Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Departement Informatik
Wintersession 2022

Prof. Ueli Maurer

Exam
Diskrete Mathematik

25. Januar 2022

Hinweise:

1.) **Erlaubte Hilfsmittel:** Selbstverfasste, handgeschriebene Notizen auf 6 A4-Seiten. Es ist erlaubt ein Wörterbuch zu benutzen. Es sind keine weiteren Hilfsmittel erlaubt.

2.) Falls nicht explizit ausgeschlossen dürfen Resultate (z.B. Lemmas oder Theoreme) aus dem Skript mit entsprechendem Verweis (z.B. *"Lemma Skript"*; die Nummer ist nicht notwending falls klar ist welches Resultat gemeint ist) ohne Beweis verwendet werden. Resultate aus der Übung dürfen **nicht** ohne Beweis verwendet werden.

3.) Die Aufgaben sind in drei Schwierigkeitsstufen von ($\star$) bis ($\star\star\star$) eingeteilt.

4.) Die Aufgaben sind direkt auf dem Prüfungsblatt zu lösen. Bei Platzmangel befinden sich am Ende der Prüfung vier Zusatzblätter. Weitere Zusatzblätter können während der Prüfung bei uns bezogen werden. **Nur von uns verteilte Zusatzblätter sind erlaubt.**

5.) Die Antwortfelder unter den Aufgaben sind jeweils grosszügig bemessen. Es ist oft nicht die Erwartung, dass eine Antwort das ganze Feld füllt.

6.) Bitte verwenden Sie einen dokumentenechten Stift (also keinen Bleistift) und nicht die Farben Rot oder Grün.

7.) Bitte legen Sie die Legi für die Ausweiskontrolle auf den Tisch.

8.) Sie dürfen bis 10 Minuten vor Ende der Prüfung vorzeitig abgeben und den Raum still verlassen.

9.) Mobiltelefone und Smartwatches müssen komplett ausgeschaltet sein (kein Standby) und dürfen nicht am Körper getragen werden.

Prüfungs-Nr.

Stud.-Nr.:

Korrektur:

	Punkte		Unterschrift	
Aufgabe	Max	Erreicht	Korr.	Ver.
1	31			
2	20			
3	25			
4	28			
Total	104			

Task 1. Sets, Relations and Functions .... **31 Points**

a) **Short Questions.** Each correct answer gives the indicated number of points. An unanswered question gives zero points. For each **wrong answer**, the indicated number of points are **deducted**. Overall, at least 0 points are given for the whole task. No justification is required.

1.) The sets $\varnothing \times \varnothing$ and $\{\varnothing\} \times \{\varnothing\}$ are equal. *(1 Point)*

☐ True ☐ False

2.) The set $\{\varnothing, \{\varnothing\}\}$ is a subset of $\{\varnothing\}$. *(1 Point)*

☐ True ☐ False

3.) For any two finite sets A and B we have $|A \cup B| = |A| + |B|$. *(1 Point)*

☐ True ☐ False

4.) For any two sets A and B there exists a set C such that

$$A = B \cap C \quad \text{or} \quad B = A \cap C.$$

(1 Point)

☐ True ☐ False

5.) For any set A, we have $A \cap \mathcal{P}(A) = \varnothing$. *(1 Point)*

☐ True ☐ False

6.) The relation $\rho = \{(1,2),(2,1)\}$ is transitive. *(1 Point)*

☐ True ☐ False

7.) The composition of two reflexive relations on some set A is always reflexive. *(1 Point)*

☐ True ☐ False

8.) 72 is the least upper bound of $\{4,6,9\}$ in the poset $(\{4,6,9,18,24,48,54,72,288\}; |)$. *(1 Point)*

☐ True ☐ False

9.) The set $\{f \in \{0,1\}^{\mathbb{N}} \mid \forall n \in \mathbb{N} \;\; f(2n) = f(4n)\}$ is countable. *(2 Points)*

☐ True ☐ False

10.) If the transitive closure of a binary relation ρ is uncountable, then ρ must be uncountable. *(2 Points)*

☐ True ☐ False

b) ($\star$) Let ρ and σ be relations on some non-empty set A. Prove or disprove:

If ρ is antisymmetric and σ is antisymmetric, then $\rho \circ \sigma$ is antisymmetric.

(4 Points)

c) ($\star$) Let A and B be two sets.

(i) Describe the set $(A \setminus B) \cup (B \setminus A)$ with the two sets

$$A \cap B \quad \text{and} \quad A \cup B$$

in an expression which contains only $A \cap B$, $A \cup B$, parentheses, as well as the symbols $\cup$, $\cap$, $\setminus$, and $\times$. Each of $A \cap B$ and $A \cup B$ is allowed to appear *at most twice*. No justification is required. *(1 Point)*

(ii) We fix an arbitrary element x. Phrase the statement that x is in the set $(A \setminus B) \cup (B \setminus A)$ if and only if it is in the set described in your answer of (i) as an equivalence of two propositional formulas F and G. Use only two atomic formulas U and V, where U being true is interpreted as $x \in A$ and V being true is interpreted as $x \in B$. No justification is required. *(2 Points)*

(iii) Prove that the two formulas described in (ii) are equivalent. *(2 Points)*

d) ($\star$) Let ρ be a reflexive relation on a non-empty A set such that

$$a \,\rho\, b \wedge b \,\rho\, c \quad \Longrightarrow \quad c \,\rho\, a$$

for any $a, b, c \in A$. Prove that ρ is an equivalence relation. *(4 Points)*

e) $(\star\,\star)$ Let Y be a non-empty finite set and let $f : \mathbb{N} \to Y$ be an arbitrary function. Prove the following statement:

There exists a strictly increasing function $g : \mathbb{N} \to \mathbb{N}$ such that $f \circ g$ is constant.

(6 Points)

Hint: A function $h : A \to B$ is constant if $h(a_1) = h(a_2)$ for all $a_1, a_2 \in A$.
Hint: A function $h : \mathbb{N} \to \mathbb{N}$ is strictly increasing if $x < y \implies h(x) < h(y)$ for any $x, y \in \mathbb{N}$.

Task 2. Number Theory .... **20 Points**

a) **Short Questions.** Each correct answer gives the indicated number of points. An unanswered question gives zero points. For each **wrong answer**, the indicated number of points are **deducted**. Overall, at least 0 points are given for the whole task. No justification is required.

1.) For any $n \in \mathbb{N} \setminus \{0\}$ and any $x, y, z \in \mathbb{Z}$: $x + y \equiv_n z$ if and only if $x \equiv_n z$ and $y \equiv_n z$. *(1 Point)*

☐ True ☐ False

2.) For any $a, b \in \mathbb{N} \setminus \{0\}$ and any $x, y \in \mathbb{Z}$: $x \equiv_{ab} y$ if and only if $x \equiv_a y$ and $x \equiv_b y$. *(1 Point)*

☐ True ☐ False

3.) For any $a, b \in \mathbb{Z}$: If there exist $u, v, d \in \mathbb{Z}$ such that $ua + vb = d$, then $\gcd(a, b) = d$. *(1 Point)*

☐ True ☐ False

b) ($\star$) Prove that for any $a, b \in \mathbb{Z}$ such that $a^2 = b^3 + 2$, we have $a^2 = 4q + 1$ for some $q \in \mathbb{Z}$. *(4 Points)*

c) ($\star\,\star$) Let $S \subseteq \mathbb{Z}$ be an infinite set such that

(i) $a - b \in S$ for any $a \in S$ and $b \in S$, and

(ii) $(c) \subseteq S$ for any $c \in S$.

Prove that there exists $u \in S$ such that $(u) = S$. *(6 Points)*

Hint: Recall that for any $d \in \mathbb{Z}$, we have $(d) = \{\, l \cdot d \mid l \in \mathbb{Z} \,\}$.

d) $(\star\star\star)$ Prove that for any $a, b, c, d \in \mathbb{N} \setminus \{0\}$ we have

$$ab = cd \quad \implies \quad a + b + c + d \text{ is not prime.}$$

(7 Points)

Task 3. Algebra .... **25 Points**

a) Short Questions. Each correct answer gives the indicated number of points. An unanswered question gives zero points. For each **wrong answer**, the indicated number of points are **deducted**. Overall, at least 0 points are given for the whole task. No justification is required.

1.) The polynomial $x + 5$ in $\mathbb{Z}_7[x]$ is irreducible. *(1 Point)*

☐ True ☐ False

2.) For any ring R: If there exist $a, b \in R \setminus \{0\}$ such that $a \cdot b = 0$, then R is not a field. *(1 Point)*

☐ True ☐ False

3.) The polynomial $x + 1$ divides the polynomial $x^7 + x^4 + x^2 + 4$ in the ring $\mathbb{Z}_5[x]$. *(1 Point)*

☐ True ☐ False

4.) In the ring $\mathbb{Z}_2[x]$, the polynomials $x^2 + 1$ and $x + 1$ are equal. *(1 Point)*

☐ True ☐ False

5.) Let $G = \langle g \rangle$ be an infinite cyclic group. For any $i, j \in \mathbb{Z}$ with $i \neq j$ we have $g^i \neq g^j$. *(1 Point)*

☐ True ☐ False

b) ($\star$) Compute the inverse of x in the group $\mathbb{Z}_5[x]^*_{x^2+1}$. *(1 Point)*

c) ($\star$) Let $\langle G; \cdot, {}^{-1}, e \rangle$ be a commutative group and fix an arbitrary element $z \in G$. Consider the algebra $\langle G; \star \rangle$ with

$$a \star b \stackrel{\text{def}}{=} z \cdot (a \cdot b) \qquad \text{for any } a, b \in G.$$

Prove that there exists $e' \in G$ such that $\langle G; \star, e' \rangle$ is a monoid. *(4 Points)*

d) ($\star$) **Disprove** the following claim:

For any two groups G and H, all subgroups of the direct product group $G \times H$ are of the form $G' \times H'$, where G' is a subgroup of G and H' a subgroup of H.

(3 Points)

e) (i) ($\star\,\star$) Let $\langle G; \star, \widehat{\ }, e_G \rangle$ and $\langle H; \odot, ^{-1}, e_H \rangle$ be two finite groups, and let $\psi : G \to H$ be an *injective* group homomorphism. Prove that for any $x \in G$ we have

$$\operatorname{ord}(x) = \operatorname{ord}(\psi(x)).$$

(4 Points)

Hint: You can use the fact that for any $x \in G$ and any $i \in \mathbb{Z}$ we have $\psi(x^i) = \psi(x)^i$.

(ii) ($\star\,\star$) Prove or disprove: There exists an injective homomorphism from $\mathbb{Z}_{14}^*$ to $\mathbb{Z}_{14}$.

(4 Points)

Hint: You can use the result from (i) *even if you did not prove it.*

f) ($\star$) Consider the ring $R = \mathbb{Z}_2[x]_{x^2+x+1}[y]$. Find a polynomial $p(y) \in R$ of degree 1 such that

$$p(1) = x \quad \text{and} \quad p(x) = x + 1.$$

(4 Points)

Task 4. Logic .... **28 Points**

a) Short Questions. Each correct answer gives the indicated number of points. An unanswered question gives zero points. For each **wrong answer**, the indicated number of points are **deducted**. Overall, at least 0 points are given for the whole task. No justification is required.

1.) The formulas $\exists x P(x) \vee \exists y Q(y)$ and $\exists x \exists y (Q(x) \vee P(y))$ are equivalent. *(1 Point)*

☐ True ☐ False

2.) For any formula F, the formulas $\forall x F$ and $\forall y F$ are equivalent. *(1 Point)*

☐ True ☐ False

3.) For any formula F, the formula $\exists x F$ is satisfiable if and only if F is satisfiable. *(1 Point)*

☐ True ☐ False

4.) The statement

$$F \wedge G \text{ is satisfiable} \quad \text{if and only if} \quad F \text{ is satisfiable and } G \text{ is satisfiable}$$

is true for any formulas F and G. *(1 Point)*

☐ True ☐ False

5.) The following derivation rule

$$\varnothing \quad \vdash \quad F \to (\neg F \to \neg G)$$

for a propositional calculus is correct (sound). *(1 Point)*

☐ True ☐ False

6.) The following derivation rule

$$F \quad \vdash \quad \neg G \to \neg(F \to G)$$

for a propositional calculus is correct (sound). *(1 Point)*

☐ True ☐ False

b) ($\star$) Consider the universe $U = \mathbb{Z}$. Express each of the following statements with a formula, in which the only predicates appearing are `less`, `equals` and `prime` (instead of `less`(n, m) and `equals`(n, m) you can write $n < m$ and $n = m$ accordingly). You can also use the symbols $+$ and $\cdot$ to denote addition and multiplication, and you can use constants (e.g., $0, 1, \ldots$). No justification is required. *(4 Points)*

i) The sum of two primes is never a prime.

ii) Every integer that is divisible by 3 and greater than 2 is the product of two primes.

c) ($\star$) Consider the formula

$$\exists z \forall y \; \big(P(z, f(y), x) \land \neg \exists x Q(x)\big) \;\; \lor \;\; \neg \exists z \forall x \; \neg R(z, g(x, z)).$$

Give an equivalent formula in prenex form. *(4 Points)*

Calculation. You will get full points if the answer above is correct. Otherwise, you may get partial points for the calculation in this box.

d) ($\star$) Let $\Pi_1 = (\mathcal{S}_1, \mathcal{P}_1, \tau_1, \phi_1)$ and $\Pi_2 = (\mathcal{S}_2, \mathcal{P}_2, \tau_2, \phi_2)$ be two proof systems. We combine Π_1 and Π_2 into a third proof system

$$\Pi_3 = (\mathcal{S}_1 \times \mathcal{S}_2, \mathcal{P}_1 \times \mathcal{P}_2, \tau_3, \phi_3),$$

where

$$\tau_3(s_1, s_2) = 1 \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \tau_1(s_1) = 1 \text{ or } \tau_2(s_2) = 1,$$

and

$$\phi_3((s_1, s_2), (p_1, p_2)) = 1 \quad \stackrel{\text{def}}{\Longleftrightarrow} \quad \phi_1(s_1, p_1) = 1 \text{ or } \phi_2(s_2, p_2) = 1.$$

Prove or disprove: *If Π_3 is complete, then Π_1 or Π_2 is complete.* *(4 Points)*

e) ($\star$) Consider the calculus consisting of the following three derivation rules:

$$\begin{aligned}\{F \to G, F\} &\quad \vdash_{R_1} \quad G \\ \varnothing &\quad \vdash_{R_2} \quad F \to (G \to F) \\ \varnothing &\quad \vdash_{R_3} \quad (\neg F \to \neg G) \to ((\neg F \to G) \to F)\end{aligned}$$

Formally derive B from $\{A, \neg A\}$ in the calculus. *(5 Points)*

f) ($\star$) Prove, **without** using any lemmas or theorems from the lecture notes, that for any formula F we have

$$F \models \exists x F.$$

Use the definition of $\models$ and the semantics of predicate logic. *(5 Points)*

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, "Task 3 b)").

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b)”).

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b)”).

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, "Task 3 b)").