This is (a lower bound on) what I expect you to know about group theory starting this course. If you are rusty on this stuff now is a good time to brush up.

(1) A *group* is a nonempty set equipped with an associative binary operation, which has an identity element and inverses. The (unique) identity element is usually written as e, and the (unique) inverse of a is usually written as a^{-1}.

We can summarise the axioms equationally as $eg = ge = g$, $a(bc) = (ab)c$, $aa^{-1} = a^{-1}a = e$.

(2) $(ab)^{-1} = b^{-1}a^{-1}$, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

(3) G is *abelian* if and only if the group operation is commutative.

(4) If X is a set then a *permutation* of X is a bijection from X to X. The permutations of X form a group under composition, which we denote by Σ_X.

(5) If G is a group a *subgroup* is a nonempty subset closed under the group operation, and itself forming a group. H is a subgroup if and only if H is nonempty and closed under the operation $(g, h) \mapsto gh^{-1}$. We write $H \leq G$ for "H is a subgroup of G".

(6) If $H \leq G$ then the map $a \mapsto a^{-1}$ is a permutation of H.

(7) A *homomorphism (HM)* from G_1 to G_2 is a map $\phi : G_1 \to G_2$ such that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G_1$. Easily $\phi(e) = e$ and $\phi(a^{-1}) = \phi(a)^{-1}$. The composition of two HMs is a HM.

(8) If ϕ is a HM from G_1 to G_2 then the *image* of ϕ is $\{\phi(g) : g \in G_1\}$. It forms a subgroup of G_2.

(9) An injective HM from G_1 to G_2 is called a *monomorphism (MM)*. If ϕ is such a map then the *image* of ϕ is isomorphic to G_1 via ϕ.

(10) If G is a group and $g \in G$ then the map $h \mapsto gh$ is a permutation of G. This defines an injective HM from G to Σ_G. Slogan: "every group is isomorphic to a subgroup of a permutation group".

(11) An *isomorphism (IM)* is a bijective HM, and two groups are *isomorphic* if and only if there is an IM between them. We write $A \simeq B$ in this case. Isomorphism is an equivalence relation.

(12) An *automorphism (AM)* of G is an IM from G to G. The automorphisms of G form a group under composition which we write as $Aut(G)$.

(13) If G is a group and $X \subseteq G$ then we write $\langle X \rangle$ for the least subgroup containing X. $\langle X \rangle$ is the set of all elements $x_1^{n_1} \ldots x_j^{n_j}$ for $x_i \in X, n_i \in \mathbb{Z}$. By convention the empty product is e, and of course $\langle \emptyset \rangle = \{e\}$.

(14) Let $H \leq G$, and define a binary relation on G in which x is related to y if and only if there is $h \in H$ such that $hx = y$. This is an equivalence relation, and the class to which x belongs is Hx, the *right coset of* x. The map $h \mapsto hx$ sets up a bijection between H and Hx. The right cosets form a partition of G. Similarly for *left cosets* xH.

Note that $Hx = Hy$ if and only if $y \in Hx$ and so forth.

(15) If $H \leq G$ and $x \in G$ then the map $g \mapsto g^{-1}$ sets up a bijection between xH and Hx^{-1}, and so $Hx = Hy$ if and only if $x^{-1}H = y^{-1}H$. This gives a bijection between the set of left cosets and the set of right cosets. The cardinality of the set of left (right) cosets is called the *index* of H in G and is written $[G : H]$.

WARNING: DO NOT ASSUME THAT GROUPS ARE FINITE IN THIS COURSE! IN PARTICULAR INDICES MAY BE INFINITE.

(16) If G is finite and $H \leq G$ then $|G| = |H| \times [G : H]$, in particular the order of H divides the order of G (Lagrange's theorem).

(17) If G is a group and x, g then the *conjugate of* x *by* g is gxg^{-1}, which we usually write as x^g. For each g the map $x \mapsto x^g$ is an AM of G. Since $x^{gh} = (x^h)^g$ this induces a HM from G to $Aut(G)$. When $X \subseteq G$ we often write X^g for $\{x^g : x \in X\}$.

(18) A subgroup $N \leq G$ is *normal* if it satisfies any one of the following list of equivalent conditions:
 (a) For all g, $gN = Ng$.
 (b) For all g, $N^g = N$.
 (c) For all g, $N^g \subseteq N$.

In ths case we write $N \lhd G$.

(19) Let $N \lhd G$. Then the product of an element of aN and an element of bN is an element of abN. We write G/N for the set of cosets and define an operation $(aN)(bN) = abN$. G/N forms a group under this operation and the map $g \mapsto gN$ is a HM from G to G/N.

(20) Let $\phi : G_1 \to G_2$ be a HM. Then the *kernel of* ϕ is $\{g \in G_1 : \phi(g) = e\}$. $\ker(\phi) \lhd G_1$. If $N \lhd G$ then the kernel of the *quotient HM* $g \mapsto gN$ is N.

(21) (FIRST IM THM, MOST IMPORTANT THM IN ELEMENTARY GROUP THEORY!!!!) Let $\phi : G_1 \to G_2$ be a HM and let $N = \ker(\phi)$. Then the map $gN \mapsto \phi(g)$ is an IM from G/N to $im(\phi)$.

(22) Let $\phi : G_1 \to G_2$ be a HM, then ϕ is injective if and only if $\ker(\phi) = \{e\}$.

(23) Let $N \lhd G$. Then there is a bijection between subgroups of G/N and subgroups of G containing N. Explicitly if $N \le M \le G$ then M corresponds to M/N, and M is the union of the cosets which comprise M/N. Moreover $M \lhd G$ if and only if $M/N \lhd G/N$, and in this case $G/M \simeq (G/N)/(M/N)$ via an IM which takes gM to $(gN)M/N$.

(24) Let G be a group and $a \in G$. Then $\langle a \rangle = \{a^m : m \in \mathbb{Z}\}$ is the image of the HM $m \mapsto a^m$ from $\mathbb{Z}$ to G. The kernel has form $n\mathbb{Z}$ for a unique $n \geq 0$, so $\langle a \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. If $n = 0$ then we say a has *infinite order*, otherwise we say that a *has order* n. We write $|a|$ for the order of a. If G is finite then $|a|$ divides $|G|$.