ALGEBRA I (GROUPS)

Paul Taylor (Trinity).

SETS AND FUNCTIONS.

This is not a course on set theory and logic: if you're interested in that subject there's a Part II course of the same name which is independent of most of Parts IA & IB. In this course you are required only to be familiar with the notation, although the axioms of extent [two sets are equal iff they have the same elements] and specification [there is a set having elements all those things which satisfy a given condition] are important.

LOGIC: $\wedge$ and $\vee$ or $\neg$ not $\Rightarrow$ implies
$\Leftrightarrow$, iff is equivalent to, implies and is implied by
SETS: $\cap$ intersection $\cup$ union Δ symmetric difference
$\setminus$ difference, relative complement $\varnothing$ empty set
MEMBERSHIP: $\in$ is an element of $\subseteq$ is a subset of or is equal to
$\subset$ is a proper subset of
SPECIFICATION: $\{ x : p(x) \}$ the set of all x such that $p(x)$ holds
[also $|$ or $\ni$ for the colon]
QUANTIFIERS: $\forall$ for all $\exists$ for some, there exists $\exists!$ there exists uniquely

Note that "or" always means "or ... or both". The symmetric difference of two sets is $A \Delta B = (A \cup B) \setminus (A \cap B)$; the difference or complement is $A \setminus B = \{ x \in A : x \notin B \}$. Note the use of a slash to indicate "not".

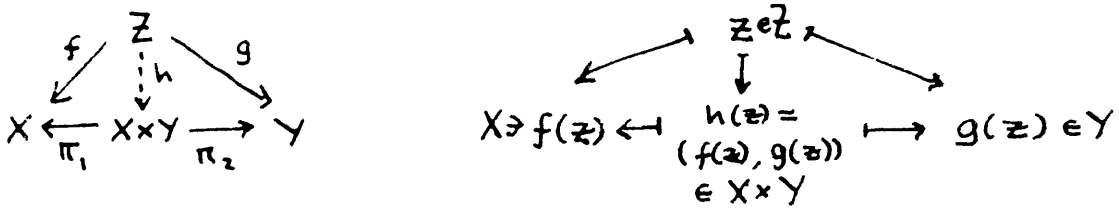
The sets $\{a,b\}$ and $\{b,a\}$ are the same, as are $\{a,a\}$ and $\{a\}$, because they have the same elements. The notation (a,b), however, means the ordered pair; $(a,b) \neq (b,a)$. As a set this may be "coded" as $\{\{a\},\{a,b\}\}$ - you should check that this has the required properties, especially if $a=b$. The set of all such pairs with $a \in A, b \in B$ is the cartesian product $A \times B$. Multiple (and also infinite) products may also be defined. A relation is just a subset $R \subseteq A \times B$; write aRb if $(a,b) \in R$.

A function or map from A to B, written $f : A \to B$, is a rule assigning some element of B to each element of A: write $b = f(a)$ or $f : a \mapsto b$ [note the two different types of arrow]. Formally, a function is a relation $f \subseteq A \times B$ such that $\forall a \in A \; \exists! \, b \in B : (a,b) \in f$. A is the domain of f and B its range or codomain. The image of f is $\{b \in B : \exists a \in A \; f(a) = b\}$.

For $S \subseteq A$, $T \subseteq B$ write $Sf_* = \{af : a \in S\}$ and $Tf^* = \{a \in A : af \in T\}$, but dont confuse the latter with the inverse function, which may not necessarily exist.

If $f: A \to B$ and $g: B \to C$ are two functions, their composite is obtained by applying them successively to $a \in A$. Thus $f \circ g : A \to C$ by $a \mapsto af \mapsto afg$. Clearly composition is associative, so $(fog)oh = fo(goh)$, when it is defined. We also have the identity function $1_A : A \to A$ by $a \mapsto a$. Then $1_A \circ f = f$ for all $f: A \to B$ and $g \circ 1_A = g$ for $g: C \to A$. Observe that functions are the same iff they have the same effect. [Can you prove that, if $e \circ f = f$ and $g \circ e = g$ for all f, g, then $e = 1_A$?] Beware that half of all mathematicians write composites the other way!

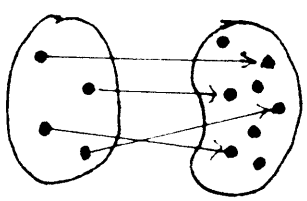
[The cartesian product, $X \times Y$, has projection maps $\pi_1 : X \times Y \to X$ by $(x,y) \mapsto x$ and $\pi_2 : X \times Y \to Y$ by $(x,y) \mapsto y$. Moreover, if $f: Z \to X$ and $g: Z \to Y$ are any two functions from another set Z, there is a unique map $h: Z \to X \times Y$ such that $h\pi_1 = f$ and $h\pi_2 = g$, as follows:



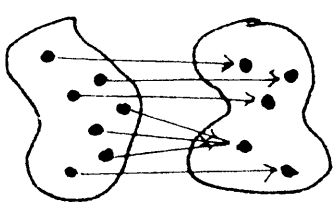
This property of $X \times Y$ is called a universal property. If Z also had this property there would be unique maps $h: Z \to X \times Y$ and $k: X \times Y \to Z$ such that $hk = 1_Z : Z \to Z$ and $kh = 1_{X \times Y} : X \times Y \to X \times Y$, so h, k would be mutually inverse. Then the elements of Z would just be those of $X \times Y$ with different names, so we say $X \times Y$ and Z are isomorphic, and in this sense $X \times Y$ is unique. Can you prove in the same way that $(X \times Y) \times Z$ and $X \times (Y \times Z)$ are isomorphic for any sets X, Y, Z?]

[The empty set has a unique map $\emptyset \to S$ into any set, and any singleton set, $* = \{x\}$, has a unique map $S \to *$ (by $s \mapsto x$ $\forall s$) from any set. These are also universal properties, so that $\emptyset$ and $*$ are unique up to isomorphism, but of course $\emptyset$ is unique anyway!]

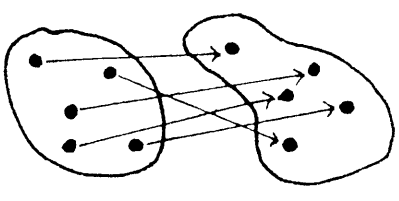
INJECTIVE, SURJECTIVE & BIJECTIVE MAPS.



injective or 1-1



surjective or onto



bijective or 1-1 correspondence

A map $f: A \to B$ is <u>injective</u> if $af = a'f \Rightarrow a = a'$. For example the <u>insertion map</u> of a subset into a set $i: A \hookrightarrow B$ is injective ($A \subseteq B$). [Such maps are <u>monic</u>: if $f \circ i = g \circ i$ then $f = g$. They also have <u>postinverses</u>, so define $bg_R = a_0$ for some $a_0 \in A \neq \emptyset$ if $b \notin \text{image}(f)$, and $bg_R = a$ if $af = b$. Then $fg_R = 1_A$, but $gf \neq 1_B$; g_R is not unique.]

$f: A \to B$ is <u>surjective</u> if $b = af$ for all $b \in B$. Projections, such as $\pi_1: X \times Y \twoheadrightarrow X$ by $(x,y) \mapsto x$ are surjective. [Such maps are <u>epic</u>: if $\pi \circ f = \pi \circ g$ then $f = g$. The <u>axiom of choice</u> says that they have <u>preinverses</u>: define $bg_L = a$ for some $a \in A$ st. $af_L = b$. Again g_L is not unique. $gf = 1_B$ $fg_L \neq 1_A$.] However if g_R and g_L both exist, they are equal and unique.

A surjective map $\pi: A \twoheadrightarrow B$ defines a <u>partition</u> of A as a disjoint union of subsets of the form bf^{-1} for $b \in B$. Write $a \sim a'$ if $a, a' \in A$ are in the same subset, ie $af = a'f$. Then $\sim$ is a relation which is <u>reflexive</u> [$a \sim a' \Rightarrow a' \sim a$], <u>symmetric</u> [$a \sim a$] and <u>transitive</u> [$a \sim a', a' \sim a'' \Rightarrow a \sim a''$]; such a relation is called an <u>equivalence relation</u>. For $a \in A$ the set $[a]_\sim = \{a' \in A : a \sim a'\}$ is called the <u>equivalence class</u> of a. Any equivalence relation determines a partition into equivalence classes and a <u>quotient map</u> $\pi: A \twoheadrightarrow A/\sim$ by $a \mapsto [a]_\sim$ from the set onto the set of equivalence classes, denoted $A/\sim$.

Any map $f: A \to B$ may be factored as a surjection followed by an injection:

$$A \xrightarrow[\pi]{} \!\!\!\rightarrow \text{Im} f \xhookrightarrow[i]{} B$$

Moreover if the equivalence relation $\sim$ is defined as above, we have $\text{Im} f \cong A/\sim$. This is the first isomorphism theorem for sets.

A map $f: A \to B$ is a <u>bijection</u> if it is both injective and surjective. In this case it is an isomorphism of sets, $A \cong B$, having a unique two-sided inverse, f^{-1}, with $ff^{-1} = 1_A$ and $f^{-1}f = 1_B$. Sets between which there is a bijection are <u>isomorphic</u>, <u>equipotent</u> or of the same <u>cardinality</u>. Isomorphism is an equivalence relation, the equivalence classes being called <u>cardinals</u>. Notice that the composite of two injective, surjective or bijective maps is respectively injective, surjective or bijective, and that $(fg)^{-1} = g^{-1}f^{-1}$ ["shoes & socks" rule].

COUNTABILITY AND UNCOUNTABILITY.

The <u>natural numbers</u>, $\mathbb{N} = \{0, 1, 2, \ldots\}$ may be defined recursively as $0 = \emptyset$, $1 = \{0\}$, $2 = \{0,1\}$, $\ldots$, $n = \{0, 1, \ldots, n-1\}$. The symbols

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are used to denote the integers, $\{\ldots -2, -1, 0, 1, \ldots\}$ rationals, reals and complex numbers. Any set, S, which is bijective with $\mathbb{N}$ is said to be countable; equivalently there exist $i: S \hookrightarrow \mathbb{N}$ or $\pi: \mathbb{N} \twoheadrightarrow S$. Otherwise S is uncountable. Unfortunately the term "countable" is ambiguous as to whether or not it excludes finite sets.

If X_i ($i \in I$, an indexing set) is a family of countable sets, then $\bigcup_{i \in I} X_i$ is countable if I is finite or countable, and $\prod_{i \in I} X_i$ is countable if I is finite. However Cantor's theorem shows that the power set, $P(X) = 2^X$ of any set X, defined as the set of subsets of X, is strictly bigger than X. For if $f: X \xrightarrow{\sim} P(X)$, let $A = \{x \in X : x \notin xf\}$, then $A = yf$ for some $y \in X$, but $y \in A \Leftrightarrow y \notin A$, $\ast$. By considering binary expansions, $\mathbb{R} \cong 2^{\mathbb{N}} > \mathbb{N}$. This can also be shown by other arguments. Also $\mathbb{C} \cong \mathbb{R}$ but $\mathbb{Q} \cong \mathbb{Z} \cong \mathbb{N}$. [Finally the Schröder-Bernstein theorem shows that if $f: A \hookrightarrow B$ and $g: B \hookrightarrow A$ then $\exists\, h: A \cong B$].

PERMUTATIONS

Let Ω be any set and consider the set of functions $f: \Omega \to \Omega$. On this there is a binary operation of composition [if f, g are functions, so is $f \circ g$] which is associative [$(f \circ g) \circ h = f \circ (g \circ h)$] and has an identity [$1_\Omega$; $1_\Omega \circ f = f \circ 1_\Omega = f$]. Such a thing is called a monoid. Now consider just the set $G = \{f: \Omega \to \Omega : f^{-1} \text{ exists}\}$ of invertible functions; this is also closed under compositions, for $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. This is called the symmetric group, S_Ω, on Ω, and its elements are called permutations of Ω.

If $A \subseteq \Omega$ is a subset of Ω, the set of invertible maps stabilising A [$f: \Omega \to \Omega$ s.t. $Af_* = A$ and $(\Omega \setminus A)f_* = \Omega \setminus A$] is closed under inverses and composition and forms a subgroup of S_Ω called $\mathrm{Stab}(A)$. Moreover if $\Omega = A_1 \cup A_2 \cup \ldots$ is any partition of Ω, its stabiliser is $\mathrm{Stab}(A_1) \cap \mathrm{Stab}(A_2) \cap \ldots$, which is also a subgroup. On the other hand if $A, B \subseteq \Omega$ the set $\{f: \Omega \to \Omega : Af_* = B\}$ is not a subgroup, but is of the form $f_1 H = \{f_1 f : f \in H\}$ where $f_1: \Omega \to \Omega$ is any map with $Af_{1*} = B$ and $H = \mathrm{Stab}(B)$ [or alternatively Kf_1 where $K = \mathrm{Stab}(A)$]. Such a set is called a coset of H [or K].

Ω will usually have more structure than just as a set, and the action of a group G on it will induce an action on some related object. For example if $f: \Omega \to \Omega$ is given, we also have $f_*: P(\Omega) \to P(\Omega)$ on the subsets: if $A \subseteq \Omega$, $Af_* = \{af : a \in A\} \subseteq \Omega$. Thus we have a function on the group G into the symmetric group of $P(\Omega)$, written $*: G \to S_{P(\Omega)}$.

This has the property that $(fg)_* = f_* g_*$ for all $f, g \in G$ and also (check this) $(f^{-1})_* = (f_*)^{-1}$. Thus the structure of the group (inverses and products) is preserved by $*$. Now since we're interested in this structure, this is the kind of map we want, and it's called a homomorphism of groups. Whenever G, H are groups, $\theta: G \to H$ always denotes a group homomorphism

CYCLES, TRANSPOSITIONS AND CONJUGATES.

Henceforward take Ω finite, without loss of generality $\Omega = n = \{0,1,2,\ldots,n-1\}$, so $G = S_\Omega = S_n$. Then it's not difficult to see that the order (number of elements) of G is $|G| = n!$ For inductively there are n possible images for 0 and $|\mathrm{Stab}_G(0)| = |S_{n-1}|$. (This is an example of Lagrange's theorem – see below).

$\pi \in G$ is a k-cycle $(2 \le k \le n)$ if $\pi: i_0 \to i_1 \to \ldots \to i_{k-1} \to i_k = i_0$ and fixes the remaining $n-k$ points, ie $\pi: j \to j$, where $j, i_0, i_1, \ldots, i_{k-1}$ are distinct. We could write this as $((i_0,i_1),(i_1,i_2),\ldots,(i_{k-1},i_k),(j_1,j_1),\ldots,(j_{n-k},j_{n-k}))$, but this is rather long and opaque, so instead we write just $(i_0,i_1,\ldots,i_{k-1})$, which is the same as $(i_1,i_2,\ldots,i_{k-1},i_0)$, $(i_2,i_3,\ldots,i_{k-1},i_0,i_1)$, etc. Moreover $\pi^{-1} = (i_k, i_{k-1}, \ldots, i_1)$ and so on. A 2-cycle is called a transposition. We don't bother writing down 1-cycles.

Simply by working out the repeated images under $\pi \in G$ of each point of Ω, any permutation may be written as a product of disjoint cycles (ie the subsets are disjoint). Moreover this is unique except for the order of the factors. You should experiment with multiplying permutations written as products of cycles, and verify that two cycles commute [ie $\pi\sigma = \sigma\pi$] if they are disjoint, and also that $\pi(i_0,i_1,\ldots,i_{k-1})\pi^{-1} = (i_0\pi, i_1\pi, \ldots, i_{k-1}\pi)$ for any permutation π. The reason for this is that π is acting here like an isomorphism of n to a differently labelled set n':

$$\pi: n = \{0,1,\ldots,n-1\} \longrightarrow n' = \{0\pi, 1\pi, \ldots, (n-1)\pi\} = \{0', 1', \ldots, (n-1)'\}$$

and the cycle is acting on the points $(i_0', i_1', \ldots, i_{k-1}')$, after which they're brought back to their old names by π^{-1}.

If $\sigma_1, \sigma_2 \in G$ are related by $\sigma_1 = \pi^{-1}\sigma_2\pi$ they're called conjugates. Conjugacy defines an equivalence relation on G, and the conjugacy (equivalence) classes are given by the cycle types [the collection of orders of cycle lengths, so $(1\,2\,3\,4\,5)(6\,7)(8\,9\,10)(11\,12)$ has cycle type $(2^2,3,5)$] if the group is S_n.

Any permutation may also be written as a product of transpositions, although they're not disjoint and don't commute, and the expression isn't unique. However what is unique is whether the number of transpositions is even or odd. The sign or signature of an even permutation is $+1$, and of an odd one -1. The sign of a product is given by the product of the signs, so

$$\varepsilon : S_n \longrightarrow C_2 = \{+1, -1\}$$

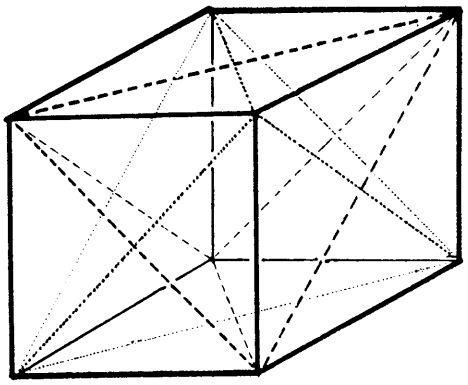
is a homomorphism. The sign may also be defined in terms of the effect of the permutation on the rows (or columns) of a determinant, $\Sigma_{\pi \in S_n} \varepsilon\pi \, a_{1,1\pi} a_{2,2\pi} \cdots a_{n,n\pi}$, or on the product $\Pi_{i<j}(x_i - x_j)$.

The subset $A_n = \{\pi \in S_n : \pi \text{ is even}\}$ forms a subgroup, the alternating group, of order $\frac{1}{2}n!$ $(n \geq 2)$. For $n \neq 4$ ε is essentially the only nontrivial homomorphism of S_n, which is what is meant by saying that A_n $(n \neq 4)$ is simple. [The cyclic groups $C_n = \{\pi \in S_n : \pi = \pi_0^r \text{ for some } r\}$ where $\pi_0 = (0\ 1\ 2\ \ldots (n-1))$ also have no nontrivial homomorphism for n prime and are also simple. The classification of all finite simple groups was completed by J.H.Conway and J.G.Thompson (inter alia) in Cambridge about four years ago.]

EXAMPLES OF GROUPS.

If G is a group we can consider the bijections of G (as a set) which preserve the group structure. These also form a group, the automorphism group of G, $\mathrm{Aut}(G)$. If you look again at conjugation $(\bar{\pi} : \sigma \mapsto \pi^{-1}\sigma\pi)$ you will see that this preserves inverses and products and is bijective, and moreover $\pi \mapsto \bar{\pi}$ gives a homomorphism $G \longrightarrow \mathrm{Aut}(G)$, of which the image is called $\mathrm{Inn}(G)$, the group of inner automorphisms of G. [An automorphism not of this form is called outer. It so happens that S_n has no outer automorphisms for $n \neq 6$, and essentially just one for $n = 6$ (ie $\mathrm{Aut}(S_6)/S_6 \cong 2$)]. Also $\ker(\pi \mapsto \bar{\pi}) = Z(G)$, the centre.

Consider the set of eight points $\{(\pm 1, \pm 1, \pm 1) \in \mathbb{R}^3\}$ forming a cube. The permutations of these points preserving the structure of the cube (ie the rotations of the cube in space) form a group, G. Since any point may be moved to any other (the group is transitive), and the cube may be placed in any of three positions if one point is fixed, $|G| = 8.3 = 2.4 = 4!$ In fact G is isomorphic to S_4, as we can see by considering the action on the four diagonals.



The group, G, acts faithfully on the diagonals (ie no nonidentity element acts as the identity, so if any point is moved, so also is some diagonal), so we have $G \hookrightarrow S_4$; but since $|G| = 24 = |S_4|$, they are isomorphic. Hence the diagonals may be permuted arbitrarily. The induced action on the two inscribed tetrahedra (see figure) gives an illustration of $\varepsilon: S_4 \twoheadrightarrow C_2$ and that on the three quadruples of parallel edges one of the exceptional "extra" homomorphism $\theta: S_4 \twoheadrightarrow S_3$ onto S_3. By placing a new vertex at the centre of each face we get the dual figure, the octahedron, whose automorphism group is then also S_4.

Similarly, the order of the automorphism group of a dodecadedron is 60, since it's transitive on the faces and the stabiliser of a face has order 5. In it may be found inscribed five interlocking cubes, whose edges are the 30 face diagonals (it's too complicated to draw here, but there's a model in DPMMS). On these the group acts faithfully, to permute them evenly, so $G \hookrightarrow .\ 5$; again the order gives $G \cong .\ 5$, so any even permutation may be achieved. The dual figure is the icosahedron, which thus has the same group. [Since A_5 is simple, in fact the smallest noncyclic simple group, there is no nontrivial "coarser" structure than these cubes].

The tetrahedron has group S_4 if reflections are allowed, or just A_4 if only rotations. In two dimensions, the rotations of an n-gon form a cyclic group, C_n, of order n. This is Abelian or commutative, ie $gh = hg$ always. The group may be written as $\langle r : r^n = 1 \rangle$, meaning that it is generated by r (ie $g = r^k$, $0 \le k < n$ for all $g \in G$) with the relation $r^n = 1$. If we allow reflections it becomes $D_n = \langle r, m : r^n = m^2 = 1, m^{-1} r m = r^{-1} \rangle$ of order $2n$, the dihedral group. Note that some authors call this D_{2n}.

[Rubik's cube has a group of order $12! 2^{12} 8! 3^8 / 3.2.2$, because the twelve edges may be permuted and flipped (but only an even number may be flipped, hence division by 2) and the eight corners may be permuted and spun (but the total spin must be zero mod 3, hence division by .). However it is only allowed to have an even permutation of corners and edges (which is independent of even flipping), so divide by 2 again. Cube experts will know that there are exactly twelve ways of building the cube, as claimed.]

GROUPS AND HOMOMORPHISMS.

We've seen that a group consists of a set G of operations, on which a binary product, $*$, (composition) is defined such that

(i) G is closed under $*$, which is associative.
(ii) G has an <u>identity</u>, 1, s.t. $1*g=g*1=g$, $\forall g\in G$
(iii) G has <u>inverses</u>, g^{-1}, st. $g^{-1}*g=g*g^{-1}=1$ $\forall g\in G$.

This is the formal definition of an <u>abstract group</u>. It coincides with our intuitive notion of a <u>concrete</u> permutation group, because of <u>Cayley's theorem</u>. For consider the action of G on itself by right-multiplication, ie $\bar{g}: h\mapsto hg$. This gives a permutation of G (as a set), so $\bar{g}\in S_G$, but clearly $\bar{g}\neq\bar{g}_1$ for $g\neq g_1$, so $g\mapsto\bar{g}$ embeds G in S_G as a subgroup, since $\overline{gg_1}=\bar{g}\bar{g}_1$.

A group <u>homomorphism</u> is a map $\theta: G\to H$ between groups G, H such that

(i) $(g_1g_2)\theta=(g_1\theta)(g_2\theta)$ [relative to the respective products]
(ii) $g^{-1}\theta=(g\theta)^{-1}$ [relative to the respective inverses]
(iii) $1\theta=1$ [relative to the respective identities]

The equivalent condition $(g_1g_2^{-1})\theta=(g_1\theta)(g_2\theta)^{-1}$ may often be easier to check.

A <u>subgroup</u> of a group G is a subset $H\subseteq G$ which is also a group under the same product (and with the same identity and inverses). Thus always $1\in H$. $\{1\}$ (written just 1) is the <u>trivial</u> subgroup. If H is a subgroup (not just a subset), write $H\leq G$; if H is also <u>proper</u> (ie $H\neq G$), write $H<G$. The insertion map $i: H\hookrightarrow G$ is an injective homomorphism, a <u>monomorphism</u>.

If $\theta: G\to H$, its <u>kernel</u>, $N=\ker\theta=\{g\in G: g\theta=1\}$, is the set of elements killed by θ; this is a subgroup. It is trivial iff $\theta: G\hookrightarrow H$ is injective. The partition of G defined by having the same image under θ is exactly the coset partition: for $g\in G$ $\{h\in G: h\theta=g\theta\}=\{gh\in G: h\theta=1\}=gN=Ng$, so $g^{-1}Ng=N$. This is a special condition on the subgroup N, which is said to be <u>normal</u>. Write $N\trianglelefteq G$, or $N\triangleleft G$ if also $N\neq G$. Note that 1 and G are both normal in G. However beware that whilst $H\trianglelefteq K\trianglelefteq G\Rightarrow H\trianglelefteq G$, $H\trianglelefteq K\leq G\not\Rightarrow H\trianglelefteq G$.

If $N\trianglelefteq G$, so $gN=Ng$ for all $g\in G$, let H be the collection of objects of the form gN for $g\in G$. This will be repetitive unless $N=1$ (for $gN=hN$ iff $gh^{-1}\in N$), but

just take one of each. Now define $\pi: G \to H$ by $g \mapsto gN$, which is clearly surjective. Check carefully that we may define a product on H (which we call G/N, the quotient group) by $(g_1N)(g_2N) = (g_1g_2N)$; you will need to use the fact that $gN = Ng$. Now check that π is a homomorphism, the projection map. Being surjective it is called an epimorphism. Finally check $N = \ker\theta$. Hence any normal subgroup is the kernel of a homomorphism.

As we did with sets, if $\theta: G \to H$ is any homomorphism, with $\ker\theta = N$, we may factor through its image as a subgroup (which it is) in H:

$$G \xrightarrow{\pi} G/N \xrightarrow{\bar{\theta}} \mathrm{Im}\,\theta \xrightarrow{i} H$$

and we have the first isomorphism theorem for groups, $\mathrm{Im}\,\theta \cong G/\ker\theta$.

[Note that whilst group monomorphisms and epimorphisms are respectively monic [$fi = gi \Rightarrow f = g$] and epic [$\pi f = \pi g \Rightarrow f = g$] they do not necessarily have inverses on either side]. However a group homo-morphism which is both a monomorphism and an epimorphism (i.e. is bijective) does have a two-sided inverse, so is an isomorphism.

The second and third isomorphism theorems may be proved by use of the obvious homomorphisms:

$$(G/K)/(N/K) \cong G/N \qquad KH/K \cong H/(H\cap K)$$

where $K, N \trianglelefteq G$ and $K \leq N$ (whence $K \trianglelefteq N$) and $H \leq G$. When we write a quotient, implicitly the denominator is normal in the numerator. Note also that the intersection (but not the union) of two [normal] subgroups is a [normal] subgroup, and if $K \trianglelefteq G, H \leq G$ then $KH = \{kh : k \in K, h \in H\}$ is a subgroup (this isn't so unless one of them is normal).

If G, H are groups, their direct product is $G \times H$ where $(g_1, h_1)\cdot(g_2, h_2) = (g_1g_2, h_1h_2)$. You should verify that this is indeed a group, [and that it has the same universal property for groups that the cartesian product had for sets earlier].

[The trivial group, 1, has a unique homomorphism both from and to each group G, $G \twoheadrightarrow 1$, $1 \hookrightarrow G$. Taking the composition of these, we have a unique trivial map $G \to H$ for all groups G, H by $g \mapsto 1$].

SUBGROUPS GENERATED BY SUBSETS.

The order of $x \in G$ is the least $n \geq 1$ such that $x^n = 1$, if this exists, or infinity if $x^k = 1 \Rightarrow k = 0$. Then $x^p = x^q$ iff $n | (p-q)$, and $x^p x^q = x^{p+q}$. Write $\langle x \rangle = \{x^p : p \in \mathbb{Z}\} \leq G$ for the subgroup generated by x. If $\langle x \rangle = G$, G is cyclic with generator x. If $|G| = n < \infty$, x^m is also a generator iff $(n,m) = 1$ (highest common factor), ie n, m are coprime. For any group G and $x \in G$ we have $\mathbb{Z} \to G$ by $m \mapsto x^m$, with kernel $n\mathbb{Z}$, the multiples of n. The image, $\mathbb{Z}/n\mathbb{Z}$, is the cyclic group C_n or $\mathbb{Z}_n$ of integers modulo n. This has application to elementary number theory in Wilson's, Fermat's and Euler's theorems: see the next section.

More generally, $S \subseteq G$ generates a subgroup $\langle S \rangle \leq G$ defined as $\cap \{H \leq G : H \supseteq S\}$. Assuming wlog that $s \in S$ implies $s^{-1} \in S$, $\langle S \rangle$ is the set of finite products in G of elements of S. G is generated by S if $\langle S \rangle = G$.

If $x, y \in G$ commute, so $xy = yx$, the order of xy is the least common multiple of the orders of x, y. Thus in particular if these orders are coprime it is the product. Hence $C_n \times C_m \cong C_{nm}$ iff $(n,m) = 1$. [In fact, all finitely generated Abelian groups ($G = \langle S \rangle$ with $|S| < \infty$) are direct products of cyclic groups, $\mathbb{Z}^r \times C_{n_1} \times C_{n_2} \times \dots \times C_{n_k}$. Here r is the Betti number of the group and is unique].

[A presentation of a group is a set of generators, S, together with a set of relations amongst them. The free group, $\tilde{S}$, on S has elements all strings of the form $w = s_1^{\alpha_1} s_2^{\alpha_2} \dots s_k^{\alpha_k}$, $s_i \in S$, $\alpha_i \in \mathbb{Z}$, with product given by juxtaposition, where $ws^0 = s^0 w = w$ and $s^p s^q = s^{p+q} = s^q s^p$. A set of relations, R, is then just a set of words also to be set to 1. Thus $\langle S; R \rangle$ is the group $\tilde{S}/\tilde{R}$ where $\tilde{R}$ is the normal subgroup of $\tilde{S}$ generated by R].

CENTRALISERS AND NORMALISERS.

For $H \leq G$, the centraliser, $C_G(H)$, of H in G is the subgroup of $g \in G$ fixing H pointwise by conjugation, ie $\{g \in G : g^{-1}hg = h \ \forall h \in H\}$. This is always normal in G. The centre, $Z(G)$ of H is the centraliser of G, $Z(G) = C_G(G) = \{g \in G : gh = hg \ \forall h \in G\}$, consisting of all the elements of G which commute with the whole of G. [$Z(G) \trianglelefteq G$ and $G/Z(G) \cong \mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ where $\mathrm{Inn}(G)$ and $\mathrm{Aut}(G)$ are the groups of inner and all automorphisms of G].

The normaliser, $N_G(H)$ of H in G, is the stabiliser of H by conjugation,

$N_G(H) = \{ g \in G : g^{-1}Hg = H \}$.

This need not be normal in G, but it does contain H, which is normal in it; indeed it is the largest subgroup of G in which H is normal. Clearly if $H \trianglelefteq G$, $N_G(H) = G$. The conjugates of H are the subgroups of G of the form $g^{-1}Hg$ for $g \in G$. G acts to permute them, the kernel of this action being $C_G(H)$ and the stabiliser of H being $N_G(H)$. The index of $N_G(H)$ (ie $|G|/|N_G(H)|$, written $|G : N_G(H)|$) is then the number of conjugates.

The action of G on itself by right multiplication permutes the cosets of $H \leq G$ transitively and so they are the same size, thus $|H||G:H| = |G|$, where $|G:H|$ is the number of cosets (this is Lagrange's theorem). The kernel of this action is $N = \bigcap \{ g^{-1}Hg : g \in G \}$ [Thus if $H \leq G$ with $|G:H| = n$, $\exists\, N \trianglelefteq G$ with $N \leq H$ and $|G:N| \leq n!$]

In particular $|\langle x \rangle|$, the order of $x \in G$, divides $|G|$. Thus if $G = U_n$ is the group of units of $\mathbb{Z}_n$, ie $\{ m \in \mathbb{Z}_n : (m,n) = 1 \}$, which has order $\varphi(n)$ (Euler's function), $a \in U_n$ has order dividing $\varphi(n)$, thus $a^{\varphi(n)} = 1$ (Euler's theorem). If $n = p$, prime, $\varphi(p) = p-1$, so $a^{p-1} = 1$ in U_p; alternatively $p \mid a^p - a$ in $\mathbb{Z}$ (Fermat's theorem). Finally, in U_p, $(p-1)! = \prod_{m \in U_p} m = \left(\prod_{m=2}^{p-2} m m^{-1} \right).(-1) = -1$ (Wilson's theorem).

Considering the conjugation action on elements of G, the orbit of $x \in G$, $\{ g^{-1}xg : g \in G \}$, is its conjugacy class, whose order divides $|G|$. Notice $Z(G) = \{ x \in G : \{ g^{-1}xg \} = \{ x \} \}$. [Thus if G is a p-group (ie $|G| = p^n$ where p is prime), $|Z(G)| = |G| - \sum |C_i|$ where C_i are the nonsingleton conjugacy classes (this is the class equation) and the right-hand side is a multiple of p. Thus since $|Z(G)| \geq 1$, the centre is nontrivial.]

[Finally, for $x, y \in G$, the commutator of x, y is $[x,y] = x^{-1}y^{-1}xy$. Let $G' = \langle [x,y] : x, y \in G \rangle$, the commutator subgroup or derived group; then $G' \trianglelefteq G$. If $G' = G$ (such as for A_n; $n \geq 5$) the group is perfect. G/G' is the Abelianisation of G: it's the group you get if you impose the relations $xy = yx$ for all $x, y \in G$ on G. $G' = 1$ iff G is Abelian].

GROUPS OF SMALL ORDER.

Using the elementary theory you have so far it's not difficult to list all of the groups up to order 15, although it's much easier with Sylow theory (see Part II Groups). Five classes, together with direct products of them, are represented; * indicates nonAbelian.

Cyclic groups $n = C_n = Z_n = \langle x : x^n = 1 \rangle = \{ e^{2\pi i k/n} \in \mathbb{C} : k = 0, 1, \dots, n-1 \}$

Dihedral groups $^*D_n = \langle m, r : m^2 = r^n = 1,\ m^{-1}rm = r^{-1} \rangle$ order $2n$
(Sometimes called D_{2n}; symmetry groups of regular n-gons).

Symmetric groups $^*S_n = \{ f : n \cong n \}$ order $n!$

Alternating groups $^*A_n = \{ f \in S_n : f \text{ even} \}$ order $\frac{1}{2}n!$ $(n \neq 2)$

Generalised quaternion, or dicyclic groups $^*Q_{4n} = \{ m, r : r^n = m^2,\ m^4 = 1,\ m^{-1}rm = r^{-1} \}$
[This is only included for completeness since $|Q_8|, |Q_{12}| \leq 15$; "dicyclic" is obsolete, but "generalised quaternion" isn't quite standard for $n \neq 2^k$. You should be aware of the existence of Q_8].

Note that $1 \cong C_1 \cong S_1 \cong A_1 \cong A_2$; $C_2 \cong D_1 \cong S_2$; $C_3 \cong A_3$; $^*D_3 \cong {}^*S_3$
and $C_2 \times C_2 \cong D_2$ (sometimes called the four-group); $C_2 \times {}^*S_3 \cong {}^*D_6$.
Also $C_2 \times C_3 \cong C_6$; $C_2 \times C_5 \cong C_{10}$; $C_2 \times C_7 \cong C_{14}$; $C_3 \times C_4 \cong C_{12}$; $C_3 \times C_5 \cong C_{15}$.

Products up to order 15:
$C_2 \times C_4$ and $C_2 \times C_2 \times C_2$ (order 8)
$C_3 \times C_3$ (order 9) $C_3 \times C_2 \times C_2 \cong C_6 \times C_2$ (order 12)

$^*Q_8$ is the Quaternion group with elements $\pm 1 = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\pm i = \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $\pm j = \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ $\pm k = \pm \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$ as matrices over $\mathbb{C}$.
Then $i^2 = j^2 = k^2 = ijk = -1$. [Taking the $\mathbb{R}$-algebra (ie vector space over $\mathbb{R}$ with these as basis, and multiplication defined linearly by these relations) we have a division ring or skew field: it is noncommutative, but every element has an inverse (except 0, of course). This is called $\mathbb{H}$].

Full list of groups up to order 15.

1:	1	6:	$6, {}^*S_3$	11:	11
2:	2	7:	7	12:	$2.6, 12, {}^*D_6, {}^*A_4, {}^*Q_{12}$
3:	3	8:	$2^3, 2.4, 8, {}^*D_4, {}^*Q_8$	13:	13
4:	$2^2, 4$	9:	$3^2, 9$	14:	$14, {}^*D_7$
5:	5	10:	$10, {}^*D_5$	15:	15.

ALGEBRA I.

1. Demonstrate the equivalence of the following three concepts:
   (i) equivalence relation R on a set X
   (ii) partition $X = \cup X_i$
   (iii) surjective map $X \twoheadrightarrow I$

2. Given an infinite set X, show that
   (i) there's a bijection $X \cong \mathbb{N}$
   $\Leftrightarrow$ (ii) there's an injection $X \hookrightarrow \mathbb{N}$
   $\Leftrightarrow$ (iii) there's a surjection $\mathbb{N} \twoheadrightarrow X$

3. Show that each of the following statements is either always true or always false, or else give an example and a counterexample:
   (i) a subset of a countable set is countable
   (ii) a surjective image of a " " " "
   (iii) a countable union of " sets " "
   (iv) " " product " " " " "
   (v) the powerset of a " set " "
   *(vi) a product of nonempty sets is nonempty.
   (vii) every injection has a postinverse
   *(viii) " surjection " " preinverse

4. Demonstrate the equivalence of the following concepts:
   (i) congruence R on a group G
   (an equiv. rel? s.t. R is a subgroup of $G \times G$)
   (ii) equiv. relⁿ. on G s.t. $[x][y] = [xy]$ is well-defined
   (iii) normal subgroup (ie s.t. $g^{-1}Ng = N \ \forall g \in G$)
   (iv) partition of a group s.t. product is well-defined
   (v) transitive (permutation) action of G
   (vi) kernel of homomorphism
   (vii) left & right cosets coincide

5. Demonstrate the equivalence of the following concepts:
   (i) subgroup (subset closed under 1, inverse & composite)
   (ii) image of homomorphism
   (iii) stabiliser of a point in a permutation action

6. What is Cayley's theorem and how does it justify the study of (finite) abstract groups?

7. What is Lagrange's theorem and why is it obvious even before you've defined a group?

8. Prove the following corollaries of Lagrange's theorem:
   (i) Fermat's little theorem: $a^{p-1} \equiv 1 \pmod p$ if $(a,p)=1$
   (ii) Euler's theorem: $a^{\varphi(n)} \equiv 1 \pmod n$ if $(a,n)=1$
   (iii) Wilson's theorem: $(p-1)! \equiv -1 \pmod p$

9. Define the group of units mod n and show that if $(m,n)=1$, $U_{mn} \cong U_m \times U_n$

*10. Show that every finite Abelian group is of the form $C_{n_1} \times C_{n_2} \times \dots \times C_{n_k}$ with $n_1 | n_2 | n_3 | \dots | n_k$.

*11. Classify the groups of order ≤ 15 up to isomorphism.

12. Show that any element of S_n may be written as a product of disjoint cycles in an essentially unique way (explaining "essentially unique") and that two elements are conjugate iff they have the same cycle type

*13. Classify the conjugacy classes of A_n

14. Show that the following generate S_n:
   (i) all cycles
   (ii) all transpositions
   (iii) all adjacent transpositions, ie $(i\ i+1)$
   (iv) (12) and $(1\ 2\ 3\ \dots\ n)$

*15. Show that the three-cycles generate A_n and that A_n is simple (has no normal subgroups apart from 1 and A_n) unless $n=4$.

16 Define inner and outer automorphisms and show that $\mathrm{Inn}(G) \cong G/Z$ and $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.
* Investigate $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ for some finite groups; ** Show that $\mathrm{Out}(S_n)=1$ unless $n=6$ and that $\mathrm{Out}(S_6)=2$.

*17. We may characterise a product of sets (or groups) X, Y as the "universal" diagram of the form

$$Z \rightarrow X, \quad Z \rightarrow Y$$

ie $Z = X \times Y$ gives such a diagram (with the projection maps onto the first and second coordinates) and given any other such diagram there's a unique $Z \to X \times Y$ s.t. the diagram commutes.

Formulate the notions of quotient set/group, sup (or inf) of real numbers, disjoint union of sets, empty set, trivial group (in two ways), one-point set, kernel, etc. in a similar way. You will have to choose the nature and direction of the arrows carefully in each case.

*18. A <u>category</u> is a structure with objects and arrows as in 17. Formulate a definition, and by analogy with group homomorphisms formulate the definition of a <u>functor</u> (category homomorphism). Give some examples of categories and show that the Abelianisation $G \mapsto G/G'$ is a functor, but $G \to Z(G)$ is not.

*19 Define a product of categories and show that $\times : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a functor, as is the diagonal $\Delta : \mathcal{C} \to \mathcal{C} \times \mathcal{C}$ by $X \mapsto (X,X)$. Reformulate the universal property of $\times$ as in 17 as a relationship between the arrow $X \times Y \to Z$ and pairs of arrows $X \to Z$, $Y \to Z$

*20 (a better example). We have a "forgetful" functor $\underline{\mathrm{AbGp}} \to \underline{\mathrm{Gp}}$ and the Abelianisation $\underline{\mathrm{Gp}} \to \underline{\mathrm{AbGp}}$. Show that for any group G and Abelian group A there's a (natural) bijection between homomorphisms $G \to A$ and $G/G' \to A$. We write this as

$$\underline{\mathrm{AbGp}}(F(G), A) \cong \underline{\mathrm{Gp}}(G, U(A))$$

Formulate quotient groups, bases of vector spaces and other concepts in this form. We say that Abelianisation is <u>left adjoint</u> to the forgetful functor.

*21 What are the group-theoretic analogues of a vector-space generated by a basis and of a disjoint union of sets?

22 Prove unique factorisation for $\mathbb{Z}$

Note: * means difficult or outside the syllabus but accessible with a little thought
** means very difficult.