.

## Exercise 3.20

Prove this last assertion. [For context, it is asked to show that in the integral domain $\mathbb{Z}[x]$ the ideals $(x)$ and $(2, x)$ are prime ideals.]

We start by showing that the residue class ring $\mathbb{Z}[x]/(x)$ has no zero divisors by letting $p_1p_2 \equiv 0 \ (x)$ with $p_1 \notin (x)$ and $p_1, p_2 \in \mathbb{Z}[x]$. Since $\mathbb{Z}[x]$ has a unit, every element of the ideal $(x)$ is a multiple of $x$, so we have $p_1p_2 = rx$ with some $r \in \mathbb{Z}[x]$. Let us evaluate both sides at 0, so that $p_1(0)p_2(0) = r(0)0 = 0$, meaning $p_1(0) = 0$ or $p_2(0) = 0$. The latter can't happen as it would imply that every term in $p_1$ has degree $\geq 1$, meaning it is a multiple of $x$, so we have $p_2(0) = 0$, likewise meaning that $p_2$ is a multiple of $x$, i.e., $p_2 \equiv 0 \ (x)$.

We now show that the residue class ring $\mathbb{Z}/(2, x)$ also has no zero divisors by letting $p_1p_2 \equiv 0 \ (2, x)$ with $p_1 \notin (2, x)$ and $p_1, p_2 \in \mathbb{Z}[x]$. Since $\mathbb{Z}[x]$ has a unit, every element of the ideal $(2, x)$ is of the form $r_1x + 2r_2$ with $r_1, r_2 \in \mathbb{Z}[x]$. Let us again evaluate both sides at 0, so that $p_1(0)p_2(0) = r_1(0)0 + 2r_2(0) = 2r_2(0)$. Since $2r_2(0)$ is an even integer and $p_1(0)$ can't be even (otherwise it would belong to the ideal $(2, x)$), so we have $p_2(0)$ even, meaning $p_2 = rx + 2c$ with $r \in \mathbb{Z}[x]$ and some $c \in \mathbb{Z}$, implying $p_2 \equiv 0 \ (2, x)$.

## Exercise 3.21

Discuss the properties of the residue class rings of the ideals (2) and (3) in the ring of integers, and prove that these ideals are prime.

We shall show that both these ideals are maximal. Let $\mathfrak{a} \subseteq \mathbb{Z}$ be a proper overideal of (2), so it contains every even integer and an integer of the form $2k+1$, then $1 = 2k+1-2k \in \mathfrak{a}$ and therefore $\mathfrak{a} = \mathbb{Z}$. Similarly, let $\mathfrak{b}$ be a proper overideal of (3), so it contains every multiple of 3 and either an integer of the form $3k+1$ or $3k+2$. In the first case, we have $1 = 3k+1-3k \in \mathfrak{b}$. In the second case, $1 = 3k+3-(3k+2) \in \mathfrak{b}$. Either way, $\mathfrak{b} = \mathbb{Z}$. Since the ideals (2) and (3) are maximal, they are also prime.

## Exercise 3.22

The relation $(a, b) = d$ remains valid when the ring $\mathfrak{o}$ is extended to any larger ring $\overline{\mathfrak{o}}$.

Let $(a, b) = d$, meaning there exist $r, s, g, h \in \mathfrak{o}$ with $d = ra + sb$, $a = gd$ and $b = hd$. In $\overline{\mathfrak{o}}$ it still holds that $d$ is a common divisor of $a$ and $b$ and that it divides every other common divisor of $a$ and $b$, i.e., $d$ is a greatest common divisor in $\overline{\mathfrak{o}}$

## Exercise 3.23

Every element $a$ of order $r \cdot s$ in a group $\mathfrak{G}$ is the product of a unique determined $a^{\lambda r}$ of order $s$ and a unique determined element $a^{us}$ of order $r$, provided the numbers $r$ and $s$ are relatively prime.

We first show that if relatively elements $a$ and $b$ divide $x$ in a Euclidean ring, then so does $ab$. Since $a$ and $b$ divide $x$, there exist $p, q$ with $x = pa$ and $x = qb$. Since $a$ and $b$ are also relatively prime, there exist $r, s$ with $ra+sb = 1$, meaning we have $x = (ra + sb)x = rax + sbx = raqb + sbpa = (rq + sp)ab$, thus $ab$ divides $x$.

The integers $r$ and $s$ being relatively prime implies existence of integers $\lambda$ and $u$ with $\lambda r + us = 1$, meaning $a^{\lambda r} a^{us} = a^{\lambda r + us} = a^1 = a$. We now show that the elements $a^{\lambda r}$ and $a^{us}$ are uniquely determined. Let $\lambda'$ and $u'$ also be a pair of integers with $\lambda' r + u' s = 1$. Then $(\lambda - \lambda')r + (u - u')s = (\lambda r + us) - (\lambda' r + u' s) = 0$. Clearly, $(\lambda - \lambda')r$ is divisible by $r$ and by $s$, hence it should be a multiple of $rs$ as well, meaning $a^{\lambda r} = a^{\lambda r - \lambda' r + \lambda' r} = a^{(\lambda - \lambda')r} a^{\lambda' r} = a^{\lambda' r}$.

## Exercise 3.24

A cyclic group of order $n$ with the generating element $a$ can also be generated by any power $a^\mu$, provided $(\mu, n) = 1$.

It is sufficient to show that $a$ can be expressed using $a^\mu$. Since $(\mu, n) = 1$, there exist integers $r, s$ with $r\mu + sn = 1$, meaning $a = a^1 = a^{r\mu + sn} = a^{r\mu} a^{sn} = a^{r\mu}$.

## Exercise 3.25

Solve the congruence

$$6x \equiv 7 \ (19)$$

using the Euclidean algorithm.

We start by finding the g.c.d. of 6 and 19 using the Euclidean algorithm.

$$19 = 3 \cdot 6 + 1$$

$$3 = 1 \cdot 3 + 0$$

So, we have $19 - 3 \cdot 6 = 1$, meaning $19 \cdot 7 - 3 \cdot 6 \cdot 7 = 7$, $-3 \cdot 6 \cdot 7 \equiv 7 \ (19)$, i.e., $x = -3 \cdot 7 = -21$ yields a solution.

## Exercise 3.26

If in a principal ideal ring a product $ab$ is divisible by $c$ and $a$ is not divisible by $c$, then $b$ is divisible by $c$. [$c$ is assumed to be a prime element as the assertion is not necessarily true otherweise; Consider $a = b = 2$ and $c = 4$.]

If $ab$ is divisible by $c$, there exists an element $k$ with $ab = kc$. Since $a$ is not divisible by $c$, $a$ is not in the ideal $(c)$. Also, since these are elements of a principal ideal ring, including $a$ in $(c)$ would make it equal to the unit ideal, i.e., $(a, c) = 1$, meaning there exist elements $r, s$ with $ra + sc = 1$. Multiplying both sides by $b$ gets us $rab + scb = b$ and $rkc + scb = b$, meaning $b$ is divisible by $c$.

## Exercise 3.27

The integral polynomials $f(x)$ modulo any prime $p$ are uniquely decomposable into factors which are irreducible modulo $p$.

Since integers modulo $p$ form a field, the integral polymials modulo $p$ form a principal ideal ring (a Euclidean ring, even), hence the theorem derived in the book applies. (I.e., we have unique prime factorisations)

## Exercise 3.28

What are the units of the Gaussian number ring? Decompose into prime factors the numbers 2, 3 and 5 in this ring.

As we already know, in the quotient field of the Gaussian number ring, given a nonzero $\alpha$, we have $\alpha^{-1} = \frac{a-bi}{N(\alpha)}$ where $a, b$ are real and complex parts of $\alpha$ and $N(\alpha) = a^2 + b^2$. For $\alpha$ to be invertible in the Gaussian number ring, $\frac{a-bi}{N(\alpha)}$ should be identified with some Gaussian number, which would happen if and only if $N(\alpha)$ divides both $a$ and $b$. So there exist integers $k, k'$ with $a = k(a^2 + b^2)$ and $b = k'(a^2 + b^2)$. In the first equation, we obtain

$a = ka^2 + kb^2$, meaning $b$ should be divisible by $a$, say, $b = ma$ for some integer $m$, then $a = ka^2 + km^2a^2$. If $a = 0$, then we have $b = k'b^2$. We can't have $b = 0$ since $\alpha$ is nonzero, so $k'b = 1$, meaning $b$ is a unit in $\mathbb{Z}$, i.e., $b = 1$ or $b = -1$. For the case $a \neq 0$, we have $1 = ka + km^2a$, meaning $a$ is a unit in $\mathbb{Z}$, i.e., $a = 1$ or $a = -1$. In either case, $b = k' + k'b^2$, so $k'$ and $b$ are integers divisible by one another. The latter implies that they differ by a unit. If $k' = b$, then $b = b + bb^2$, $b^3 = 0$ and $b = 0$ since the integers form an integral domain. If $k' = -b$, then $b = -b - b^3$, $2b = -b^3$ and $b^2 = -2$, however, no such integer $b$ exists. We now verify that the Gaussian numbers $1, -1, i$ and $-i$ are indeed units. $1 \cdot 1 = 1$, $(-1) \cdot (-1) = 1$ and $i \cdot (-i) = 1$.

Before we move on, we need to prove a few things, namely, a Gaussian integer is invertible (resp. prime) if and only if its complex conjugate is invertible (resp. prime). (In fact, due to involution, it is sufficient to show just one direction.) Let $g$ be invertible, then it's a unit, which we have already listed. It is apparent that the complex conjugate of $g$ is also invertible. Now, let some Gaussian integer $x + yi$ be prime, i.e., if there are Gaussian integers $a, b$ with $x + yi = ab$, then either $a$ or $b$ is invertible. Let $c, d$ be Gaussian integers with $x - yi = cd$, then $x + yi = \overline{x - yi} = \overline{cd} = \overline{c}\overline{d}$. Since $x + yi$ is prime, either $\overline{c}$ or $\overline{d}$ is a unit and thus either $c$ or $d$ is a unit, meaning $x - yi$ is also a prime. Due to this result, we don't need to show that a Gaussian integer is a prime if we have already shown that its complex conjugate is a prime.

Observe that $2 = (1 + i)(1 - i)$. Our claim is that $1 + i$ is prime in the Gaussian numbers. Let $a, a', b, b'$ be integers with $(a + bi)(a' + b'i) = 1 + i$. Our goal is to show that one of $a + bi$ or $a' + b'i$ is a unit. We again obtain Diophantine equations for the unknowns, namely, $aa' - bb' = 1 = ab' + a'b$. Squaring both equations and adding them up yields $a^2(a')^2 + b(b')^2 + a^2(b')^2 + (a')^2b^2 = 2$ or $(a^2 + b^2)((a')^2 + (b')^2) = 1$. If $a = 0$, then $b = \pm 1$, but, in either case, $a + bi$ is a unit. Symmetry takes care of the other cases.

Our claim is that 3 is prime. Let $a, a', b, b'$ be integers with $(a + bi)(a' + b'i) = 3$. Our goal is to show that one of $a + bi$ or $a' + b'i$ is a unit. We again arrive at $(a^2 + b^2)((a')^2 + (b')^2) = 9$, meaning $a^2 + b^2$ are positive divisors of 9. We can't have $a^2 + b^2 = 1$ with $a, b$ both nonzero and, clearly, if one of them is $= 0$, then it follows that $a + bi$ is a unit. We can't have $a^2 + b^2 = 3$. (By contradiction assume otherwise, then we can't have neither $|a| \geq 2$ nor $|b| \geq 2$, so $|a| \leq 1$ and $|b| \leq 1$, but then $a^2 + b^2 \leq 1^2 + 1^2 = 2 < 3$.) We also can't have $a^2 + b^2 = 9$ as it would imply $(a')^2 + (b')^2 = 9$, which, as we have already shown, is impossible.

Observe that $5 = (2+i)(2-i)$. Our claim is that $2+i$ is prime. Let $a, a', b, b'$ be integers with $(a+bi)(a'+b'i) = 2+i$. Our goal is to show that one of $a+bi$ or $a'+b'i$ is a unit. We again arrive at $(a^2+b^2)((a')^2+(b')^2) = 5$, meaning $a^2+b^2$ is a positive divisor of 5. If $a^2+b^2$, then it follows that $a+bi$ is a unit. If $a^2+b^2 = 5$, then $(a')^2+(b')^2 = 5$ and $a'+b'i$ is a unit. (One could also verify that another decomposition is $5 = (1+2i)(1-2i)$.)

## Exercise 3.29

For the number 4 in the ring of the numbers $a + b\sqrt{-3}$ there are two substantially different factorizations into prime factors:

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3}).$$

The equalities are clearly true, we move onto showing that the factors are indeed prime.

We first need to identity the units of this ring. Let $a, a', b, b'$ be integers with $(a+b\sqrt{-3})(a'+b'\sqrt{-3}) = 1$, i.e., $aa' - 3bb' = 1$ and $ab' + a'b = 0$. Squaring both equations, scaling the second one by 3, adding them up and factoring yields $(a^2+3b^2)((a')^2+3(b')^2) = 1$. Clearly, We can't have neither nonzero $b$ nor nonzero $b'$, so $b = b' = 0$, $a = \pm$ and $a' = \pm$. Conversely, 1 and $-1$ are trivially invertible.

Let $a, a', b, b'$ be integers with $(a+b\sqrt{-3})(a'+b'\sqrt{-3}) = 2$, i.e., $aa'-3bb' = 2$ and $ab'+a'b = 0$. We again obtain $(a^2+3b^2)((a')^2+3(b')^2) = 4$. We can't have both $b$ and $b'$ nonzero at the same time, so we consider cases. If $b = 0$ and $b' = 0$, then $a = \pm 2$ and $a' = \pm 1$ or $a = \pm 1$ and $a' = \pm 2$. If $b \neq 0$ and $b' = 0$, then $a = \pm 1$, $b = \pm 1$ and $a' = \pm 1$. Symmetry takes care of the last case. Either way, we have that $a + b\sqrt{-3}$ or $a' + b'\sqrt{-3}$ is a unit, proving 2 to be prime.

Similarly, let $a, a', b, b'$ be integers with $(a+b\sqrt{-3})(a'+b'\sqrt{-3}) = 1+\sqrt{-3}$, i.e., $aa' - 3bb' = 1$ and $ab' + a'b = 1$. We obtain $(a^2+3b^2)((a')^2+3(b')^2) = 4$. As we have already shown, it follows that $a + b\sqrt{-3}$ or $a' + b'\sqrt{-3}$ is a unit, proving $1+\sqrt{-3}$ to be prime.

The proof that a number of the form $a + b\sqrt{-3}$ is prime if and only if its complex conjugate is is proven as previously.

### Exercse 3.30

In a principal ideal ring the residue classes modulo $a$ consisting of elements relatively prime to $a$ form a group under multiplication.

Residue classes modulo $a$ in a principal ring forms a ring where elements can be represented with $0, 1, \ldots, a-1$. Obviously, excluding noninvertible elements from a ring yields a field. We thus show that only the elements relatively prime to $a$ are invertible modulo $a$. Let $(a, n) = 1$ for some ring element $n$, then there exist ring elements $r, s$ with $ar + ns = 1$, meaning $ns \equiv 1\ (a)$, i.e., the inverse of $n$ is $s$. Conversely, assume $n$ has an inverse in the residue classes modulo $a$, call it $s$. Then $ns = 1 + ap$ for some ring element $p$, meaning $ns - ap = 1$, meaning $1 = (n, s)$.

### Exercise 3.31

Prove that for all rings with unique factorization every two or more elements have a "greatest common divisor" and a "least common multiple," both of them being determined except for unit factors.

Let two elements of such a ring $a$ and $b$ have prime factorizations $a = \prod\limits_{v=1}^{n} p_v$ and $b = \prod\limits_{v=1}^{m} q_v$. Clearly, the prime factorization of a divisor should consist of prime factors present in the given number, so taking the common prime factors of $a$ and $b$ yields a divisor of $a$ and $b$. Our claim is that this divisor is the g.c.d.. Again, if some element divides $a$ and $b$ simultaneously, then its prime factors have to appear in both prime factorizations of $a$ and $b$, i.e., all prime factors of the divisor are common prime factors of $a$ and $b$, meaning it also divides the product of all common prime factors. The proof for the least common multiple is likewise.

## 8.7 Algebra by Waerden, Chapter 4

### Exercise 4.1

If we go over from one basis to $p_1, \ldots, p_n$ to another basis $e_1, \ldots, e_n$ of the same vector space and if the old basis elements $p_k$ are expressed in terms of the new basis elements $e_i$ with coefficients $p_k^i$:

$$p_k = \sum e_i p_k^i$$

then the new coordinates $'x^i$ of a vector $x$ are expressed in terms of the old coordinates by

$$'x_i = \sum p_k^i x^k$$

Let $x^k$ be the old coordinates of $x$, i.e.,

$$x = \sum p_k x^k.$$

Since each old basis vector can be expressed in terms of the new basis vectors, we may rewrite that as

$$x = \sum \left( \sum e_i p_k^i \right) x^k = \sum_k \sum_i e_i p_k^i x^k = \sum_i \sum_k e_i p_k^i x^k = \sum_i e_i \left( \sum_k p_k^i x^k \right)$$

Clearly, $'x_m$, the coefficient of some $e_m$, with $0 \leq m \leq n$ would be $\sum p_k^m x^k$.

## Exercise 4.2

The ordinary complex numbers $a + bi$ form a two-dimensional vector space over the field of real numbers.

We recognize the complex numbers as an additive Abelian group and move onto proving the vector space axioms. Let $a, b, r \in \mathbb{R}$ so that $a+bi \in \mathbb{C}$, then $(a + bi)r = ar + bri \in \mathbb{C}$ since $ar, br \in \mathbb{R}$. The second and third axioms follow from distributivity of multiplication of complex numbers over addition of complex numbers (since real numbers are also complex). The fourth axiom also follows from associativity of multiplication of complex numbers and the fifth axiom is also true since the unit elements of $\mathbb{R}$ and $\mathbb{C}$ are the same.

We now show that this vector space is indeed two-dimensional by considering the set of vectors $\{1, i\}$. Let $z \in \mathbb{C}$, i.e., there exist $a, b \in \mathbb{R}$ with $z = a+bi$, then, clearly, $z = a\cdot 1+b\cdot i$, so the vectors 1 and $i$ generate the vector space. We also have that none of the vectors can be expressed as a linear combination of another. (Since $r_1 \cdot 1$ always has zero as its imaginary part whereas $i$ has imaginary part 1, hence $i$ will never have that form and similarly $r_2 \cdot i$ has zero as its real part whereas 1 has real part 1, hence 1 will never have that form.) Thus the set of complex numbers form a two-dimensional vector space over the field of real numbers.

## Exercise 4.3

The continuous real functions $f(x)$ on the interval $0 \leq x \leq 1$ form a vector space which is not of finite rank over the field of real numbers.

Let $r \in \mathbb{R}$, $f : [0,1] \to \mathbb{R}$ be continuous and $x_0 \in [0,1]$, then $\lim\limits_{x \to x_0} rf(x) = r \lim\limits_{x \to x_0} f(x) = rf(x_0)$, i.e., the function $rf$ is also continuous. Now let $g : [0,1] \to \mathbb{R}$ also be continuous, then $(r(f+g))(x_0) = r(f+g)(x_0) = r(f(x_0) + g(x_0)) = rf(x_0) + rg(x_0) = (rf)(x_0) + (rg)(x_0)$, i.e., the functions $r(f+g)$ and $rf + rg$ are equal. Similarly, let $s \in \mathbb{R}$, then $((r+s)f)(x_0) = (r+s)f(x_0) = rf(x_0) + sf(x_0) = (rf)(x_0) + (sf)(x_0)$, i.e., the functions $(r+s)f$ and $rf+sf$ are equal. The fourth axiom follows from associativity of multiplication of functions (since real numbers can be identified with constant functions). The fifth axioms follows in the same manner.

We now prove that this vector space is not of finite rank by showing that for every nonnegative integer $n$ there is a linearly independent set of $n$ vectors. Our claim is that the set $\{1, x, \ldots, x^{n-1}\}$ is linearly independent. If $n = 0$, then we have the empty set, which is defined to be linearly independent. By induction, assume the set $\{1, x, \ldots, x^{n-1}\}$ is linearly independent. Let $a_0, \ldots, a_n$ be real numbers so with $a_0 + a_1 x + \cdots + a_n x^n = 0$ for all $x \in [0,1]$. Clearly, $a_0 = 0$ by letting $x = 0$, so we have $x(a_1 + \cdots + a_n x^{n-1}) = 0$ for all $x \in [0,1]$. Then $a_1 + \cdots + a_n x^{n-1} = 0$ for all $x \in (0,1]$. By continuity, this means $a_1 + \cdots + a_n x^{n-1} = 0$ for all $xin[0,1]$ and, by inductive hypothesis, $a_i = 0$ for all $i \in \{1, \ldots, n\}$. We also know that $a_0 = 0$, so $a_i = 0$ for all $i \in \{0, \ldots, n\}$, meaning the set is indeed linearly dependent.

## Exercise 4.4

The system (4.18) is solvable precisely when each linear dependence between the linear forms $a_i$ also holds for the $c_i$, that is, when

$$\sum b^i a_i = 0 \quad \text{implies} \quad \sum b^i c_i = 0$$

...

## Exercise 4.5

A system of $n$ homogeneous linear equations in $n$ unknowns has a non-trivial solution only if the linear forms $a_1, \dots, a_n$ are linearly dependent; that is, only if the "transposed system of linear equations"

$$\sum y^i a^{ik} = 0$$

has a nontrivial solution $(y^1, \dots, y^n)$.

By contrapositive, let $a_1, \dots, a_n$ be linearly independent. Then the solutions form a subspace of dimension $n - n = 0$, i.e., the only solution is the zero vector, which is the trivial solution.

## Exercise 4.6

The nonsingular linear transformations of a space $\mathfrak{M}$ into itself form a group.

Let the operation be composition. Let $R, S$ be nonsingular linear transformations of $\mathfrak{M}$ into itself with inverses $R^{-1}$ and $S^{-1}$ respectively. Then $RS$ is also linear a linear transformation as $RS(x + y) = R(S(x + y)) = R(S(x) + S(y)) = R(S(x)) + R(S(y)) = RSx + RSy$ and $RS(xc) = R(S(xc)) = R(S(x)c) = R(S(x))c = (RSx)c$ for all vectors $x, y \in \mathfrak{M}$ and scalars $c$. It is also invertible, namely, its inverse it $S^{-1}R^{-1}$. Associativity is true in general. The neutral element of this group is the identity transformation, i.e., $I : \mathfrak{M} \to \mathfrak{M}$ given by $I(x) = x$ for all $x \in \mathfrak{M}$. It is clearly a linear transformation and, for any linear transformation $A$ of $\mathfrak{M}$ into itself, we have $AIx = A(Ix) = Ax = I(Ax) = IAx$, so it is indeed the neutral element. The inverses exist for all elements by definition.

## Exercise 4.7

If for linear transformations of $\mathfrak{M}$ to $\mathfrak{R}$ we define the *sum* $A + B$ by

$$(A + B)x = Ax + Bx$$

then $A + B$ is again a linear transformation. Its matrix is the sum of the matrices $A$ and $B$; that is, its matrix elements are

$$c^i_k = a^i_k + b^i_k$$

The sum $A+B$ is a linear transformation as $(A+B)(x+y) = A(x+y)+B(x+y) = Ax+Ay+Bx+By = Ax+Bx+Ay+By = (A+B)(x)+(A+B)(y)$ and $(A + B)(xc) = A(xc) + B(xc) = A(x)c + B(x)c = (A(x) + B(x))c = (A + B)(x)c$ for all vectors $x, y \in \mathfrak{M}$ and scalars $c$.

For the matrix elements, let $a^i_k$, $b^i_k$ and $c^i_k$ be the matrix elements of the matrices of $A$, $B$ and $A + B$ respectively in the $i$th row and $k$th column. Then we have

$$\sum c^i_k x^k = (A + B)x = Ax + Bx = \sum a^i_k x^k + \sum b^i_k x^k = \sum (a^i_k + b^i_k)x^k$$

Hence we have $c^i_k = a^i_k + b^i_k$

## Exercise 4.8

The rank of $A^t$ is equal to the rank of $A$.

...

## Exercise 4.9

The rank of $A^t$ is also equal to the row rank of $A$, that is, equal to the number of linearly independent rows. The rows are here to be interpreted as the elements of a left vector space and the columns as elements of a right vector space.

The set of row vectors of $A^t$ matches the set of column vectors of $A$, so the number of independent vectors in each set is the same.

## Exercise 4.10

From Exercises 4.8 and 4.9 it follows that the row rank of a matrix $A$ is equal to its column rank.

Indeed.

## Exercise 4.11

A tensor of rank two is symmetric in $\mathbf{x}$ and $\mathbf{y}$, that is,

$$\mathbf{t} \cdot \mathbf{xy} = \mathbf{t} \cdot \mathbf{yx}$$

if and only if its coordinates are symmetric:

$$\mathbf{t}_{ik} = \mathbf{t}_{ki}$$

We first show that a tensor sends every pair to 0 only if all of its coordinates are 0. Let $\mathbf{t}$ be such a tensor, i.e., $\sum \mathbf{t}_{ik}\mathbf{x}^i\mathbf{y}^k = 0$ where $x^i, y^i$ are the $i$th coordinates of $\mathbf{x}$ and $\mathbf{y}$ respectively for all vectors $\mathbf{x}$ and $\mathbf{y}$. For every $1 \leq p, q \leq n$, choose $\mathbf{x}$ and $\mathbf{y}$ so that $\mathbf{x}^i = \delta_p^i$ and $\mathbf{y}^k = \delta_q^k$ so that $\sum \mathbf{t}_{ik}\mathbf{x}^i\mathbf{y}^k$ becomes $t_{pq}$ and we thus have $t_{pq} = 0$ for all $1 \leq p, q \leq n$.

Let $\mathbf{t}$ be a tensor of rank two that is symmetric in $\mathbf{x}$ and $\mathbf{y}$, i.e., $\mathbf{t} \cdot \mathbf{xy} = \mathbf{t} \cdot \mathbf{yx}$. Then $\sum \mathbf{t}_{ik}\mathbf{x}^i\mathbf{y}^k = \sum \mathbf{t}_{ik}\mathbf{y}^i\mathbf{x}^k$. In the second sum we may rename $i$ as $k$ and $k$ as $i$, so that it becomes $\sum \mathbf{t}_{ki}\mathbf{y}^k\mathbf{x}^i$ and $\sum \mathbf{t}_{ik}\mathbf{x}^i\mathbf{y}^k$ since our field is commutative. From $\sum \mathbf{t}_{ik}\mathbf{x}^i\mathbf{y}^k = \sum \mathbf{t}_{ki}\mathbf{x}^i\mathbf{y}^k$, it follows that $\sum(\mathbf{t}_{ik} - \mathbf{t}_{ki})\mathbf{x}^i\mathbf{y}^k = 0$ for all vectors $\mathbf{x}, \mathbf{y}$. According to our recent result, $\mathbf{t}_{ik} - \mathbf{t}_{ki} = 0$ for all $1 \leq i, k \leq n$, i.e., $\mathbf{t}_{ik} = \mathbf{t}_{ki}$.

Conversely, let $\mathbf{t}_{ik} = \mathbf{t}_{ki}$ for all $1 \leq i, k \leq n$. Then $\mathbf{t} \cdot \mathbf{xy} = \sum \mathbf{t}_{ik}x^iy^k = \sum \mathbf{t}_{ki}\mathbf{x}^i\mathbf{y}^k = \sum \mathbf{t}_{ik}\mathbf{x}^k\mathbf{y}^i = \sum \mathbf{t}_{ik}\mathbf{y}^i\mathbf{x}^k = \mathbf{t} \cdot \mathbf{yx}$.

## Exercise 4.12

The mixed tensors $\mathbf{a}$ of rank two with coordinates $a_k^i$ are in one-to-one correspondence with linear transformations of $\mathbf{A}$ of the space $\mathfrak{M}$ into itself with matrix elements $a_k^i$. This correspondence is given by

$$\mathbf{a} \cdot \mathbf{ux} = \mathbf{u} \cdot \mathbf{Ax}$$

invariant; that is, it is defined independently of the coordinate system.

The correspondence is trivial, we move onto solving for the matrix elements of $\mathbf{A}$ in $\mathbf{a} \cdot \mathbf{ux} = \mathbf{u} \cdot \mathbf{Ax}$. Rewriting both sides with sums, we obtain $\sum a_i^k u^i x_k = \sum u^i \cdot A_k^i x_k$ and $\sum (a_i^k - A_i^k) u^i x_k = 0$ and $a_i^k - A_i^k$ for all $1 \leq i, k \leq n$, meaning $a_i^k = A_i^k$.

### Exercise 4.13

A covariant tensor $\mathbf{g}$ with coordinates $g_{ik}$ defines a linear transformation $\mathbf{x} \to \mathbf{u}$ of the space into the dueal space $\mathfrak{M}*$ by the formula

$$\mathbf{u} \cdot \mathbf{z} = \mathbf{g} \cdot \mathbf{zx}$$

or

$$u_i = \sum g_{ik} x^k.$$

If the transformation is nonsingular, then it can be inverted:

$$x^k = \sum g^{kl} u_l$$

The product of the matrices $(g_{ik})$ and $(g^{kl})$ is then the identity matrix

$$\sum g_{ik} g^{kl} = \delta_i^l$$

...

## 8.8 Algebra by Waerden, Chapter 6

### Exercise 6.1

Prove for characteristic $p$ that

$$(a+b)^{p^f} = a^{p^f} + b^{p^f}$$

$$(a-b)^{p^f} = a^{p^f} - b^{p^f}$$

by the method of induction on $f$.

We shall prove the first iquality and then derive the other one using it. The base case, for $f = 1$, has already been proven, so we move onto the inductive step, Let $(a+b)^{p^f} = a^{p^f} + b^{p^f}$ for all field elements $a, b$ for some positive integer $f$. Then we have

$$(a+b)^{p^{f+1}} = (a+b)^{p^f \cdot p} = \left((a+b)^{p^f}\right)^p = \left(a^{p^f} + b^{p^f}\right)^p =$$

$$= \left(a^{p^f}\right)^p + \left(b^{p^f}\right)^p = a^{p^f \cdot p} + b^{p^f \cdot p} = a^{p^{f+1}} + b^{p^{f+1}}$$

Which finishes the proof by induction. Now, for the other equality,

$$a^{p^f} - b^{p^f} = ((a-b)+b)^{p^f} - b^{p^f} = (a-b)^{p^f} + b^{p^f} - b^{p^f} = (a-b)^{p^f}$$

For all field elements $a, b$ and positive integers $f$.

## Exercise 6.2

Similarly

$$(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_n^p.$$

The base case, for $n = 2$, has already been proven, so we move onto the inductive step. Assume that $(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_n^p$ for some positive integer $n$. Then we have

$$(a_1+a_2+\cdots+a_n+a_{n+1})^p = (a_1+a_2+\cdots+a_n)^p+a_{n+1}^p = a_1^p+a_2^p+\cdots+a_n^p+a_{n+1}^p$$

## Exercise 6.3

Apply Exercise 6.2 to a sum $1 + 1 + \cdots + 1$ modulo $p$.

By letting $a_v = e$ for all $v \in \{1, \ldots, n\}$, we obtain $(e+\cdots+e)^p = e+\cdots+e$ with $n$ number of $e$'s in each sum, giving up $n^p e = n^p e^p = (ne)^p = ne$, or, rewritten using modulo $p$, $n^p \equiv n \ (p)$.

## Exercise 6.4

Prove for characteristic $p$:

$$(a-b)^{p-1} = \sum_{j=0}^{p-1} a^j b^{p-1-j}.$$

We shall consider two cases, namely, $a-b=0$ or $a-b \neq 0$, i.e., $a-b$ is invertible. In the first case, we have

$$(a-b)^{p-1} = 0^{p-1} = 0 = pa^{p-1} = \sum_{j=0}^{p-1} a^{p-1} = \sum_{j=0}^{p-1} a^{j+p-1-j} =$$

$$= \sum_{j=0}^{p-1} a^j a^{p-1-j} = \sum_{j=0}^{p-1} a^j b^{p-1-j}$$

In the second case, as proven previously, we have $(a-b)^p = a^p - b^p$. We also know that $a^n - b^n = (a-b)\left(\sum\limits_{j=0}^{n-1} a^j b^{n-1-j}\right)$ for all positive integers $n$. Hence $(a-b)^p = (a-b)\left(\sum\limits_{j=0}^{p-1} a^j b^{p-1-j}\right)$. Given invertibility of $a-b$, we obtain $(a-b)^{p-1} = \sum\limits_{j=0}^{p-1} a^j b^{p-1-j}$.

## Exercise 6.5

For the case of a simple algebraic extension the irreduciblity of the minimal polynomial $\phi(x)$ as well as statements (a) to (e) are to be proved directly, that is, without using the law of homomorphism or the field properties of $\Delta[x]/(\phi(x))$. [The order of the propositions is: Irreduciblity, (c), (b), (a), (d), (e). For (a) use (c).]

...

## 8.9 Algebra by Waerden, Chapter 7

### Exercise 7.1

The intersection of two admissible groups is itself an admissible subgroup; the same is true for admissible normal divisors.

Let $\mathfrak{g}_1, \mathfrak{g}_2$ be admissible subgroups of a group $\mathfrak{G}$ relative to a set of operators $\Omega$. Obviously, the intersection of two subgroups is also a group. Let $x \in \mathfrak{g}_1 \cap \mathfrak{g}_2$, i.e., $x \in \mathfrak{g}_1$ and $x \in \mathfrak{g}_2$. Then, by definition of $\mathfrak{g}_1$ and $\mathfrak{g}_2$, we have $\Theta x \in \mathfrak{g}_1$ and $\Theta x \in \mathfrak{g}_2$ for all operators $\Theta \in \Omega$, meaning $\Theta x \in \mathfrak{g}_1 \cap \mathfrak{g}_2$. This shows that $\mathfrak{g}_1 \cap \mathfrak{g}_2$ admits the operators of $\Omega$ and is thus an admissible subgroup.

Now assume that $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are also normal subgroups and consider the same $x$ as before. Since $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are normal, we have $axa^{-1} \in \mathfrak{g}_1$ and $axa^{-1} \in \mathfrak{g}_2$ for all elements $a \in \mathfrak{G}$, meaning $axa^{-1} \in \mathfrak{g}_1 \cap \mathfrak{g}_2$. This shows that $\mathfrak{g}_1 \cap \mathfrak{g}_2$ is also closed under conjugation and is thus an admissible normal subgroup.

### Exercise 7.2

The product $\mathfrak{A}\mathfrak{B}$ of two admissible subgroups which commute is again an admissible subgroup. For modules we have in particular; The sum $(\mathfrak{A}, \mathfrak{B})$ of two admissible submodules is itself an admissible submodule.

Let $\mathfrak{g}_1, \mathfrak{g}_2$ be subgroups which commute of a group $\mathfrak{G}$. Let $a, b \in \mathfrak{g}_1\mathfrak{g}_2$, i.e., there exist $x, x' \in \mathfrak{g}_1$ and $y, y' \in \mathfrak{g}_2$ with $a = xy$ and $b = x'y'$. We then have $ba^{-1} = x'y'(xy)^{-1} = x'y'(y^{-1}x^{-1}) = x'(y'y^{-1})x^{-1} = x'x^{-1}(y'y^{-1}) \in \mathfrak{g}_1\mathfrak{g}_2$, meaning the product $\mathfrak{g}_1\mathfrak{g}_2$ is indeed a subgroup.

Now assume that $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are admissible relative to a set of operators $\Omega$. Let $a \in \mathfrak{g}_1\mathfrak{g}_2$, meaning there exist $x \in \mathfrak{g}_1$ and $y \in \mathfrak{g}_2$ such that $a = xy$. Then $\Theta a = \Theta(xy) = \Theta x \cdot \Theta y \in \mathfrak{g}_1\mathfrak{g}_2$ since $\Theta x \in \mathfrak{g}_1$ and $\Theta y \in \mathfrak{g}_2$ by definition. This shows that the subgroups $\mathfrak{g}_1\mathfrak{g}_2$ admits the operators of $\Omega$ and is thus an admissible subgroups.

Restating the assertion for modules yields the last result mentioned.

## Exercise 7.3

The ideals (1) and (2) in the ring of the integers are isomorphic modules, but not isomorphic rings.

Consider the mapping $\varphi : (1) \to (2)$ given by $\varphi : n \mapsto 2n$. Our claim is that this is a module isomorphism. It is clearly a bijection. The homomorphism property holds, $\varphi(n_1 + n_2) = 2(n_1 + n_2) = 2n_1 + 2n_2 = \varphi(n_1) + \varphi(n_2)$ for all integers $n_1, n_2$. Finally, since the set of operators is the set of ring elements, we have $\varphi(\Theta n) = 2\Theta n = \Theta(2n) = \Theta\varphi(n)$ for all integers $n$ and operators $\Theta$.

As rings, they are not isomorphic since one contains an identity whereas the other does not.

## Exercise 7.4

In the ring of the number pairs $(a_1, a_2)$ (Exercise 3.1) the ideals generated by $(1, 0)$ and $(0, 1)$ are isomorphism rings, but not isomorphic modules.

For such number pairs $z$ there exist integers $a, b$ with $z = (a, b)$, define $\overline{z} = (b, a)$ and consider the mapping $\varphi : ((1, 0)) \to ((0, 1))$ given by $\varphi : z \mapsto \overline{z}$. Our claim is that $\varphi$ is a ring isomorphism. It is clearly a bijection with the inverse map $\varphi^{-1} : ((1, 0)) \to ((0, 1))$ given by $\varphi^{-1} : z \mapsto \overline{z}$. It is also a homomorphism as $\varphi(z_1 + z_2) = \varphi((n_1, 0) + (n_2, 0)) = \varphi((n_1 + n_2, 0)) = (0, n_1 + n_2) = (0, n_1) + (0, n_2) = \varphi(n_1) + \varphi(n_2)$ and $\varphi(z_1 \cdot z_2) = \varphi((n_1, 0) \cdot (n_2, 0)) = \varphi((n_1 n_2, 0)) = (0, n_1 n_2) = (0, n_1) \cdot (0, n_2) = \varphi((0, n_1))\varphi((0, n_2))$ for all such elements $z_1, z_2$ of the ideal generated by $(1, 0)$ where $n_1, n_2$ are the integers such that $z_1 = (n_1, 0)$ and $z_2 = (n_2, 0)$. Thus $\varphi$ is a ring homomorphism and the ideals are isomorphic rings.

Now, assume that there is a module isomorphism $\omega : ((1, 0)) \to ((0, 1))$. Let $n$ be the integer such that $\omega((1, 0)) = (0, n)$ and consider $\Theta = (1, 2)$. Then $\omega\Theta(1, 0) = \omega(1, 0) = (0, n)$ whereas $\Theta\omega(1, 0) = \Theta(0, n) = (0, 2n)$. We clearly can't have $n = 0$ as $(0, 0)$ is already mapped by itself. By contradiction, the ideals are not isomorphic modules.

## Exercise 7.5

Show by means of the first law of isomorphism that the factor group of the symmetric group $\mathfrak{S}_4$ with respect to the four-group $\mathfrak{B}_4$ (Exercise 2.20) is isomorphic with the symmetry group $\mathfrak{S}_3$.

Via the first law of isomorphism we obtain $\mathfrak{S}_3\mathfrak{B}_4/\mathfrak{B}_4 \cong \mathfrak{S}_3/(\mathfrak{S}_3 \cap \mathfrak{B}_4)$ (we have already shown that $\mathfrak{B}_4$ is a normal subgroup of $\mathfrak{S}_4$). Obviously, the intersection is the trivial subgroup and factor group by the trivial subgroup is isomorphic to the original group itself, meaning we can rewrite the right handside as $\mathfrak{S}_3$. In Exercise 2.20 we have also noticed that the cosets of $\mathfrak{B}_4$ obtained by multiplying it by the elements of $\mathfrak{S}_3$ are the only its cosets, i.e., the product $\mathfrak{B}_4\mathfrak{S}_3$ is the group $\mathfrak{S}_4$ itself, so we obtain $\mathfrak{S}_4/\mathfrak{B}_4 \cong \mathfrak{S}_3$.

## Exercise 7.6

Show in like manner that in every permutation group which does not consist of even permutations alone, the even permutations form a normal divisor of index 2.

Via the first law of isomorphism we obtain $\mathfrak{H}_n\mathfrak{A}_n/\mathfrak{A}_n \cong \mathfrak{H}_n/(\mathfrak{H}_n \cap \mathfrak{A}_n)$ where $\mathfrak{H}_n$ is the subgroup generated by $(1, 2)$ of $\mathfrak{S}_n$. Clearly, the only even permutations in $\mathfrak{H}_n$ is the identity permutation, so $\mathfrak{H}_n \cap \mathfrak{A}_n$ is the trivial subgroup, making $\mathfrak{H}_n/(\mathfrak{H}_n \cap \mathfrak{A}_n) \cong \mathfrak{H}_n$. We now show that $\mathfrak{H}_n\mathfrak{A}_n$ is the group $\mathfrak{S}_4$. Let $\pi \in \mathfrak{S}_4$ be a permutation. If $\pi$ is an even permutation, it's already in $\mathfrak{A}_n$. If it's an odd function, then $\pi = (1\ 2)(1\ 2)\pi$; Since $(1\ 2) \in \mathfrak{H}_n$ and $(1\ 2)\pi \in \mathfrak{A}_n$, we still have $\pi \in \mathfrak{H}_n\mathfrak{A}_n$. Hence we have $\mathfrak{S}_4/\mathfrak{A}_n \cong \mathfrak{H}_n$, meaning the cosets of $\mathfrak{A}_n$ form a cyclic group of order two, so the subgroup $\mathfrak{A}_n$ is of index 2.

## Exercise 7.7

Show in like manner that the factor group of the Euclidean group of motions with respect to the normal divisor of the translations is isomorphic with the group of rotations about a point. [I assume Waerden to have meant the special Euclidean group as the assertion is false otherwise.]

Geometric intuition suggests that $\mathfrak{T}_n$ is a normal subgroup.

Let $\mathfrak{E}_n$, $\mathfrak{R}_n$ and $\mathfrak{T}_n$ be the special Euclidean group, subgroup of rotations and subgroup of translations respectively. Via the first isomorphism theorem, we get $\mathfrak{R}_n\mathfrak{T}_n/\mathfrak{T}_n \cong \mathfrak{R}_n/(\mathfrak{R}_n \cap \mathfrak{T}_n)$. Obviously, the only motion that's a rotation and a translation simultaneously is the identity motion and, also, $\mathfrak{R}_n\mathfrak{T}_n = \mathfrak{E}_n$, meaning we obtain $\mathfrak{E}_n/\mathfrak{T}_n \cong \mathfrak{R}_n$.

## Exercise 7.8

Every finite group possesses a composition series.

If every normal series of a finite group could be refined without, then we could pick a normal series without repetition of arbitrary length, however, finite groups have finite amount of subgroups.

## Exercise 7.9

Form all possible composition series of a cyclic group of order 20.

Let $a$ be the generating element of a cyclic group $\mathfrak{G}$ of order 20. Our claim is that the only composition series of are $\mathfrak{G} = \langle a\rangle \supset \langle a^2\rangle \supset \langle a^{10}\rangle \supset \{a^0\}$, $\mathfrak{G} = \langle a\rangle \supset \langle a^5\rangle \supset \langle a^{10}\rangle \supset \{a^0\}$ and $\mathfrak{G} = \langle a\rangle \supset \langle a^2\rangle \supset \langle a^4\rangle \supset \{a^0\}$ (All of which are, of course, isomorphic). It is a normal series as $\mathfrak{G}$ is abelian, so are its subgroup and so every subgroup is a normal in another subgroup as long as it is contained. The factors of the normal series are groups of prime order, which are simple, so the normal series are indeed composition series.

We now show that there are no other composition series. Let $\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \mathfrak{G}_3 \supset \mathfrak{G}_4$ (The length has been determined via Jordan-Holder theorem.), we can't have $\mathfrak{G}_1 = \langle a^4\rangle$ or $\mathfrak{G}_1 = \langle a^{10}\rangle$ as then the first factor is not a simple group, so we have cases $\mathfrak{G}_1 = \langle a^2\rangle$ or $\mathfrak{G}_1$ $\langle a^5\rangle$ (Every subgroup of a cyclic group is also cyclic). In the first case, $\mathfrak{G}_2$ can be either $\langle 4\rangle$ or $\langle a^{10}\rangle$ or $\{a^0\}$ as those are the only subgroups contained in $\langle a^2\rangle$; Obviously, we can't have $\mathfrak{G}_2 = \{a^0\}$ as $\langle a^2\rangle$ is not simple, so $\mathfrak{G}_2 = \langle a^4\rangle$ or $\mathfrak{G}_2 = \langle a^{10}\rangle$. In the second case, $\mathfrak{G}_2$ can be either $\langle a^{10}\rangle$ or $\{a^0\}$. Again, $\mathfrak{G}_2$ can't be the trivial group as $\langle a^5\rangle$ is not simple, so $\mathfrak{G}_2 = \langle a^{10}\rangle$.

## Exercise 7.10

An Abelian group (without operators) is simple only if it is cyclic of prime order.

Let $\mathfrak{G}$ be a simple Abelian group. Since $\mathfrak{G}$ is Abelian, every subgroup is normal and since $\mathfrak{G}$ is simple, the only normal subgroups are itself and the trivial subgroup; This means that we have only two subgroups. Let $a \in \mathfrak{G}$ be an nonneutral element and consider the subgroup generated by it. Obviously, the subgroup is not trivial, so $a$ generated the entire group $\mathfrak{G}$, meaning it is cyclic. Let $n$ be the order of $\mathfrak{G}$ and $n = bc$ for some positive integers $b, c$. Since the subgroups $\left\langle a^b \right\rangle$ and $\langle a^c \rangle$ should be either trivial or the entire $\mathfrak{G}$, we have that $b$ is a multiple of $n$ or $(b, n) = 1$. In the first case we end up with $c = 1$. In the second case $b = 1$. This shows that $n$ is prime.

## Exercise 7.11

In any composition series of a finite solvable group the composition factors are cyclic of prime order.

By definition, solvable group has a normal series with every factor an Abelian group. Refining the normal series preserves this property, meaning in the composition series every composition factor is Abelian. Also, every composition factor is simple by definition. According to the previous exercise, every composition factor in the composition series should be cyclic of prime order.

## Exercise 7.12

If $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, $\mathfrak{G}'$ is a subgroup of $\mathfrak{G}$, and $\mathfrak{G}' \supseteq \mathfrak{A}$, then $\mathfrak{G}' = \mathfrak{A} \times \mathfrak{B}'$, where $\mathfrak{B}'$ is the intersection of $\mathfrak{G}'$ and $\mathfrak{B}$.

Since $\mathfrak{A}$ is normal in $\mathfrak{G}$, i.e., is closed under conjugation by every $g \in \mathfrak{G}$, then it is also closed under conjugation by every $g \in \mathfrak{G}'$, i.e., is normal in $\mathfrak{G}'$ (since we also have $\mathfrak{A} \subseteq \mathfrak{G}'$). Similarly, $\mathfrak{B}$ is closed under conjugation by every $g \in \mathfrak{G}'$ and so is the subgroup $\mathfrak{B}' = \mathfrak{B} \cap \mathfrak{G}'$. We also have $\mathfrak{B}' \subseteq \mathfrak{G}'$, so $\mathfrak{B}'$ is normal in $\mathfrak{G}'$. Let $g' \in \mathfrak{G}'$ be written as the product $ab$ with $a \in \mathfrak{A}$ and $b \in \mathfrak{B}$. Since $\mathfrak{A} \subseteq \mathfrak{G}'$, we have $a \in \mathfrak{G}'$, $b \in \mathfrak{G}'$ follows. Thus $\mathfrak{g} \in \mathfrak{A}\mathfrak{B}'$, so $\mathfrak{G}' \subseteq \mathfrak{A}\mathfrak{B}'$ and, since the converse holds, $\mathfrak{G}' = \mathfrak{A}\mathfrak{B}'$. Finally, $\mathfrak{A} \cap \mathfrak{B}' = \mathfrak{A} \cap (\mathfrak{B} \cap \mathfrak{G}') = (\mathfrak{A} \cap \mathfrak{B}) \cap \mathfrak{G}' = \{e\} \cap \mathfrak{G}' = \{e\}$ where $e$ is the neutral element. Hence $\mathfrak{G}' = \mathfrak{A} \times \mathfrak{B}'$.

## Exercise 7.13

A cyclic group $\{a\}$ of order $n = r \cdot s$ with $(r, s) = 1$ is the direct product of its subgroups $\{a^r\} \cdot \{a^s\}$ of orders $s$ and $r$.

In Exercise 3.23 (Waerden), we have shown that every element of order $r \cdot s$ in a group is the product of a uniquely determined $a^{\lambda r}$ and $a^{us}$ of orders $s$ and $r$ respectively provided $(r, s) = 1$. Also, every element from $\langle a^r \rangle$ commutes with every element from $\langle a^s \rangle$ since the group generated by $a$ is cyclic by definition. Via alternate definition of the direct product, we obtain $\langle a \rangle = \langle a^r \rangle \times \langle a^s \rangle$.

## Exercise 7.14

A finite cyclic group is the direct product of its subgroups of the highest possible prime power orders.

Let $\mathfrak{G}$ be a finite cyclic group with order $n$ whose prime factorization is $p_1^{r_1} \cdots p_k^{r_k}$ with each $p_i$ distinct. By induction on $k$ we shall show that $\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_k$ with $|\mathfrak{G}_i| = p_i^{r_i}$ for all $i \in \{1, \ldots, k\}$. The base case is trivial. Assume the assertion is true for some $k$ and let $\mathfrak{G}$ be a finite cyclic group of order $p_1^{r_1} \cdots p_k^{r_k} p_{k+1}^{r_{r+1}}$ with each $p_i$ distinct. Clearly, we have $(p_1^{r_1} \cdots p_k^{r_k}, p_{k+1}^{r_{k+1}}) = 1$ and, according to the previous exercise, $\mathfrak{G}$ is the direct product of a subgroups $\mathfrak{G}'$ and $\mathfrak{G}_{k+1}$ of order $p_1^{r_1} \cdots p_k^{r_k}$ and $p_{k+1}^{r_{k+1}}$. The former is a finite cyclic group, so it can be rewritten as the direct product $\mathfrak{G}_1 \times \cdots \times G_k$ with $|G_i| = p_i^{r_i}$ for all $i \in \{1, \ldots, k\}$. We thus have $\mathfrak{G} = \mathfrak{G}_1 \times \cdots \times \mathfrak{G}_{k+1}$ with orders of each factor as desired.

## Exercise 7.15

Prove that, for $n \neq 4$, the alternating group $\mathfrak{A}_n$ is the only normal divisor of the symmetric group $\mathfrak{S}_n$, except the latter itself and the trivial group.

We have already shown that for $n = 2$ and $n = 3$, so we may let $n > 4$. Let $\mathfrak{N}$ be a nontrivial normal subgroup of $\mathfrak{S}_n$. The proof is the same as the one of the lemma given in the book since it mostly used the fact that $\mathfrak{N}$ must be closed under conjugation by even permutations. The only change that we need to do is consider the case when a product of two disjoint transpositions is present in $\mathfrak{N}$. Without the loss of generality, let $(1\ 2)(3\ 4) \in \mathfrak{N}$. Then, via normality, we have $(2\ 5)(3\ 4) = (1\ 2\ 5)(1\ 2)(3\ 4)(1\ 2\ 5)^{-1} \in \mathfrak{N}$ and $(1\ 2\ 5) = (1\ 2)(3\ 4)(2\ 5)(3\ 4) = \mathfrak{N}$. By conjugations we, per usual, conclude that every 3-cycle is present in $\mathfrak{N}$ and, since $\mathfrak{A}_n$ is generated by those cycles, we have $\mathfrak{A}_n \subseteq \mathfrak{N}$. As we already know, $\mathfrak{S}_n/\mathfrak{A}_n$ is simple, so $\mathfrak{N}$ is either the alternating group or $\mathfrak{S}_n$ itself.

## Exercise 7.16

If the number of elements in the set $\mathfrak{M}$ is a prime number, every transitive group is primitive.

By contradiction, assume $\mathfrak{M}$ is primitive with imprimitive systems $\mathfrak{M}_1, \ldots, \mathfrak{M}_k$. Each system has the same number of elements call it $n > 1$. Then $|M| = nk$ and, since we also have $k > 1$, this contradicts the number of elements in $\mathfrak{M}$ being prime. Hence $\mathfrak{M}$ is primitive.

## Exercise 7.17

The group $\mathfrak{h}$ defined above is transitive over $\mathfrak{M}_1$. [For context, see the book.]

Let $a, a' \in \mathfrak{M}_1$. Via transitivity of $\mathfrak{G}$, there exists a permutation that sends $a$ to $a'$. That permutation also belongs to $\mathfrak{h}$ as it should leave $\mathfrak{M}_1$ invariant.

## Exercise 7.18

Let the set $\mathfrak{M}$ be divided into three systems of imprimitivity, each having two elements; let the group $\mathfrak{G}$ be of order 12. What is

a. The index of $\mathfrak{h}$ in $\mathfrak{G}$;

b. The index of $\mathfrak{g}$ in $\mathfrak{h}$;

c. The order of $\mathfrak{g}$?

[For context, see the book.]

Let $\mathfrak{M}$ have the systems of imprimitivity $\{a, b\}$, $\{c, d\}$ and $\{e, f\}$. Since there is a one-to-one correspondence between the cosets of $\mathfrak{g}$ and elements of $\mathfrak{M}$, we know that the index of $\mathfrak{g}$ is 6 and thus its order is 2. Now, consider the set $\mathfrak{h} \setminus \mathfrak{g}$. Since $a$ is not fixed by any permutation in that complex, but it must stay within $\{a, b\}$, every permutation in $\mathfrak{h} \setminus \mathfrak{g}$ maps $a$ to $b$. In fact, $\mathfrak{h} \setminus \mathfrak{g}$ is the subset of $\mathfrak{G}$ of permutations mapping $a$ to $b$, meaning it is some coset of $\mathfrak{g}$ and has order 2. Therefore $\mathfrak{h}$ has 4 elements, meaning its index in $\mathfrak{G}$ is 3 and, also, the index of $\mathfrak{g}$ in $\mathfrak{h}$ is 2.

## Exercise 7.19

The order of a transitive group of permutations of a finite number of objects is divisible by the number of these objects.

Let a nonempty set $\mathfrak{M}$ have transitive group of permutations $\mathfrak{G}$ and $\mathfrak{G}_a$ be the subgroup of permutations that fix a fixed element $a \in \mathfrak{M}$. As we already know, its cosets are in one-to-one correspondence with the element of $\mathfrak{M}$, so the order of $\mathfrak{G}_a$ is $\mathfrak{M}$. Via Lagrange theorem, $\mathfrak{M}$ thus divides the order of the group $\mathfrak{G}$.

# 8.10 Definitions

**Definition 63** (Binary operation)**.** *Let $A$ be a set. A mapping $*$ is a binary operation on $A$ if and only if its domain and codomain are $A \times A$ and $A$ respectively.*

**Definition 64** (Associativity)**.** *A binary operation $*$ on $M$ is associative on $M$ if and only if $a * (b * c) = (a * b) * c$ for all $a, b, c \in M$.*

**Definition 65** (Neutral element/Identity)**.** *An element $e \in M$ is a left neutral element if and only if $e * a = a$ for all $a \in M$.*

*An element $e \in M$ is a right neutral element if and only if $a * e = a$ for all $a \in M$.*

*An element $e \in M$ is a neutral element if and only if $e$ is a left neutral element and a right neutral element.*

*The term "identity" is synonimous to "neutral element".*

**Definition 66** (Commutativity)**.** *Elements $a, b$ of $M$ commute with respect to a binary operation $*$ on $M$ if and only if $a * b = b * a$.*

*A binary operation $*$ on $M$ is commutative if and only if all $a, b \in M$ commute with respect to $*$.*

**Definition 67** (Solvability)**.** *Let $M$ be a set and $*$ a binary operation on $M$. The equations $a * x = b$ and $y * a = b$ with some $a, b \in M$ are solvable for $x$ and $y$ if and only if there exist $x, y \in M$ satisfying those equations respectively. The elements $x, y$ defined as above are called solutions to the equations respectively. A solvable equation is uniquely solvable if and only if the solutions are unique.*

**Definition 68** (Inverses)**.** *An element $a'$ is an left inverse of $a$ with respect to a binary operation $*$ if and only if $a' * a = e$ where $e$ is the neutral element of $*$.*

*An element $a'$ is a right inverse of $a$ with respect to a binary operation $*$ if and only if $a' * a = e$ where $e$ is the neutral element of $*$.*

*An element $a'$ is an inverse of $a$ with respect to a binary operation $*$ if and only if $a'$ is a left and right inverse of $a$ with respect to $*$.*

*An element $a \in S$ is invertible with respect to a binary operation $*$ in $S$ if and only if there exists $a' \in M$ where $a'$ is an inverse of $a$ with respect to $*$.*

**Definition 69** (Magma)**.** *Let $M$ be a set and $*$ be a binary operation on $M$. Then $(M, *)$ is a magma. Sometimes we may write that $M$ is a magma if the operation is clear from the context.*

**Definition 70** (Semi-group)**.** *A magma $(M, *)$ is a semi-group if $*$ is associative on $S$.*

**Definition 71** (Unital magma)**.** *A magma $(M, *)$ is unital magma if and only if $M$ contains a neutral element of $*$.*

**Definition 72** (Quasigroup)**.** *A magma $(M, *)$ is a quasigroup if and only if for all $a, b \in M$ the equations $a * x = b$ and $y * a = b$ are uniquely solvable for $x, y$.*

**Definition 73** (Monoid)**.** *$(S, *)$ is a monoid if and only if it is a semi-group and a unitral magma with respect to the same operation.*

**Definition 74** (Associative quasigroup)**.** *$(A, *)$ is an associative quasigroup if and only if it is a quasigroup and a semi-group with respect to the same operation.*

**Definition 75** (Loop)**.** *$(L, *)$ is a loop if and only if it is a quasigroup and a unitral magma with respect to the same*

**Definition 76** (Group)**.** *$(G, *)$ is a group if and only if $(G, *)$ is a monoid with all elements invertible.*

*$(G, *)$ is also an Abelian group given $*$ is commutative on $G$.*

**Definition 77** (Subgroup)**.** *A subset $H$ of a group $G$ is a subgroup of $G$ if and only if $H$ with the same binary operation is a group.*

**Definition 78** (Coset)**.** *A subset of a group $G$ is a left/right coset of a subgroup $H$ of $G$ if and only if all its elements are of the form $ah/ha$ for some $h \in H$ and a fixed $a \in G$. The coset is denoted by $aH$ or $Ha$ respectively.*

**Definition 79** (Index)**.** *The index of a subgroup of a group is the number of its left cosets within that group.*

**Definition 80** (Conjugate, conjugacy class)**.** *Elements $a, b$ of a group are conjugate if and only if there exists an element $g$ of the same group with $a = gbg^{-1}$.*

*A subset of the group is the conjugacy class of $a$ if and only if it contains every elements of the group conjugate to $a$.*

**Definition 81** (Normal subgroup)**.** *A subgroup $H$ of $G$ is normal if and only if it is classed under conjugation by any element of $G$.*

**Definition 82** (Factor group)**.** *Let $H$ be a normal subgroup of a group $G$. The group formed by the cosets of $H$ is a factor group of $G$ denoted by $G/H$.*

**Definition 83** (Order)**.** *Let $a \in G$ with $G$ a group. If $a^n$ is the identity element for some integer $n$, then the order of $a$ denoted by $O(a)$ is the smallest positive $n$ with that property. Otherwise the order of $a$ is $\infty$.*

*The order of a group is its cardinality.*

**Definition 84** (Group homomorphism/isomorphism)**.** *A $\varphi : G \to G'$ is a group homomorphism if and only if $G, G'$ are groups and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.*

*A mapping is a group isomorphism if and only if it is a group homomorphism and is bijective. The domain and codomain are then isomorphic groups.*

**Definition 85** (Center)**.** *The center of a group is the subset of the group with elements that commute with every other elements of the group.*

**Definition 86** (Ring)**.** *$(R, +, \cdot)$ where $+$ and $\cdot$ are binary operations on $R$ is a ring if and only if $(R, +)$ is an Abelian group and $(R, \cdot)$ is a semi-group. A ring is also unital if $(R, \cdot)$ is a monoid and commutative if $\cdot$ is commutative on $R$.*

**Definition 87** (Unit)**.** *An element of a ring $(R, +, \cdot)$ is a unit if and only if it is invertible with respect to $\cdot$.*

**Definition 88** (Field)**.** *A ring is a field if and only if every its nonzero element is a unit.*