Final Exam

Reference Sheet

Set operations and functions

Definition 1. The *empty set* $\emptyset$ is the set that contains no elements.

Definition 2. The *union* of A and B is

$$A \cup B = \big\{x \,|\, x \in A \text{ or } x \in B\big\}.$$

Definition 3. The *intersection* of A and B is

$$A \cap B = \big\{x \,|\, x \in A \text{ and } x \in B\big\}.$$

Definition 4. We say that A and B are *disjoint* when $A \cap B = \emptyset$.

Definition 5. We say that A is a *subset* of B if

$$\forall x : \big(x \in A \to x \in B\big).$$

In this case, we write $A \subseteq B$.

Definition 6. The *difference* of A and B is

$$B \backslash A = \{x \in B \,|\, x \notin A\}.$$

Definition 7. The *symmetric difference* of A and B is $A \,\Delta\, B = A \backslash B \cup B \backslash A$.

Definition 8. If $A \subseteq B$, then the *complement* of A in B is $A^c = B \backslash A$.

Definition 9. The *composition* of $f : A \to B$ and $g : B \to C$ is

$$\begin{aligned} g \circ f : A &\to C \\ x &\mapsto g(f(x)). \end{aligned}$$

Injective and surjective functions

Definition 10. The function $f : A \to B$ is said to be *injective* if $f(x) = f(y)$ implies $x = y$.

Definition 11. The function $f : A \to B$ is called *surjective* when for every $y \in B$ there is an $x \in A$ with $f(x) = y$.

Definition 12. We say that $f : A \to B$ is *bijective* when it is both injective and surjective.

Definition 13. The *restriction* of $f : A \to B$ to S is the function

$$\begin{aligned} f|_S : S &\to B \\ x &\mapsto f(x). \end{aligned}$$

Limits

Definition 14. We say that $f(x) \to \infty$ as $x \to \infty$, or that $\lim_{x\to\infty} f(x) = \infty$, when

$$\forall M > 0 : \exists N > 0 : \forall x > N : f(x) > M.$$

In this case, we write $\lim_{x\to\infty} f(x) = \infty$.

Definition 15. Fix $L \in \mathbb{R}$. We say that $f(x) \to L$ as $x \to \infty$, or that $\lim_{x\to\infty} f(x) = L$, when

$$\forall \epsilon > 0 : \exists N > 0 : \forall x > N : |f(x) - L| < \epsilon.$$

Definition 16. Fix $x_0 \in \mathbb{R}$. We say that $f(x) \to \infty$ as $x \to x_0$, or that $\lim_{x\to x_0} f(x) = \infty$, when

$$\forall M > 0 : \exists \delta > 0 : \forall x \in \mathbb{R} : |x - x_0| < \delta \implies f(x) > M.$$

Definition 17. Fix $x_0 \in \mathbb{R}$ and $L \in \mathbb{R}$. We say that $f(x) \to L$ as $x \to x_0$, or that $\lim_{x\to\infty} f(x) = L$, when

$$\forall \epsilon > 0 : \exists \delta > 0 : \forall x \in \mathbb{R} : |x - x_0| < \delta \implies |f(x) - L| < \epsilon.$$

Relations

Definition 18. The *Cartesian product* of A and B is the set of ordered pairs

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Definition 19. A *relation* from A to B is a subset $R \subseteq A \times B$.

Definition 20. The *domain* of $R \subseteq A \times B$ is the subset

$$\operatorname{Dom} R = \{a \in A \mid \exists b \in B : aRb\},$$

and the *range* is

$$\operatorname{Rng} R = \{b \in B \mid \exists a \in A : aRb\}.$$

Definition 21. A *function* from A to B is a relation $f \subseteq A \times B$ such that

$$\forall a \in A : \exists!\, b \in B : (a, b) \in f.$$

We usually write $(a, b) \in f$ as $f(a) = b$.

Definition 22. If $R \subseteq A \times B$ is a relation from A to B, then the *inverse* of R is the relation $R^{-1} \subseteq B \times A$ given by

$$bR^{-1}a \iff aRb.$$

Definition 23. If R is a relation from A to B, and if S is a relation from B to C, then the *composition* of R and S is

$$S \circ R = \{(a, c) \mid \exists b \in B : aRb \wedge bSc\}.$$

Equivalence relations and partial orders

Definition 24. We say that the relation R on A is

- *reflexive* when $\forall a \in A : aRa$
- *transitive* when $\forall a, b, c \in A : (aRb \wedge bRc) \implies aRc$

- *symmetric* when $\forall a, b \in A : aRb \implies bRa$
- *antisymmetric* when $\forall a, b \in A : (aRb \wedge bRa) \implies a = b$

Definition 25. The relation R on A is

- an *equivalence relation* when it is reflexive, transitive, and symmetric;
- a *partial order* when it is reflexive, transitive, and antisymmetric.

Definition 26. A set A equipped with a partial order R is called a *partially ordered set* or a *poset*.

Definition 27. The *quotient map* associated to a set A with equivalence relation $\sim$ is the function

$$\begin{aligned} q : A &\to A/\!\sim \\ a &\mapsto [a]. \end{aligned}$$

Number systems

Definition 28. The *complex numbers* $(\mathbb{C}, +, \times)$ comprise

1. the set $\mathbb{C} = \mathbb{R}^2$,
2. the binary operation

$$\begin{array}{rccc} + : & \mathbb{C}^2 & \longrightarrow & \mathbb{C} \\ & ((a,b),(a',b')) & \longmapsto & (a+a', b+b'), \end{array}$$

3. the binary operation

$$\begin{array}{rccc} \times : & \mathbb{C}^2 & \longrightarrow & \mathbb{C} \\ & ((a,b),(a',b')) & \longmapsto & (aa'-bb', ab'+a'b). \end{array}$$

Definition 29. The *rational numbers* $(\mathbb{Q}, +, \times)$ consist of

1. the set $\mathbb{Q} = \{(p,q) \in \mathbb{Z}^2 \mid q \neq 0\} /\!\sim$,
2. the binary operation

$$\begin{array}{rccc} + : & \mathbb{Q}^2 & \longrightarrow & \mathbb{Q} \\ & \big([(p,q)],[(p',q')]\big) & \longmapsto & \big[(pq'+p'q, qq')\big], \end{array}$$

3. the binary operation

$$\begin{array}{rccc} \times : & \mathbb{Q}^2 & \longrightarrow & \mathbb{Q} \\ & \big([(p,q),(p',q')]\big) & \longmapsto & \big[(pp', qq')\big]. \end{array}$$

Definition 30. The *integers* $(\mathbb{Z}, +, \times)$ consist of

i. the set $\mathbb{Z} = \mathbb{N}^2$,

ii. the binary operation

$$\begin{array}{rccc} + : & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z} \\ & ((m,n),(m',n')) & \longmapsto & (m+m', n+n'), \end{array}$$

iii. the binary operation

$$\begin{array}{rccc} \times : & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z} \\ & ((m,n),(m',n')) & \longmapsto & (mm'+nn', mn'+m'n). \end{array}$$

Algebraic structures with one binary operation

Definition 31. A *binary operation* on A is a function

$$* : A \times A \to A.$$

Definition 32. A *magma* $(A, *)$ is a set A equipped with a binary operation $* : A \times A \to A$.

Definition 33. We say that $*$ is

- *commutative* when
$$\forall a, b \in A : a * b = b * a$$
- *associative* when
$$\forall a, b, c \in A : (a * b) * c = a * (b * c)$$

Definition 34. We say that $(A, *)$ is a *semigroup* when $*$ is associative. If $*$ is additionally commutative, then $(A, *)$ is called a *commutative semigroup*.

Definition 35. We say that $e \in A$ is an *identity element* for $* : A \times A \to A$ when

$$\forall a \in A : a * e = a = e * a.$$

Definition 36. A semigroup $(A, *)$ that admits an identity element $e \in A$ is called a *monoid*.

Definition 37. Fix an element $a \in A$. If $b \in A$ satisfies

$$a * b = e = b * a$$

then b is called an *inverse element* of a, and we write $b = a^{-1}$.

Definition 38. A semigroup $(A, *)$ is called a *group* when every $a \in A$ has an inverse $a^{-1} \in A$.

Definition 39. A group $(A, *)$ is an *abelian group* when $*$ is commutative.

Algebraic structures with multiple binary operations

Definition 40. A *ring* $(R, +, \cdot)$ comprises a set R and two binary operations $+, \cdot : R \times R \to R$, such that

i. $(R, +)$ is an abelian group,

ii. $(R, \cdot)$ is a monoid,

iii. the operation $\cdot$ *distributes* over $+$, that is, for all $a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Definition 41. A *zero divisor* in a commutative ring $(A, +, \cdot)$ is an element $a \in A$ for which there exists a nonzero $b \in A$ with $ab = 0$.

Definition 42. A commutative ring $(R, +, \cdot)$ is called an *integral domain* when

i. it does not contain any nonzero zero divisor,

ii. $0 \neq 1$.

Definition 43. An integral domain $(R, +, \cdot)$ is called a *field* when every nonzero element $a \in R \backslash \{0\}$ has a multiplicative inverse $a^{-1} \in R$,

Definition 44. A *k-vector space* $(V, +, \cdot)$ comprises a set V together with operations

$$+ : V \times V \to V$$

and

$$\cdot : k \times V \to V$$

such that

i. $(V, +)$ is an abelian group

ii. *scalar multiplication* $\cdot$ and *vector addition* $+$ satisfy

$$\begin{aligned} 1 \cdot u &= u \\ (a + b) \cdot u &= (a \cdot u) + (b \cdot u) \\ a \cdot (b \cdot u) &= (a \cdot b) \cdot u \\ a \cdot (u + v) &= (a \cdot u) + (a \cdot v) \end{aligned}$$

Definition 45. An *R-module* $(V, +, \cdot)$ comprises a set V together with operations

$$+ : V \times V \to V$$

and

$$\cdot : k \times V \to V$$

that together satisfy the familiar vector space conditions.

Homomorphisms

Definition 46. A homomorphism $f : X \to Y$ is called a

i. *monomorphism* if

$$\forall\, (g, g' : Z \to X) : (f \circ g = f \circ g') \implies g = g',$$

that is, f is *left-cancellative*,

ii. *epimorphism* if

$$\exists\, (h : Y \to X) : (h \circ f = h' \circ f) \implies h = h',$$

that is, f is *right-cancellative*,

iii. *isomorphism* if

$$\exists\, (k : Y \to X) : (f \circ k = \mathrm{id}_Y) \,\wedge\, (k \circ f = \mathrm{id}_X),$$

that is, f has an *inverse* k.

Definition 47. i. A homomorphism $f : X \to X$ is called an *endomorphism.*

ii. An isomorphism $f : X \to X$ is called an *automorphism.*

Definition 48. We say that X and Y are *isomorphic* if there exists an isomorphism $f : X \xrightarrow{\sim} Y$.

Definition 49. A *group homomorphism* from $(G, \cdot)$ to $(H, *)$ is a function $f : G \to H$ such that

$$\forall g, g' \in G \;:\; f(g \cdot g') = f(g) * f(g').$$

Definition 50. A *ring homomorphism* from $(R, +, \cdot)$ to $(S, \oplus, *)$ is a function $f : R \to S$ such that for all $r, r' \in R$,

i. $f(r + r') = f(r) \oplus f(r')$,

ii. $f(r \cdot r') = f(r) * f(r')$,

iii. $f(1_R) = 1_S$.

Definition 51. A *field homomorphism* is a ring homomorphism between fields.

Definition 52. A *monotone map* of posets from $(A, \leq)$ to $(B, \preccurlyeq)$ is a function $f : A \to B$ such that

$$\forall a, a' \in A : a \leq a' \implies f(a) \preccurlyeq f(a').$$

An *order embedding* is an injective monotone map, and an *order isomorphism* is a bijective monotone map.

Definition 53. A *linear map* of k-vector spaces from U to V is a function $f : U \to V$ such that

i. $f(u + u') = f(u) + f(u')$ for all $u, u' \in U$, and

ii. $f(su) = sf(u)$ for all $u \in U$ and $s \in k$.

Metric spaces

Definition 54. A *metric* on X is a function

$$d : X \times X \to \mathbb{R}_{\geq 0}$$

satisfying

i. $d(x, y) = 0$ if and only if $x = y$,

ii. $d(x, y) = d(y, x)$,

iii. $d(x, z) \leq d(x, y) + d(y, z)$ (*triangle inequality*).

The pair (X, d) is called a *metric space*.

Definition 55. A *norm* on a vector space V is a function

$$\| \cdot \| : V \to \mathbb{R}_{\geq 0}$$

such that

i. $\|v\| = 0$ if and only if $v = 0$,

ii. $\|sv\| = |s| \, \|v\|$,

iii. $\|u + v\| \leq \|u\| + \|v\|$ (*triangle inequality*).

The pair $(V, \| \cdot \|)$ is called a *normed vector space*.

Definition 56. Let $(x_i)_i$ be a sequence in (X, d) and fix $x \in X$. We say that $(x_i)_i$ *converges* to x if

$$\forall \epsilon > 0 : \exists N \in \mathbb{N} : \forall n \geq N : d(x_n, x) \leq \epsilon.$$

In this case, we write $x_i \to x$ or $\lim_{i \to \infty} x_i = x$ and we say that x is the *limit* of $(x_i)_i$.

Definition 57. If the sequence $(x_i)_i$ does not converge to any point $x \in X$, then $(x_i)_i$ is said to *diverge*.

Continuous functions

Definition 58. A function $f : X \to Y$ is *continuous at* $x \in X$ when

$$\forall \epsilon > 0 : \exists \delta > 0 : \forall y \in X : d_X(x, y) < \delta \implies d_Y(f(x), f(y)) < \epsilon.$$

Definition 59. We say that $f : X \to Y$ is *continuous* if it is continuous at every $x \in X$.

Cardinality

Definition 60. Two sets A and B are *equivalent* (or in *one-to-one correspondence*) if there exists a bijection from A to B. In this case, we write $A \approx B$.

Definition 61. The *cardinality* of a finite set $A = \{a_1, \ldots, a_k\}$ is the number $k \in \mathbb{N}$ of elements in A.

Definition 62. We write

$$\begin{aligned}
&|A| = |B| \text{ when } \exists \text{ bijection } f : A \xrightarrow{\sim} B, \\
&|A| \leq |B| \text{ when } \exists \text{ injection } f : A \hookrightarrow B, \\
&|A| < |B| \text{ when } |A| \leq |B| \text{ and } |A| \neq |B|.
\end{aligned}$$