Exam topics

1. Basic structures: sets, lists, functions
   (a) Sets $\{\ \}$: write all elements, or define by condition
   (b) Set operations: $A\cup B$, $A\cap B$, $A\backslash B$, A^c
   (c) Lists $(\ )$: Cartesian product $A\times B$
   (d) Functions $f : A \to B$ defined by any input-output rule
   (e) Injective function: $\forall a_1, a_2\in A$: $a_1\neq a_2 \Rightarrow f(a_1)\neq f(a_2)$
   (f) Surjective function: $\forall b\in B$, $\exists a\in A$ with $f(a) = b$
   (g) A, B have same cardinality: there is a bijection $f : A \to B$
   (h) A is countable: there is a bijection $f : \mathbb{N} \to A$
2. Formal logic
   (a) Statements: definitely true or false
   (b) Conditional (open) statement $P(x)$: true/false depends on variable x
   (c) Logical operations: *and*, *or*, *not*, *implies*
   (d) Truth tables and logical equivalence
   (e) Implication $P \Rightarrow Q$ equivalent to: contrapositive $not(Q) \Rightarrow not(P)$;
   independent from: converse $Q \Rightarrow P$; inverse $not(P) \Rightarrow not(Q)$
   (f) Negate implication: $not(P \Rightarrow Q)$ is equivalent to: P *and* $not(Q)$
   (g) Quantifiers: $\forall$ for all , $\exists$ there exists;
   (h) Negate quantifiers: $not(\forall x, P(x))$ is equivalent to: $\exists x, not(P(x))$
   (i) Logical equivalences and set equations
   (j) Logic in mathematical language versus everyday language
3. Methods of proof (can be combined)
   (a) Direct proof
   (b) Proof by cases
   (c) Proof of the contrapositive
   (d) Proof by contradiction
   (e) Proof by induction (also complete induction)
4. Axioms of a Group $(G, *)$ (All variables below mean elements of G.)
   (a) Closure: $a * b \in G$.
   (b) Associativity: $(a * b) * c = a * (b * c)$
   (c) Identity: There is e with $e * a = a$ and $a * e = a$ for all a.
   (d) Inverses: For each a, there is some b with $a * b = e$ and $b * a = e$.
   Extra axioms
   (e) Commutativity: $a * b = b * a$.
   (f) Distributivity of times over plus: $a\cdot(b + c) = a\cdot b + a\cdot c$ and $(b + c)\cdot a = b\cdot a + c\cdot a$.
5. Divisibility of integers (All variables below mean integers.)
   (a) Divisibility: $a|b$ means $b = ac$ for some $c \in \mathbb{Z}$

(b) Properties of divisibility:
- $a \mid b, c \implies a \mid mb{+}nc$ for all m, n
- $a|b$ and $b|c \implies a|c$.
- $a|b$ and $b|a \implies a = \pm b$.

(c) Prime and composite
- Test: a is composite $\implies a$ has prime factor $p \leq \sqrt{a}$.

(d) Greatest common divisor $\gcd(a, b)$; relatively prime means $\gcd(a, b) = 1$.

(e) Division Lemma: $a = qb + r$ with remainder $0 \leq r < b$.

(f) Euclidean Algorithm computes remainders $a > b > r_1 > \cdots > r_k > 0$.
- Computes $\gcd(a, b) = r_k$.
- Finds m, n with $\gcd(a, b) = ma + nb$.

(g) Consequences of $\gcd(a, b) = ma + nb$
- Find integer solutions (x, y) to equation $ax + by = c$, if $\gcd(a, b) \mid c$.
- If $e|a$ and $e|b$, then $e| \gcd(a, b)$.
- Euclid's Lemma: If $c \mid ab$ and $\gcd(c, a) = 1$, then $c|b$.
- Prime Lemma: If p is prime with $p \mid ab$, then $p|a$ or $p|b$.
- For $\bar{a} \in \mathbb{Z}_n$, find multiplicative inverse $\bar{b} = \bar{a}^{-1}$, i.e $ab \equiv 1 \pmod{n}$.

(h) Fundamental Theorem of Arithmetic
- $n > 1$ is a product of primes uniquely, except for rearranging factors.
- There is a unique list of powers $s_1, s_2, s_3, \ldots \geq 0$ with: $n = 2^{s_1} 3^{s_2} 5^{s_3} 7^{s_4} 11^{s_5} \cdots$.

6. Equivalence relation $\sim$ on a set S

(a) Defining properties:
- Reflexive: $a \sim a$
- Symmetric: If $a \sim b$, then $b \sim a$.
- Transitive: If $a \sim b$ and $b \sim c$, then $a \sim c$

(b) Equivalence class $[a] = \{b \in S \mid b \sim a\}$. Following are logically the same:
- $a \sim b$
- $a \in [b]$
- $[a] = [b]$, the same set

7. Clock arithmetic $\mathbb{Z}_n$

(a) Modular equivalence: $a \equiv b \pmod{n}$ means $n \mid a{-}b$. Class $\overline{a} = [a]$.

(b) Equivalence class $\overline{a} = [a]$. $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n{-}1}\}$

(c) Modular addition and multiplication satisfy all usual rules of algebra

(d) Modular division: $\overline{a}^{\,-1} = \overline{b}$, where $\overline{a}\overline{b} = \overline{1}$, provided $\gcd(a, n) = 1$.

(e) In $\mathbb{Z}_p$ with p prime, every $\overline{a} \neq \overline{0}$ has $\overline{a}^{\,-1} \in \mathbb{Z}_p$.

8. Limits

(a) Completeness: If $S \subset \mathbb{R}$ has upper bound, then $\text{lub}(S) = \sup(S) \in \mathbb{R}$.

(b) Convergent sequence $\lim\limits_{n\to\infty} a_n = \ell$: $\forall \epsilon{>}0, \exists N \in \mathbb{N},\ n \geq N \Rightarrow |a_n{-}\ell| < \epsilon$

(c) Divergent sequence (a_n): $\forall \ell \in \mathbb{R}, \exists\, \epsilon{>}0, \forall N \in \mathbb{N}, \exists\, n{\geq}N$ with $|a_n{-}\ell| \geq \epsilon$.

(d) Infinite limit $\lim\limits_{n\to\infty} a_n = \infty$: $\forall B \in \mathbb{R}, \exists N \in \mathbb{N},\ n \geq N \Rightarrow a_n > B$.