PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com
PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

ask 1. Sets, Relations, Functions, and Proof Patterns .... 41 Poin

a) Short Questions. Each correct answer gives the number of points indicated in the brackets. No justification is required. In the following subtasks, let $A = \{\varnothing, \{\varnothing\}\}$.

1.) List all subsets of A which are elements of A. *(1 Point)*

2.) List all elements of $(A \cap \{\varnothing\}) \times \{A\}$. *(2 Points)*

3.) Compute the number of subsets of the set $\mathcal{P}(\mathcal{P}(A) \setminus A)$. *(2 Points)*

4.) Consider the relation $\rho = \{(\varnothing, \{\varnothing\}), (\{\varnothing\}, A), (A, \{\{\varnothing\}\})\}$ on $\mathcal{P}(A)$. Write the matrix representation of the transitive closure ρ^* of ρ. *(3 Points)*

5.) Find a non-empty set S and a relation ρ on S which is both an equivalence relation and a partial order relation. *(2 Points)*

6.) Give an explicit expression for an injective function $f : \mathbb{Z} \to \mathbb{N}$ such that $f(0) = 11$. *(2 Points)*

7.) Draw the Hasse Diagram of the poset $(\{1, 2, 3, 4, 6, 8, 12, 24\}; |)$. *(2 Points)*

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

(⋆) Consider the set $A = \mathbb{N}^{\mathbb{N}}$ of functions from natural numbers to natural numbers. On the set consider the relation ρ defined as

$$f \, \rho \, g \iff f(n) \mid g(n) \text{ for all but finitely many } n \in \mathbb{N}.$$

Prove or disprove that ρ is a partial order relation.

(3 Points)

c) (⋆) Let X be a non-empty set and let ρ and τ be relations on X. **Prove** the following statement:

$$(\tau \circ \rho) \circ \tau \subseteq \tau \Longrightarrow \rho \circ \tau \text{ is transitive .}$$

Explicitly justify each step in your solution. *(6 Points)*

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com
PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

) $(\star\,\star)$ Consider the following relation $\preccurlyeq$ on the set of integers $\mathbb{Z}$:

$$a \preccurlyeq b \iff |a| < |b| \quad \text{or} \quad |a| = |b| \text{ and } a \leq b.$$

Prove that $(\mathbb{Z}, \preccurlyeq)$ is a poset and that it is well-ordered. *(8 Points)*

$(\star\star\star)$ Consider the set A of sequences of natural numbers whose n-th value is a multiple of a values at indices which divide n:

$$A = \left\{ f \in \mathbb{N}^{\mathbb{N}} \mid \text{ for all } i, j \in \mathbb{N} \text{ if } i \mid j \text{ then } f(i) \mid f(j) \right\}.$$

Prove or disprove that the set A is countable. *(10 Points)*

.

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

ask 2. Number Theory . . . . 22 Poin

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

a) Short Questions. Each correct answer gives 1.5 points. No justification is required. *(6 Points)*

1.) Compute $R_{13}\left(7^{2024}\right)$.

2.) Compute $R_{77}(100000^{60})$.

3.) Compute $\varphi(\gcd(126, 72) \cdot 3^2)$.

4.) Compute $R_{100}(99^{99} + 99^{98} + 99^{97} \cdots + 99^{0})$.

b) ($\star$ $\star$) The servers of the bank *Debit Bliss* have been hacked. A list of usernames and respective **RSA-encrypted** passwords are leaked online. The encrypted password of a certain `ronalddump@potus.com` is 2. Knowing that the public-key is $(N, e) = (299, 151)$, recover Ronald Dump's password. **Show your work.**

Hint: $1 = 151 \cdot 7 - 4 \cdot 264$. *(6 Points)*

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com
PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

($\star$) Find all solutions in $\mathbb{Z}$ of the following system of equations:

$$x \equiv_3 2,$$
$$x \equiv_{10} 4,$$
$$x \equiv_7 6.$$

Show your work. *(4 Points)*

d) ($\star\star$) Let $a, b, c \in \mathbb{Z} \setminus \{0\}$. **Prove** that the equation $ax + by = c$ has solutions $(x, y) \in \mathbb{Z}^2$ if and only if $\gcd(a, b) \mid c$. *(6 Points)*

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

ask 3. Algebra . . . . 37 Poin

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

a) Short Questions. Each correct answer gives the indicated number of points. No justification is required.

1.) List all elements of the group $\langle \mathbb{Z}_{26}; \oplus_{26} \rangle$ which are *not* generators. *(2 Points)*

2.) Consider the ring $\mathbb{Z}_{11}[x]$. Write $x^2 + 5x + 8$ as a product of irreducible elements. *(2 Points)*

3.) Find a polynomial $m(x) \in \mathbb{Z}_7[x]$ such that $\mathbb{Z}_7[x]_{m(x)}$ is a field with 49 elements. *(2 Points)*

4.) What is the number of non-isomorphic groups of order 37? *(1 Point)*

5.) Consider the $(5, 2)$-code $\{(0,0,0,0,0), (1,1,1,0,0), (0,0,1,1,1), (1,1,0,1,1)\}$ over the alphabet $\{0, 1\}$. What is its minimum distance? *(2 Points)*

6.) Let G be a group and let $x \in G$ be an element of order 8. What is the order of (x^{10}, x^{12}) in the direct product $G \times G$? *(2 Points)*

b) $(\star)$ Consider a group $\langle G; \star, \widehat{\ }, e_G \rangle$. **Prove** that $\widehat{(\widehat{a})} = a$. Each step in your solution must be justified explicitly by one of the group axioms. *(4 Points)*

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

($\star$ $\star$) Let $\langle G; \star, \widehat{\ }, e_G \rangle$ and $\langle H; \cdot, {}^{-1}, e_H \rangle$ be groups. Let $\phi : G \to H$ be an injective group homomorphism. **Prove** that for all $g \in G$ it holds that $\text{ord}(g) = \text{ord}(\phi(g))$. *(6 Points)*

d) ($\star$ $\star$) Consider a *finite* group $\langle G; \star, \widehat{\ }, e_G \rangle$. Let H be a subgroup of G. **Prove** that

$$T = \{g \in G \mid g \star h \star \widehat{g} \in H\}$$

is a subgroup of G.

Hint: use without proof that any injective function from a finite set to itself is also surjective. *(8 Points)*

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

($\star\,\star$) Let F be a field. **Prove** that the following two statements are equivalent.

1.) Every polynomial $a(x) \in F[x]$ with $\deg(a(x)) \geq 1$ has a root in F.

2.) For all $a(x), b(x) \in F[x]$, if $a(x)$ and $b(x)$ have no common root, then $\gcd(a(x), b(x)) = 1$.

(8 Points)

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

a) Short Questions. Each correct answer gives the indicated number of points. No justification is required.

1.) Circle all *symbols* that occur free in the formula

$$\forall x (P(x) \land Q(x, g(y))) \land \exists y\, Q(y, x).$$

(2 Points)

2.) Find a formula in disjunctive normal form which is equivalent to

$$(A \to B) \land \neg(A \land \neg C)$$

in which each atomic formula appears at most once. *(2 Points)*

3.) Circle *all* the correct derivation rules among the following.

$\{F, \neg F\} \vdash_{R1} G$ $\quad F \to G \vdash_{R2} G$ $\quad \vdash_{R3} (F \to G) \lor (G \to F)$ $\quad \{F \lor G, \neg G\} \vdash_{R4} F \lor H$

(2 Points)

4.) Find a formula in prenex normal form equivalent to

$$\exists x ((\forall y\, P(x, y)) \to Q(z)) \land P(y, x).$$

(2 Points)

b) ($\star$) Let F, G and H be formulas in propositional logic. **Prove or disprove** the following statement: if G is satisfiable, and $\neg H$ is a tautology, then $(F \to H) \to G$ is satisfiable. *(5 Points)*

(⋆ ⋆) Use the resolution calculus to **prove** the statement

$$\neg(A \land B) \land (\neg B \to \neg D) \land (A \to D) \models \neg(C \to A) \lor (\neg A \land \neg C)$$

(10 Points)

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

(⋆) Consider the proof systems

$$\Sigma_1 = (\mathcal{S}_1, \mathcal{P}_1, \tau_1, \phi_1),$$
$$\Sigma_2 = (\mathcal{S}_2, \mathcal{P}_2, \tau_2, \phi_2).$$

Consider the new proof system derived from Σ_1 and Σ_2 as follows:

$$\Sigma = (\mathcal{S}_1 \times \mathcal{S}_2, \mathcal{P}_1 \times \mathcal{P}_2, \tau, \phi)$$

where

$$\tau(s_1, s_2) = 1 \iff \text{at least one of } \tau_1(s_1) \text{ and } \tau_2(s_2) \text{ equals 1.}$$

and

$$\phi((s_1, s_2), (p_1, p_2)) = 1 \iff \text{exactly one of } \phi_1(s_1, p_1) \text{ and } \phi_2(s_2, p_2) \text{ equals 1.}$$

Prove or disprove the following statement: if both Σ_1 and Σ_2 are sound, then Σ is sound. *(4 Points)*

Prove or disprove the following statement: if both Σ_1 and Σ_2 are complete, then Σ is complete. *(4 Points)*

($\star\star$) **Prove** that for all formulas F and G

$$(\exists x\, F) \wedge \forall x (F \rightarrow G) \ \models\ \exists x (F \wedge G).$$

Do **not** use any theorems or lemmas from the lecture notes. Use the definition of $\models$ and the semantics of predicate logic. *(8 Points)*

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com
PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

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)").

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

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)”).

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

PDF-XChange Editor
Click to BUY NOW!
www.pdf-xchange.com

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)”).