Remark: The list of topics below is not exhaustive. It is likely that there will be things on the exam which do not appear in this study guide.

Know the definition of ...

(1) ... \( g.c.d.(a, b) \) the greatest common divisor of 2 integers.
(2) ... multiplication of complex numbers, and multiplication of complex numbers in polar form.
(3) ... a binary structure.
(4) ... an isomorphism of binary structures.
(5) ... a group.
(6) ... a subgroup, \( H \leq G \).
(7) ... \( \mathbb{Z}_n \), the group of integers modulo \( n \).
(8) ... \( U_n \), the \( n \)th roots of unity.
(9) ... \( \text{GL}_n(\mathbb{R}) \), the general linear group.
(10) ... \( \text{SL}_n(\mathbb{R}) \), the special linear group.
(11) ... \( S_n \), the \( n \)th symmetric group.
(12) ... \( S_A \), the group of permutations of \( A \).
(13) ... the order of an element \( x \in G \).
(14) ... \( \langle x \rangle \), the subgroup generated by an element \( x \in G \).
(15) ... an equivalence relation \( \sim \) on a set \( S \).
(16) ... an equivalence class of an equivalence relation \( \sim \).
(17) ... congruence modulo \( n \).

For every subgroup in the list of definitions above, you should know how to prove it’s a subgroup.

Be comfortable with the following:

(1) For any \( n > 0 \), and any \( m \in \mathbb{Z} \), \( m = qn + r \) for unique \( q, r \in \mathbb{Z} \) with \( 0 \leq r \leq n - 1 \).
(2) \( g.c.d.(m, n) = am + bn \) for some \( a, b \in \mathbb{Z} \).
(3) A nonempty subset \( S \subset G \) is a subgroup \( \iff S \) is closed under \(*\), and for all \( x \in S \), \( x^{-1} \in S \).
(4) **Theorem.** Any subgroup of a cyclic group is cyclic.
(5) **Theorem.** Two cyclic groups are isomorphic \( \iff \) they have the same order.
(6) **Theorem.** If \( G \) is a cyclic group of order \( n \), with generator \( x \in G \), then

\[ \langle x^k \rangle = \langle x^\ell \rangle \iff g.c.d.(k, n) = g.c.d.(\ell, n). \]

(7) Finding all the subgroups of cyclic groups.
(8) Finding all the generators of cyclic groups.
(9) Standard operations with permutations (composition, taking inverses).