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) ... \((a, b)\) the greatest common divisor of 2 integers.
(2) ... multiplication of complex numbers, and multiplication of complex numbers in polar form.
(3) ... a group.
(4) ... a subgroup, \(H \leq G\).
(5) ... \(S_n\), the \(n\)th symmetric group.
(6) ... \(A(S)\), the group of bijections of a set.
(7) ... \(D_{2n}\), the dihedral group of order \(2n\).
(8) ... \(\mathbb{Z}_n\), the integers modulo \(n\).
(9) ... \(Z(G)\), the center of a group.
(10) ... \(U_n\), the group of integers with multiplicative inverses modulo \(n\).
(11) ... \(C(x)\), the centralizer of an element \(x \in G\).
(12) ... \(\langle x \rangle\), the order of an element \(x \in G\).
(13) ... \(\langle S \rangle\), the subgroup generated by a subset \(S \subset G\).
(14) ... an equivalence relation \(\sim\) on a set \(S\).
(15) ... an equivalence class of an equivalence relation \(\sim\).
(16) ... congruence modulo \(n\).
(17) ... a left coset \(aH\) of a subgroup \(H \leq G\).
(18) ... a right coset \(Ha\) of a subgroup \(H \leq G\).
(19) ... a homomorphism \(\varphi:\ G \to H\).
(20) ... \(\text{Ker}(\varphi)\), the kernel of a homomorphism \(\varphi\).
(21) ... \(\text{Im}(\varphi)\), the image of a homomorphism \(\varphi\).
(22) ... \(N \trianglelefteq G\), a normal subgroup of \(G\).

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

Know the statement and or proof of the following:

(1) Euclid’s algorithm for g.c.d.s.
(2) \((a, b) = ma + nb\) for some \(m, n \in \mathbb{Z}\).
(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) \(Z(D_{10}) = \{e\}\).
(5) If \(G\) is finite then for all \(x \in G\) there exists a positive integer \(n\) such that \(x^n = e\).
(6) If \(H, K \leq G\) are subgroups of \(G\), prove that \(H \cap K\) is a subgroup of \(G\).
(7) If \(H \leq G\), then \(x \sim y \iff xy^{-1} \in H\) is an equivalence relation on \(G\).
(8) For the above equivalence relation the equivalence classes are \([a] = Ha\), i.e. the right cosets.
(9) Lagrange’s Theorem.
(10) If \(a, n \in \mathbb{Z}\) and \((a, n) = 1\) then \(a^{\varphi(n)} \equiv 1 \pmod{n}\).
(11) Let \(a, p \in \mathbb{Z}\). If \(p\) is a prime and \(p \nmid a\), then \(a^{p-1} \equiv 1 \pmod{p}\).
(12) There is an injective homomorphism \(\varphi: S_n \to GL_n(\mathbb{R})\).
(13) Cayley’s Theorem.