DS Final Exams solutions

Irakli Diasamidze

Contents

Chapter 1

Final Exam 2022-2023

1.1 Group 5

Problem 1

Let $X = \{4, -1, -2\}$. Determine $X \cap \mathcal{P}(X)$.

Since $\mathcal{P}(X)$ contains sets whereas X contains number, they have no elements in common, i.e., $X \cap \mathcal{P}(X) = \varnothing$.

Problem 2

Show that $A \setminus B = (A \cup B) \setminus B$.

Let $x \in A \setminus B$, i.e., let $x \in A$ such that $x \notin B$. Since $x \in A$ holds, so does the statement "$x \in A$ or $x \in B$", meaning we have $x \in A \cup B$ with $x \notin B$, i.e., $x \in (A \cup B) \setminus B$. This shows that $A \setminus B \subseteq (A \cup B) \setminus B$.

Let $x \in (A \cup B) \setminus B$, i.e., let $x \in A \cup B$ and $x \notin B$. Since $x \notin B$ and $x \in A$ or $x \in B$, $x \in A$, meaning we have $x \in A$ with $x \notin B$, i.e., $x \in A \setminus B$. This shows that $(A \cup B) \setminus B \subseteq A \setminus B$.

Since $A \setminus B \subseteq (A \cup B) \setminus B$ and $(A \cup B) \setminus B \subseteq A \setminus B$, we have $A \setminus B = (A \cup B) \setminus B$.

Problem 3

Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ which is injective.

The identity function on $\mathbb{R}$.

Problem 4

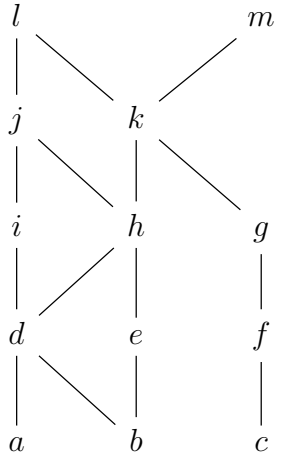
Show that the relation $R = \varnothing$ on a nonempty set S is symmetric, but not reflexive.

Reflexivity states that if $(a, b) \in R$, then $(b, a) \in R$. Since R, in this case, is empty, the premise never holds, making the implication true. Hence R is symmetric.

Since S is nonempty, there exists $a \in S$. We have $(a, a) \notin R$ as R is empty, making R not reflexive.

Problem 5

Find all minimal elements for the partial order represented by this Hasse diagram on Figure 1. Is there a smallest element?



The minimal elements of the given poset are a, b and c as there does not exist an element below each.

If there was a smallest element, there would be exactly one minimal element.

Problem 6

Is $(\mathbb{Z}, =)$ a partial order? Explain.

The relation $=$ is reflexive, symmetric and transitive on any arbitrary set S, making $(\mathbb{Z}, =)$ indeed a partially ordered set.

Problem 7

How many elements are in the set $B(5)$?

In general, $B(n)$ contains 2^n elements, making the number of elements in $B(5)$ equal to $2^5 = 32$.

Problem 8

Construct the Conjunctive Normal Form for a function $f : B(3) \to \{0, 1\}$ given by

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

We begin by identifying all inputs $(x, y, z) \in B(3)$ such that $f(x, y, z) = 0$. The latter can be rewritten as $(x \to \neg z) \wedge (\neg y \to z) = 0$. By definition of conjunction, we have $x \to \neg z = 0$ or $\neg y \to z$. By definition of implication, we have $x = 1$, $\neg z = 0$ or $\neg y = 1$, $z = 0$. The first case yields the inputs $(1, 0, 1)$ and $(1, 1, 1)$. The second case yields the inputs $(0, 1, 1)$ and $(1, 1, 1)$. The maxterms of $(0, 1, 1)$, $(1, 1, 0)$ and $(1, 1, 1)$ are $x + y' + z'$, $x' + y' + z$ and $x' + y' + z'$ respectively. This makes the Conjunctive Normal Form of f be the following.

$$f(x, y, z) = (x + y' + z')(x' + y' + z)(x' + y' + z')$$

Problem 9

How many different ways are there to choose 3 out of the 6 pairs of shorts that you will take on your vacation?

In general, the number of ways to choose k out of n items is $\binom{n}{k}$. The latter is equal to $\frac{n!}{k!(n-k)!}$, making the number of different ways to choose 3 out of 6 pairs of shorts equal to $\binom{6}{3} = \frac{6!}{3!(6-3)!} = \frac{4 \cdot 5 \cdot 6}{6} = 20$.

Problem 10

How many functions are there from the set $\{-2, 1, 1120\}$ to the set $\{4, -3, 0, 14\}$?

In general, given finite sets A, B, the number of functions $f : A \to B$ is $|B|^{|A|}$, making the number of functions from the set $\{-2, 1, 1120\}$ to the set $\{4, -3, 0, 14\}$ equal to $4^3 = 64$ as $|\{-2, 1, 1120\}| = 3$ and $|4, -3, 0, 14| = 4$.

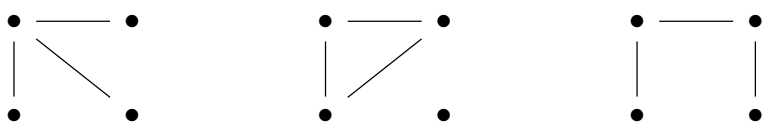
Problem 11

Give an example of function $f : \mathbb{N} \to \mathbb{R}$ such that $f = O(3x^5 + 1)$.

$f(x) = 3x^5 + 1$.

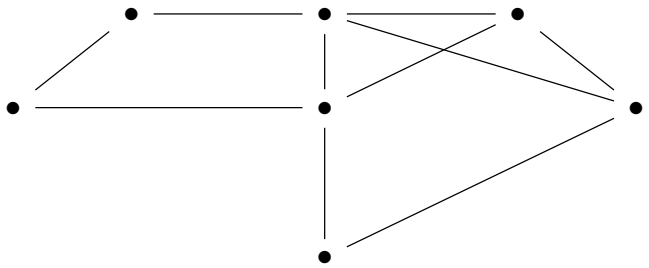
Problem 12

Sketch two graphs with 4 vertices and 3 edges that are *not* isomorphic.



Problem 13

How many rows does an adjacency matrix of the graph on Figure 1 have?



The number of rows in an adjancency matrix is always equal to the number of vertices in a graph. The given graph has 7 vertices, its adjacency matrix thus has 7 rows.

Problem 14

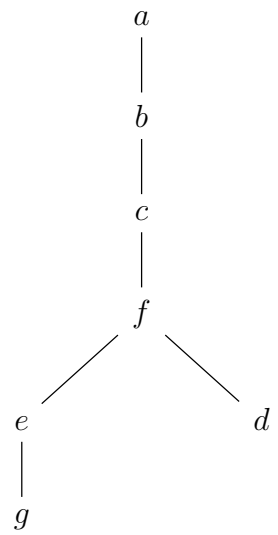
Say $G = (V, E)$ with $|V| = 5$. Sketch $G \setminus E$.

Problem 15

Perform Depth-First search to find a spanning tree (if it exists) on a graph by the following list of neighbours

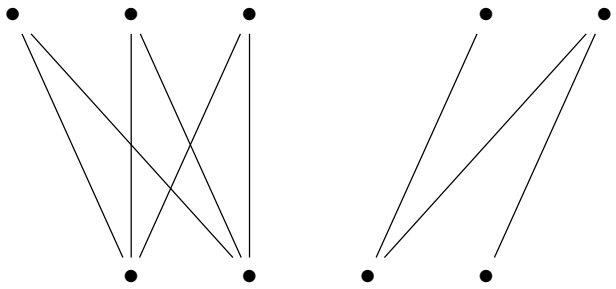
a	b	c	d	e	f	g
b	a	b	b	b	c	e
	c	f	f	f	d	
	d			g	e	
	e					

With Depth-First search, one may obtain the following spanning tree.

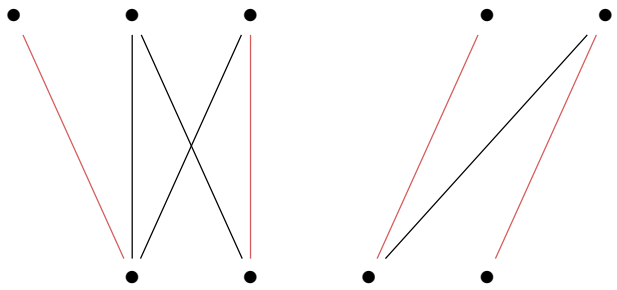


Problem 16

Does there exist a matching of size 4 for the graph on Figure 2. Explain your answer.



There exists a matching of size 4 for the given graph, namely, the one visualized (in red) below.



Problem 17

Is M a maximal matching if we can *not* find any M-alternating paths? Explain.

During the lecture we have proven a theorem stating that a matching M is maximal if and only if there is no M-alternating path in the given graph. It hence follows that if there is no M-alternating path, M is not a maximal matching.

Problem 18

Determine whether $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $a * b := 3a + 2b$ possesses a neutral element.

By contradiction, assume that there is a neutral element $e \in \mathbb{R}$. Then

$$0 = 1 - 1 = 1 * e - 1 = 3 \cdot 1 + 2e - 1 = 2 + 2e$$

Implying $e = -1$. However, $0 * e = 0 * (-1) = 3 \cdot 0 + 2(-1) = 0 - 2 = -2 \neq 0$. Contradicting the definition of e. Thus no neutral element exists.

Problem 19

Identify the subgroup of $(\mathbb{Z}_6, +)$ of order 2.

$\{0, 3\}$ is a subgroup of $(\mathbb{Z}_6, +)$ with order 2. We now claim that it is the only subgroup of order 2. Let $H \subseteq \mathbb{Z}_6$ with $|H| = 2$. Every group of order 2 contains a neutral element and an element of order 2. The only element in $\mathbb{Z}_6$ of order 2 is 3, making $H = \{0, 3\}$.

Problem 20

Perform the following calculation in $\mathbb{Z}_{13}$.

$$-10 \cdot (4 \cdot 4 + 6)$$

$$-10 \cdot (4 \cdot 4 + 6) \equiv 3 \cdot (16 + 6) \equiv 3 \cdot (3 + 6) = 3 \cdot 9 = 27 \equiv 1 \mod 13$$

Problem 21

Find all units of $\mathbb{Z}_{12}$.

The elements of $\mathbb{Z}_{12}$ are $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$. Since the prime factorization of 12 is $2^2 \cdot 3$, extracting all multiples of 2 and 3 leaves us with exactly the integers coprime to 12. The invertible elements are thus $1, 5, 7, 11$.

Problem 22

Is every infinite group cyclic? Explain?

The additive group of rational numbers is an infinite group that is not cyclic.

Pick an arbitrary $q \in \mathbb{Q}$ and consider $\langle q \rangle$. There exists no integer n with $nq = \frac{q}{2}$ (by contradiction, we would have $2n = 1$.), meaning $\mathbb{Q} \not\subseteq \langle q \rangle$. Thus no rational q is a generator of $\mathbb{Q}$. (In fact, $\mathbb{Q}$ is not even finitely generated.)

Problem 23

Decompose

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

into a product of disjoint cycles.

We see that the given permutation has mappings $1 \mapsto 4$, $4 \mapsto 3$ and $3 \mapsto 1$, meaning the 3-cycle $(1, 4, 3)$ will be a term in the decomposition. We also have the mappings $2 \mapsto 5$ and $5 \mapsto 2$, meaning the transposition $(2, 5)$ will also appear in the decomposition. We have exhausted all the elements, thus the algorithm halts and we obtain $(1, 4, 3)(2, 5)$.

Problem 24

Show that $2x^2 - 6$ is irreducible over $\mathbb{Q}[x]$.

Assume, by contradiction, that $2x^2-6$ is irreducible in $\mathbb{Q}[x]$. Since $2x^2-6$ has degree 2, it would be reducible into linear factors, implying that there exists $q \in \mathbb{Q}$ with $2q^2 - 6 = 0$. The latter implies that there exist coprime integers (since any rational number can be written in lowest terms) $a, b \in \mathbb{Z}$ with $2\left(\frac{a}{b}\right)^2 - 6 = 0$. Rewriting the equation yields $a^2 = 3b^2$. $3b^2$ is divisible by 3 and so is a^2. Since $\mathbb{Z}_p$ has no zero divisors with p a prime and since 3 is prime, this implies a to be divisible by 3, i.e., there exists $k \in \mathbb{Z}$ with $a = 3k$. The equation can now be rewritten as $(3k)^2 = 3b^2$, $9k^2 = 3b^2$ and $3k^2 = b^2$. Using the same reasoning as before, b is divisible by 3. This makes 3 a common divisor of a and b, forcing the gcd of a and b to be greater than 1, which is a contradiction. Thus $2x^2 - 6$ is irreducible in $\mathbb{Q}[x]$.

Problem 25

Write out Cayley table for addition for a four-element field.

See the last central Problem of week 14.

Problem 26

Two groups $(G, \cdot)$ and $(H, *)$ are *isomorphic* if there exists a bijection $f : G \to H$ such that $f(x \cdot y) = f(x) * f(y)$ for all $x, y \in G$. In other words, f maps neutral element to neutral element and Cayley tables of G and H are the same up to "renaming".

How many non-isomorphic groups are there with exactly 3 elements? How many non-isomorphic groups are there with exactly 4 elements? [The author is assumed to be asking for the number of isomorphism classes as for any given order of a group infinitely many pairs of non-isomorphic groups can be provided.]

We claim that, up to "renaming", there is only one group with exactly 3 elements by showing that every group of order 3 is isomorphic to $\mathbb{Z}_3$. Name the elements e, a, b. Without the loss of generality, assume e to be the neutral element. We can't have $a^2 = e$ as 2 does not divide 3 (recall an implication of Lagrange's theorem), hence $a^2 = b$ and $a^3 = e$ (recall another implication of Lagrange's theorem). We now construct a mapping $f : \{e, a, b\} \to \mathbb{Z}_3$ given by $f(e) = 0$, $f(a) = 1$ and $f(a) = 2$. We have $f(a^2) = f(b) = 2 = 1 + 1 = f(a)+f(a)$, $f(b^2) = f(bb) = f(a^2a^2) = f(a^4) = f(a) = 1 = 2+2 = f(b)+f(b)$ and $f(ab) = f(e) = 0 = 1 + 2 = f(a) + f(b)$ (the first equation follows from the fact that we can't have $ab = a$ nor $ab = b$ as they imply that $b = e$ and $a = e$ respectively.) The rest is taken care of by commutativity or triviality. f is clearly a surjection from sets of equal cardinality, making it bijective. Finally, existence of f implies that $\{e, a, b\}$ and $\mathbb{Z}_3$ are isomorphic.

We claim that, up to "renaming", there are only two groups with exactly 4 elements by showing that every group of order 4 is isomorphic to either $\mathbb{Z}_4$ (the latter two are not isomorphic as $\mathbb{Z}_4$ contains an element of order 4, namely, 1, whereas the Klein four group does not). Name the elements e, a, b, c. Without the loss of generality, assume e to be the neutral element. We consider two cases, namely, there exists an element of order 4 or it does not.

In the first case, without the loss of generality, let $O(a) = 4$. Due to minimality of $O(a)$, we can't have $a^2 = e$. Without the loss of generality, assume $a^2 = b$ and $a^3 = c$ (we can't have $a^2 = a^3$). We now construct a mapping $f : \{e, a, b, c\} \to \mathbb{Z}_4$ given by $f(e) = 0$, $f(a) = 1$, $f(b) = 2$ and

$f(c) = 3$. We have the following.

$$
\begin{aligned}
f(aa) = f(a^2) = f(b) = 2 = 1 + 1 = f(a) + f(a) \\
f(ab) = f(aa^2) = f(a^3) = f(c) = 3 = 1 + 2 = f(a) + f(b) \\
f(ac) = f(aa^3) = f(a^4) = f(e) = 0 = 4 = 1 + 3 = f(a) + f(c) \\
f(bb) = f(a^2a^2) = f(a^4) = f(e) = 0 = 4 = 2 + 2 = f(b) + f(b) \\
f(bc) = f(a^2a^3) = f(a^5) = f(a) = 1 = 5 = 2 + 3f(b) + f(c)
\end{aligned}
$$

f is clearly a surjection from sets of equal cardinality, making it bijective. Finally, existence of f implies that $\{e, a, b, c\}$ and $\mathbb{Z}_4$ are isomorphic.

In the other case, $O(a) = O(b) = O(c) = 2$, i.e., $a^2 = b^2 = c^2 = e$. We can't have $ab = e$ as it would imply $a = b$. Thus $ab = c$ and, similarly, $ac = b$ and $bc = a$. The Cayley table of $\{e, a, b, c\}$ is thus as follows.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Which matches the Cayley table of Klein four group as defined during the lecture but with 1 renamed as e. Therefore $\{e, a, b, c\}$ and the Klein four group are isomorphic.

1.2 Group 6

Problem 1

Write down a seven element subset of the set of integers $\mathbb{Z}$.

$\{534, 1729, 5050, 6174, 31415, 8080174247945128758864599049617107570057543680 \cdot 10^9, 1.201 \cdot 10^{57}\}$ is a subset of $\mathbb{Z}$ with exactly seven elements.

Problem 2

Let $f : \mathbb{N} \to \mathbb{N}$ be a function given by $f(n) = 3n$. Determine $f^{-1}(\{4, 5, 6, 7, 8, 9, 10\})$.

Clearly, the integers in im f are multiples of 3, meaning $f^{-1}(\{4, 5, 6, 7, 8, 9, 10\}) = f^{-1}(\{6, 9\})$. Since f is injective, $f(2) = 3 \cdot 2 = 6$ and $f(3) = 3 \cdot 3 = 9$, we have $f^{-1}(\{6, 9\}) = \{2, 3\}$.

Problem 3

Is the relation

$$R = \{(a, b) \in \mathbb{N}_0 \times \mathbb{N}_0 : a \text{ divides } b\}$$

on the set of non-negative integers transitive? Explain your answer.

Let $(a, b) \in R$ and $(b, c) \in R$ for some $a, b, c \in \mathbb{N}_0$, i.e., let a divide b and b divide c. By definition of divisibility, there exist $x, y \in \mathbb{Z}$ with $b = ax$ and $c = by$. This implies that $c = by = (ax)y = a(xy)$, meaning a divides c, i.e., $(a, c) \in R$. Hence R is indeed transitive.

Problem 4

How many equivalence relations are there on the set $X = \{1, -7, -2\}$? Explain.

In general, the number of equivalence relations on a finite is equal to the number of partitions of that set. We shall hence identify all partitions P of $\{1, -7, -2\}$. If P contains exactly one set, then, obviously, it is X itself. If P contains exactly two sets, then one of them must be an arbitrary singleton subset of X. The latter implies that $\{\{1\}, \{-7, -2\}\}$, $\{\{-7\}, \{1, -2\}\}$ and $\{\{-2\}, \{1, -7\}\}$ are the only possibilities for P in this case. One may verify that those are indeed partitions of X. If P contains exactly three sets, then, obviously, those must be singleton sets containing 1, -7 and -2 respectively. P cannot contain more than 3 sets as each set is supposed to be nonempty, meaning their union (since they are disjoint) would contain more than 3

elements contradicting its equality to $\{1, -7, -2\}$. Finally, we have identified all 5 partitions of X, meaning there are that many equivalence relations on that set.

Problem 5

Write down three integers congruent to 16 modulo 3.

19, 67 and 115 are three integers congruent to 16 modulo 3.

Problem 6

Does every subset in $(\mathbb{N}, \subseteq)$ possess a supremum? Explain.

No as the entire poset itself possesses no upper bound and hence no supremum as well.

Problem 7

Compute the following in $B(5)$:

$$(1,1,1,0,1)(1,0,1,0,1) + \overline{(0,1,0,1,0)}$$

We have

$$(1,1,1,0,1)(1,0,1,0,1) + \overline{(0,1,0,1,0)} = (1,0,1,0,1) + (1,0,1,0,1) =$$

$$= (1,0,1,0,1)$$

Problem 8

Construct the Disjunctive Normal Form for the function $f : B(3) \to \{0,1\}$ given by

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

We begin by rewriting f as follows.

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

$$\neg(\neg x \vee \neg z) \vee (\neg y \wedge z) = (x \wedge z) \vee (\neg y \wedge z)$$

Now that $f(x,y,z) = xy+y'z$, we also have $f(x,y,z) = xy(z+z')+(x+x')y'z$, i.e., $f(x,y,z) = xyz + xyz' + xy'z + x'y'z$.

Problem 9

Find the supremum of the set $\{(1,0,1,1),(0,0,1,1),(1,0,0,1)\}$ in $B(4)$.

In general, the supremum of a set of $0,1$-words is equal to their sum, we thus have

$\sup\{(1,0,1,1),(0,0,1,1),(1,0,0,1)\} = (1,0,1,1)+(0,0,1,1)+(1,0,0,1) = (1,0,1,1).$

Problem 10

Does there exist a bijection between the sets $\{9, 67, 1, 14, \pi, \frac{1}{2}\}$ and $\{\pi, 9, 67, 15, 1\frac{1}{2}\}$? Explain your answer

Let $f : \{9, 67, 1, 14, \pi, \frac{1}{2}\} \to \{\pi, 9, 67, 15, 1, \frac{1}{2}\}$ be given by

$$f(x) = \begin{cases} 15, & x = 14 \\ x, & \text{otherwise} \end{cases}$$

Then the inverse function f^{-1} of f is given by

$$f^{-1}(x) = \begin{cases} 14, & x = 15 \\ x, & \text{otherwise} \end{cases}$$

As one may verify. Existence of the inverse function implies f to be a bijection.

Problem 11

Evaluate the following

$$\sum_{j=1}^{4}\prod_{i=2}^{4}\frac{j+2}{i^2-1}$$

We first have

$$\prod_{i=2}^{4}\frac{j+2}{i^2-1}=\frac{j+2}{2^2-1}\cdot\frac{j+2}{3^2-1}\cdot\frac{j+2}{4^2-1}=$$

$$=\frac{j+2}{3}\cdot\frac{j+2}{8}\cdot\frac{j+2}{15}=\frac{(j+2)^3}{3\cdot 8\cdot 15}$$

Meaning

$$\sum_{j=1}^{4}\prod_{i=2}^{4}\frac{j+2}{i^2-1}=\sum_{j=1}^{4}\frac{(j+2)^3}{3\cdot 8\cdot 15}=$$

$$=\frac{(1+2)^3}{3\cdot 8\cdot 15}+\frac{(2+2)^3}{3\cdot 8\cdot 15}+\frac{(3+2)^3}{3\cdot 8\cdot 15}+\frac{(4+2)^3}{3\cdot 8\cdot 15}=\frac{3^3+4^3+5^3+6^3}{3\cdot 8\cdot 15}=$$

$$=\frac{27+64+125+216}{3\cdot 8\cdot 15}=\frac{432}{360}=\frac{6}{5}$$

Problem 12

Rank the following functions from the slowest growing to the fastest growing (that is, using the relation $\prec$):

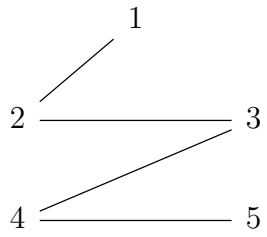
$$0.01n^2, 2\log n, (11/10)^n, 8, 1.3n!, n^5, 2n^n, n.$$

The ranking is as follows.

$$8 \prec 2\log n \prec n \prec 0.01n^2 \prec n^5 \prec (11/10)^n \prec 1.3n! \prec 2n^n$$

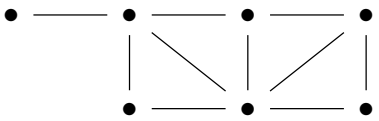
Problem 13

Sketch the graph $G = (V, E)$ with $V = \{1, 2, 3, 4, 5\}$ and $E = \{\{2, 3\}, \{1, 2\}, \{3, 4\}, \{4, 5\}\}$.



Problem 14

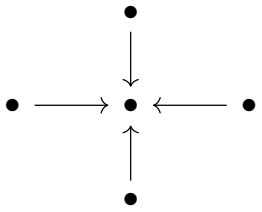
Write down the sequence of degrees for the graph on Figure 1.



The degree sequence of the given graph is 5, 4, 3, 3, 2, 2, 1.

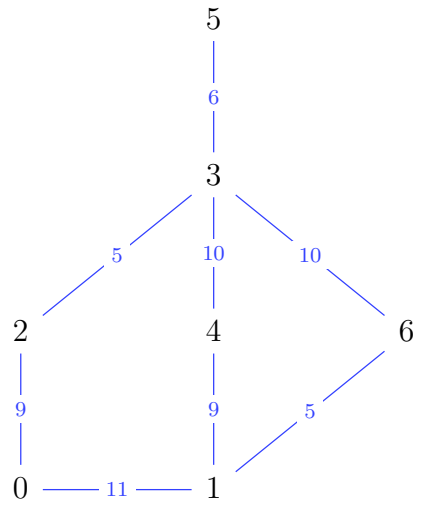
Problem 15

Sketch a directed graph with 1 sink and 4 sources.

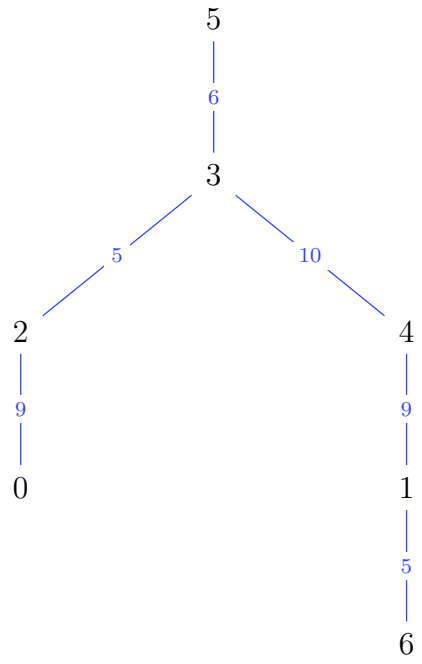


Problem 16

Find a minimal spanning tree for the weighted graph on Figure 2. Explain why the tree you gave is indeed minimal.



A minimal spanning tree for the given weighted graph is given below.



This is indeed a minimal spanning tree as any spanning tree of the graph will contain 6 edges and the edges chosen in the above spanning tree contains edges with exactly the 6 lowest values of weights.

Problem 17

The cost matrix is given by the table of distances (in meters) on Figure 3 between different buildings on KIU campus. Use the "cheapest insertion" algorithm to find a short trip through every building starting at building E.

	K	E	F	G	H
K	-	1620	1510	1380	1320
E	1620	-	110	240	310
F	1510	110	-	120	210
G	1380	240	120	-	90
H	1320	310	210	90	-

The trip starting at the building E achieved through the "cheapest insertion" algorithm is

$$E \xrightarrow{110} F \xrightarrow{120} G \xrightarrow{90} H \xrightarrow{1320} K$$

with total distance of 1640 meters.

Problem 18

Is the graph on Figure 1 Hamiltonian? Explain your answer?

The graph is not Hamiltonian as there is a vertex with degree 1 preventing the existence of a Hamiltonian circuit.

Problem 19

Show that division operation $\div : (\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\}) \to (\mathbb{R} \setminus \{0\})$ is not associative.

We have $1, 2 \in \mathbb{R} \setminus \{0\}$, however, $1 \div (1 \div 2) = 1 \div \frac{1}{2} = \frac{1}{\frac{1}{2}} = 2 \neq \frac{1}{2} = 1 \div 2 = \frac{1}{1} \div 2 = (1 \div 1) \div 2$. Hence division is not associative in $\mathbb{R} \setminus \{0\}$.

Problem 20

Show that $4 \in \left\langle \frac{1}{9} \right\rangle$, where $\left\langle \frac{1}{9} \right\rangle$ is the subgroup of $(\mathbb{Q}, +)$ generated by $\frac{1}{9}$.

There indeed exists an integer n with $n \cdot \frac{1}{9} = 4$, namely, $n = 36$ as $36 \cdot \frac{1}{9} = 4$.

Problem 21

Find all zero divisors in $\mathbb{Z}_{14}$.

In an arbitrary finite unital ring, an element is a zero divisor if and only if it is not a unit, we therefore extract all elements of $\mathbb{Z}_{14}$ coprime to 14 and obtain the zero divisors, namely, 2 and 7.

Problem 22

Solve the following equation in S_5.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix} \circ x &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} \\ x &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}^{-1} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} \\ x &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix} \\ x &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} \end{aligned}$$

Problem 23

Decompose

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$

into a product of disjoint cycles.

We see that the given permutation has mappings $1 \mapsto 5$, $5 \mapsto 4$ and $4 \mapsto 1$, meaning the 3-cycle $(1, 5, 4)$ will be a term in the decomposition. We also have the mappings $2 \mapsto 3$ and $3 \mapsto 2$, meaning the transposition $(2, 3)$ will also appear in the decomposition. We have exhausted all the elements, thus the algorithm halts and we obtain $(1, 5, 4)(2, 3)$.

Problem 24

Give an example of a non-trivial ideal in $\mathbb{Z}_{10}$ (that is, $I \neq \mathbb{Z}_{10}$ and $I \neq \{0\}$).

The principal idea generated by 2 is obviously nonempty and also does not equal $\mathbb{Z}_{10}$ as it would imply that 2 is a unit in $\mathbb{Z}_{10}$ (it is not as $\gcd(2, 10) = 2$).

Problem 25

Write down a Cayley table for multiplication for a four-element field.

See the last central exercise of week 14.

Problem 26

Prove that for any finite group G, the number of elements (order) in every subgroup of G divides the number of elements (order) of G.

See my video about Lagrange's theorem.

1.3 Group 9

Problem 1

Write down a six element subset of the set of integers $\mathbb{Z}$.

$\{1729, 5050, 6174, 31415, 8080174247945128758864599049617107570057543680000000000, 1.201 \cdot 10^{57}\}$ is a subset of $\mathbb{Z}$ with exactly six elements.

Problem 2

Let $f : \mathbb{N} \to \mathbb{N}$ be a function given by $f(n) = 2n$. Determine $f^{-1}(\{4, 5, 6, 7, 8\})$.

Clearly, the integers in $\operatorname{im} f$ are multiples of 2, meaning $f^{-1}(\{4, 5, 6, 7, 8\}) = f^{-1}(\{4, 6, 8\})$. Since f is injective, $f(2) = 2 \cdot 2 = 4$, $f(3) = 2 \cdot 3 = 6$ and $f(4) = 2 \cdot 4 = 8$, we have $f^{-1}(\{4, 6, 8\}) = \{2, 3, 4\}$.

Problem 3

Is the relation

$$R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a \text{ divides } b\}$$

on the set of natural numbers transitive? Explain your answer.

Let $(a, b) \in R$ and $(b, c) \in R$ for some $a, b, c \in \mathbb{N}$, i.e., let a divide b and b divide c. By definition of divisibility, there exist $x, y \in \mathbb{Z}$ with $b = ax$ and $c = by$. This implies that $c = by = (ax)y = a(xy)$, meaning a divides c, i.e., $(a, c) \in R$. Hence R is indeed transitive.

Problem 4

How many equivalence relations are there on the set $X = \{0, 5, -2\}$? Explain.

In general, the number of equivalence relations on a finite is equal to the number of partitions of that set. We shall hence identify all partitions P of $\{0, 5, -2\}$. If P contains exactly one set, then, obviously, it is X itself. If P contains exactly two sets, then one of them must be an arbitrary singleton subset of X. The latter implies that $\{\{0\}, \{5, -2\}\}$, $\{\{5\}, \{0, -2\}\}$ and $\{\{-2\}, \{0, 5\}\}$ are the only possibilities for P in this case. One may verify that those are indeed partitions of X. If P contains exactly three sets, then, obviously, those must be singleton sets containing 0, 5 and -2 respectively. P cannot contain more than 3 sets as each set is supposed to be nonempty, meaning their union (since they are disjoint) would contain more than 3 elements contradicting its equality to $\{0, 5, -2\}$. Finally, we have identified all 5 partitions of X, meaning there are that many equivalence relations on that set.

Problem 5

Write down three integers congruent to 17 modulo 5.

22, 107 and 192 are three integers congruent to 17 modulo 5.

Problem 6

Does every non-empty subset in $(\mathbb{N}, \leq)$ possess an infimum? Explain.

For every nonempty set A of natural numbers, there exists a minimal element $n \in A$. Since $(\mathbb{N}, \leq)$ is a totally ordered set, that makes $n \in A$ a lower bound of A. We can't have a lower bound greater than n, meaning all lower bounds of A are $\{1, \ldots, n\}$. Clearly, n is the greatest lower bound of A, i.e., the infimum.

Problem 7

Compute the following in $B(5)$:

$$(0,1,1,0,1)(1,0,0,1,1) + \overline{(0,1,0,0,0)}.$$

We have

$$(0,1,1,0,1)(1,0,0,1,1)+\overline{(0,1,0,0,0)} = (0,0,0,0,1)+(1,0,1,1,1) = (1,0,1,1,1)$$

Problem 8

Construct the Disjunctive Normal Form for the function $f : B(3) \to \{0,1\}$ given by

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

We begin by identifying all $(x,y,z) \in B(3)$ for which $f(x,y,z) = 1$. The latter can be rewritten as $(x \to z)\wedge(\neg y \wedge z) = 1$. By definition of conjunction, we have $x \to z = 1$ and $\neg y \wedge z = 1$. The latter implies that $\neg y = 1$ and $z = 1$ similarly. $x \to z$, since $z = 1$, simplifies to 1. We thus have obtained the inputs $(0,0,1)$ and $(1,0,1)$. The minterms of $(0,0,1)$ and $(1,0,1)$ are $x'y'z$ and $xy'z$ respectively. The latter yields $f(x,y,z) = x'y'z + xy'z$.

Problem 9

Find the infimum of the set $\{(1,0,1,1),(0,0,1,1),(1,0,0,1)\}$ in $B(4)$.

In general, the infimum of a set of $0,1$-words is equal to their product, we thus have

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

Problem 10

Does there exist a bijection between the sets $\{2,-3,1,14,\pi,\frac{1}{2}\}$ and $\{\pi,2,-3,15,1,\frac{1}{2}\}$? Explain your answer

Let $f:\{2,-3,1,14,\pi,\frac{1}{2}\}\to\{\pi,2,-3,15,1,\frac{1}{2}\}$ be given by

$$f: x \mapsto \begin{cases} 15, & x = 14 \\ x, & x \neq 14 \end{cases}$$

Then f is bijective as its inverse $f^{-1}:\{\pi,2,-3,15,1,\frac{1}{2}\}\to\{2,-3,1,14,\pi,\frac{1}{2}\}$ is given by

$$f^{-1}: x \mapsto \begin{cases} 14, & x = 15 \\ x, & x \neq 15 \end{cases}$$

Problem 11

Evaluate the following

$$\sum_{j=1}^{4}\prod_{i=1}^{3}\frac{j+1}{i^2}.$$

First we have

$$\prod_{i=1}^{3}\frac{j+1}{i^2} = \frac{j+1}{1^2}\cdot\frac{j+1}{2^2}\cdot\frac{j+1}{3^2} =$$

$$\frac{(j+1)^3}{4 \cdot 9} = \frac{(j+1)^3}{36}$$

Meaning

$$\begin{aligned}\sum_{j=1}^{4} \prod_{i=1}^{3} \frac{j+1}{i^2} &= \sum_{j=1}^{4} \frac{(j+1)^3}{36} = \\ &= \frac{(1+1)^3}{36} + \frac{(2+1)^3}{36} + \frac{(3+1)^3}{36} + \frac{(4+1)^3}{36} = \\ &= \frac{2^3 + 3^3 + 4^3 + 5^3}{36} = \frac{8 + 27 + 64 + 125}{36} = \\ &= \frac{35 + 189}{36} = \frac{224}{36} = \frac{56}{9}\end{aligned}$$

Problem 12

Rank the following functions from the slowest growing to the fastest growing (that is, using the relation $\prec$):

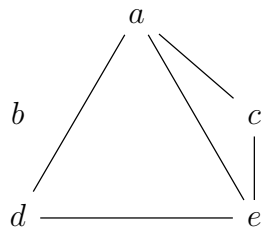
$$0.1n^2, (8/7)^n, \log n, 3, n^4, 2n^n, 1.2n!, n.$$

The ranking is as follows.

$$3 \prec \log n \prec n \prec 0.1n^2 \prec n^4 \prec (8/7)^n \prec 1.2n! \prec 2n^n$$

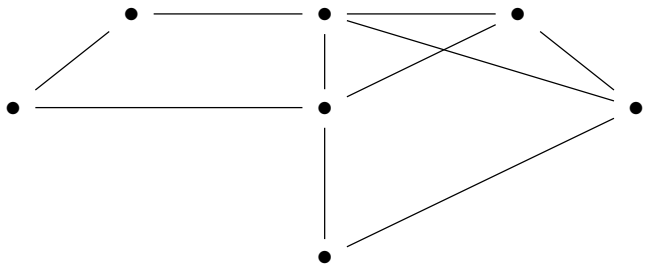
Problem 13

Sketch the graph of $G = (V, E)$ with $V = \{a, b, c, d, e\}$ and $E = \{\{c, a\}, \{a, d\}, \{a, e\}, \{d, e\}, \{e, c\}\}$.



Problem 14

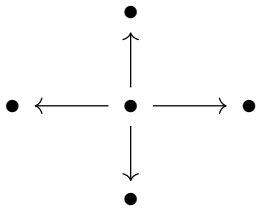
Write down the sequence of degrees for the graph on Figure 1.



The degree sequence of the given graph is 4, 4, 3, 3, 2, 2, 2.

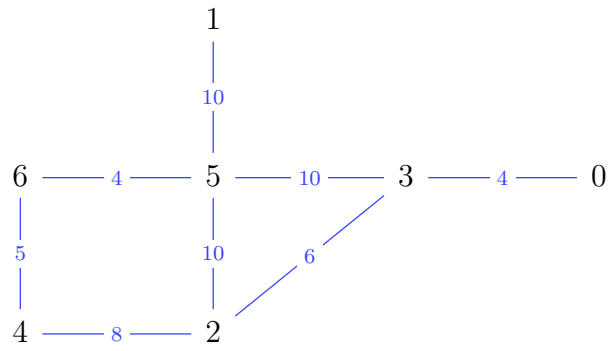
Problem 15

Sketch a directed graph with 1 source and 4 sinks.



Problem 16

Determine a minimal spanning tree for the weighter graph on Figure 3. Explain why the tree you gave is indeed minimal.



A minimal spanning tree for the given weighted graph is given below.

This is indeed a minimal spanning tree as any spanning tree of the graph will contain 6 edges and the edges chosen in the above spanning tree contains edges with exactly the 6 lowest values of weights.

Problem 17

The cost matrix is given by the table of distances (in meters) on Figure 2 between different buildings on KIU campus. Use the "cheapest insertion" algorithm to find a short trip through every building starting at building F.

	K	E	F	G	H
K	-	1620	1510	1380	1320
E	1620	-	110	240	310
F	1510	110	-	120	210
G	1380	240	120	-	90
H	1320	310	210	90	-

The trip starting at the building F achieved through "cheapest insertion" algorithm is

$$F \xrightarrow{110} E \xrightarrow{240} G \xrightarrow{90} H \xrightarrow{1320} K$$

with total distance of 1760 meters.

Problem 18

Is the graph on Figure 1 Hamiltonian? Explain your answer.

Yes as the outer edges on the picture form a Hamiltonian circuit.

Problem 19

Show that division operation $\div : (\mathbb{Q} \setminus \{0\}) \times (\mathbb{Q} \setminus \{0\}) \to (\mathbb{Q} \setminus \{0\})$ is not associative.

We have $1, 2 \in \mathbb{Q} \setminus \{0\}$, however, $1 \div (1 \div 2) = 1 \div \frac{1}{2} = \frac{1}{\frac{1}{2}} = 2 \neq \frac{1}{2} = 1 \div 2 = \frac{1}{1} \div 2 = (1 \div 1) \div 2$. Hence division is not associative in $\mathbb{Q} \setminus \{0\}$.

Problem 20

Show that $3 \in \left\langle \frac{1}{7} \right\rangle$, where $\left\langle \frac{1}{7} \right\rangle$ is the subgroup of $(\mathbb{Q}, +)$ generated by $\frac{1}{7}$.

There indeed exists an integer n with $n \cdot \frac{1}{7} = 3$, namely, $n = 21$ as $21 \cdot \frac{1}{7} = 3$.

Problem 21

Find all zero divisors in $\mathbb{Z}_{12}$.

In an arbitrary finite unital ring, an element is a zero divisor if and only if it is not a unit, we therefore extract all elements of $\mathbb{Z}_{12}$ coprime to 12 and obtain the zero divisors, namely, 2, 3, 4 and 6.

Problem 22

Solve the following equation in S_5:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} \circ x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4&5\\5&4&2&3&1\end{pmatrix} \circ x = \begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix}$$
$$x = \begin{pmatrix}1&2&3&4&5\\5&4&2&3&1\end{pmatrix}^{-1} \circ \begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix}$$
$$x = \begin{pmatrix}1&2&3&4&5\\5&3&4&2&1\end{pmatrix} \circ \begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix}$$
$$x = \begin{pmatrix}1&2&3&4&5\\5&2&3&1&4\end{pmatrix}$$

Problem 23

Decompose

$$\begin{pmatrix}1&2&3&4&5\\5&4&2&1&3\end{pmatrix}$$

into a product of disjoint cycles.

We see that the given permutation has mappings $1 \mapsto 5$, $5 \mapsto 3$ and $3 \mapsto 2$, $2 \mapsto 4$ and $4 \mapsto 1$, it itself is a cycle, namely, $(1, 5, 3, 2, 4)$.

Problem 24

Give an example of a non-trivial ideal I in $\mathbb{Z}_{12}$ (that is, $I \neq \mathbb{Z}_{12}$ and $I \neq \{0\}$).

The principal idea generated by 2 is obviously nonempty and also does not equal $\mathbb{Z}_{12}$ as it would imply that 2 is a unit in $\mathbb{Z}_{12}$ (it is not as $\gcd(2, 12) = 2$).

Problem 25

Write down a Cayley table for multiplication of a four-element field.

Problem 26

Prove that for any finite group G, the number of elements (order) in every subgroup of G divides the number of elements (order) of G.

See my video about Lagrange's theorem.

1.4 Group 11

See the section "Group 6".

Chapter 2

Final Exam Retake 2022-2023

2.1 Group 8

Problem 1

Show that $n^3 + 2n$ is divisible by 3 for every natural number $n \in \mathbb{N}$.

We consider three cases. If n is divisible by 3, then so is $n(n^2 + 2) = n^3 + 2n$. If n is not divisible by 3, then $n^2 + 2$ is divisible by three as we either have $x = 3k + 1$ or $x = 3k + 2$ and $n^2 + 2 = (3k + 1)^2 + 2 = 9k^2 + 6k + 1 + 2 = 9k^2 + 6k + 3 = 3(3k^2 + 2k + 1)$ or $n^2 + 2 = (3k + 2)^2 + 2 = 9k^2 + 12k + 4 + 2 = 9k^2 + 12k + 6 = 3(3k^2 + 4k + 2)$ respectively. $n^2 + 2$ being divisible by 3 implies $n(n^2 + 2) = n^3 + 2n$ to also be divisible by 3.

Problem 2

Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ which is injective.

The identity function on $\mathbb{R}$.

Problem 3

Give an example of an equivalence relation on $\mathbb{R}$.

$\mathbb{R} \times \mathbb{R}$.

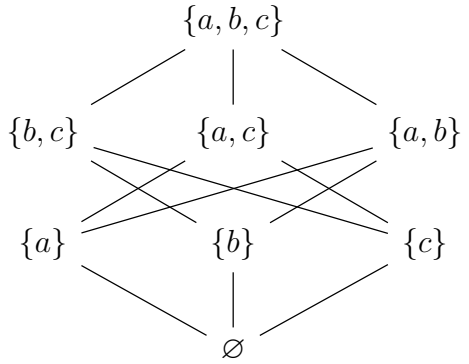
Problem 4

Determine whether the partially ordered set $(\{1, 3, 6, 9\}, |)$ is a lattice.

It is not a lattice as there is element divisible by 6 and 9, i.e., no upper bound for $\{6, 9\}$ and hence no supremum as well.

Problem 5

Draw a Hasse diagram from $(\mathcal{P}(\{a, b, c\}), \subseteq)$.



Problem 6

Let $S = \{1, 2, 3\}$ and $B(3)$ be the set of $0, 1$-words of length 3. Construct a bijective function $f : \mathcal{P}(S) \to B(3)$.

Let $f : \mathcal{P}(S) \to B(3)$ be given by

$$\begin{aligned} f(\varnothing) &= (0,0,0) & f(\{1,2,3\}) &= (1,1,1) \\ f(\{1\}) &= (1,0,0) & f(\{2,3\}) &= (0,1,1) \\ f(\{2\}) &= (0,1,0) & f(\{1,3\}) &= (1,0,1) \\ f(\{3\}) &= (0,0,1) & f(\{1,2\}) &= (1,1,0) \end{aligned}$$

Then f is clearly bijective as different subsets of $\{1,2,3\}$ are mapped to different $0,1$-words of length 3 (injectivity) and all $0,1$-words of length 3 are have some preimage (surjectivity).

Problem 7

Determine whether the function $f : B(3) \to \{0,1\}$ given by

$$f(x,y,z) = (x \wedge z) \implies (\neg y \vee z)$$

is monotone.

If $z = 0$, then $x \wedge z = 0$ and $f(x,y,z) = (x \wedge z) \implies (\neg y \vee z) = 1$. If $z = 1$, then $\neg y \vee z = 1$ and $f(x,y,z) = (x \wedge z) \implies (\neg y \vee z) = 1$. Since f is always 1, it is monotone.

Problem 8

Find the supremum of the set $\{(1,0,1,1),(0,0,1,1),(1,0,0,1)\}$ in $B(4)$.

In general, the supremum of a set of $0,1$-words is equal to their sum, we thus have

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

Problem 9

Write down all unordered 4-partitions of integer 7.

Here are the unordered 4-partitions of integer 7.

$$4+1+1+1$$
$$3+2+1+1$$
$$2+2+2+1$$

Problem 10

26 out of the class of 85 students speak German, 42 speak English and 6 speak both, English and German. How many students speak English or German?

Let G and E denote the sets of students speaking German and of students speaking English respectively (the students, in question, from the given class). According to the inclusion-exclusion principle, we have

$$|G \cup E| = |G| + |E| - |E|$$
$$|G \cup E| = 26 + 42 - 6$$
$$|G \cup E| = 20 + 42$$
$$|G \cup E| = 62$$

Problem 11

Explain why $\frac{\sin n}{n} = o(1)$.

For all $\varepsilon > 0$, pick $n_0 = \frac{1}{\varepsilon}$ so that $n \geq n_0$ implies the following.

$$\begin{aligned} |\sin n| \leq 1 \quad 1 &\leq n\varepsilon \\ \frac{|\sin n|}{n} &\leq \varepsilon \\ \left|\frac{\sin n}{n}\right| &\leq \varepsilon \end{aligned}$$

Problem 12

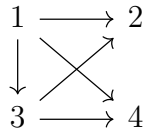
Say v is a vertex in a hypercube Q_3. What is the degree of v?

During the lecture we mentioned that every vertex in the hypercube Q_n has degree n. Thus, for the case $n = 3$, the vertex v has degree 3.

Problem 13

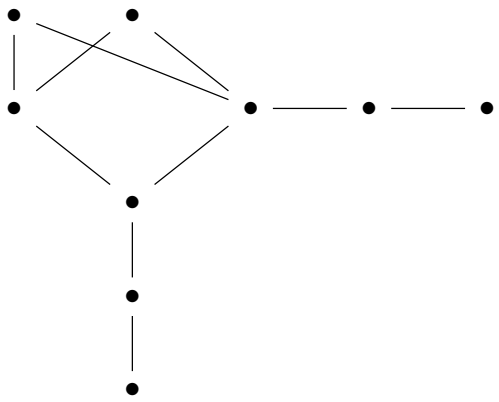
Sketch the directed graph with the following incidence matrix

$$\begin{pmatrix} -1 & 0 & -1 & 0 & -1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$



Problem 14

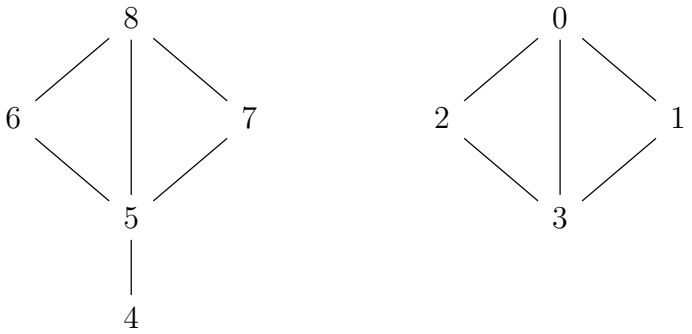
Is the graph on Figure 1 bipartite? Explain your answer.



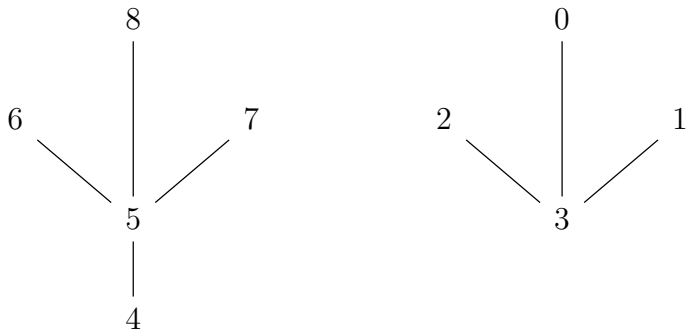
During the lecture we proved a theorem stating a graph to be bipartite if and only if every circuit it contains is of even length. Every circuit the given graph contains is of even length.

Problem 15

Determine a spanning forest for the graph given on Figure 2.

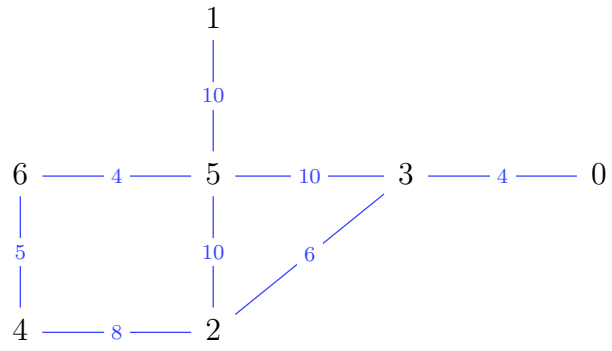


We proceed by removing edges contained in circuits until no circuits remain. One may obtain the following spanning forest of the given graph.

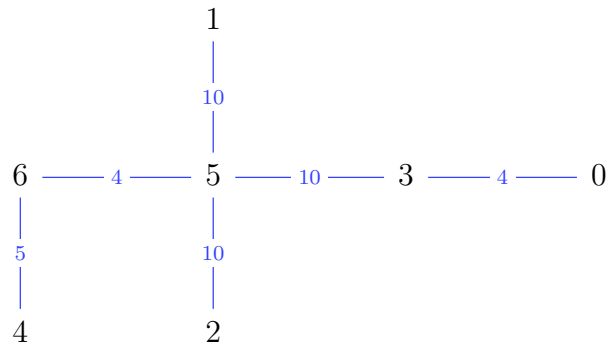


Problem 16

Construct a spanning tree for the graph on Figure 3 such that the unique path from vertex 5 to any other vertex is always the *shortest*, in the sense that the weighted path is minimal.

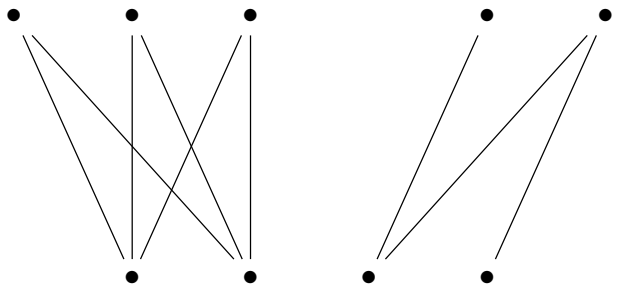


We shall apply the greedy algorithm which yields the following spanning tree.



Problem 17

Determine the number of vertices in the minimal vertex cover of the graph on Figure 4.



This is a bipartite graph where the upper and lower nodes form the parts. Observe that the three nodes in the top-left corner have two neighbours. Since three is larger than two, marriage theorem suggests that the size of a maximal matching in the graph is not five and is hence lower for all matchings. By equilibrium theorem that we have proven during the lecture, a vertex cover suffices to have four vertices in order to be minimal. The four vertices on the bottom form exactly that.

Problem 18

Give an example of noncommutative binary operation.

The binary operation $* : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ defined by $q_1 * q_2 = q_1 - q_2$ is noncommutative as $1 * 0 = 1 - 0 = 1 \neq -1 = 0 - 1 = 0 * 1$ despite $0, 1 \in \mathbb{Q}$.

Problem 19

Write down Cayley table for rotations of an equilateral triangle in the plane.

Let 1 and r denote the neutral element and rotation of the triangle by either 60 or 120 degrees respectively. Then $\{1, r, r^2\}$ forms a group of all rotations of an equilateral triangle with the following Cayley table.

$\circ$	1	r	r^2
1	1	r	r^2
r	r	r^2	1
r^2	r^2	1	r

Problem 20

Give an example of a group where every non-neutral element has infinite order. [The zero element is assumed to mean the neutral element.]

Every non-neutral element of the additive group of integers has infinite order.

Problem 21

Does a Lattice $(L, \wedge, \vee)$ form a ring under $\wedge$ and $\vee$? Explain.

The lattice $(\mathbb{Z}, \wedge, \vee)$ with the usual ordering does not form a ring under $\wedge$ and $\vee$ as there is no neutral element for $\wedge$. (Assume n is the neutral element for $\wedge$, then $(n-1) \wedge n = n - 1$ as $n - 1 \leq n$, but $n - 1 \neq n$, yielding a contradiction.)

Problem 22

How many generators does $(\mathbb{Z}_{11}, +)$ have?

The generators of $(\mathbb{Z}_{11}, +)$ are exactly the elements x of order 11, meaning there does not exist a positive integer n smaller than 11 with $nx = 0$. According to ring theory, the latter implies that x is not a zero divisor and is a unit. The number of units in $\mathbb{Z}_{11}$ is $\varphi(11) = 11 - 1 = 10$ as 11 is prime.

Problem 23

Solve the following equation in $\mathbb{Z}_{127}$:

$$103 \cdot x - 6 = 4.$$

Hint: You can use the Euclidean algorithm to compute multiplicative inverses in $\mathbb{Z}_{127}$.

$$\begin{aligned} 103 \cdot x - 6 &= 4 \\ 103 \cdot x &= 4 + 6 \\ 103 \cdot x &= 10 \end{aligned}$$

We now find the multiplicative inverse of 103 via the Euclidean algorithm. Namely, the following steps are produced.

$$\begin{aligned} 127 &= 1 \cdot 103 + 24 \\ 103 &= 4 \cdot 24 + 7 \\ 24 &= 3 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

Meaning $1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (24 - 3 \cdot 7) = 7 \cdot 7 - 2 \cdot 24 = 7 \cdot (103 - 4 \cdot 24) - 2 \cdot 24 = 7 \cdot 103 - 30 \cdot 24 = 7 \cdot 103 - 30 \cdot (127 - 103) = 37 \cdot 103 - 30 \cdot 127$. Therefore

the multiplicative inverse of 103 modulo 127 is 37 and we continue solving the equation as follows.

$$\begin{aligned} 103 \cdot x &= 10 \\ x &= 37 \cdot 10 \\ x &= 370 \\ x &= 116 \end{aligned}$$

Problem 24

Give an example of a field $\mathbb{F}$ such that $(a+b)^2 = a^2 + b^2$ for all $a, b \in \mathbb{F}$.

In the field $\mathbb{Z}_2$ we have $x^2 = x$ for all $x \in \mathbb{Z}_2$, meaning $(a+b)^2 = a+b = a^2 + b^2$ for all $a, b \in \mathbb{Z}_2$.

Problem 25

Show that the hypercube Q_n is Hamiltonian.

See the central exercise 7 of week 10.

2.2 Group 11

Problem 1

Show that $n^3 - n + 3$ is divisible by 3 for every natural number $n \in \mathbb{N}$.

$n-1$, n and $n+1$ are three consecutive integers, meaning one of them must be divisible by 3, making their product also divisible by 3. But their product is $(n-1)n(n+1) = n(n^2-1) = n^3 - n$. Since 3 is obviously divisible by 3 and since sum of numbers divisible by 3 is also divisible by 3, this implies $n^3 - n + 3$ to be divisible by 3 for all $n \in \mathbb{N}$.

Problem 2

Let $f : (-\infty, 0] \to \mathbb{R}$ be a function given by $f(x) = x^2 + 1$. What is the *range* of f?

The range of f is $[1, \infty)$ as for all $y \in [1, \infty)$ we have $f(-\sqrt{y-1}) = (-\sqrt{y-1})^2 + 1 = y - 1 + 1 = y$, meaning $[1, \infty)$ is a subset of the range of f. Conversely, $x^2 \geq 0$ for all real x and $x^2 + 1 \geq 1$, making $f(x) \in [1, \infty)$ for all $x \in (-\infty, 0]$, i.e., the range of f is a subset of $[1, \infty)$. Hence we have that the range of f is equal to $[1, \infty)$.

Problem 3

Give an example of an equivalence relation on $\mathbb{Z}$.

$\mathbb{Z} \times \mathbb{Z}$.

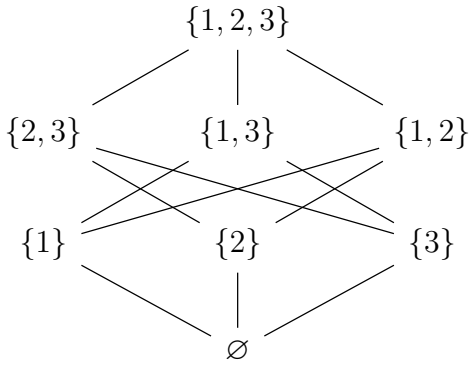
Problem 4

Determine whether the partially ordered set $(\{1, 5, 10, 15\}, |)$ is a lattice.

The given poset is not a lattice as there is no upper bound for $\{10, 15\}$ (otherwise there would be an integer divisible by 30), meaning there is also no supremum for $\{10, 15\}$.

Problem 5

Draw a Hasse diagram for $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$.



Problem 6

Let $S = \{1, 2, 3, 4\}$ and $B(4)$ be the set of $0, 1$-words of length 4. Construct a bijective function $f : \mathcal{P}(S) \to B(4)$.

Let $f : \mathcal{P}(S) \to B(4)$ be given by

$$\begin{aligned}
f(\varnothing) &= (0,0,0,0) & f(\{1,2,3,4\}) &= (1,1,1,1)\\
f(\{1\}) &= (1,0,0,0) & f(\{2,3,4\}) &= (0,1,1,1)\\
f(\{2\}) &= (0,1,0,0) & f(\{1,3,4\}) &= (1,0,1,1)\\
f(\{3\}) &= (0,0,1,0) & f(\{1,2,4\}) &= (1,1,0,1)\\
f(\{4\}) &= (0,0,0,1) & f(\{1,2,3\}) &= (1,1,1,0)\\
f(\{1,2\}) &= (1,1,0,0) & f(\{3,4\}) &= (0,0,1,1)\\
f(\{1,3\}) &= (1,0,1,0) & f(\{2,4\}) &= (0,1,0,1)\\
f(\{1,4\}) &= (1,0,0,1) & f(\{2,3\}) &= (0,1,1,0)
\end{aligned}$$

Then f is clearly bijective as different subsets of $\{1, 2, 3, 4\}$ are mapped to different $0, 1$-words of length 4 (injectivity) and all $0, 1$-words of length 4 are have some preimage (surjectivity).

Problem 7

Write down the truth table for the function $f : B(3) \to \{0, 1\}$ given by

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

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

Problem 8

Find the infimum of the set $\{(1,1,1,1),(0,0,1,1),(1,0,1,0)\}$ in $B(4)$.

In general, the infimum of a set of $0,1$-words is equal to their product, we thus have

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

Problem 9

Write down all unordered 5-partitions of 8.

Here are the unordered 5-partitions of 8.

$$4+1+1+1+1$$
$$3+2+1+1+1$$
$$2+2+2+1+1$$

Problem 10

24 out of the class of 85 students speak German, 52 speak English and 8 speak both, English and German. How many students speak English or German?

Problem 11

Show that $2n + 4 = \Omega(3n - 3)$.

By definition, $2n + 4 = \Omega(3n - 3)$ if and only if $3n - 3 = O(2n + 4)$. The latter is true as for $n \geq 1$ we have

$$\begin{aligned} -11 &\leq n \\ -3 &\leq n + 8 \\ 3n - 3 &\leq 4n + 8 \\ 3n - 3 &\leq 2(2n + 4) \\ |3n - 3| &\leq 2\,|2n + 4| \end{aligned}$$

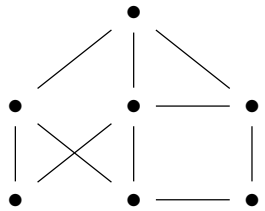
Problem 12

Say v is a vertex in a hypercube Q_4. What is the degree of v?

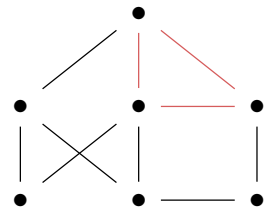
During the lecture we mentioned that every vertex in the hypercube Q_n has degree n. Thus, for the case $n = 4$, the vertex v has degree 4.

Problem 13

Is the graph on Figure 1 bipartite? Explain your answer.

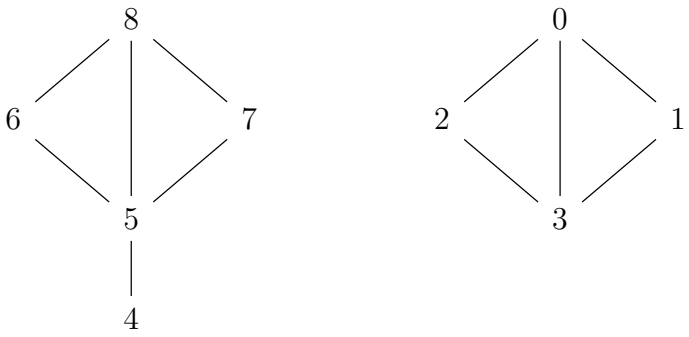


During the lecture we proved a theorem stating a graph to be bipartite if and only if every circuit it contains is of even length. However, the given graph contains a circuit of odd length as visualized (in red) below.

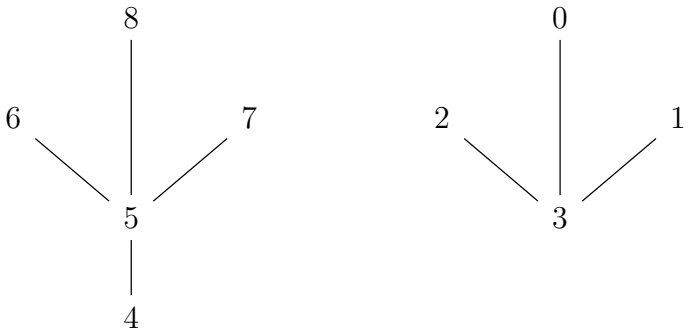


Problem 14

Determine a spanning forest for the graph on Figure 2.

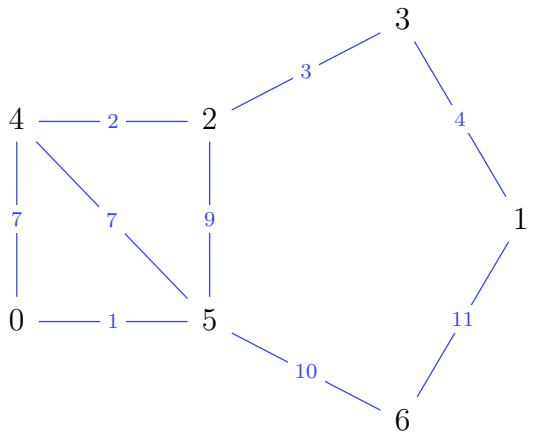


We proceed by removing edges contained in circuits until no circuits remain. One may obtain the following spanning forest of the given graph.

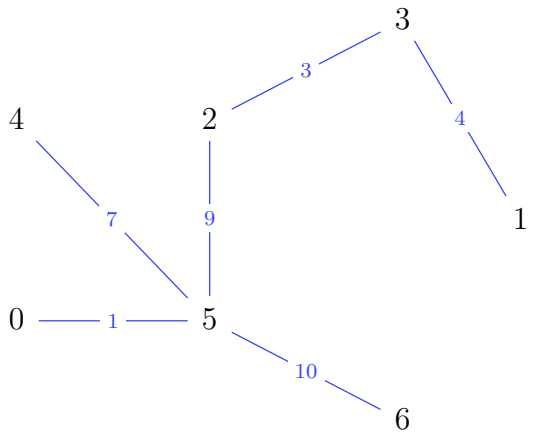


Problem 15

Construct a spanning tree for the graph on Figure 3 such that the unique path from 5 to any other vertex is always the *shortest*, in the sense that the weighted path is minimal.

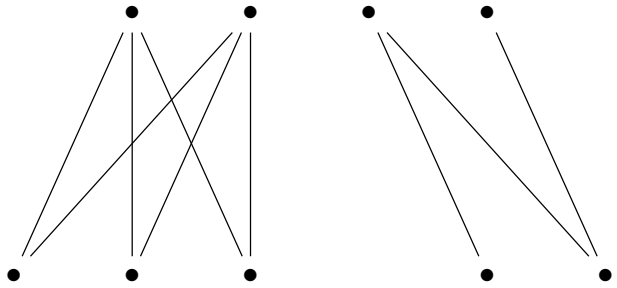


We shall apply the greedy algorithm which yields the following spanning tree.



Problem 16

Determine the number of vertices in the minimal vertex cover on Figure 4.



This is a bipartite graph where the upper and lower nodes form the parts. Observe that the three nodes in the bottom-left corner have two neighbours. Since three is larger than two, marriage theorem suggests that the size of a maximal matching in the graph is not five and is hence lower for all matchings. By equilibrium theorem that we have proven during the lecture, a vertex cover suffices to have four vertices in order to be minimal. The four vertices on the top form exactly that.

Problem 17

Give an example of commutative binary operation.

Addition of natural numbers is a commutative binary operation.

Problem 18

Identify the group of invertible elements of $(\mathbb{Z}_8, \cdot)$.

The elements of $\mathbb{Z}_8$ are $0, 1, 2, 3, 4, 5, 6, 7$. Since the prime factorization of 8 is 2^3, extracting all multiples of 2 leaves us with exactly the integers coprime to 8. The invertible elements are thus $1, 3, 5, 7$.

Problem 19

Write down a Cayley table for rotations of a square in the plane.

Let 1 and r denote the neutral element and rotation of the square by 90 degrees respectively. Then $\{1, r, r^2, r^3\}$ forms a group of all rotations of a square with the following Cayley table.

$\circ$	1	r	r^2	r^3
1	1	r	r^2	r^3
r	r	r^2	r^3	1
r^2	r^2	r^3	1	r
r^2	r^3	1	r	r^2

Problem 20

Give an example of a group where every element has a finite order.

The trivial group.

Problem 21

Do binary operations $\wedge$ and $\vee$ turn a lattice $(L, \wedge, \vee)$ into a ring? Explain.

The lattice $(\mathbb{Z}, \wedge, \vee)$ with the usual ordering does not form a ring under $\wedge$ and $\vee$ as there is no neutral element for $\wedge$. (Assume n is the neutral element for $\wedge$, then $(n-1) \wedge n = n - 1$ as $n - 1 \leq n$, but $n - 1 \neq n$, yielding a contradiction.)

Problem 22

Solve the following equation in $\mathbb{Z}_{127}$:

$$107 \cdot x - 6 = 4.$$

Hint: You can use the Euclidean algorithm to compute multiplicativeinverses in $\mathbb{Z}_{127}$.

$$\begin{aligned} 107 \cdot x - 6 &= 4 \\ 107 \cdot x &= 4 + 6 \\ 107 \cdot x &= 10 \end{aligned}$$

We now find the multiplicative inverse of 107 via the Euclidean algorithm. Namely, the following steps are produced.

$$\begin{aligned} 127 &= 1 \cdot 107 + 20 \\ 107 &= 5 \cdot 20 + 7 \\ 20 &= 2 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0 \end{aligned}$$

Meaning $1 = 7 - 6 = 7 - (20 - 2 \cdot 7) = 3 \cdot 7 - 20 = 3 \cdot (107 - 5 \cdot 20) - 20 = 3 \cdot 107 - 16 \cdot 20 = 3 \cdot 107 - 16 \cdot (127 - 107) = 19 \cdot 107 - 16 \cdot 127$. Therefore the multiplicative inverse of 107 modulo 127 is 19 and we continue solving the equation as follows.

$$\begin{aligned} 103 \cdot x &= 10 \\ x &= 19 \cdot 10 \\ x &= 190 \\ x &= 63 \end{aligned}$$

Problem 23

What is the characteristic of $\mathbb{Z}_7$?

$7 \cdot 1 = 7 = 0$ and there is no positive $n < 7$ with $n \cdot 1 = 0$, meaning 7 is the characteristic of $\mathbb{Z}_7$.

Problem 24

Show that the hypercube Q_n is Hamiltonian.

See the central exercise 7 of week 10.

Chapter 3

Second midterm 2023-2024

Problem 1

Let G be a group. $a \in G$ and $O(a) = 70$. Find $O\left(a^{2023}\right)$. Justify your answer.

According to a formula proven during the lecture, we have $O\left(a^n\right) = \frac{O(a)}{\gcd(n, O(a))}$ for all integers n, and thus

$$O\left(a^{2023}\right) = \frac{O(a)}{\gcd(2023, O(a))} = \frac{70}{\gcd(2023, 70)} = \frac{70}{7} = 10$$

Problem 2

Show that $n^7 + 3n^6 + n^5 = O\left(n^7\right)$.

For all $n \geq 1$, we have the following.

$$\begin{aligned} \left|n^7 + 3n^6 + n^5\right| &\leq \left|n^7\right| + 3\left|n^6\right| + \left|n^5\right| \leq \\ &\leq \left|n^7\right| + 3\left|n^7\right| + \left|n^7\right| = 5\left|n^7\right| \end{aligned}$$

Meaning $n^7 + 3n^6 + n^5 \in O(n^7)$ indeed holds (with $n_0 = 1$ and $C = 5 > 0$).

Problem 3

Show that $n^2 = o\,(n!)$.

For every $\varepsilon > 0$, choose $n_0 = 3 + \frac{1}{\varepsilon}$, so that for all $n \geq n_0$ we have

$$\begin{aligned}
3 + \frac{1}{\varepsilon} &\leq n \\
\frac{1}{\varepsilon} &\leq n - 3 \\
\frac{1}{\varepsilon} &\leq n - 3 \leq n - 3 + \frac{2}{n} \\
\frac{1}{\varepsilon} &\leq n - 3 + \frac{2}{n} \\
\frac{1}{\varepsilon} &\leq \frac{n^2 - 3n + 2}{n} \\
1 &\leq \varepsilon \frac{n^2 - 3n + 2}{n} \\
n &\leq \varepsilon(n^2 - 3n + 2) \\
n &\leq \varepsilon(n-1)(n-2) \\
n &\leq \varepsilon(n-1)(n-2) \leq \varepsilon(n-1)! \\
n &\leq \varepsilon(n-1)! \\
n \cdot n &\leq \varepsilon n \cdot (n-1)! \\
n^2 &\leq \varepsilon n! \\
\left|n^2\right| &\leq \varepsilon\,|n!|
\end{aligned}$$

Problem 4

Show that $4 \in \left\langle \frac{1}{4} \right\rangle$, where $\left\langle \frac{1}{4} \right\rangle$ is a subgroup of $(\mathbb{Q}, +)$ generated by $\frac{1}{4}$.

By definition, we have $\left\langle \frac{1}{4} \right\rangle = \left\{ n \cdot \frac{1}{4} \mid n \in \mathbb{Z} \right\}$. There exists $n \in \mathbb{Z}$ with $4 = n \cdot \frac{1}{4}$, namely, $n = 16$, as $4 = 16 \cdot 14$. Therefore 4 is indeed an element of $\left\langle \frac{1}{4} \right\rangle$.

Problem 5

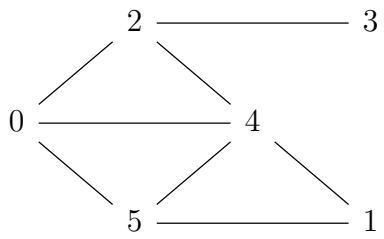
Determine the neutral element if it exists show why it does not exist for the composition on real numbers given by

$$a \star b = \min(a, |b|)$$

Assume that there exists a neutral element and name it $e \in \mathbb{R}$, i.e., let $\min(a, |e|) = a$ for all $a \in \mathbb{R}$. If $e \geq 0$, then $(e+1) \star e = \min(e+1, |e|) = \min(e+1, e) = e \neq e+1$, which is a contradiction. If $e < 0$, then $e \star 0 = \min(e, |0|) = \min(e, 0) = e \neq 0$, which is also a contradiction. Hence no neutral element exists.

Problem 6

Find the adjacency matrix of the following graph.



The adjacency matrix for the given graph is illustrated below.

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Problem 7

The cost matrix is given by the table of distances (in kilometers) below between different cities in France. Use the "double nearest neighbour" algorithm to find a short trip through every city starting at Montpellier.

	M	N	T	P	L
M	-	826	242	748	307
N	826	-	585	384	685
T	242	585	-	679	541
P	748	384	679	-	468
L	307	685	541	468	-

The "double nearest neighbour" algorithm with the starting node at Montpellier yields the following short trip.

$$N \xrightarrow{384} P \xrightarrow{468} L \xrightarrow{307} M \xrightarrow{242} T \xrightarrow{585} N$$

In order for the trip to actually start in Montpellier, we shift it and obtain the following equivalent short trip.

$$M \xrightarrow{242} T \xrightarrow{585} N \xrightarrow{384} P \xrightarrow{468} L \xrightarrow{307} M$$

Chapter 4

Final Exam 2023-2024

Problem 1

Show that $33n^{99} + 18n^3 \prec n^{100} + 3n^3$.

For all $\varepsilon > 0$ choose $n_0 = \max(1, \frac{18}{\varepsilon} - 3, \frac{1}{\varepsilon})$ so that for $n \geq n_0$ we have

$$\begin{aligned}
\frac{18}{\varepsilon} - 3 &\leq n \\
18 - 3\varepsilon &\leq \varepsilon n \\
18 - 3\varepsilon &\leq \varepsilon n - 1 \leq n^{96}(\varepsilon n - 1) \\
18 - 3\varepsilon &\leq n^{96}(\varepsilon n - 1) \\
18 - 3\varepsilon &\leq \varepsilon n^{97} - 33n^{96} \\
33n^{96} + 18 - 3\varepsilon &\leq \varepsilon n^{97} \\
33n^{96} + 18 &\leq \varepsilon n^{97} + 3\varepsilon \\
33n^{96} + 18 &\leq \varepsilon(n^{97} + 3) \\
n^3 \cdot (33n^{96} + 18) &\leq n^3 \cdot \varepsilon(n^{97} + 3) \\
33n^{99} + 18n^3 &\leq \varepsilon(n^{100} + 3n^3) \\
\left|33n^{99} + 18n^3\right| &\leq \varepsilon \left|n^{100} + 3n^3\right|.
\end{aligned}$$

Problem 2

Algorithms **A** and **B** spend exactly $T_{\mathbf{A}}(n) = 0.1n^3 \log_{10} n$ and $T_{\mathbf{B}}(n) = 1.5n^3$ microseconds, respectively, for a problem of size n. If your problem are of the size $n \leq 10^{12}$, which algorithm will you recommend to use? Explain your answer.

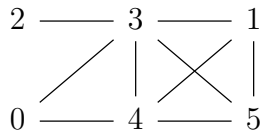
Since $n \leq 10^{12}$ and $10^{12} \leq 10^{15}$, we also have $n \leq 10^{15}$ and it follows that

$$\begin{aligned} n &\leq 10^{15}. \\ \log_{10} n &\leq 15 \\ 0.1 \log_{10} n &\leq 1.5 \\ 0.1n^3 \log_{10} n &\leq 1.5n^3 \\ T_{\mathbf{A}}(n) &\leq T_{\mathbf{B}}(n) \end{aligned}$$

Assuming both algorithms **A** and **B** complete the same favourable task, algorithm **A** should be the one recommended.

Problem 3

Write down the set of vertices V and the set of edges E for the graph $G = (V, E)$ in Figure 1.



For the given graph, the set of vertices $V = \{0, 1, 2, 3, 4, 5\}$ and the set of edges $E = \{\{0, 3\}, \{0, 4\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{3, 4\}, \{3, 5\}, \{4, 5\}\}$.

Problem 4

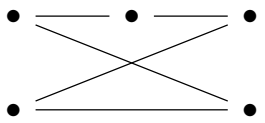
Write down the adjacency matrix for the graph on Figure 1.

The adjacency matrix for the given graph is illustrated below.

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Problem 5

Draw the circuit graph C_5.



Problem 6

Which vertices of the graph in Figure 1 has the highest degree?

In the given graph, the vertex 3 has degree equal to 5 and no other vertex with higher degree can be found.

Problem 7

What is the bandwidth of the chosen labeling for the graph on Figure 1.

The bandwidth of the chosen labeling for the given graph is equal to 4 as the vertices labeled by 1 and 5 are adjacent, $5 - 1 = 4$ and no other pair of adjacent vertices with higher difference can be found.

Problem 8

How many edges does a tree with 932 vertices have?

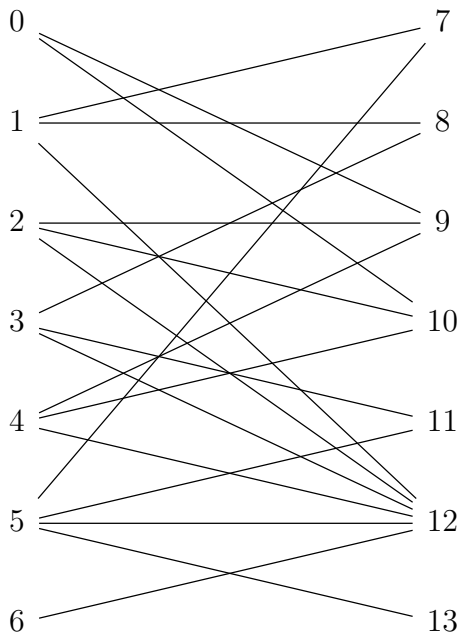
In general, a tree with n vertices has $n - 1$ edges as can be proven by induction. Thus, a tree with 932 vertices would have $932 - 1 = 931$ edges.

Problem 9

The set $\{1, 3, 5, 9, 10, 12\}$ is a minimum vertex cover for the left graph in Figure 2 (A). Let M be a matching given by

$$M = \{\{1, 7\}, \{2, 9\}, \{3, 8\}, \{4, 10\}, \{5, 11\}, \{6, 12\}\}.$$

Does an M alternating path exist? Explain your answer.

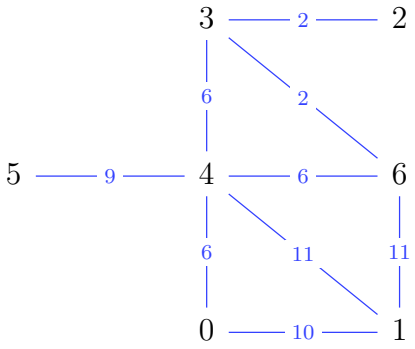


Since the given minimum vertex cover has 6 elements, according to the equilibrium theorem, the matching number of the given graph is 6. The given

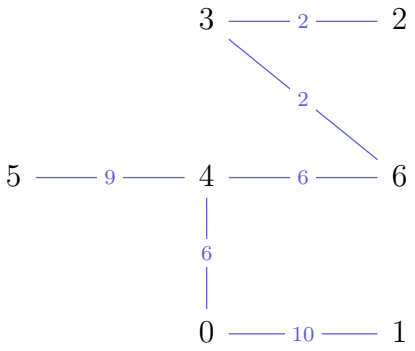
matching M has exactly that many vertices, making it a maximal matching. By a theorem proven during the lecture, a matching M is maximal if and only if there is no M alternating path. The latter theorem makes the given matching M have no alternating path.

Problem 10

Apply the greedy algorithm to find a minimal spanning tree for the weighted graph given in Figure 2 (B).



Applying the greedy algorithm for the given weighted graph yields the following (minimal) spanning tree.



Problem 11

The cost matrix is given by the table of distances (in meters) below between different buildings on KIU campus. Use the "double nearest neighbor" algorithm to find the short trip through every building starting at building F.

	K	E	F	G	H
K	-	1620	1510	1380	1320
E	1620	-	110	240	310
F	1510	110	-	120	210
G	1380	240	120	-	90
H	1320	310	210	90	-

The trip starting at the building F achieved through the "double nearest neighbour" algorithm is

$$F \xrightarrow{110} E \xrightarrow{240} G \xrightarrow{90} H \xrightarrow{1320} K \xrightarrow{1510} F$$

With total distance of 3270 meters.

Problem 12

Let X be a set. Determine the neutral element for the composition on the power set $\mathcal{P}(X)$ defined by

$$A * B := A \cup B.$$

For all $A \in \mathcal{P}(X)$, we have $A \cup \varnothing = \varnothing \cup A = A$ and $\varnothing \in \mathcal{P}(X)$ as $\varnothing \subseteq X$, making $\varnothing$ the neutral element for the given composition.

Problem 13

Show that division is not an associative composition (binary operation) on the set of rational numbers without zero $\mathbb{Q} \setminus \{0\}$.

Division is not an associative composition on the set of nonzero rationals as $1/(1/2) = 1/\frac{1}{2} = \frac{1}{\frac{1}{2}} = 2 \neq \frac{1}{2} = 1/2 = \frac{1}{1}/2 = (1/1)/2$ despite $1, 2 \in \mathbb{Q}$.

Problem 14

Show that the group given by the following composition table is not abelian

	e	a	a^2	b	c	d
e	e	a	a^2	b	c	d
a	a	a^2	e	c	d	b
a^2	a^2	e	a	d	b	c
b	b	d	c	e	a^2	a
c	c	b	d	a	e	a^2
d	d	c	b	a^2	a	e

As suggested by the composition table, $ab = c$ and $ba = d$. Assuming $c \neq d$, we have $ab = c \neq d = ba$, meaning the group given by the composition table is not abelian.

Problem 15

What is the order of the element corresponding to the rotation by 135° in the symmetry group of an octagon (regular eight-sided polygon).

For a rotation by α degrees to be equal to the identity element of the symmetry group, α needs to be an integer divisible by 360. The rotation by 135° to the power of a positive n is equal to the rotation by $n \cdot 135°$. For the latter to be divisible by 360, since 135 is not even and 8 is a factor of 360, n needs to be divisible by 8. Also, $8 \cdot 135 = 8 \cdot 45 \cdot 3 = 360 \cdot 3$. Since there is no smaller positive multiple of 8 than 8 itself, $n = 8$ is the degree of the given rotation.

Problem 16

Describe the subgroup of $\mathbb{Z}$ generated by -190, 10 and 8.

The subgroup of $\mathbb{Z}$ generated by -190, 10 and 8, since $\mathbb{Z}$ is Abelian, consists of integers of the form $-190a + 10b + 8c$ with $a, b, c \in \mathbb{Z}$. We shall

prove that $\langle -190, 10, 8\rangle = \langle 2\rangle$. Let $x \in \langle -190, 10, 8\rangle$, i.e., there exist $a, b, c \in \mathbb{Z}$ with $x = -190a + 10b + 8c$. Then we also have $x = 2(-95a + 5b + 4c)$. But since $-95a + 5b + 4c \in \mathbb{Z}$, the latter implies $x \in \langle 2\rangle$. This shows that $\langle -190, 10, 8\rangle \subseteq \langle 2\rangle$. Now, let $x \in \langle 2\rangle$, i.e., there exists $a \in \mathbb{Z}$ with $x = 2a$. Then we also have $x = (-190\cdot 0+10\cdot 1+8\cdot(-1))a = (-190\cdot 0+10\cdot a+8\cdot(-a)$. But since $-a \in \mathbb{Z}$, the latter implies that $x \in \langle -190, 10, 8\rangle$. This shows that $\langle 2\rangle \subseteq \langle -190, 10, 8\rangle$. Finally, $\langle -190, 10, 8\rangle = \langle 2\rangle$.

Problem 17

Perform the following calculation in $\mathbb{Z}_5$:

$$4 \cdot 3^{-1} + 2 \cdot 6.$$

The multiplicative inverse of 3 modulo 5 is 2 as $3 \cdot 2 = 6 \equiv 1 \mod 5$. We thus have

$$4 \cdot 3^{-1} + 2 \cdot 6 \equiv 4 \cdot 2 + 12 \equiv 3 + 2 = 5 \equiv 0 \mod 5$$

Problem 18

Find the multiplicative inverse of 20 in $\mathbb{Z}_{97}$.

Hint: You may use the Euclidean algorithm to compute multiplicative inverses in $\mathbb{Z}_{97}$.

Using the Euclidean algorithm yields the following

$$\begin{aligned} 97 &= 4 \cdot 20 + 17 \\ 20 &= 1 \cdot 17 + 3 \\ 17 &= 5 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Meaning $1 = 3 - 2 = 3 - (17 - 5 \cdot 3) = 6 \cdot 3 - 17 = 6 \cdot (20 - 17) - 17 = 6 \cdot 20 - 7 \cdot 17 = 6 \cdot 20 - 7 \cdot (97 - 4 \cdot 20) = 34 \cdot 20 - 7 \cdot 97$, the inverse of 20 modulo 97 is thus 34.

Problem 19

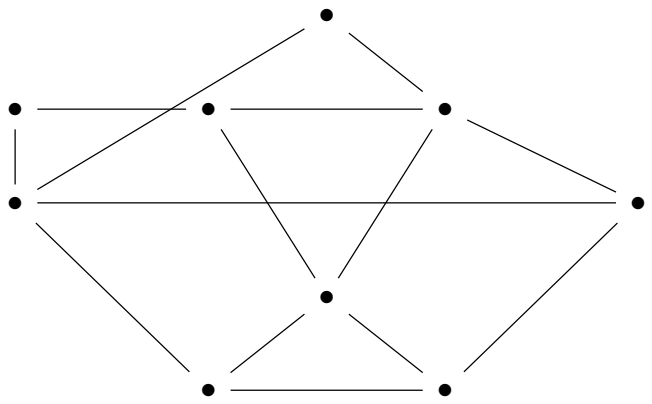
Is the following statement true? If H is a group and G_1, G_2 are its subgroups, then $G_1 \cup G_2$ is a subgroup of H. Prove or give a counter example.

Consider $H = D_3$ with $G_1 = \langle r \rangle$ and $G_2 = \langle s \rangle$ where r denotes an arbitrary nonneutral rotation and s denote reflection about an arbitrary fixed axis. Then $|G_1 \cup G_2| = 4$, but that means the order of $G_1 \cup G_2$ does not divide the order of D_3 as the latter is equal to 6. By the contrapositive statement of the Lagrange's theorem, $G_1 \cup G_2$ is not a subgroup of H in this case.

Problem 20

Bonus. In Figure 3 is a graph representing friendships between a group of students (each vertex is a student and each edge is a friendship).

Show whether it is possible for the students to sit around a round table in such a way that every students sits between two friends?



For that to be possible, we would require the graph to be Hamiltonian. The graph, in fact, does contain a Hamiltonian circuit as shown below.