MATH 843/4/5 Notes

# BASIC GRADUATE ALGEBRA

**843/844/845 Algebra Notes. Table of Contents**

Roy Smith

**843: Galois' necessary criterion for solvable polynomials**

**844: Characterizing polynomials that can be solved**

**844 I: Rings, Factorization, and the fundamental theorem of Galois theory**



**844 II: Identifying (and solving) "solvable" polynomials, eg. solution formulas for cubics and quartics over Q**

**845: Linear Algebra: canonical forms of matrices, modules, Hom and the tensor product**

**845 I: Decomposing modules and homomorphisms**



**845II: Decomposition over algebraically closed fields: Jordan forms, semi simple and nilpotent operators**



**845 III: Universal constructions**

**Groups, Fields and Galois Theory**


We begin with groups in the context in which they were used by Galois, the problem of existence of formulas using only algebraic operations and radicals, for roots of polynomial equations. After we introduce the language of groups, and the properties needed to calculate with them, we will begin studying Galois' use of them to solve this problem. The first part of these notes ends with the proof of Galois' necessary condition for a polynomial to be solvable via radicals, and its application to show that $X^5 - 80X + 2 = 0$ in particular is not solvable. [We use the abbreviations "$\forall$" = "for all", "$\exists$" = "for some", "iff" = "if and only if", and "$\amalg$" = "disjoint union".]

## Group actions, and a counting principle.

### §1) Definition of a group, and the fundamental example $S_n$.

Groups represent the algebraic version of symmetry. In fact, the fundamental example of a finite group, $S_n$ = the set of all bijections of the set $\{1,...,n\}$ with itself, is called the "symmetric group". [Recall $f:S \to T$ is a bijection iff for every $y$ in $T$ there is a unique $x$ in $S$ with $f(x) = y$.] We denote the family of bijections of $S$ with itself as $Bij(S)$. Note that the family $Bij(S)$ of self maps of $S$ has nice properties, reminiscent of those for addition of integers:

i) The composition of two bijections of $S$ is again a bijection
ii) Associativity holds, i.e. $(f\circ g)\circ h = f\circ(g\circ h)$ for any three bijections $f,g,h$, of $S$.
iii) The identity map of $S$, $1_S = 1$, is a bijection, s.t., $\forall$ $f$, $f\circ 1 = 1\circ f = f$
iv) $\forall$ $f$ in $Bij(S)$, $\exists$ $f^{-1}$ in $Bij(S)$ s.t. $f(x) = y$ iff $f^{-1}(y) = x$; equivalently s.t. $f\circ f^{-1} = f^{-1}\circ f = 1$.
Abstracting these properties gives the definition of a group, i.e.

**Definition**: A <u>group</u> is a set $G$, closed under a binary operation $\cdot : G\times G \to G$, which is associative, has an identity, and such that every element has an inverse. We may write $ab$ (and sometimes $a\cdot b$) for $a\cdot b$. Thus (since closure has been assumed) the axioms are:
i) $\forall$ $a$, $b$, $c$, in $G$, $a(bc) = (ab)c$,
ii) $\exists$ an element $e$ in $G$ such that $\forall$ $a$ in $G$, $ea = ae = a$,
iii) $\forall$ $a$ in $G$, $\exists$ $a^{-1}$ in $G$ such that $aa^{-1} = a^{-1}a = e$

G is called commutative (or abelian) if also, for every a, b in G we have $ab = ba$

**Exercise #1)** (i) Show that in any group G, e is unique, and that for each a in G, $a^{-1}$ is unique.
(ii) Show $S_n$ is not abelian for any $n \geq 3$.

We usually write just G for the pair $(G,\cdot)$, although the operation is even more important to the structure of the group than is the set.

**Definition**: A subgroup H of a group G, is a subset $H \subset G$ which is closed under the operation of G, and which is itself a group for that operation.

**Remark**: The fundamental nature of the groups $S_n$ is revealed by the fact, proved later, that any finite group can be embedded as a subgroup of some $S_n$.

**Exercise #2)** (i) The identity element of a subgroup $H \subset G$ is the identity of G, and inverses of elements of H are their inverses in G.
(ii) If H is non empty, H is a subgroup iff $\forall$ a, b in H, $a^{-1}b$ is in H.
(iii) If x is any element of a group $(G,\cdot)$, the set of all integral powers $\{x^n\}$ of x, is an abelian subgroup $\langle x \rangle$ of G, where we define $x^1 = x$, $x^r = x(x^{r-1})$ for $r \geq 2$, $x^0 = e$, and $x^{-r} = (x^{-1})^r$, for $r \geq 1$.

## §2) More examples of groups:

It is often interesting to consider those bijections of a set S which leave some important property of S unchanged or "invariant".
i) "Isometries", $\mathrm{Isom}(\mathbb{R}^n)$ = the subgroup of $\mathrm{Bij}(\mathbb{R}^n)$ consisting of those bijections which leave the Euclidean distance between pairs of points in $\mathbb{R}^n$ unchanged, (for example translation by a: $f(x) = a+x$).
ii) The subgroup of elements of $\mathrm{Isom}(\mathbb{R}^n)$ which leave the origin fixed is the "orthogonal group" O(n) of linear isometries of $\mathbb{R}^n$. It can be shown that $O(n) = \{\text{maps } \mathbb{R}^n \to \mathbb{R}^n \text{ given by multiplication by those } n \times n \text{ matrices } M \text{ such that } M^t = M^{-1}\}$.
iii) The subgroup $SO(n) \subset O(n)$ consisting of elements which are also "orientation preserving" (corresponding to the matrices in O(n) which have determinant = 1) is called the *special* orthogonal group For example SO(2) is the group of rotations of the plane about the

origin, and SO(3) is the group of rotations of three space about axes through the origin of $\mathbb{R}^3$.

We can obtain other, sometimes finite, subgroups of Isom($\mathbb{R}^n$) by considering those motions that leave a particular interesting geometric figure invariant. Examples include:
iv) the subgroup Cube of SO(3) mapping a cube centered at the origin into itself, or
v), vi) the subgroups Tet, Icos of SO(3) mapping a regular tetrahedron or regular icosahedron centered at the origin into themselves.

We may call the groups Cube, Tet, Icos, the (oriented, or rotation) groups of the cube, tetrahedron, and icosahedron.
vii) The subgroup $Z_n$ of rotations of a regular plane polygon of n sides, centered at the origin, about an axis perpendicular to the plane of the polygon is finite cyclic, of order n (see definition below).
viii) The "dihedral" group $D_n \subset O(2)$, the isometry group of a polygon of n sides, includes not only the rotations about an axis through the origin and perpendicular to the plane of the polygon, but also reflections about an axis of symmetry contained in the plane of the polygon [These reflections are the restriction to the polygon of a rotation of three space about the same axis.] $D_n$ has 2n elements.

**Challenge**: Are there any more finite subgroups of SO(3), other than subgroups of those above? Make a conjecture and try to come up with an idea for proving it.

The only abelian groups among the examples above are the rotation groups $Z_n$ of a regular plane polygon. We make precise the term "cyclic" which applies to these.
**Definition**: A group is cyclic iff it consists of the integral powers of a single element. An element whose integral powers exhaust a cyclic group is called a "generator" of the cyclic group.

**Remarks**: (i) By exercise #2 every cyclic group is abelian.
(ii) For a group G written additively, an element $\alpha$ generates G iff every non zero element of G is expressible as $\alpha + \alpha$, or $-\alpha - \ldots - \alpha$.
(iii) The subgroup $Z_n$ of rotations of a regular plane polygon of n sides is cyclic, since it is generated by a counterclockwise rotation through $2\pi/n$ radians.

(iv) The integers $\mathbf{Z}$ form an infinite cyclic group under addition, with 1 and -1 as (the only) generators.
(v) If x is any element of a group G, the subgroup $\langle x \rangle$ "generated by x", consisting of all integral powers $\{x^n\}$ of x, is cyclic. Both x and $x^{-1}$ are generators and there may be others (see the next exercise).

**Exercise #3)** (i) Prove an infinite cyclic group has exactly two generators
(ii) Prove the generators of a finite cyclic group $\langle x \rangle$ of order $n>1$, are exactly those elements of form $x^k$ where $0 < k < n$ and $\gcd(k,n) = 1$.
(iii) Prove the set $\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$, is a cyclic group under the following addition law: given s, t in $\mathbf{Z}_n$, $s + t$ = the remainder after dividing the usual integer sum $s + t$ by n. (For example in $\mathbf{Z}_5$, $2+2 = 1+3 = 4$, and $2+4 = 3+3 = 1$.)
(iv) Prove the set $\mathbf{Z}_n^* = \{\text{integers } k \text{ with } 1 \leq k < n \text{ and } \gcd(k,n) = 1\}$ is an abelian group with the following multiplication: given s, t in $\mathbf{Z}_n^*$, let st = the remainder after dividing the usual integer product st by n. (For example in $\mathbf{Z}_8^* = \{1,3,5,7\}$, $3 \cdot 5 = 7$, $3 \cdot 7 = 5$, $3 \cdot 3 = 1$.)

Other examples of groups are easy to construct from the ones we know using the fundamental product construction.
**Definition:** If G, H are any two groups, their "product" is the group whose underlying set is the Cartesian product $G \times H = \{\text{all ordered pairs } (g,h) \text{ where } g \text{ is in } G, h \text{ is in } H\}$, and with the operation $(g,h)\cdot(\tilde{g},\tilde{h}) = (g\tilde{g},h\tilde{h})$.

**Remark:** The product $\prod G_i = G_1 \times \ldots \times G_n$, of a finite sequence of groups $G_1, \ldots, G_n$, is defined analogously as the Cartesian product with the group operation again defined "pointwise".

**Exercise #4)** (i) If G,H are groups, check that $G \times H$ is a group
(ii) If $G_1, \ldots, G_n$ are abelian groups, show their product $\prod G_i$ is abelian; in particular a product of cyclic groups $Z_n$ is abelian.
(iii) Prove $Z_2 \times Z_3$ is cyclic but $Z_2 \times Z_2$ is not.
(iv) Analyze some other examples of form $Z_n \times Z_m$ and make a conjecture as to precisely when such products are cyclic.
(v) Prove your conjecture from part (iv).

**Remark:** Eventually we will prove a strong converse to exercise

4(ii) for finite groups, that every finite abelian group has the same structure as a product of cyclic groups $\Pi Z_n$. Thus if we were only interested in finite abelian groups, our investigation would be over. Understanding non abelian finite groups is more challenging, and there is no comparably simple way to classify all of them, even though they do all occur as subgroups of the symmetric groups $S_n$.

We naturally want to know something about the structure of groups we encounter, and the simplest question we can ask is for the "order" or number of elements of a group G. So how do we count the number #(G) of elements of a (finite) group G? The cyclic group $Z_n$ has n elements, and the order of the product $\Pi G_i$ is the product of the orders of the $G_i$. But how do we compute the order of the geometric symmetry groups above? Clearly the number of elements of the group of the cube should have something to do with the number of faces or vertices of a cube, and presumably the fact that the cube has more faces than the tetrahedron may be reflected in the group C being larger than the group T. This is not entirely clear, but we can make the connection more precise via the concept of a "group action", a fundamental tool for analyzing finite groups..

**§3) Action of a group on a set:** A group <u>G acts on the set S</u> (from the left) if $\exists$ a map $G \times S \to S$, where the image of (g,s) is written g(s) (or gs, or $\langle g,s \rangle$), such that e(s) = s, and g(h(s)) = (gh)(s), for all s, g, h. This means that, in our notation, gh acts on an element s by h acting first on s and then g acting on h(s). [Be careful to note in each book you read whether this is the convention or whether instead they assume (gh)(s) = h(g(s)), which means that g acts first and then h. That latter convention should perhaps be written (s)(gh) = ((s)g)h, with the action on the right, and is often used in connection with the standard notation for permutations.] An action is called "transitive" iff for every pair of elements s, t in S there is some g in G with g(s)=t In general, the "orbit" of an element s of S is the subset of those elements t of S such that there does exist some g in G with g(s) = t.

So every action is transitive on each orbit, and a transitive action on S is one such that for every element s of S, the orbit of s is S itself. In general, the set S is partitioned into disjoint subsets by the family of orbits. The following counting principle relates the size of an orbit of a G action to the size of G, and since G acts transitively

on each orbit, it is sufficient to state it for the case of transitive actions. The idea is to show that for any two possible destinations for a given point, there are the same number of group elements taking it to one destination as there are taking it to the other. Hence the number of elements in the group is the product of the number of possible destinations of a given point, times the number of group elements that leave it where it is.

First we distinguish those elements that leave a given point fixed.
**Definition:** (i) If G acts on S and x is an element of S, the "stabilizer subgroup" or "isotropy subgroup" of x is the subgroup $G_x \subset G$ of elements that leave x fixed, i.e. f in G belongs to $G_x$ iff f(x) = x.
(ii) The "orbit" of x, denoted O(x), is the set of images of x under all elements of G, O(x) = {all points in S of form f(x) for some f in G}.

The following principle is absolutely fundamental:
**Lemma (a counting principle):** If G acts on S, then for any element x of S, the number of elements of G is the product of the number of elements of O(x) and the number of elements of $G_x$, i e $\#(G) = \#(G_x)\#(O(x))$, where $G_x$ = the stabilizer subgroup of x, and O(x) = the orbit of x under G.
**proof:** Since the statement only involves the action of G on the orbit O(x), we may as well assume that O(x) = S, i.e. that the action is transitive. First we partition the group G according to how elements affect x. I.e. setting $f \sim g$ iff f(x) = g(x) defines an equivalence relation on G, hence a partition of $G = \amalg_s G_{x,s}$, into disjoint subsets or "equivalence classes" $G_{x,s}$ = {f in G : f(x) = s}, for each s in S. Next we show these classes are all the same size. (Note that $G_{x,x} = G_x$.)

**Claim:** For all s, t in S, $\#(G_{x,s}) = \#(G_{x,t})$.
**proof of claim:** We will define mutually inverse bijections between the two subsets. Since the action is transitive, there is an element g of G such that g(s) = t. Then $G_{x,t} \supset gG_{x,s}$, since if h is in $G_{x,s}$, then (gh)(x) = g(h(x)) = g(s) = t. On the other hand, since $g^{-1}(t) = s$ [why?], the same argument shows that $g^{-1}G_{x,t} \subset G_{x,s}$ Thus the two maps $G_{x,s} \to G_{x,t}$, $G_{x,t} \to G_{x,s}$, given respectively by left multiplication by g and by $g^{-1}$, are mutually inverse, hence both are bijections, and so $\#(G_{x,s}) = \#(G_{x,t})$. QED claim.
Consequently, the partition $G = \amalg_s G_{x,s}$, of G is by disjoint subsets,

all of the same cardinality, hence $\#(G) = \#(S)\#(G_{x,s})$ for any element s of S If we choose $s = x$ then $G_{x,x} = G_x$, hence our counting principle holds **QED lemma**.

**Note**: If $h(x) = s$, and $g(x) = x$, then $(hg)(x) = s$, and in fact {the set of all products of form hg with g in $G_x$} = $hG_x = G_{x,s}$, but there is no reason for $(gh)(x)$ to equal s, so we do not expect $G_x h$ to equal $hG_x$. Thus the "right translate" of a subgroup $G_x$ by an element h, does not necessarily equal the left translate of that subgroup by h.

**Corollary**: Whenever a finite group G acts on a set, the order of every stabilizer subgroup, and also the order of every orbit, divides the order of G.

Now it is easy to count the elements of the groups Cube, Tet, Icos of rotations leaving invariant the classical regular solids:
**Application**: We have $\#(\text{Cube}) = 24$.
**proof**: The group Cube acts on the set of faces of the cube, and the rotations that leave say the top face invariant, are precisely the four rotations of the top face through a multiple of $90^0$. (Note the axis of the rotation must be perpendicular to the top face.) Since there are 6 faces and the stabilizer group of the top face has 4 elements, the counting principle above implies $\#(\text{Cube}) = 4 \times 6 = 24$. [Alternatively, Cube acts on the set of 8 vertices, with stabilizer subgroups of order 3, and on the set of 12 edges with stabilizer subgroups of order 2.] **QED**.

**Exercise #5) (i)** Check that the rotation group Tet of the tetrahedron consists of 12 elements, and the rotation group Icos of the icosahedron consists of 60 elements. What are the orders of the rotation groups of the octahedron and the dodecahedron? Why?
**(ii)** Show the dihedral group $D_n$ of all symmetries (containing both rotations and reflections in axes of symmetry) of a regular plane polygon with $n \geq 3$ sides has order 2n, and is not abelian.
**(iii)** If $\rho$ is counterclockwise rotation through $120^0$, and R is reflection in an axis of symmetry of an equilateral triangle, show that D3 consists of the elements $(id, \rho, \rho^2, R, \rho R, \rho^2 R)$, and $R\rho = \rho^2 R$.
**(iv)** Make a similar analysis of D4.
**(v)** Make a conjecture for $D_n$ generalizing parts (iii), (iv).

**Terminology**: A subset of a group G is said to "generate" the group iff every element of G can be written as a product of integral powers of those elements. Thus a group is cyclic iff it can be generated by one element. From ex. 5, the group D3 is not abelian hence not cyclic, but can be generated by two elements Can you find generators of some of the other groups above, such as Cube, Tet, or Icos? Non trivial equations involving generators, such as $R\rho = \rho^2 R$ for D3 in ex.5(iii) above, are called "relations" (among the generators) Note a subset S of G generates G iff no proper subgroup of G contains S We agree that the empty set generates the trivial group {e}.

**Remark**: There are many interesting ways a group can act on various sets, in particular on itself, and thus the counting principle above is extremely useful in practice, as we will see.

**§4) Cosets of a subgroup, and LaGrange's theorem**

The counting principle involving the action of a group G on a set S can be made more intrinsic, in that we can dispense with the set S, as follows. Notice that if f, g are elements of a group G acting on a set S, and x is a point of S, then f and g are equivalent in the sense that $f(x) = g(x)$, iff $f^{-1}g(x) = x$, iff $f^{-1}g$ belongs to $G_x$. Thus to define the equivalence relation, and essentially the action of G on the orbit O(x), we only need the stabilizer subgroup $G_x$. I.e. in some sense $G_x$ represents the element x. Similarly the subset $G_{x,s}$ of elements of G taking x to s, can be used to represent the element s.

As noted in the previous section, if $h(x) = s$, and $g(x) = x$, then $(hg)(x) = s$, and in fact {the set of all products of form hg with g in $G_x$} = $hG_x = G_{x,s}$, so the left translate $hG_x$ of $G_x$ by h, can be used in place of $G_{x,s}$ to represent the element s of O(x). Note that $hG_x = G_{x,s}$ if and only if h belongs to $G_{x,s}$, and $hG_x = kG_x$ if and only if $h^{-1}k$ belongs to $G_x$. We develop this point of view next, without mentioning S

The following terminology for translates of subgroups is standard:
**Definition**: If $H \subset G$ is a subgroup and x in G is any element, the set $xH = \{xh: \text{for all } h \text{ in } H\}$ of left translates, i.e. left multiples, by x of elements of H, is called a (left) <u>coset</u> of H in G. Similarly, we define

the right coset Hx = {hx: for all h in H}.

**Action on cosets of a subgroup by translation:**
Define a (left) action of G on the set $\mathcal{S}$ of all subsets of G, by left translation. I.e. for every element g of G, and every subset T of G let gT be the set of (left) translates of T, where gT = {gt. for all t in T}. This is an action since g(kT) = (gk)T by associativity of multiplication. Let H be any subgroup of G and let S be the orbit of the subset H under this action. Then S is the set of all left cosets of H in G, and G acts transitively on these cosets by left translation.

**Remark:** Similarly the orbit of H under right translation is the set of right cosets of H, but we prefer left cosets and left actions, whose notation agrees with that for composition of functions in calculus.

**Lemma:** If H⊂G is a subgroup, g, k in G, then
(i) gH = H if and only if g belongs to H; more generally
(ii) gH = kH iff g belongs to kH, iff $g^{-1}k$ belongs to H.
(iii) two cosets gH and kH are either equal or disjoint.

**Exercise #6)** Prove the previous lemma.

**Corollary:** If H⊂G is a subgroup, then:
(i) the stabilizer subgroup of the coset eH = H, is H itself,
(ii) the subset of G taking H to gH, is the subset gH itself,
**proof:** (i), (ii) follow from (i), (ii) in the lemma above. QED.

**Moral:** A subgroup H of a group G is always a stabilizer subgroup for some action, i.e. H is the stabilizer subgroup of *itself* for the action of G by left translation on the set $\mathcal{S}$ of subsets of G. Thus the apparently geometric notions of group actions and stabilizer subgroups are present within the algebraic structures of a group and its subgroups.

For the action of a group by translation, on cosets of a given subgroup, the counting principle has a famous name:
**LaGrange's Theorem:** If H is any subgroup of G, then #(G) = #(H)#(distinct left cosets of H). In particular #(H) divides #(G).
**proof:** For the action of left translation, H = $G_H$, and the orbit of H is the set of distinct cosets of H, so this follows from the counting

principle above. **QED.**

**Terminology:** The number of distinct left cosets of H in G, is called the "index" of H in G. (It also equals the number of right cosets.) It is denoted $[G:H]$. Thus $[G:H] = \#(G)/\#(H)$.

**Exercise #7)** (i) Prove every subgroup of a cyclic group is cyclic.
(ii) Prove that every group of prime order is cyclic.
(iii) Prove that every abelian group of order 5 is cyclic.
(iv) Prove every abelian group of order pq where p, q are distinct primes is cyclic

Now we make precise the idea that all group actions are equivalent to translation of cosets of subgroups. If $G\times S\to S$ is any (left) action of G on a set S, and if $\varphi:S\to T$ is a bijection of sets, we get an equivalent (left) action of G on T by defining $G\times T\to T$ as follows: $g(t) = \varphi(g(\varphi^{-1}(t)))$ The following problem shows how to replace any set S acted on by G, with a set T of cosets of a subgroup of G.

**Challenge:** Now let $G\times S\to S$ be any transitive action, and choose a point p of S. If $\mathcal{S}$ is the set of all subsets of G define $\varphi:S\to\mathcal{S}$ by $\varphi(q) = \{g: g(p) = q\} \subset G$, and let $T\subset\mathcal{S}$ be the image of the map $\varphi$.
(i) With notation as above, show that T is precisely the set of left cosets of the stabilizer subgroup $G_p$, and that $\varphi:S\to T$ is a bijection
(ii) With notation as above, show that the action $G\times T\to T$ induced by the action $G\times S\to S$ and the bijection $\varphi$, is left translation of cosets.

## §5) Homomorphisms: a way to compare groups

Another way to view the action of a group on a set is to view each element of the group as a permutation of the elements of the set. Thus, when the group of the cube acts on its six faces, each rotation of the cube can be considered as giving a permutation of the six faces. Thus we have a function $\text{Cube}\to S_6$, which "preserves composition", i.e. for any two rotations f, g of the cube, if we write $\overline{f}$, $\overline{g}$, for the associated permutations of the set of faces of the cube, then $\overline{(f\circ g)} = \overline{f}\circ\overline{g}$.

Since two rotations of the cube are equal iff they permute the faces in the same way, the map $\text{Cube}\to S_6$ is injective, hence embeds the group Cube inside the permutation group $S_6$. [Recall $f:S\to T$ is

injective or "1-1" iff for all x,y in S, $x \neq y$ implies $f(x) \neq f(y)$.] We can also view the group of the cube as a permutation group on the 8 vertices, or on the 12 edges, obtaining embeddings of Cube inside the groups $S_8$, and $S_{12}$.

It is more informative however to map Cube into a smaller group of permutations, so we consider its action on the set of 4 diagonals of the cube. This gives a composition - preserving map into the group $S_4$, which also has order 24. It is possible then that Cube maps bijectively onto this group. Indeed this is so. In fact, suppose a rotation of the cube maps each of the 4 diagonals into itself. Then each vertex maps either to itself or to the diagonally opposite vertex. If even one vertex maps to itself, then a glance at a picture of a cube shows that the three vertices adjacent to that one must also remain fixed. But then the three faces adjacent to that vertex are also fixed, and hence so is the entire cube.

Thus the only possible maps leaving all 4 diagonals invariant are the identity map and the antipodal map taking each vertex to its diagonal opposite. But the antipodal map is not a rotation (the axis of rotation would have to be perpendicular to all four diagonals). Thus the only rotation acting as the identity permutation of the four diagonals is the identity rotation.

We claim it then follows that no two distinct rotations act alike as permutations of the diagonals. For if f, g act the same on all diagonals, then $f^{-1}g$ would act as the identity permutation, and then by what we have seen, $f^{-1}g$ would be the identity rotation, and so $f = g$. Thus in fact the map Cube$\rightarrow S_4$, which lets a rotation be regarded as a permutation of the 4 diagonals, is an embedding of Cube into the group $S_4$.

Since Cube and $S_4$ both have 24 elements, the embedding Cube$\rightarrow S_4$ is a bijection, and since in both groups the group operation is composition, which is preserved by this map, we can regard the group Cube as structurally the same as $S_4$.

**The most fundamental concept in all of algebra.**

Abstracting this construction yields the concept of "homomorphism":

**Definition**: Let G,H be two groups, and $f:G\rightarrow H$ a map. Then f is called a (group) <u>homomorphism</u> from G to H iff f "preserves the

group operations", i.e. iff $\forall a,b$ in G, we have $f(ab) = f(a)f(b)$, where on the left side the product of a and b is taken in G, and on the right side the product of f(a) and f(b) is taken in H.

Just as stabilizer groups, i.e. those elements which act as the identity on a given element, are crucial to understanding group actions, so the sets of elements which map to the identity element are crucial to understanding homomorphisms:
**Definition**: If $f:G \to H$ is a homomorphism, the subset $G \supset \ker(f) = \{x \text{ in } G: f(x) = e \text{ in } H\}$, is called the kernel of f.

The following general results are used constantly:
**Lemma**: If $f:G \to H$ is a homomorphism, then
i) $f(e) = e$, so that e is in ker(f).
ii) For every x in G, $f(x^{-1}) = f(x)^{-1}$, and
iii) $f:G \to H$ is injective iff $\ker(f) = \{e\}$.
**proof**: Note $f(e) = f(ee) = f(e)f(e)$, so by multiplying by $f(e)^{-1}$ gives $f(e) = e$, (where of course the e in f(e) is the identity in G and the e on the right side of the equation is the identity in H). Thus e belongs to ker(f) Since $e = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$, we see $f(x^{-1})$ is the inverse of f(x), i.e. $f(x^{-1}) = f(x)^{-1}$. If f is injective, ker(f) consists of only one element, so $\ker(f) = \{e\}$. Conversely if $\ker(f) = \{e\}$ and $f(x) = f(y)$, then $f(x^{-1}y) = f(x)^{-1}f(y) = f(y)f(y)^{-1} = e$, so $x^{-1}y$ is in ker(f). Since $\ker(f) = \{e\}$, then $x^{-1}y = e$, and $x = y$, so f is injective. QED.

**Advice**: Practice until you can do this type of proof in your sleep

**Definition**: A group homomorphism $f:G \to H$ is called a (group) isomorphism iff there is a group homomorphism $k:H \to G$ which is inverse to f, i.e. such that $fk = 1_H$, and $kf = 1_G$.
If there is an isomorphism from G to H we write $G \cong H$, read "G is isomorphic to H". Isomorphism is an equivalence relation

The next problem contains some useful criteria for isomorphisms. Recall that a function $f:S \to T$ is injective iff for every y in T there is at most one x in S with $f(x) = y$, that f is surjective iff for every y in T there is at least one x in S with $f(x) = y$, and f is bijective iff f is both injective and surjective.

**Exercise #8)**
(i) A homomorphism $f:G \to H$ is an isomorphism iff f is bijective.
(ii) A surjective homomorphism f is an isomorphism iff $\ker(f) = \{e\}$.
(iii) If G, H are finite groups of the same order, then a homomorphism $f:G \to H$ is an isomorphism iff $\ker(f) = \{e\}$.

**Definition**: If $f:G \to H$ is a homomorphism, and $K \subset G$, $L \subset H$ are subgroups, the subset $H \supset f(K) = \{y \text{ in } H \text{ such that } y = f(x) \text{ for some } x \text{ in } K\}$, is called the "image of K under f" The subset $G \supset f^{-1}(L) = \{x \text{ in } G \text{ such that } f(x) \text{ is in } L\}$, is called the "inverse image (or preimage) of L under f". Observe $\ker(f) = f^{-1}(\{e\})$. We also write $\mathrm{Im}(f)$ for $f(G)$.

**Exercise #9)** If $f:G \to H$ is a homomorphism, and $K \subset G$, $L \subset H$ are subgroups, then $f(K)$ is a subgroup of H, and $f^{-1}(L)$ is a subgroup of G.

**Definition**: A group isomorphism $f:G \to G$ from a group G to itself, is called an "automorphism".

**Exercise #10)** Show that for any group G, the set Aut(G) of all automorphisms of G is a subgroup of Bij(G).

The next problem shows that giving a (left) action of G on a set S is equivalent to giving a homomorphism $G \to \mathrm{Bij}(S)$.
**Exercise #11)** (i) If $\varphi:G \to \mathrm{Bij}(S)$ is a homomorphism, show that setting $\langle g,s \rangle = (\varphi(g))(s)$ for g in G, s in S, defines an action of G on S
(ii) Conversely, given a (left) action of G on S, show that for each g in G, the function $\varphi(g)$ defined by $(\varphi(g))(s) = \langle g,s \rangle$, gives a well defined homomorphism $\varphi:G \to \mathrm{Bij}(S)$.
(iii) What happens in (ii) if you have a right action?

**Exercise #12)** (i) If $D_3$ is the full symmetry group of a regular (equilateral) triangle $\Delta$, show $D_3 \cong S_3$ by letting $D_3$ act on the vertices of $\Delta$.
(ii) Show that the full symmetry group of a tetrahedron is isomorphic to $S_4$.
(iii) Show every infinite cyclic group is isomorphic to $\mathbb{Z}$.
(iv) Show a cyclic group of order n is isomorphic to $\mathbb{Z}_n$.
(v) Show $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}_n^*, \cdot)$, the group defined in ex. 3(iv).

**§6) Normal subgroups, and the action of "conjugation"**

We have seen that the kernel of a homomorphism is useful in analyzing a homomorphism. Next we will study kernels, and learn that not every subgroup of a group can be the kernel of a homomorphism. Those which can, the "normal" subgroups, were singled out already by Galois and play an important role in the theory of equations.

Let $f:G \to H$ be a homomorphism with kernel $K \subset G$, and consider the right and left translates, or "cosets" of K by an element x in G. Note that if $f(x) = y$, then $xK$ consists of all elements mapped to y by f. I.e. $f(xk) = f(x)f(k) = ye = y$, for any k in K. Conversely if $f(g) = y = f(x)$, then $f(x^{-1}g) = e$, as we saw before, so $x^{-1}g = k$ for some k in K, and thus $g = xk$, belongs to $xK$. However, since $f(kx) = f(k)f(x) = ey = y$ also, we see by the same argument that $Kx$ also consists of those elements g in G s.t. $f(g) = y$. In particular, $xK = Kx$. Thus the right coset of K by x is the same as the left coset of K by x, something which did not usually happen for cosets of the stabilizer subgroups $G_x$ we met earlier in examining group actions.

Suppose $G_s$ is the subgroup of Cube leaving the top face s of the cube invariant, and that x is the $90^0$ clockwise rotation about the axis passing through the centers of the front and back faces, and hence leaving those faces invariant. Then for every g in $G_s$, xg carries the top face to the right face, hence the left coset $xG_s$ consists of elements carrying the top face to the right face. However the product in the opposite order gx carries the top face to the right face only if g in $G_s$ is the identity element. Otherwise, x carries the top face to the right face and then g rotates the right face to one of the other three faces adjacent to the top face. In particular, the two cosets $xG_s$ and $G_sx$ are not the same. [Check that $G_sx$ consists of those rotations carrying the left face to the top face.]

**Definition**: A subgroup H of a group G is called "normal" (normal *in G*, for this concept is a relative one), iff for every x in G the two cosets xH and Hx consist of the same elements.

**Remarks**: (i) We have shown above that the kernel of a homomorphism $f:G \to H$ is always a normal subgroup of G.
(ii) Every subgroup of an abelian group G is normal in G.
(iii) A subgroup $H \subset G$ is normal in G iff for every x in G, $xHx^{-1} = H$.

The last remark above leads to a very important concept:
**Definition**: (i) If G is a group and x any element, the mapping $f: G \to G$ defined by $f(g) = xgx^{-1}$, is called "conjugation" by x.
(ii) If H is a subgroup of G and x any element, the subset $xHx^{-1}$ of elements of form $xyx^{-1}$ for all y in H, is said to be "conjugate" to H.

**Exercise #13)** (i) For every x in a group G, prove that conjugation by x defines a group automorphism of G, and the map $G \to Aut(G)$ taking x to conjugation by x is a homomorphism.
(ii) If H is a subgroup of G and x is any element, prove $xHx^{-1}$ is also a subgroup of G.
(iii) Prove the relation $H \approx K$ iff H is conjugate to K, is an equivalence relation on the set of subgroups of G.
(iv) Prove a subgroup $H \subset G$ is normal iff for all x in G, $xHx^{-1} \subset H$.

**Definition**: If H is a subgroup of G, its "conjugacy class" is the set of subgroups of G to which H is conjugate

**Remark**: The operation of conjugation thus gives a useful way to measure how far a subgroup is from being normal. I.e. H is normal iff its conjugacy class consists of only one element, H itself; the larger the conjugacy class, the farther the subgroup is from being normal.

**The action on subgroups by conjugation**: Since normality is so fundamental a notion, conjugation is one of the most insightful ways to define an action of G on subsets of itself. For instance, G acts on its set of subgroups by conjugation. Thus if S is the set of subgroups of G, the action is the map $G \times S \to S$ where (g,H) goes to $g(H) = gHg^{-1}$. (This defines a left action. For a right action send (g,H) to $g^{-1}Hg$.) Since $xyH(xy)^{-1} = x(yHy^{-1})x^{-1}$, and $eHe^{-1} = H$, G acts by conjugation on the set of its subgroups, and the orbit of a subgroup H is its conjugacy class.

**Definition**: If G acts on its subgroups by conjugation, then for any subgroup H of G, the stabilizer subgroup of H for conjugation is called the normalizer of H, and denoted N(H). Thus $N(H) = \{x \text{ in } G : xHx^{-1} = H\}$ H is thus a normal subgroup of N(H). Indeed N(H) is by definition

the largest subgroup of G in which H is normal.

**The fundamental conjugation formula.**
The counting principle, for a group G acting on its subgroups by conjugation, takes the following form: for any subgroup H of G,

$$\#(G) = \#(N(H))\#(\text{conjugacy class of } H).$$

The phrase usually memorized is: "**the order of the conjugacy class is the index of the normalizer** (for any subgroup).

**The action on elements by conjugation:** G also acts on itself by conjugation, i.e. define $G\times G\to G$ by sending $(x,y)$ to $xyx^{-1}$. The stabilizer group of y for this action is the set of all x which commute with y, $N(y) = \{x: xyx^{-1} = y\} = \{x: yx = xy\}$. We call this group the normalizer of y, (also called the "centralizer" of y). As above:
$\#(G) = \#(N(x))\#(\text{conjugacy class of } x)$, for any x in G;
i.e. **the order of the conjugacy class of x = the index of the normalizer of x.**

**Definition**: The subset of those elements of g which commute with all other elements is called the <u>center of G</u> and denoted Z(G). Thus Z(G) = {those x in G such that xy = yx, for all y in G}.

**Definition**: The product $xyx^{-1}y^{-1}$ is called the <u>commutator</u> of x and y. The set of all commutators in G, $\{xyx^{-1}y^{-1}$, for all x,y, in G} is called the <u>commutator subgroup</u> of G, and denoted [G,G].

**Remark**: Two elements x,y commute with each other if and only if their commutator equals e, the identity of G.

**Definition**: A subgroup H of G such that $\varphi(H) = H$ for all automorphisms $\varphi$ of G, is called a <u>characteristic</u> subgroup of G.

**Exercise #14) (i)** Prove Z(G) is a normal subgroup of G.
**(ii)** Prove that if a subgroup H of G such that $\varphi(H) \subset H$ for all automorphisms $\varphi$ of G is a characteristic subgroup of G
**(iii)** Prove that [G,G] is a characteristic subgroup of G.
**(iv)** Prove that every characteristic subgroup is a normal subgroup.

**The "Class Equation"**: Any group action on a set S decomposes S into disjoint orbits, hence yields an equation for the order of S as a

sum of the orders of the orbits. Since the order of the orbit of x is the index of the stabilizer subgroup of x, the terms in the sum are factors of the order of G, by LaGrange. In the example of G acting on itself by conjugation, #(G) hence equals a sum of indices of normalizers of elements of G. This is the class equation:

$\#(G) = \Sigma_x \text{ ind}(N(x))$, where x ranges over a set of representatives for the distinct conjugacy classes in G.

Note that an element x is in Z(G) iff its orbit under conjugation contains just one point, x itself; equivalently, iff index(N(x)) = 1. Thus if we sum first over elements of the center, we get:

$$\#(G) = \#(Z(G)) + \Sigma_x \text{ ind}(N(x)),$$

where x ranges over a set of representatives for those conjugacy classes in G containing more than one element, i.e. for which N(x) is a proper subgroup of G.

**Useful remark**: In a non abelian group G, the normalizer of any element is always strictly larger than the center, since for x in Z(G), N(x) = G, and for x not in Z(G), N(x) contains both x and Z(G).

**Application to "p groups"**: The following is a typical, and useful, application of the class equation to groups of order $p^n$.
**Lemma**: A p - group has non trivial center; more precisely, if $\#(G) = p^n$ for $n \geq 1$, and p is prime, then #(Z(G)) is divisible by p.
**proof**: This follows immediately from the class equation in the second form above, $\#(G) = \#(Z(G)) + \Sigma_x \text{ ind}(N(x))$, where the terms in the sum are indices of proper subgroups of G, hence all are divisible by p. Since the left hand side is also divisible by p, so is #(Z(G)). Since e belongs to Z(G), #(Z(G)) > 0, so $\#(Z(G)) \geq p > 1$. QED.

**Corollary**: Every group G of order $p^2$ is abelian.
**proof**: By the lemma and the "useful remark" above, if G were not abelian, then for every element x, N(x) = G. But N(x) = G iff x commutes with everything, iff x is in the center! Since every element lies in the center, G is abelian QED.

**Exercise #15)** If p is a prime integer, prove any group of order $p^2$ is isomorphic either to the cyclic group $Z_{p^2}$ or to $Z_p \times Z_p$.

**Examples of normal, and of non normal, subgroups.**

Examples of non normal subgroups come from stabilizer subgroups of many non trivial actions by the following.

**Lemma**: Let a group G act on a set S, and let x, y be two points in the same orbit. Then the stabilizer subgroups $G_x$ and $G_y$ are conjugate in G. In fact the set of all stabilizer subgroups of a given orbit form a conjugacy class of subgroups of G.

**proof**: Choose f in G such that f(x) = y. Then for every g in $G_x$, $(fgf^{-1})(y) = (fg)(x) = f(x) = y$, so $(fgf^{-1})$ belongs to $G_y$. Thus $(f\ G_x f^{-1}) \subset G_y$. Similarly $(f^{-1}G_y f) \subset G_x$. Conjugating this last inclusion by f gives $G_y \subset (f\ G_x f^{-1})$, whence $G_y = (f\ G_x f^{-1})$. Now let H be any subgroup of G conjugate to $G_x$, i.e. $H = f\ G_x f^{-1}$, for some f in G, and let y = f(x). Then by the same argument, $f\ G_x f^{-1} = G_y$. **QED.**

**Remarks**: There is no claim in the Lemma that distinct elements of an orbit have distinct stabilizer subgroups, and in fact they may all have the same stabilizer subgroup. In some common examples the stabilizer subgroups are all equal to {e}, for example in the action of the group of translations on the plane, or the group of rotations on the circle. More generally, since all subgroups of an abelian group are normal, if an abelian group acts transitively on a set S, then all elements of S have the same stabilizer subgroup.

Since a subgroup is normal iff its conjugacy class consists of one element we have the following result

**Corollary**: If a group acts transitively on a set S, then either every point of S has the same stabilizer subgroup, or none of the stabilizer subgroups is normal.

**Example**: For the action of Cube $\cong S_4$ on the faces of the cube, every non trivial rotation leaving the top face invariant fails to leave the front face invariant, hence the three (4 element) stabilizer subgroups of the faces are non normal in Cube. Further, since the two non trivial rotations in Cube leaving a particular vertex of the cube fixed, do not fix either of the three adjacent vertices, the four (3 element) stabilizer subgroups of the vertices are not normal either. The six (2 element) stabilizer subgroups of the edges are similarly non normal. Hence, although Cube has plenty of

subgroups, normal subgroups are somewhat scarce.

We can produce a normal subgroup however, by representing Cube inside a still smaller permutation group. Consider the action of Cube on the three mutually perpendicular axes passing through the centers of opposite pairs of faces of the cube. This action, by an earlier exercise, yields a homomorphism Cube$\to$S3, which cannot be injective since #(S3) = 6 < #(Cube) = 24. Moreover the action is transitive, so the homomorphism is non trivial, hence has a kernel which is a proper normal subgroup of Cube.

In fact a glance at a cube shows that the axes can be permuted in at least 4 ways by the rotations of the cube, so the homomorphism Cube$\to$S3 is surjective, and the kernel has order 4 So Cube contains at least one normal subgroup of order 4. In fact, the subgroup A of Cube of order 12, consisting of the 8 rotations which each fix a pair of diagonally opposite vertices, plus the three $180^0$ rotations, each about one of the axes passing through a pair of opposite faces, plus the identity, is a normal subgroup of Cube too. Do you see how to represent it as a kernel of a homomorphism? Alternatively, if you check A is a subgroup, normality follows from the next exercise.

**Exercise #16)** **(i)** A subgroup of index 2 in a finite group is normal.
**(ii)** The subsets $G\times\{e\}$ and $\{e\}\times H$ are normal subgroups of $G\times H$.
**(iii)** If $f:G\to H$ is a homomorphism and $L\subset H$ is a normal subgroup, then the subgroup $f^{-1}(L)\subset G$ is also normal.
**(iv)** If $f:G\to H$ is a homomorphism and $K\subset G$ is a normal subgroup, is $f(K)\subset H$ always normal? Prove, or find a counterexample.
**(v)** If p is the smallest prime factor of #(G), prove any subgroup of index p is normal.

**Definition**: An element x of G has <u>order n</u> if there are exactly n distinct elements of G among the powers of x: $e = x^0, x^1, x^2, x^3, \ldots\ldots$ If finite, the order is the smallest positive integer n such that $x^n = e$.

**Definition**: A non trivial group G is called <u>simple</u> if the only normal subgroups are {e} and G. [We do not consider {e} a simple group.]

**Exercise #17)** **(i)** Prove an abelian group is simple if and only if it has prime order.

(ii) Prove a product of two non trivial groups is never simple.
(iii) Prove if G is simple, a non constant homomorphism $f:G \to H$ is always injective.
(iv) If G is simple, $f:G \to H$ is a homomorphism, and $L \subset H$ is a normal subgroup such that $f(x)$ is in L for some $x \neq e$, then $f(G) \subset L$.

**Example: The icosahedral group is simple.**

This is surprisingly easy. We will show that if a normal subgroup of Icos contains a non trivial element which leaves fixed one vertex, then it contains every element leaving fixed any vertex, and similarly for the elements leaving fixed a face, or an edge. This forces a non trivial normal subgroup to be so large it must equal Icos.

So consider the elements of Icos which leave fixed some vertex. There are 12 vertices of an icosahedron, each surrounded by 5 triangles, so each vertex is left fixed by a group of rotations of order 5. Each such group of rotations fixes just two opposite vertices, so there are 6 such groups of order 5 in Icos, containing all elements which fix some vertex Since distinct groups of prime order cannot intersect except in the identity, this accounts for 24 elements of Icos of order 5

Similarly, there are 20 triangular faces, left fixed in pairs by 10 subgroups, each of order three, accounting for 20 elements of order three in Icos fixing some face. The elements fixing some one of the 30 edges comprise 15 subgroups, each of order 2, giving 15 elements of order two. This gives 24+20+15 = 59 elements of Icos, and the identity makes 60 elements. Moreover, since the rotations in Icos act transitively on vertices, faces, and edges of the icosahedron, the 6 stabilizer subgroups of the 12 vertices are conjugate, as are the 10 groups of the 20 faces and the 15 groups of the 30 edges.

Now suppose a normal subgroup N of Icos contained one of the elements of order 5. It would then contain all 5 of its powers, hence the whole stabilizer subgroup containing it. But since N is closed under conjugation, N would also contain all elements conjugate to elements of that subgroup, i.e. it would contain all the groups conjugate to that subgroup as well. The same holds for the elements of orders 3 and 2

Hence any non trivial normal subgroup N of Icos must contain, in addition to the identity, all 24 elements of order 5 or none of

them, all 20 elements of order 3 or none, and all 15 elements of order 2 or none. Thus #(N) equals 1 plus some of the numbers 15, 20, 24 Since #(N) divides 60 by LaGrange's theorem, the only possibility is #(N) = 1 + 15 + 20 + 24 = 60, (since no other sum of these numbers is a factor of 60). Thus Icos is simple.

**Exercise #18)** Find the class equation explicitly for the group Icos.

**Remark**: Since Icos has no proper normal subgroups, there are no non trivial homomorphisms defined on Icos; every homomorphism f:Icos→H is either constant, or an embedding. In particular Icos cannot act non trivially on any set of fewer than 5 elements.

**Remark**: A deep theorem due to Feit and Thompson says that a simple group of odd order must have prime order, so all "interesting" simple groups have even order. The next interesting one after Icos has order 168, and was studied by Felix Klein as the subgroup of those linear transformations of the complex projective plane which carry the curve with equation $x^3y + y^3z + z^3x = 0$ in homogeneous coordinates, into itself. We will look at this interesting group later.

## §7) Normal subgroups are kernels of homomorphisms into appropriate "quotient groups"

We show next how to recover a surjective homomorphism from its kernel. The key is to look at cosets of the kernel. The idea is that the kernel tells you which elements go to the identity, and its cosets tell you which elements go to other things. Thus the cosets of ker(f) in G give a substitute for the image of f:G→H. More precisely:

**Lemma**: If f:G→H is a homomorphism with kernel K⊂G, the cosets of K are exactly the equivalence classes of the equivalence relation: a~b iff f(a) = f(b) In other words, b belongs to aK iff f(b) = f(a).
**proof**: If b belongs to aK, then b = ak for some k in K. Then f(b) = f(ak) = f(a)f(k) = f(a)e = f(a). Conversely, if f(a) = f(b), then e = $f(a)^{-1}f(b) = f(a^{-1}b)$, so $a^{-1}b = k$ for some k in K. Left-multiplying this last equation by a shows that b = ak belongs to aK. QED.

As a consequence, we can reconstruct a version of f as follows: let G/K denote the set of left cosets of K in G, and define $\overline{f}$: G→G/K by setting $\overline{f}(a) = aK$ Then $\overline{f}$, like f, has the property that $\overline{f}(a) = \overline{f}(b)$ iff

b belongs to aK, iff $a^{-1}b$ belongs to K. Thus to some extent, $\bar{f}$ is a reconstruction of f. But f was a homomorphism and $\bar{f}$ is only a function to a set of cosets. But we can remedy this, too! We can define a natural group operation on G/K so that, like f, $\bar{f}$ is a homomorphism.

To define an operation on G/K we must decide how to define the product of two cosets aK, bK. The most obvious thing is to try to set (aK)(bK) = (ab)K. I.e. the product of two cosets should be the coset containing the product of two representative elements, one from each coset. But the problem, which is a subtle one, is which representatives to choose?

It is wrong to think that when we write aK we have some way of recognizing a in the coset aK. But aK simply means the coset containing a, and if K ≠ {e}, it contains other things as well. I.e. if aK = cK, and bK = dK, how do we know (ab)K = cdK? The only way our definition of multiplication makes sense, is if the product is the same for every choice of representative elements of aK and bK.

**Lemma**: When K is normal, for every a,b in G and every $k_1,k_2$ in K the product $ak_1bk_2$ belongs to the same coset of K as does ab.
**proof**: We must show that $(ab)^{-1}(ak_1bk_2)$ is in K. This is where we use that K is normal in G The normality of K tells us that bK = Kb, and hence there is some $k_3$ in K such that $k_1b = bk_3$. Then we are reduced to showing that $(ab)^{-1}(ak_1bk_2) = (ab)^{-1}(abk_3k_2) = (ab)^{-1}(ab)(k_3k_2) = k_3k_2$ belongs to K, which is clear. QED.

Since a coset is a collection of elements, you might reason that the correct definition of the product of two cosets is be to take the collection of all products, one factor from one coset, one factor from the other coset Then we would need to know that those products do form a coset. Check this is true, i.e. prove the following:
**Lemma**: If K is normal in G, then for any two cosets X, Y of K, the set of pairwise products xy, with x in X, and y in Y (in that order!), forms a single coset of K.

**Exercise #19)** If K is a normal subgroup of G,
(i) prove G/K is a group with identity element eK = K, and $a^{-1}K$ is the inverse of aK;
(ii) prove the map G→G/K, taking a to aK is a surjective

homomorphism with kernel K.
**(iii)** If G is abelian, prove G/K is also abelian.
**(iv)** If G is cyclic, prove G/K is also cyclic.

**Terminology**: The group G/K is called the "quotient group of G modulo K", or simply "G mod K".

To what extent have we achieved our goal of recovering a homomorphism $f:G\to H$ from its kernel K? Essentially, K determines by the quotient construction, a group G/K isomorphic to the image subgroup $\mathrm{Im}(f) \subset H$, and a homomorphism $G\to G/K$ which is "equivalent to f", in the sense that there is an isomorphism $G/K \cong \mathrm{Im}(f)$ such that the composition $G\to G/K \cong \mathrm{Im}(f) \subset H$, equals f. But we get no information at all from K about the part of H not contained in Im(f), which is not too surprising. How could we learn anything from f about the part of H not "touched" by f?

To sum up, we prove next a theorem giving the basic facts about quotient groups. The first property below is the key to defining homomorphisms on quotient groups without struggling with the cumbersome fact that the actual elements of G/K are cosets. This is the "universal property" of quotient groups, and should be mastered to deal with them efficiently.

**Theorem: (basic properties of quotient groups, and homoms.)**
**1) How to define a homomorphism $G/K\to H$:** If K is normal in G, any homomorphism $f:G\to H$ such that $f(K) = \{e\}$, determines a unique homomorphism $\overline{f}:G/K\to H$ such that for every a in G $\overline{f}(aK) = f(a)$.
**2) When is a homomorphism injective?**
A homomorphism $f:G\to H$ is 1-1 iff $\ker(f) = \{e\}$.
**3) When is the homomorphism $G/K\to H$ induced by $f:G\to H$ an isomorphism?**
If the homomorphism $f:G\to H$ is onto, and $K = \ker(f)$, then the unique map $\overline{f}: G/K\to H$, determined by f is an isomorphism.
**4) What is the relation between subgroups of G and subgrioups of G/K?**
If a homomorphism $f:G\to H$ is onto, and $K = \ker(f)$, there is a 1-1, inclusion preserving, correspondence between {subgroups of H} and {subgroups of G containing K} set up by the map $H\supset M\mapsto f^{-1}(M)\subset G$.
**5) How are repeated quotient groups related?**
If H,K are normal subgroups of G and $K\subset H\subset G$, then K is normal in H,

H/K is normal in G/K, and G/H ≅ (G/K)/(H/K).

**6) When is the product of two subgroups a subgroup?**

If H,K are subgroups of G and K is normal, then the set of pairwise products HK = {hk  h in H and k in K} ⊂G is a subgroup, (H∩K)⊂H is a normal subgroup of H, and H/(H∩K) ≅ (HK)/K.

**proof of 1)**: Uniqueness is clear since $\bar{f}$ is specified on every element of G/K by the rule $\bar{f}(aK) = f(a)$. The question is whether $\bar{f}$ is well defined (independent of choice of representative a for aK), and whether it is a homomorphism. The main point is well definedness. So assume that f(K) = {e}, and let aK = bK. To show our definition is independent of choice of coset representative we need to show that f(a) = f(b). But since aK = bK iff $a^{-1}b$ belongs to K, we see that $f(a^{-1}b) = f(a)^{-1}f(b) = e$, so f(a) = f(b). That $\bar{f}$ is a homomorphism follows easily, since $\bar{f}(aKbK) = f(abK) = f(ab) = \bar{f}(aK)\,\bar{f}(bK)$. **QED for 1)**.

**proof of 2)**: Since a homomorphism f:G→H always satisfies f(e) = e, if f is 1-1 then ker(f) = {e}. Conversely, if ker(f) = {e} and f(a) = f(b), then $f(a^{-1}b) = f(a)^{-1}f(b) = e$, so $a^{-1}b$ belongs to ker(f) = {e}. Thus $a^{-1}b = e$, whence a = b and f is 1-1. **QED 2)**.

**proof of 3)**: Since K = ker(f) is normal and f(K) = {e}, the homomorphism $\bar{f}$ is well defined. If f(a) = x, then $\bar{f}(aK) = x$ also, hence if f is onto so is $\bar{f}$. Since $\bar{f}(aK) = e$ iff f(a) = e, iff a is in ker(f) = K, we see that ker($\bar{f}$) = {K}. Since K is the identity element of G/K, part 2) shows that $\bar{f}$ is also 1-1 hence an isomorphism. **QED 3)**.

**proof of 4)**: It is a trivial (but useful) general fact that for any set map f:S→T the inverse image map T⊃M ↦ $f^{-1}(M)$⊂S on subsets preserves inclusions (and intersections and unions). It is easy to check if f is a homomorphism, it also preserves subgroups. Since every subgroup M⊂T contains e, $f^{-1}(M)$ always contains $f^{-1}(e)$ = K. To show the claimed 1-1 correspondence, work the next exercise.

**Exercise #20)** The correspondence G⊃N⊃K ↦ f(N)⊂H is inverse to the correspondence in part 4) of the Thm. above, i.e. $f(f^{-1}(M)) = M$ for all M, and $f^{-1}(f(N)) = N$, whenever N contains K. **QED 4)**.

**proof of 5)**: This is the interesting one, since it illustrates the value

of the innocent sounding property 1). I.e. when the objects at hand are horribly complicated such as the elements of (G/K)/(H/K), which are cosets of subgroups whose elements themselves are cosets, it is very helpful to have a clean way to guarantee that you have a homomorphism without actually dealing with the nature of the elements of the super quotient group. So look at property 1) closely.

Notice that the property guaranteeing a homomorphism on G/K is stated entirely in terms of G and K⊂G. You never mention cosets nor actually deal with G/K. So at least you get rid of one level of abstraction. In the current setting where we have a sort of "double cosets", it means we will only have to deal with single cosets at worst. I.e. we will have to deal with elements of G/H and G/K, but not with elements of (G/K)/(H/K).

We will use part 1) to define a homomorphism $\tilde{f}:(G/K)/(H/K)\to G/H$, and part 3) to check it is an isomorphism. (To convince yourself of the value of part 1), just try proving this result with your bare hands. Even the notation is a problem.)
First note that since K is normal in G, K is also normal in H [Why?].

We will check soon that H/K is normal in G/K. The natural homomorphism $f:G\to G/H$, where f(a) = aH, has kernel H, from a previous exercise. Since K⊂H, we see that f(K) = {e}, so there is by 1) a unique associated homomorphism $\bar{f}:G/K\to G/H$, where $\bar{f}(aK) = f(a) = aH$.

We claim the kernel of this homomorphism is H/K = {hK: h is in H}. Since the identity element of G/H is H, aK is in $\ker(\bar{f})$ iff $\bar{f}(aK) = H$. But $\bar{f}(aK) = aH$, so aK is in $\ker(\bar{f})$ iff aH = H, iff a is in H, iff aK is in H/K. Thus H/K = $\ker(\bar{f})$, hence H/K is a normal subgroup, and part 3) shows the induced map $\tilde{f}:(G/K)/(H/K)\to G/H$ is an isomorphism. **QED 5)**.

**proof of 6)**: Here is the acid test of whether you have grasped the use of these methods.
**Exercise #21)** Prove part 6 in a similar way. I.e. first show HK is a subgroup, and K is normal in it. Then consider the homomorphism defined by inclusion H⊂HK. Compose this with the canonical map HK→(HK)/K to get a homomorphism H→(HK)/K, and check that this last map is surjective with kernel H∩K. **QED for theorem.**

**Exercise #22) (i)** If x is any element of a group G there is a unique homomorphism $f:\mathbb{Z}\to G$ taking 1 to x.

**(ii)** If $(\mathbf{Z},+)$ is the integers, and $n\mathbf{Z} \subset \mathbf{Z}$ the subgroup of multiples of n, prove $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n \cong Z_n$, the cyclic group of order n.
**(iii)** If a divides n, prove $\mathbf{Z}_n$ has a unique subgroup K of order a, namely K = ker(f), where $f:\mathbf{Z}_n \to \mathbf{Z}_n$ is defined by f(x) = ax.
**(iv)** If a divides n, prove $\mathbf{Z}_n/a\mathbf{Z}_n \cong \mathbf{Z}_a$.

**Terminology**: Two elements of G which represent the same element of the quotient group G/K are called "equivalent mod K". Integers x,y representing the same element in $\mathbf{Z}_r$ are said to be "congruent mod r", written $x \equiv y(\text{mod } r)$, or $x \equiv y(r)$.

**§8) Sylow's Theorems**:

Just as we study polyhedra by their faces, edges, vertices, we analyze groups by their subgroups. We want to know what the orders of the subgroups are and which subgroups are conjugate to which others, in particular which ones are normal. Of course if we have an action of our group on a polyhedron, then a knowledge of the faces, edges, and vertices of the polyhedron translates into information on the corresponding stabilizer subgroups of the group and their conjugacy classes, as we have seen.

Conversely a knowledge of the subgroups and conjugacy classes in a given group gives us information on the possible actions of the group, since each group acts by translation and conjugacy on its own subgroups. Hence for an abstract group which does not come to us with a given action, to analyze it we need to know something about its subgroups and their conjugacy classes.

The fundamental results on the existence and conjugacy of subgroups of arbitrary groups are the three Sylow theorems (which we state together below). Recall that LaGrange's theorem gives us a necessary condition for the existence of a subgroup: the order of the subgroup must be a factor of the order of the group. This condition is not sufficient for existence of a subgroup - a group need not have a subgroup corresponding to every factor of its order. Sylow's theorem says a group does have subgroups corresponding to every <u>prime power factor</u> of its order.

**Exercise #23)** We know the rotation group Tet has order 12.
(i) Find subgroups of Tet whose orders correspond to all but one of the factors of 12
(ii) Prove there is no subgroup of Tet of that one missing order.

**Terminology**: A group of order $p^s$ where p is prime and $s > 0$, is called a "p-group". A subgroup of G of order $p^s$ is called a "p-subgroup" of G, and a subgroup of G of order $p^s$ such that $p^{s+1}$ does not divide #(G) is called a "Sylow" (or maximal) p-subgroup of G.

**Theorem (Sylow)**:
1) If G is a finite group, p a prime number, $r \geq 0$ an integer, and if $p^r$ divides #(G), then G has a subgroup of order $p^r$.
2) If $p^\alpha$ is the <u>maximal</u> power of the prime p dividing #(G), then the subgroups of G of order $p^\alpha$ (the *Sylow* p-subgroups) form a single conjugacy class
3) The number of Sylow p-subgroups of G has form $1 + np$, for some $n \geq 0$, and divides their common index $(\#(G)/p^\alpha)$, where $p^\alpha$ is the maximal power of p that divides #(G).

**Proof**: [This is an expanded version of the proof in Lang's Algebra.]
Recall the *order* of an element x is the smallest positive power of x that equals the identity, i.e. ord(x) = k, iff $k > 0$, $x^k = e$, and $x^s \neq e$ whenever $0 < s < k$. In particular e is the only element of order 1.

**Useful remark**: If $k = ord(x)$ and $x^t = e$, then k divides t.
[Why? because any t can be divided by k and written as $t = nk + m$, where $0 \leq m < k$. Then $x^t = x^{nk+m} = x^{nk}\, x^m = e^n\, x^m = x^m \neq e$, since $m < k$, unless $m = 0$, i.e. unless k divides t evenly. In particular, if ord(x) = k, and $x^r$ is any power of x, then $(x^r)^k = x^{rk} = (x^k)^r = e^r = e$. Thus $ord(x^r)$ divides ord(x).]
Note also that if p is prime, then a group has an element of order p if and only if it has a subgroup of order p. [Why?]

**proof of Sylow 1)**: We prove this result in easy stages, for progressively more general powers r and groups G.
**Case (i) G is cyclic and r =1.**
**proof**: I.e. we assume G is cyclic, p divides #(G) = n, and want to prove there is a subgroup H of order p. Since G is cyclic, there is an element x in G with $G = \langle x \rangle$ = the subgroup consisting of powers of x. Then $x^n = e$, but no smaller positive power of x equals e. Since p divides n, say $n = pm$, consider the element $y = x^m$. Then $y^p =$

$x^{mp} = x^n = e$, so ord(y) divides p. Hence ord(y) is either 1 or p. But if ord(y) = 1, then $e = y = x^m$, and x would have order dividing m, where $m < n$, a contradiction to ord(x) = n. So $y = x^m$ generates a subgroup $\langle y \rangle$ of order p. **QED.**

**Case (ii): G is abelian, and r = 1.**
**proof:** If G is abelian and p divides #(G) we want to find a subgroup, equivalently an element, of order p. We use induction on #(G). We are ok if #(G) = p, so assume the result for all abelian groups whose order is less than #(G). Now let $x \neq e$ be any non trivial element of G and denote its order by ord(x) = n. If p divides n, we are done, since then by case (i) the cyclic subgroup $\langle x \rangle$ contains an element and thus a subgroup of order p, which are also contained in G.

So assume p does not divide n, and consider the quotient group $G/\langle x \rangle$. This group is defined and is abelian, because G is abelian, hence all its subgroups are normal, and all its quotient groups are abelian (why?). Since by LaGrange's theorem $\#(G) = \#(G/\langle x \rangle)\cdot\#(\langle x \rangle)$, and p does not divide $\#(\langle x \rangle)$, p must divide $\#(G/\langle x \rangle)$, and by the inductive hypothesis there is an element y of order p in $G/\langle x \rangle$.

Now consider the natural surjective homomorphism $f:G \to G/\langle x \rangle$, and choose an element z of G such that f(z) = y. If z has order s, then $e = z^s$ and hence $e = f(e) = f(z^s) = (f(z))^s = y^s$, so ord(y) = p divides s, by the useful remark above Now we are done by the cyclic case applied to $\langle z \rangle$, i.e. the cyclic subgroup $\langle z \rangle$ has order divisible by p, hence contains an element w of order p, which also belongs to G **QED.**

**Next we prove Sylow 1) by induction:**
Since Sylow 1) holds for groups of order p, we may assume it is true for all groups of order less than #(G), and we suppose $p^r$ divides #(G). There are two possibilities which we shall call cases (iii) and (iv).

**Case (iii) Assume p divides #(Z(G)).**

Since the center Z(G) is abelian, by the previous case there is an element x in Z(G) having order p. Then $\langle x \rangle$ is a normal subgroup of G of order p, and we can consider the quotient group $G/\langle x \rangle$. Since $\#(G) = p\cdot\#(G/\langle x \rangle)$, and $p^r$ divides #(G), then $p^{r-1}$ divides $\#(G/\langle x \rangle)$. Hence by the inductive hypothesis, there is a subgroup L of $G/\langle x \rangle$ with $\#(L) = p^{r-1}$. Now if a surjective homomorphism $f:G \to M$ has

kernel $f^{-1}(e) = K$, then for every element y in M, $f^{-1}(y)$ is a coset of K.

Hence for every y in M, $f^{-1}(y)$ contains the same number of elements as K, and thus every element of M has the same number of preimages in G. In particular, for the natural surjection $f:G \to G/\langle x \rangle$, since the kernel of this map is $\langle x \rangle$ and $\#(\langle x \rangle) = p$, it follows that every element of $G/\langle x \rangle$ has exactly p preimages in G. Thus the inverse image $H = f^{-1}(L)$ of the subgroup L consists of exactly $p \cdot \#(L) = p \cdot p^{r-1} = p^r$ elements QED.

**Case (iv): Assume p does not divide #(Z(G)).** Now we need the class equation: $\#(G) = \#(Z(G)) + \Sigma \#(G/N(x))$, where the indices $\#(G/N(x))$ in the sum are all greater than one. Since p divides #(G) but p does not divide #(Z(G)), then at least one of the terms $\#(G/N(x))$ in the sum is not divisible by p. I.e. there is some subgroup N(x) such that p does not divide its index $\#(G/N(x))$.

Since $\#(G) = \#(G/N(x)) \cdot \#(N(x))$, and $p^r$ divides #(G) but p does not divide $\#(G/N(x))$, it follows that $p^r$ divides $\#(N(x))$. Moreover, since the indices $\#(G/N(x))$ occurring in the class equation are all greater than one, then $\#(N(x)) < \#(G)$. Hence by the inductive hypothesis N(x) contains a subgroup of order $p^r$, which is then also a subgroup of G **QED for Sylow 1).**

Before proving parts 2) and 3), it is instructive to present a general fixed point principle which will be used in the proofs. Recall the basic fact that the index of a subgroup of a group always divides the order of the group.

**Proposition:** (i) Suppose a p - group P acts on a finite set $\mathcal{S}$ such that p does not divide $\#(\mathcal{S})$. Then there is at least one fixed point for the action, i.e. there is a some point x in $\mathcal{S}$ such that $\gamma(x) = x$ for every $\gamma$ in P.
(ii) More generally, for any finite set $\mathcal{S}$ acted on by a p -group P, $\#(\mathcal{S}) = \#$(fixed points of the action) + np, for some integer n.
**Proof:** Since the distinct P - orbits give a disjoint decomposition of $\mathcal{S}$, the size of $\mathcal{S}$ is the sum of the sizes of the various orbits. Since $\#(\mathcal{S})$ is not divisible by p, it follows that p cannot divide the order of every orbit. The basic counting principle says that for each x in $\mathcal{S}$, the size of the orbit of x equals the index of the stabilizer subgroup

of x in P.

Since the index of a subgroup is always a factor of the order of the group, each of these indices is a power of p, and hence the size of each orbit is a power of p. Since the only power of p not divisible by p is $p^0 = 1$, there must be some orbit of size 1, i.e. there is some fixed point, proving part (i). Since in any case, each orbit either has size divisible by p, or is a one - point orbit containing a single fixed point, $\#(\mathcal{S})$ is a sum of multiples of p, plus the number of fixed points, which proves part (ii). **QED.**

**proof of Sylow 2)**: Now we assume the hypotheses of part 2) of Sylow's theorem, that $p^\alpha$ is the maximal power of p dividing #(G), that P and Q are subgroups of G of order $p^\alpha$, and we want to prove P and Q are conjugate. The trick is to let $\mathcal{S}$ be the set of all subgroups of G which are conjugate to Q, and try to show P is in the set $\mathcal{S}$. We will do this by letting P act on $\mathcal{S}$ by conjugation, applying the previous proposition to show there is a fixed point, and then observing that the fixed "point" must be P itself.

First we check one of the hypotheses of the fixed - point proposition.
**Claim**: $\#(\mathcal{S})$ is not divisible by p.
**proof**: Recall $\#(\mathcal{S}) = \text{index}_G(N(Q))$. Since $Q \subset N(Q)$, and $p^\alpha = \#(Q)$, it follows that $p^\alpha$ divides the order of N(Q). But then p cannot divide the index of N(Q). I.e. since $Q \subset N(Q) \subset G$, and $\#(G) = p^\alpha n$, the orders of these subgroups are of form $p^\alpha$, $p^\alpha d$, $p^\alpha de$, where $de = n$. Then $\text{index}_G(N(Q)) = (p^\alpha n)/(p^\alpha d) = e$, and since n is not divisible by p by hypothesis, neither is e. **QED.**

Now we let P act on $\mathcal{S}$ by conjugation. That is, if R is some element of $\mathcal{S}$, hence a subgroup which is conjugate to Q, we act on R by conjugating it by elements from P. In this way we will get some of the subgroups in $\mathcal{S}$ which are conjugate to R, but probably not all of them. But since any subgroup which is P - conjugate to R is also G - conjugate to it, P does act on the set $\mathcal{S}$.

Then by the fixed point proposition, there is some fixed point for the action. I.e. there is at least one subgroup R in $\mathcal{S}$ which is left fixed under conjugation by every element of P. We claim this element of $\mathcal{S}$ is P itself. Note that P leaves R fixed by conjugation if and only if $P \subset N(R)$. Hence our result follows from the next lemma.

**Lemma**: If P, R are p-Sylow subgroups of G such that $P \subset N(R)$, i.e. such that $xR = Rx$ for every x in P, then $P = R$.
**proof**: We know from the proof of exercise #21, that if $P \subset N(R)$, then PR is a subgroup of G, R is normal in PR, and $(PR)/R \cong P/(P \cap R)$, from which it follows that $\#[(PR)/R] = \#[P/(P \cap R)]$ is a divisor of #(P), hence a power of p. Since $\#(PR) = \#[(PR)/R] \cdot \#(R)$, thus #(PR) is also a power of p, hence PR is a p - subgroup of G. But P and R are both contained in PR, and P and R are both *maximal* p - subgroups of G. Hence $P = PR = R$. **QED.**

Since for any p - Sylow subgroups P and Q, the conjugacy class of Q contains P, all p - Sylow subgroups are conjugate. **QED Sylow 2).**

**proof of Sylow 3)**: This is a corollary of the fixed point proposition and the argument for part 2). I.e. if $\mathcal{S}$ = the class of all Sylow p - subgroups of G, and we let one of them, say P, act on $\mathcal{S}$ by conjugation, then by the fixed point proposition $\#(\mathcal{S}) = \#(\text{fixed points}) + mp$, for some $m \geq 0$. But by the previous lemma the only fixed point is P, so #(fixed points) = 1, and $\#(\mathcal{S}) = 1 + mp$, for some $m \geq 0$. **QED Sylow 3), (after proving the next exercise).**

**Exercise #24)** (i) Prove the rest of Sylow 3), that the number of Sylow p-subgroups divides the index of any one of them.
(ii) Use the group action technique to reprove Sylow 1) as follows: if $\#(G) = p^r m$ where $p^s$ divides m but $p^{s+1}$ does not divide m, let $\mathcal{S}$ be the set of all subsets of G of order $p^r$, and let G act on $\mathcal{S}$ by left translation. Prove $p^{s+1}$ does not divide $\#(\mathcal{S})$ and deduce that some orbit of the action is not divisible by $p^{s+1}$ either. [Hint: $\#(\mathcal{S})$ is a certain binomial coefficient.] Hence the stabilizer subgroup of this orbit is divisible by $p^r$. Prove this stabilizer subgroup is not all of G and deduce by induction that it contains a subgroup of order $p^r$. (This proof is said to be due to H. Wielandt.)
(iii) Use a different action to reprove Sylow 2) as follows: let P, Q be Sylow p-subgroups, and let $\mathcal{S}$ be the set of all left cosets of Q. Let P act on $\mathcal{S}$ by left translation and prove there is a fixed point, i.e. a coset xQ such that $(Px)Q = P(xQ) = xQ$. Deduce that $Px = xQ$, and then prove that P and Q are conjugate.

**Applying Sylow to finding normal subgroups:**

One way to show a group is not simple is to find a non constant homomorphism to a smaller group. Then the kernel is a non trivial normal subgroup. We know that an action of G on a set S of n elements is equivalent to a homomorphism of G into $S_n$ = Bij({1,2,...,n}), where $\#S_n = n! = n(n-1)(n-2)(\ \ )(2)(1)$. Thus if we can find a transitive action of G on a set of $n \geq 2$ elements where $\#(G) > n!$, then the homomorphism $G \to S_n$ is non trivial but not injective, hence G is not a simple group.

We know for example that if H is any subgroup of G, then G acts transitively by translation on the cosets of H, and also acts transitively by conjugation on the conjugacy class of H. Moreover we know the number of cosets of H is the index of H in G = $\#(G)/\#(H)$. So for example if G is a group of order $28 = (2^2)(7)$, then G has a Sylow subgroup H of order 7, and index 4. Then G acts by translation, transitively, on the set of cosets of H, yielding a non constant homomorphism $G \to S_4$. Since $\#(G) = 28 > 24 = \#(S_4)$, the map is not injective, and the kernel is a non trivial normal subgroup in G.

This argument proves a stronger version of our result that the tetrahedral group Tet is not simple, i.e. no group G of order 12 is simple. For if H is a Sylow 2-subgroup of G, then index(H) = 3, and we get a non constant homomorphism from G to $S_3$. Since $\#(S_3) = 6 < 12 = \#(G)$, the kernel is a non trivial normal subgroup of G.

**Exercise #25)** (i) Prove if G acts transitively on a set S with $\#(S) = n$, and $\#(G)$ does not divide n!, then G is not simple.
(ii) Prove a group of order pq, where p, q are distinct primes is never simple.
(iii) More generally a group of order $p^r n$ where $p > n > 1$, is not simple if p is prime.
(iv) Prove a group of order $p^r$, where $r > 1$, p prime, is not simple

Look now at action by conjugation on Sylow subgroups. This is harder because we do not know in general how many p-Sylow subgroups there are. We know the number is congruent to 1 modulo p, and divides the index of one of them. Consider a group G of order $72 = 9(8) = (3^2)(2^3)$ The Sylow 2-subgroups have index 9, and the Sylow 3-subgroups have index 8, but 72 divides 9!, and 8!,

so we might not get a non trivial kernel from our homomorphisms to $S_8$ or $S_9$. But if we look at the action of G by conjugation on the set of Sylow 3 subgroups, we see the number of such subgroups is of form 1,4,7,10,....., and divides 8. So it can only be 1 or 4.

If there is only one, it is normal and we are done. If there are 4, we get a non constant homomorphism to $S_4$, and since 72 does not divide 4! = 24, again we get a non trivial normal subgroup. The argument does not work as well with the Sylow 2-subgroups since the number of them is an odd factor of 9, hence either 1,3,or 9. But if there are 9, then the homomorphism to $S_9$ could be injective, hence the kernel might be only {e}, a trivial normal subgroup.

**Summary:** **(i)** To show a group G is not simple, look for a homomorphism to some $S_n$ with n small relative to #(G), and to do that look for a subgroup $H \subset G$ of small index, or with a small number of conjugates; i.e. look for either a large subgroup of G or a subgroup of G whose normalizer is large.
(ii) Although computing the index of H is easier, remember that index(N(H)) divides index(H), and a smaller index subgroup is better

**Examples:** What if #(G) = 100? Then $100 = 4(25) = 2^2(5^2)$, and we have Sylow 2 and 5-subgroups to work with. This is easy since the 5-subgroups have index 4, and we get a non trivial normal subgroup from the action on cosets. Note also there are either 1,6,11,16,....of them and the only one of these numbers that divides 4 is 1. So the Sylow 5-subgroup is itself normal.

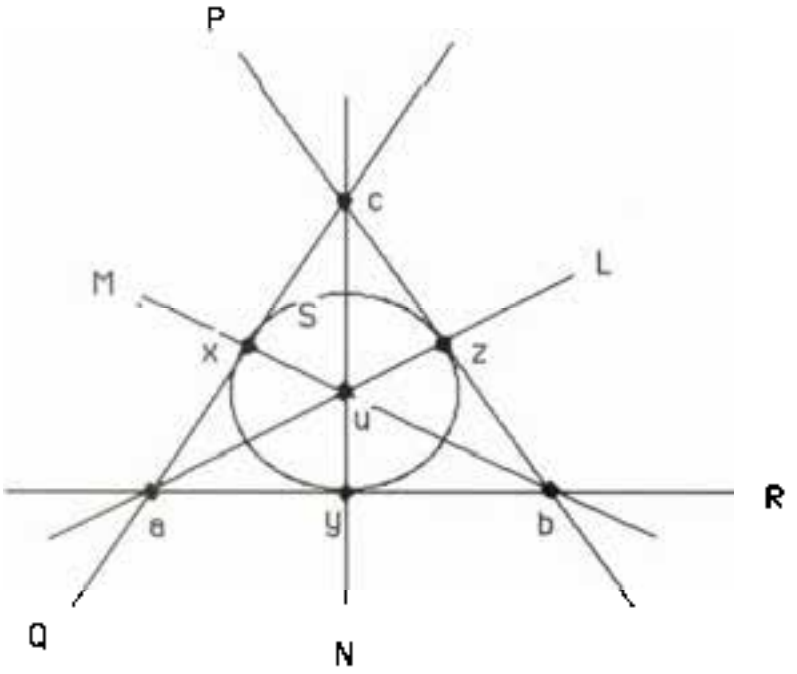
If #(G) = 30, then 30 = 2(3)(5), so the Sylow subgroups have indices 15, 10, and 6. But 30 divides 6!, 10!, and 15!, so we don't get anywhere acting by translation on cosets. What about conjugacy classes? The number of Sylow 2- subgroups could be any odd factor of 15, the number of Sylow 3-subgroups could be either 1 or 10, and the number of Sylow 5-subgroups could be 1 or 6. Since 30 divides 15!, 10!, and 6!, we still seem to have a problem.

But look at the Sylow 3 and 5 subgroups. If neither is normal, there are 10 Sylow 3-subgroups and 6 Sylow 5-subgroups, so there are 20 elements of order 3, and 24 elements of order 5 (Why?). This cannot happen in a group with only 30 elements. So G is not simple.

**Exercise #26) (i)** If G is simple and #(G) < 60, then #(G) is prime
(ii) Prove the same result for 60 < #(G) < 168.

**The simple group of order 168:** Let's look at this interesting group in its incarnation as the "collineation group" of the 7-point projective plane. Recall that in a projective plane no two distinct lines are parallel. Thus not only do any two distinct points determine a line but also any two distinct lines determine a point, hence a projective plane enjoys a more perfect duality then do Euclidean planes.

The simplest example is the finite plane $\Pi$ containing seven points. Each line has three points, and the seven lines are shown, where one looks like a circle. Since we drew the picture in the Euclidean plane, there are three apparent intersections which do not correspond to points in $\Pi$. These are not darkened, and not lettered, in the picture below. There is also a lack of symmetry in our picture since it can be drawn with any one of the lines in $\Pi$ as the one labelled S, looking like the circle.




A "collineation" of $\Pi$ is a permutation of the points of $\Pi$ which takes lines to lines Then the induced map on lines is also a permutation, so the inverse of a collineation is a collineation, and the collineations form a group. Let G denote the group of collineations of $\Pi$. Then by definition G acts on the set of points of $\Pi$. We claim the action is transitive.

Looking at the picture reveals that the two Euclidean rotations of our picture of $120^0$ and $240^0$ about u are collineations, permuting the points a,b,c transitively. Moreover, "reflections" in the lines L, M, N permute the points x,y,z transitively. Note that each of these reflections interchange two pairs of lines and leave three lines invariant. They also interchange two pairs of points and leave three points fixed. For example, the Euclidean reflection of our picture in L exchanges x with y, and b with c, and fixes a, u, and z. (A projective reflection in a line is not fully determined by the line; indeed there are three non trivial collineations leaving the points of a given line fixed, but only one looks like a Euclidean reflection in our picture.)

One "reflection" in the line R exchanges the points u and x, and the points z and c, fixing a, y, and b. These collineations show that all seven points are in the same G - orbit. Thus we can count the number of elements of G by computing the stabilizer group of one point, such as u. Now if u is fixed, the lines through u must be permuted, and we can divide the elements of $G_u$ into three sets according to how they act on these lines. If we consider the elements mapping L to L, these are again divided in half according to how they act on the other two points of L, namely a and z. Those collineations that fix a and z, besides the identity, are the three projective reflections in L, exchanging x with y and b with c, or x with c and b with y, or x with b and c with y.

If these four collineations fixing L pointwise are composed with the reflection in M which exchanges z with a, and c with y, we have four more collineations fixing u and interchanging a with z. Composing these eight collineations fixing u and leaving L invariant, with the two (Euclidean) rotations about u, leaving the triangle abc invariant, gives 16 more elements of $G_u$ which carry L to M or to N. Thus the stabilizer group $G_u$ contains 24 elements and hence G contains $7 \times 24 = 168 = 2^3 \cdot 3 \cdot 7$ elements.

Now recall the proof that the icosahedral group was simple. We were able to compute all the elements of each order in the group simply by enumerating the stabilizer subgroups of the vertices, edges, and faces of the icosahedron. We were helped by the fact that each stabilizer group had prime order, all were disjoint, and every element of the group belonged to at least one stabilizer group, i.e. each element fixed either a vertex, an edge, or a face. The orders being prime allowed us to argue that if a normal subgroup contained

one element of an stabilizer subgroup, it contained the whole subgroup. Then the conjugacy of the stabilizer subgroups of the vertices, for instance, implied that if a normal subgroup contained an element fixing a vertex, it contained all elements fixing any vertex.

Things are not as easy for the present group G = Collin($\Pi$). For example, the stabilizer group of a point of $\Pi$ has order 24, so although we know there are seven such subgroups, all conjugate, they are not of prime order and in fact they intersect non trivially as one can observe, so we do not even know yet how many elements they represent Also if a normal subgroup N of G contains an element of one of these groups it does not follow that it must contain the whole subgroup. Since there are seven lines, also acted on transitively, the stabilizer subgroup of a line also has order 24.

Since points and lines are somehow analogous to vertices and edges, we might use triangles as an analog of faces. A triangle is determined by choosing any two distinct lines, then any third line except the one passing through the point common to the first two lines. Thus the three lines can be chosen in $7\times6\times4 = 6\times28$ ways, and since they can be ordered in $3! = 6$ ways, there are 28 triangles in $\Pi$. Since G acts transitively on these, the stabilizer subgroup of a triangle has 6 elements Observe that of the stabilizer subgroups for points, lines and triangles, none has order divisible by 7, so we are not yet getting at the elements of order 7 in our group G this way.

We can analyze the elements of order three however, by using the subgroups leaving triangles invariant. The stabilizer subgroup of a triangle contains 6 elements, two of order 3, three of order 2, and the identity. We claim all elements of G of order three belong to such subgroups. I.e. an element of G of order three generates a subgroup of order three which acts on the 28 triangles of $\Pi$, dividing them into disjoint orbits each of order 1 or 3. Since 3 does not divide 28, there must be at least one orbit consisting of one triangle, i.e. an element of order three belongs to the stabilizer group of some triangle.

Since the stabilizer subgroups of all triangles are conjugate, we can study the subgroup for any one triangle, such as $\Delta abc$. We claim a rotation $\rho$ about u in the stabilizer group of $\Delta abc$ does not leave invariant any other triangle. An invariant triangle would consist of an orbit of three lines under the action of $\rho$, or three

orbits of fixed lines. Looking at the picture we see that the orbits of ρ are the three lines in Δabc, the three lines through u, and the line S. Thus the only possibility is the three lines through u, which do not form a triangle. Since an element of order three thus leaves one and only one triangle invariant, there are exactly two such elements for each triangle, so G contains exactly 56 elements of order 3.

We can also study elements of order two, since such an element must leave invariant some line, and by acting on this line must fix at least one point. Hence the element permutes the other two points. Thus we get all such elements by looking at the action of G on unordered pairs of points. There are 21 such pairs and hence the subgroup permuting two given points has order 8. We saw above what this group was for the pair {a,z}, since it coincides with the subgroup fixing u and leaving L invariant.

By continuing this geometric analysis, one should be able to show that there are exactly 21 elements in G of order 2, all conjugate, and 42 elements of order 4, all conjugate, but it is still not clear where the elements of order 7 are. For now we will postpone this project until we have the tools of linear algebra available, but you may wish to experiment a bit further.

Representing G as a group of matrices, we will show later, using matrix algebra, that in addition to the elements mentioned above, there are exactly eight conjugate subgroups of order 7. With the identity, this gives the whole group. Assuming these facts, any normal subgroup N of G would have order n, where n divides 168, and n is a sum of the integers 1, 56, 21, 42, 48. Consequently #(N) = 1 or 168, which would prove that G is simple

**Challenge**: (i) Prove G has 21 elements of order 2, all conjugate.
(ii) Prove G has 42 elements of order 4, all conjugate.
(iii) Find an element of order 7 in G.
(iv) Find all elements of order 7 in G.

**Applying Sylow to classifying groups of small order**

As we have seen, the Sylow theorems give information on the subgroups of a group, in terms of the order of the group. Is it possible that this information is so complete that given the order of a group, we can list all possible structures for that group? That seems like a formidable problem to solve in any reasonably efficient

way (although one might write a computer program to list all possible group multiplication tables with n symbols), but some modest yet pretty results are possible. Of course a group of prime order p is cyclic, isomorphic to $\mathbb{Z}_p$.

More generally, presumably the fewer the prime factors in the order, the fewer groups of that order. It turns out that for a group whose order is a product of two prime factors there are three possibilities: either a cyclic group, a (direct) product of two cyclic groups, or a "semi direct" product of two cyclic groups (a generalization of a dihedral group). The point is that the two prime factors of #(G) give two interesting subgroups H, K, and then one must consider whether H, K commute with each other in G, or not. That exhausts all orders up to 15, except for 8 and 12.

When #(G) = 12 there are again two interesting subgroups from which G is constructed, but more possibilities for them and for how they interact. In all but one of these cases the group G is constructed from the subgroups H, K by either the (direct) product construction or the "semi direct product" construction, which builds in the conjugation action of one of the subgroups on the other.

For #(G) = 8, there still remains one possibility, the unit group of the integral "quaternions", a special case of a construction discovered by Hamilton and Gauss, generalizing the complex numbers, and even this group can be realized as a quotient of a semi direct product.

The point is that to recover the structure of a group from that of its subgroups you need to know how the subgroups fit together to make up the group. For example the groups $S_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ both contain subgroups isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_3$, which in both cases generate the whole group and have trivial intersection. But the groups they generate are different because in $\mathbb{Z}_2 \times \mathbb{Z}_3$ the subgroups are both normal (they commute with each other) while in $S_3$ they are not. I.e. knowing the subgroups H, K of G only reveals the multiplication law for elements of H and K; we also need to know how to multiply products of such elements. I.e. even if the products in HK exhaust the group G, trying to rewrite an element of form (hk)(h'k') as one of form h''k'' requires knowing to what extent elements of H commute with elements of K.

In particular we need to know when $hkh^{-1} = k$, i.e. we need to know the action of H (or G) on K by conjugation. As mentioned

above, with enough of this information, we can sometimes reconstruct G from the subgroups H, K by the "semi direct product", which generalizes the construction of dihedral and product groups.

Note that the classification of groups has two parts, uniqueness and existence. I.e. the Sylow theorems start only with the order of a potential group and give restrictions on the possible subgroups, but to produce actual groups satisfying those restrictions we must construct them. This is where the product and semi direct product constructions come in. We will also simply pull a couple of groups out of the air We start with a couple of easy results on how to define homomorphisms of product groups.

**Exercise #27) (i)** If G, H, K are groups, and $\alpha: G \to H$, and $\beta: G \to K$ are homomorphisms, then the map $G \to H \times K$ defined by sending g to $(\alpha(g), \beta(g))$ in $H \times K$ is a homomorphism.
**(ii)** If $\alpha: G \to K$, and $\beta: H \to K$ are group homomorphisms where the elements of $\alpha(G)$ commute with the elements of $\beta(H)$ in K, for example if K is abelian, then there is a unique homomorphism $G \times H \to K$, defined by sending (g,h) to $\alpha(g) \cdot \beta(h)$ in K.
**(iii)** If G is a finite group with normal subgroups H, K such that $\#(H)\#(K) = \#(G)$ and $H \cap K = \{e\}$, then the natural maps $G \to G/H$, $G \to G/K$ induce an isomorphism $G \to (G/H) \times (G/K)$.
**(iv)** With the same hypotheses as in (iii) prove the elements of H and K commute with each other and that the injections $H \subset G$, $K \subset G$ induce an isomorphism $H \times K \to G$.

**Groups of order p and $p^2$**

In case you missed this exercise, we classify groups of orders p, $p^2$.
**Proposition: (i)** If $\#(G) = p$ is prime, then $G \cong \mathbf{Z}_p$.
**(ii)** If $\#(G) = p^2$ where p is prime, then $G \cong \mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \times \mathbf{Z}_p$.
**proof (i):** If $x \neq e$ is a non trivial element of G, x generates a cyclic subgroup $\langle x \rangle$ whose order is $> 1$ and divides p, hence $\langle x \rangle = G$ **QED (i).**
**proof (ii):** If $\#(G) = p^2$ where p is prime, we know G is abelian, and all non trivial elements have order p or $p^2$ by LaGrange. If any element x has order $p^2$ then $G \cong \mathbf{Z}_{p^2}$. If not, and x has order p, the subgroup $\langle x \rangle \subset G$ is isomorphic to $\mathbf{Z}_p$, and any element y not in $\langle x \rangle$ gnerates a subgroup $\langle y \rangle \subset G$ also isomorphic to $\mathbf{Z}_p$. By LaGrange, $\langle x \rangle \cap \langle y \rangle = \{e\}$. By ex. 28(i) the maps $\alpha: G \to G/\langle x \rangle$ and $\beta: G \to G/\langle y \rangle$ give a homomorphism $f: G \to (G/\langle x \rangle) \times (G/\langle y \rangle) \cong \mathbf{Z}_p \times \mathbf{Z}_p$, with kernel $\langle x \rangle \cap \langle y \rangle =$

(e), hence an isomorphism. **QED (ii) and the proposition.**

**Groups of order 2p.**

We know all groups of orders 1, 2, 3, 4 and 5, by the previous proposition, namely (e), $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_4$, $\mathbf{Z}_2\times\mathbf{Z}_2$, and $\mathbf{Z}_5$. Note these are all abelian. Now we ask for all groups of order 6. We know of only two, $\mathbf{Z}_6$ and $S_3$, which differ since $\mathbf{Z}_6$ is abelian but $S_3$ is not.

**Proposition:** There are exactly two groups of order 6. $\mathbf{Z}_6$ and $S_3$.
**Proof:** Let G be any group of order 6, hence by Sylow's theorems there exist elements x, $\alpha$ of orders 2 and 3 respectively. Thus $\langle\alpha\rangle$ is a normal subgroup of order 3 and $G = \langle\alpha\rangle \cup \langle\alpha\rangle x$ consists of the elements $(e, \alpha, \alpha^2, x, \alpha x, \alpha^2 x) = \{\alpha^s x^t : 0 \le s \le 2;\ 0 \le t \le 1\}$.

To determine G completely we need to know how to multiply any two of these elements. For example we need to know what is $x\alpha$, or what is $(\alpha^2 x)(\alpha x)$? Notice that the answer to the first question would also answer the second since $(\alpha^2 x)(\alpha x) = \alpha^2(x\alpha)x$. I.e. if we could rewrite $x\alpha$ as a product in the other order $\alpha^s x^t$, then we could write $(\alpha^2 x)(\alpha x) = \alpha^2(\alpha^s x^t)x = \alpha^{2+s}x^{1+t}$, which is a known element of G. If x commutes with y then it follows that G is commutative and we have $(\alpha^s x^t)(\alpha^u x^v) = \alpha^{s+u}x^{t+v}$.

Thus letting $\alpha^s x^t$ correspond to (s,t) gives an isomorphism of G with $\mathbf{Z}_3\times\mathbf{Z}_2$. More abstractly, since $\alpha$ and x commute, the homomorphisms $\varphi:\mathbf{Z}_3\to G$ and $\psi:\mathbf{Z}_2\to G$ with $\varphi(1) = \alpha$ and $\psi(1) = x$, define by Ex. 27 (ii) above, a homorphism $(\varphi\times\psi):\mathbf{Z}_3\times\mathbf{Z}_2\to G$ sending (s,t) to $\alpha^s x^t$, hence surjective, hence an isomorphism.

Now assume $\alpha$ and x do not commute in G. We still only need to know how to rewrite $x\alpha$ as a product of form $\alpha^s x^t$, to determine all multiplications in G, since to turn $(\alpha^s x)(\alpha^u x^v) = \alpha^s(x\alpha^u)x^v$ into a product of form $\alpha^a x^b$, we just need to move each of the left-most x past the $\alpha^u$ on its right. E.g. if $x\alpha = \alpha^k x$, then $(\alpha^s x)(\alpha x^v) = \alpha^s(x\alpha)x^v = \alpha^s(\alpha^k x)x^v = \alpha^{s+k}x^{1+v}$. The product $(\alpha^s x)(\alpha^2 x^v)$ just takes two steps, i.e. $(\alpha^s x)(\alpha^2 x^v) = \alpha^s(x\alpha)\alpha x^v = \alpha^s(\alpha^k x)\alpha x^v = \alpha^{s+k}(x\alpha)x^v = \alpha^{s+k}(\alpha^k x)x^v = \alpha^{s+2k}x^{v+1}$. If $x\alpha = \alpha^k$, it is even easier.

So which element of $(e, \alpha, \alpha^2, x, \alpha x, \alpha^2 x)$ equals $x\alpha$? By hypothesis $x\alpha \ne \alpha x$. Also $x\alpha \ne x$, and $x\alpha \ne \alpha$, since neither x nor $\alpha$ is the identity. If $x\alpha = \alpha^2$, then right multiplying by $\alpha^2$ gives $x = \alpha$,

a contradiction Hence only one possibility remains, that $x\alpha = \alpha^2 x$. Thus there is only one possibility for a non abelian group structure on G, and hence it must the one corresponding to $S_3$. QED.

If we examine this argument we can simplify it a great deal. I.e. we can take more advantage of the fact that $\langle\alpha\rangle$ is a normal subgroup of G. Since $\langle\alpha\rangle$ is normal, we know $x\langle\alpha\rangle = \langle\alpha\rangle x$, so $x\alpha = \alpha^k x$ for some $k > 0$. Hence if G is not abelian then $k = 2$, and we have exactly two groups of order 6.

By taking even more advantage of normality, we can prove a much stronger result. Note that $x\alpha = \alpha^k x$ if and only if $x\alpha x^{-1} = \alpha^k$, so to determine the multiplication completely we only need to know the conjugation action by x on the normal subgroup $\langle\alpha\rangle$. Since conjugation defines a homomorphism $\mathbf{Z}_2 \cong \langle x\rangle \to \mathrm{Aut}(\langle\alpha\rangle) \cong \mathrm{Aut}(\mathbf{Z}_3) \cong \mathbf{Z}_2$, the group structure is completely determined by the conjugation homorphism $\mathbf{Z}_2 \to \mathbf{Z}_2$.

Since there are only two such homomorphisms, (the trivial one and the identity), there are only two possible group structures. Here the trivial homomorphism corresponds to the trivial conjugation action, i.e. $x\alpha x^{-1} = \alpha$, or $x\alpha = \alpha x$, so gives the abelian group $\mathbf{Z}_3 \times \mathbf{Z}_2 \cong \mathbf{Z}_6$. The non trivial homomorphism corresponds to the non trivial conjugation action $x\alpha x^{-1} = \alpha^2$, and gives the non abelian group $S_3$.

**Proposition**: There are exactly two groups of order 2p, with $p > 2$ and prime. the cyclic group $\mathbf{Z}_{2p}$ and the dihedral group $D_p$.
**Proof**: By Sylow, if G has order 2p, there are elements $\alpha$, x of orders p and 2 respectively, $\langle\alpha\rangle \cong \mathbf{Z}_p$ is a normal subgroup, and $G = \langle\alpha\rangle \cup \langle\alpha\rangle x = \{\alpha^s x^t : 0 \le s \le p-1, 0 \le t \le 1\}$. Now we need:

**Lemma**: The multiplication in G is completely determined by the conjugation action of x on $\langle\alpha\rangle$, i.e. by the conjugation homomorphism $\mathbf{Z}_2 \cong \langle x\rangle \to \mathrm{Aut}(\langle\alpha\rangle) \cong \mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p^*$(Ex. 12 (v)).
**Proof**: If this homomorphism tells us that $x\alpha^s x^{-1} = \alpha^t$, then $x\alpha^s = \alpha^t x$, and we can multiply as follows: $(\alpha^u x)(\alpha^s x) = \alpha^u(x\alpha^s)x = \alpha^u(\alpha^t x)x = \alpha^{u+t}x^2 = \alpha^{u+t}$ Since we know such a formula for every s, all multiplications are determined. **QED Lemma**.

**Corollary**: There are at most two group structures on G.

**proof**: The number of group structures is at most the number of homomorphisms $\mathbf{Z}_2 \to \mathbf{Z}_p^*$, which equals the number of elements of order two in $\mathbf{Z}_p^*$. We claim 1, and -1 (= p-1), are the only elements of order 2 in $\mathbf{Z}_p^*$. I.e. for an integer X, $X^2 = 1$ in $\mathbf{Z}_p^*$ if and only if p divides $X^2-1 = (X-1)(X+1)$, if and only if p divides either X-1 or X+1, if and only if X is equivalent modulo p to either 1 or -1 in $\mathbf{Z}_p^*$. **QED.**

Since $\mathbf{Z}_{2p}$ and $D_p$ are different groups of order 2p, we are done. **QED Prop.**

**Groups of order pq**

Can we extend these results to groups of order 3p, with $p > 3$ and prime? We can again find elements $\alpha$, x of orders p and 3 respectively, and consider the conjugation homomorphism $\mathbf{Z}_3 \cong \langle x \rangle \to \mathrm{Aut}(\langle \alpha \rangle) \cong \mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p^*$. Again we see that the number of group structures on G is at most the number of such homomorphisms. But this time, if p = 17 say, then there is no non trivial homomorphism from $\mathbf{Z}_3$ to a group of order 16 by LaGrange's theorem hence the elements $\alpha$ and x commute and (by Ex. 27(iv)) there is only the commutative group structure on G isomorphic to $\mathbf{Z}_3 \times \mathbf{Z}_{17} \cong \mathbf{Z}_{51}$.

So there is a key difference according to whether or not 3 divides p-1. But what if 3 does divide p-1, say p = 13? Then our argument shows the number of group structures on our group G of order $3 \cdot 13 = 39$, is at most equal to the number of homomorphisms $\mathbf{Z}_3 \to \mathbf{Z}_{13}^*$ This equals the number of elements of order 3 in $\mathbf{Z}_{13}^*$, and we can again argue that there are three of these, namely {1, 3, 9}, but this time it turns out that the two non trivial homomorphisms give isomorphic groups!

First we prove the easy result, then the more interesting one.
**Proposition**: If $p > q$ are primes, and q does not divide p-1, then there is only one group of order pq, the cyclic group $\mathbf{Z}_p \times \mathbf{Z}_q \cong \mathbf{Z}_{pq}$.
**Proof**: We can argue as above that if $\alpha$, x are elements of orders p, q respectively, then the group structure is determined by the conjugation homomorphism $\mathbf{Z}_q \cong \langle x \rangle \to \mathrm{Aut}(\langle \alpha \rangle) \cong \mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p^*$, and since q does not divide $p-1 = \#(\mathbf{Z}_p^*)$ there is only the trivial homomorphism by LaGrange. Hence conjugation is trivial, the group

is commutative and by Ex. 27(iv), the map $\mathbf{Z}_p \times \mathbf{Z}_q \to G$ taking (s,t) to $\alpha^s x^t$ is an isomorphism.

We could also argue using Sylow that the number of Sylow q subgroups is congruent to 1 modulo q and divides p. But if $1 + qk$ divides p, then $1 + qk$ equals either 1 or p. If $1 + qk = p$ then $qk = p-1$, and q divides p-1, a contradiction. So there is only one Sylow q subgroup which is therefore normal. Again by Ex. 27(iv) the induced map $\mathbf{Z}_p \times \mathbf{Z}_q \to G$ is an isomorphism. QED.

So far we have classified all groups of orders up to 15, except for orders 8 and 12. I.e. for each prime order 2, 3, 5, 7, 11, 13, and also for order $15 = 3 \cdot 5$, there is only the cyclic group, and for the five orders 4, 6, 9, 10, 14 there are only the ten groups $\mathbf{Z}_4$, $\mathbf{Z}_2 \times \mathbf{Z}_2$, $\mathbf{Z}_6$, $D_3 \cong S_3$, $\mathbf{Z}_9$, $\mathbf{Z}_3 \times \mathbf{Z}_3$, $\mathbf{Z}_{10}$, $D_5$, $\mathbf{Z}_{14}$, and $D_7$. To classify groups of orders 8 and 12, and non abelian groups of order pq where q divides p-1 we need a new construction: semi direct products.

**Semi direct products of groups**

In the previous cases our groups G were compounded in some way from two subgroups K and H, one of which was normal, by knowing the multiplication in each group separately, plus the conjugation action of the non normal group on the normal one. The whole group is a twisted product of the two subgroups in a way we want to make precise next. (I learned this topic from Hungerford, Algebra.)

Let H, K be groups such that H "acts" on K, i.e. let there be given a homomorphism $\alpha: H \to \mathrm{Aut}(K)$. Since K is more than a set, it is natural that elements of H should act via group automorphisms rather than just bijections. I.e. our action of H on K is not just a homomorphism $H \to \mathrm{Bij}(K)$, but a homomorphism with image in the subgroup $\mathrm{Aut}(K) \subset \mathrm{Bij}(K)$. This is natural too since we want the action to turn out to be conjugation in some bigger group.

To construct the bigger group we take the Cartesian product set $K \times H$ and we use $\alpha$ to define a multiplication different from that of the usual product group. For h in H, k in K, we denote $\alpha(h)(k)$ by $\alpha_h(k)$ or simply by $h(k)$, and then set $(k,h)\cdot(k_1,h_1) = (k \cdot h(k_1), h \cdot h_1)$; i.e. we just give $k_1$ a little twist by h before multiplying it by k. If the action $\alpha: H \to \mathrm{Aut}(K)$ is trivial, i.e. if $\alpha(h) = \mathrm{id}$ for all h, this is just the multiplication in the ordinary product group.

In general we call the new group the "semi direct product" of K and H, via $\alpha$, denoted $K\times_\alpha H$. (Of course for all we know at the moment $K\times_\alpha H$ might be isomorphic to $H\times K$ by some cleverly chosen isomorphism, even when $\alpha$ is non trivial. But see the next exercise.)

**Exercise #28)** With definitions as above, prove:
(i) The semi direct product $K\times_\alpha H$ is a group.
(ii) The subsets $\tilde{K}$ = {(k,e) for all k in K}, and $\tilde{H}$ = {(e,h) for all h in H} are subgroups of G isomorphic to K, H respectively, and $\tilde{K}$ is normal.
(iii) The action of H on K via $\alpha$ becomes the conjugation action of $\tilde{H}$ on $\tilde{K}$, i.e if $\tilde{k}$ = (k,e), $\tilde{h}$ = (e,h), then $\tilde{h}\tilde{k}\tilde{h}^{-1} = (\alpha(h)(k))\tilde{} = (h(k),e)$.
(iv) $\tilde{H}$ is normal in $K\times_\alpha H$ if and only if $\alpha$ is the trivial homomorphism.
(v) If H, K are subgroups of a group G, K is normal, and we define $\alpha: H\to \mathrm{Aut}(K)$ to be conjugation of K by H, then letting f(k,h) = kh, defines a homomorphism $f: K\times_\alpha H\to G$, which is surjective if G = KH, and injective if $K\cap H = \{e\}$.

**Remark**: (i) If $\alpha: \mathbf{Z}_2\to \mathrm{Aut}(\mathbf{Z}_p)\cong \mathbf{Z}_p^*$ is the unique non trivial homomorphism, then $\mathbf{Z}_p\times_\alpha \mathbf{Z}_2 \cong D_p$, the dihedral group, by Ex.28(v). Since the unique non trivial automorphism of order two of $\mathbf{Z}_p$ takes each element to its inverse, $\alpha$ corresponds to the formulas found in Ex.5(iii) for $D_3$, where $\alpha(R)(\rho) = R\rho R^{-1} = \rho^2 = \rho^{-1}$.
(ii) By Ex.28(ii), semi direct products with H, K both non trivial never yield simple groups.
(iii) As we will see, one can obtain all groups of order $\leq 15$ from semidirect products and their quotients.

Next we show that different homomorphisms $\alpha$ can define isomorphic semi direct product groups.
**Proposition**: Let H, K be groups, $\alpha: H\to \mathrm{Aut}(K)$ a homomorphism, $g: H\to H$ an automorphism of H, and define $\tilde{\alpha}: H\to \mathrm{Aut}(K)$ by $\tilde{\alpha} = \alpha g^{-1}$. Then the map $\varphi: K\times_\alpha H\to K\times_{\tilde{\alpha}} H$ defined by $\varphi(k,h) = (k,g(h))$, is an isomorphism.
**Proof**: $\varphi$ is a bijective function, with inverse $\varphi^{-1}(k,h) = (k,g^{-1}(h))$, so we check the homomorphism property. If (k,h), $(k_1,h_1)$ are in $K\times_\alpha H$, their product is $(k,h)\cdot(k_1,h_1) = (k\cdot\alpha(h)(k_1),hh_1)$, whose image is $\varphi(k\cdot\alpha(h)(k_1), hh_1) = (k\cdot\alpha(h)(k_1), g(hh_1))$.
On the other hand the two images of (k,h) and $(k_1,h_1)$ are $\varphi(k,h) =$

$(k,g(h))$ and $\varphi(k_1,h_1) = (k_1, g(h_1))$, hence the product of the images is $(k,g(h))\cdot(k_1, g(h_1)) = (k\tilde{\alpha}(g(h))(k_1), g(h)g(h_1))$. Since $\tilde{\alpha}g = \alpha$, and $g$ is a homomorphism, thus indeed $\varphi((k,h)\cdot(k_1,h_1)) = (k\cdot\alpha(h)(k_1), g(hh_1)) = (k\tilde{\alpha}(g(h))(k_1), g(h)g(h_1)) = \varphi(k,h)\cdot\varphi(k_1,h_1)$. **QED**.

We need an elementary fact to be proved later. We define the product $ab$ of two elements $a$, $b$ in $\mathbf{Z}_p$ by taking the remainder after division by $p$, of their usual integer product.

**Fact**: There are at most $q$ solutions in $\mathbf{Z}_p$ of the equation $X^q-1 = 0$.

**Sketch**: If we have a solution $c$ of $X^q-1 = 0$ in $\mathbf{Z}_p$, then we can divide $X^q-1$ by $X-c$ to get $X^q-1 = (X-c)f(X)$, where $f$ is a polynomial of degree $q-1$ with coefficients in $\mathbf{Z}_p$. If there are $q$ solutions $c_1,\ldots,c_q$ then we eventually get $X^q-1 = (X-c_1)(X-c_2)\ldots(X-c_q)$. If $c$ is any other solution we must have $0 = c^q-1 = (c-c_1)(c-c_2)\ldots(c-c_q)$ in $\mathbf{Z}_p$. Since $p$ divides the right hand product it divides one of the factors, but if $p$ divides the factor $(c-c_j)$ then $c = c_j$ in $\mathbf{Z}_p^*$, and thus $c$ is one of the $q$ solutions $c_1,\ldots,c_q$. **QED**.

**Corollary**: If $q$ divides $p-1$, and $q$, $p$ are prime, there are exactly $q-1$ non trivial homomorphisms $\alpha:\mathbf{Z}_q \to \mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p^*$.

**Proof**: A non trivial homomorphism $\alpha$ corresponds to a choice of the element $\alpha(1)$ of order $q$ in $\mathbf{Z}_p^*$, thus to a solution (other than $X = 1$) of the equation $X^q-1 = 0$ in $\mathbf{Z}_p^*$. By the fact above there are at most $q-1$ such solutions other than the obvious solution $X = 1$. But by Sylow, since $q$ divides $p-1 = *(\mathbf{Z}_p^*)$, there is a subgroup of order $q$ in $\mathbf{Z}_p^*$, and any non trivial element of that subgroup has order $q$. Hence there are exactly $q-1$ elements of order $q$ in $\mathbf{Z}_p^*$. **QED**.

**Corollary**: If $p$, $q$ are prime and $q$ divides $p-1$, all non abelian groups of order $pq$ are isomorphic.

**Proof**: If $*(G) = pq$, let $\beta$, $x$ be elements of $G$ of orders $p$ and $q$ respectively. Then the subgroup $\langle\beta\rangle$ of order $p$ is normal, $\langle\beta\rangle\cap\langle x\rangle = \{e\}$, and thus $G$ is the union of the $q$ cosets $\langle\beta\rangle x^t$ of $\langle\beta\rangle$ by powers of $x$. Thus $G$ = the product $\langle\beta\rangle\langle x\rangle$. Then if $\alpha:\langle x\rangle \to \mathrm{Aut}(\langle\beta\rangle)$ is the conjugation homomorphism, by Ex.28(v), since $\langle\beta\rangle \cong \mathbf{Z}_p$, and $\langle x\rangle \cong \mathbf{Z}_q$, we get a surjective homomorphism $\mathbf{Z}_p\times_\alpha\mathbf{Z}_q \to G$, which is an

isomorphism since these groups have the same order. Thus every group of order pq is isomorphic to a semi direct product $\mathbf{Z}_p \times_\alpha \mathbf{Z}_q$ for some homomorphism $\alpha: \mathbf{Z}_q \to \mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p^*$.

We know a non abelian group comes from a non trivial homomorphism, and we have just proved there are exactly q-1 non trivial such homomorphisms $\alpha$, each sending 1 to one of the q-1 elements of order q in $\mathbf{Z}_p^*$. Now let $\alpha$ be one of these homomorphisms and $\tilde{\alpha}$ any other. We wish to prove that $\mathbf{Z}_p \times_\alpha \mathbf{Z}_q \cong \mathbf{Z}_p \times_{\tilde{\alpha}} \mathbf{Z}_q$. We know the elements of order q in $\mathbf{Z}_p^*$ are the non trivial elements of the image subgroup $\alpha(\mathbf{Z}_q)$, since that is a subgroup of order q in $\mathbf{Z}_p^*$.

Since by the Fact above, there are only q-1 elements of order q in $\mathbf{Z}_p^*$, in particular the images $\alpha(\mathbf{Z}_q)$ and $\tilde{\alpha}(\mathbf{Z}_q)$ are the same subgroup in $\mathbf{Z}_p^*$. Thus there is some non zero element j in $\mathbf{Z}_q$ such that $\alpha(j) = \tilde{\alpha}(1)$. Also $\mathrm{Aut}(\mathbf{Z}_q^*) \cong \mathbf{Z}_q^*$, so an automorphism g of $\mathbf{Z}_q$ is determined by choosing a non zero element of $\mathbf{Z}_q$ to be g(1). Let g be the automorphism of $\mathbf{Z}_q$ such that g(1) = j. Then $\alpha(g(1)) = \alpha(j) = \tilde{\alpha}(1)$. Since $\alpha g$ and $\tilde{\alpha}$ agree at 1 they agree everywhere on $\mathbf{Z}_q$, so $\alpha = \tilde{\alpha} g^{-1}$. Then by the Proposition above, $\mathbf{Z}_p \times_\alpha \mathbf{Z}_q \cong \mathbf{Z}_p \times_{\tilde{\alpha}} \mathbf{Z}_q$. **QED.**

**Corollary**: If p is prime there is exactly one group of order p; if pq is a product of two primes $p \geq q$, there are one or two groups of order pq, and there are two such groups iff either p = q, or q divides (p-1).

What about groups whose order is a product of three primes? We have dealt with all groups of orders $\leq 15$ except for orders 8 and 12, precisely those groups whose orders have three prime factors.

**Exercise #29)** (i) Prove there are exactly two non isomorphic groups of order 12: $\mathbf{Z}_4 \times \mathbf{Z}_3$ and $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$.
(ii) Prove there are exactly three non isomorphic abelian groups of order 8: $\mathbf{Z}_8$, $\mathbf{Z}_2 \times \mathbf{Z}_4$, and $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

The next theorem finishes classifying groups of order 12.
**Theorem**: There are exactly three non abelian groups of order 12, the dihedral group $D_6$, the tetrahedral rotation group Tet, and the semi direct product $\mathbf{Z}_3 \times_\alpha \mathbf{Z}_4$ where $\alpha: \mathbf{Z}_4 \to \mathrm{Aut}(\mathbf{Z}_3) \cong \mathbf{Z}_2$ is the unique non trivial homomorphism.

**Proof**: By Sylow, a group G of order 12 has a subgroup H of order 4 and a subgroup K of order 3, where $H \cap K = \{e\}$ by LaGrange.

**Lemma**: In a group G of order 12, either a 2-Sylow subgroup H or a 3-Sylow subgroup K is normal.
**proof**: If K is not normal, there are 4 conjugate subgroups of order 3, hence 8 elements of order 3, leaving only four other elements. Since a 2-Sylow contains four elements, none of order three, there is only one 2-Sylow subgroup, which is thus normal. **QED Lemma.**

If both H, K are normal in G, then the map $G \to (G/H) \times (G/K)$ is an isomorphism as in ex. Z9(iv), and since we know both G/H, and G/K are abelian, G would be abelian, contrary to hypothesis. So if G is non abelian, either H or K is normal but not both.
**Assume H is normal**: then there are 4 Sylow 3-subgroups conjugate to K, and G acts transitively by conjugation on them, giving a homomorphism $\alpha: G \to S_4$ whose kernel is the intersection of the normalizers of the conjugates of K. Since the order of the conjugacy class of K equals the index of the normalizer of K, we see each conjugate of K is its own normalizer. Consequently the kernel of $\alpha$ is {e}.

We claim the image of this homomorphism is the group Tet, (thought of as a subgroup of $S_4$ via the action on the four vertices of the tetrahedron). So we must check that G acts on the conjugates of K in the same way that T acts on the vertices of the tetrahedron. First, since each conjugate of K is its own normalizer, it acts trivially only on itself, permuting the other three conjugates.

Thus the map $\alpha$ takes each conjugate of K to the stabilizer subgroup in T of one vertex. Since the eight elements of order three in those stabilizer groups generate T as a subgroup of $S_4$ we are done. In this case one can also show $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$, $K \cong \mathbf{Z}_3$, and $G \cong H \times_\alpha K$, where $\alpha: K \to \mathrm{Aut}(H) \cong S_3$ is any non trivial homomorphism [Ex.30 below].

**Assume $K \cong \mathbf{Z}_3$ is normal**: Then H is isomorphic either to $\mathbf{Z}_4$ or to $\mathbf{Z}_2 \times \mathbf{Z}_2$, and acts non trivially on K by conjugation. If $H \cong \mathbf{Z}_4$, then the conjugation action must be the unique non trivial homomorphism $\alpha: \mathbf{Z}_4 \cong H \to \mathrm{Aut}(K) \cong \mathrm{Aut}(\mathbf{Z}_3) \cong \mathbf{Z}_2$. Thus $G \cong \mathbf{Z}_3 \times_\alpha \mathbf{Z}_4$

If $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then again we need to compute the homomorphism $\alpha: H \to \mathrm{Aut}(K) \cong \mathbb{Z}_2$. Since $\mathrm{Aut}(H) \cong \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$ permutes the non trivial elements of H in all possible ways, any non trivial homomorphism $\alpha$ is equivalent to any other, up to an automorphism of H. Thus there is exactly one group G up to isomorphism in this case, namely $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times_\alpha \mathbb{Z}_3$, where $\alpha: \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ is any non trivial homomorphism.

We claim this last group is $D_6$. Note that since $D_6$ has a cyclic normal subgroup Z of order 6, and since conjugation acts to preserve the elements of order three of Z, those element form a normal subgroup K of order three. Thus one of the last two groups found in the theorem is $D_6$. Since we know too that $D_6$ has 2 elements of order 6, two elements of order 3, one of order 1, and 7 elements of order 2, there are no elements of order 4, and the Sylow 2-subgroup H is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Thus it is the last case above, and $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times_\alpha \mathbb{Z}_3 \cong D_6 \cong \mathbb{Z}_6 \times_\beta \mathbb{Z}_2$ where $\beta: \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$ is the unique non trivial homomorphism. **QED theorem.**

**Exercise #30)** (i) Show there is no nontrivial homomorphism $\alpha: \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4)$.
(ii) If G is non abelian with $\#(G) = 12$, H is a normal subgroup of order 4, and K a subgroup of order 3, prove $G \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times_\alpha \mathbb{Z}_3$, where $\alpha: \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$ is a non trivial homomorphism.
(iii) Prove there are exactly two non trivial homomorphisms $\alpha: \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$, yielding isomorphic semi direct products.
(iv) Prove no two of the three groups in the previous theorem are isomorphic.

You will show next that there are two non abelian groups of order $8 = 2^3$. We know one such non abelian group is $D_4$. If you have read some history of mathematics you may have encountered the other one, the group Q of "unit quaternions", discovered in 1843 by William Rowan Hamilton, the Irish mathematician, astronomer and poet, (although it has been found recorded earlier in Gauss' private notebooks). Hamilton was trying to generalize the familiar complex numbers a+bi to higher dimensions, and eventually realized he must give up commutativity. The rule for multiplying his

quaternions of form a+bi+cj+dk, where a, b, c, d are real numbers, is given by the rules $i^2 = j^2 = k^2 = -1$, ij = k, jk = i, ki = j, and ji = -k, kj = -i, ik = -j, and the fact that real numbers commute with all other quaternions.

[It is said that Hamilton, in celebration, carved these rules on a bridge while out walking.] Considering only quaternions with integral coefficients, those with multiplicative inverses form the group of "unit quaternions" $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. You can check that Q is a group (hint. associativity for products of i, j, k is sufficient) and that the groups $D_4$ and Q are not isomorphic (Hint: count the number of elements of orders 1,2,4 in each).

**Exercise #31)** Prove there are only two non abelian groups of order 8 [Hint: Show if #(G) = 8, there is an element x of order 4, but no element of order 8, and (x) is normal in G. If y is not in (x), then either $y^2 = x^2$ or $y^2 = e$, and $yxy^{-1} = x^3$. Each of the two cases $y^2 = x^2$ and $y^2 = e$, determine a unique group, (Q and $D_4$ respectively).]

**Remark**: We have produced all groups of order ≤ 15 by the semidirect product construction (recalling that ordinary products are a special case) except the quaternion group. Naive attempts to produce Q as a product do not succeed, so we try a modified construction where the factor groups are no longer disjoint in the "product". I.e a semi direct product of $\mathbf{Z}_4$ with $\mathbf{Z}_4$ gives enough elements of order four for Q, but too many elements of order two. One solution is to identify some elements of order two by a quotient as in the next exercise.

**Exercise #32)** (i) Prove that Q is not the semidirect product of any two of its subgroups.
(ii) If #(G) = 8, G non abelian, and x an element of order 4, let y be any element not in ⟨x⟩. If y has order 2 show that G is isomorphic to $\mathbf{Z}_4 \times_\alpha \mathbf{Z}_2 \cong D_4$, where $\alpha: \mathbf{Z}_2 \to \mathrm{Aut}(\mathbf{Z}_4) \cong \mathbf{Z}_2$ is them unique non trivial homomorphism.
(iii) If #(G) = 8, G non abelian, and x an element of order 4, and y be any element of order 4 not in ⟨x⟩, show there is a surjective homomorphism $\mathbf{Z}_4 \times_\alpha \mathbf{Z}_4 \to G$, where $\alpha: \mathbf{Z}_4 \to \mathrm{Aut}(\mathbf{Z}_4) \cong \mathbf{Z}_2$ is the unique non trivial homomorphism. Thus G is a quotient of the semi direct product $\mathbf{Z}_4 \times_\alpha \mathbf{Z}_4$ by an element of order 2.

(iv) If $\alpha: \mathbf{Z}_4 \to \mathrm{Aut}(\mathbf{Z}_4) \cong \mathbf{Z}_2$ is the unique non trivial homomorphism, prove that any point z of order two in $\mathbf{Z}_4 \times_\alpha \mathbf{Z}_4$ is in the center, hence generates a normal subgroup, and that $Q \cong (\mathbf{Z}_4 \times_\alpha \mathbf{Z}_4)/(z)$.

**Challenge**: Try to classify all groups of orders up to 31.

## §9) Symmetric and alternating groups

Abstract properties can be powerful, but it is crucial to be able to make explicit calculations with elements of groups, just as we do with coordinate vectors in Euclidean space. The finite group analogous to $\mathbf{R}^n$, i.e. an explicit finite group in which other finite groups can be embedded, and in which concrete calculations are possible, is the group $S_n$. Since there are two common but different conventions for writing the operation in this group, we first discuss a notational convention that divides algebraists from the rest of the mathematical world, namely the order in which they write compositions. To an algebraist, the composition fg of two functions f and g, means first apply f and then apply g, whereas to everyone else it means apply g first and then apply f. There is no big difference, but it is confusing if you don't know which convention is being used.

We will ordinarily stick to our usual "non algebraist" convention for composition of functions in these notes. Sometimes however I may find it convenient to use the algebraists' convention, the "opposite" convention, when dealing with multiplication of "cycles". I will never do this however without telling you so first. Thus for us the group $S_n$ equals Bij((1,2,3 ,n)) where composing is done in the usual order familiar from calculus, i.e. where fg means first g then f. If we ever wish to use the algebraists convention on composition of permutations, we will not write the group as $S_n$, but we will write it as $S_n^{op}$, the "opposite group" of $S_n$. In general every group has an opposite group, whose elements are the same but where multiplication is done in the opposite order.

[**Digression on the "opposite group"**: The remarks above are all you need, but if you want to know a somewhat tedious way to make this precise, read on Otherwise skip to "End of digression."

If G is any group, there is another group, the "opposite group of

G", denoted $G^{op}$, whose elements are the same as the elements of G but whose multiplication is defined in the opposite order to that of G. Thus if x,y are two elements of G, the product xy in $G^{op}$ is defined to be the product yx in G. Then the group $S_n{}^{op}$ has the same elements as the group $S_n$, namely bijections of the set {1,2,...,n}, but the composition is written as follows: if $\sigma,\tau$ are two permutations in $S_n{}^{op}$ the product $\sigma\tau$ denotes the permutation obtained by applying $\sigma$ first and then $\tau$.

To keep the groups G, $G^{op}$ straight, let's write $x*y$ for multiplication in $G^{op}$, and xy for multiplication in G. Thus $x*y = yx$. Now let's see if the two groups are isomorphic. In particular look at the identity map $\varphi$ from G to $G^{op}$ with $\varphi(x) = x$. Then $\varphi(xy) = xy$ [since $\varphi$ is the identity map] $= y*x = \varphi(y)*\varphi(x)$. So $\varphi$ is not an isomorphism, or even a homomorphism, since it changes order of multiplication.

Nonetheless the two groups are isomorphic, by the map taking x in G to $\psi(x) = x^{-1}$ in $G^{op}$, since then $\psi(xy) = (xy)^{-1} = y^{-1}x^{-1} = \psi(y)\psi(x) = \psi(x)*\psi(y)$. Moreover $\psi$ is its own inverse, hence is an isomorphism.

This discussion may shed light on the subject of group actions. Recall we defined an action of a group G on a set S as a map $G\times S\to S$, such that $\langle e,x\rangle = x$, and $\langle gh, x\rangle = \langle g, \langle h,x\rangle\rangle$, and we proved the map taking g to the action of g on S, is a homomorphism of $G\to Bij(S)$. Our definition is more precisely called a "left action", and if we change it to require that $\langle e,x\rangle = x$, and $\langle gh, x\rangle = \langle h, \langle g,x\rangle\rangle$, we get a definition of a right action. A right action of G on S makes the same map, the one taking g to the permutation of S given by g, a homomorphism $G\to Bij(S)^{op}$. (It may look more natural to define a right action as a map $S\times G\to S$, such that $\langle x,e\rangle = x$, and $\langle x,gh\rangle = \langle\langle x,g\rangle,h\rangle$ )

If you naively define the conjugation action of g on H to be $g^{-1}Hg$, and try to prove it gives a homomorphism of G to Bij(S), you have a problem. This is a right action, so it gives a homomorphism to $Bij(S)^{op}$. By the isomorphism we have just seen between G and $G^{op}$, taking every element to its inverse, it is not surprising that redefining conjugation by g to be $gHg^{-1}$ corrects the problem.

In general, our actions usually arise from a group and a subgroup, or a collection of elements, by translation or by conjugation., and we always have the choice of left translation or right translation. Moreover we can conjugate y by x, getting $xyx^{-1}$, with x on the left, or we can conjugate y by $x^{-1}$, getting $x^{-1}yx$, with x on the right. Hence in each case we can always choose either a left or a right action as we please. Indeed even if we have only one natural choice of action, we can always change a right action into a left action by replacing x by $x^{-1}$. So there is never a problem.

If we want the action to give a homomorphism to the usual groups Bij(S), or Bij({1,2,..,n}) = $S_n$, with usual composition, we choose a left action. If we want to get a homomorphism to the algebraists' version $Bij(S)^{op}$, or $Bij(\{1,2,...,n\})^{op} = S_n^{op}$, with composition in the opposite order, we choose a right action.
**End of digression.]**

**Cycle decomposition of a permutation.**

An element $\sigma$ of $S_n$ can always be written in a unique way as a product of disjoint "cycles". To do this simply decompose the set {1,2,3,. n} into its disjoint orbits under the action of the subgroup consisting of powers of $\sigma$, and order each orbit so that $\sigma(j)$ follows j For instance $\sigma$ = (124)(35) is the element sending 1 to 2, 2 to 4, 4 to 1, 3 to 5, and 5 to 3, and fixing all other integers between 1 and n. This $\sigma$ is composed of a 3-cycle, (124), and a 2-cycle, (35)

**Definitions:** A cycle is an element of $S_n$ for which all but at most one of the orbits are singletons. An r - cycle is a cycle whose largest orbit has length r; e.g. the 3 cycle (243), which fixes all integers from 1 to n except 2,3, and 4. A 2-cycle is called a "transposition".

**Theorem:** If G is a finite group of order n, then G is isomorphic to some subgroup of $S_n$.
**proof:** We will define a left action of G on itself, where the action of g on x is gx. then gh acts on x as (gh)x = g(hx), a left action. This gives a homomorphism $G \to Bij(G)$, and if we choose an ordering of the elements of G, i.e. a bijection $f:G \to \{1,2,...,n\}$, for n = #(G), the map $Bij(G) \to S_n$ sending $\varphi$ to $f\varphi f^{-1}$ is an isomorphism. We can then compose $G \to Bij(G) \to S_n$ to get a homomorphism $G \to S_n$ which is

injective, since only g = e acts as the identity on any element of G. QED.

**Theorem**: For $n \geq 2$, every element of $S_n$ can be written (in possibly many ways) as a product of (not necessarily disjoint) 2-cycles.
**proof**: We know every permutation can be written as a product of cycles, so it suffices to show every cycle can be written as a product of 2-cycles. Remember we are composing right to left, not as algebraists do To wit: (123) = (13)(12); (1234) = (14)(13)(12); more generally (abcdf) =(af)(ad)(ac)(ab), where a,b,c,d, are all distinct; get the idea? If you prefer, $(a_1a_2a_3.....a_r) = (a_1a_r)..... (a_1a_3)(a_1a_2)$where all the $a_j$ are distinct. QED.

**Important remark**: If $n \geq 2$, the group $S_n$ has a normal subgroup of index 2 called the subgroup of even permutations. To prove this requires a little work, and I choose to avoid this work to some extent by borrowing on the theory of determinants, which I hope is familiar to you [If not, consult the Appendix.]

**Definition**: A permutation matrix of size n is a matrix whose columns are a permutation of the columns of the n by n identity matrix

**Definition of matrix multiplication, dot product**

Now we must agree on a definition of matrix multiplication. We stipulate that when we multiply AB, the answer is the matrix whose (i,j) entry, i.e. the entry in the ith row and jth column, is the dot product of the ith row of A with the jth column of B, where the "dot product" of two numerical sequences $(a_1\ a_2\ ....\ a_n)\cdot(b_1\ b_2\ ....\ b_n)$ of the same length is the number $a_1b_1+a_2b_2+ ....\ +a_nb_n$.

**Theorem**: $S_n$ is isomorphic to the group of permutation matrices, where $\varphi$ in $S_n$ corresponds to the matrix $[\varphi]$ whose jth column is the "$\varphi(j)$-th" column of the n by n identity matrix
**"proof"**: The best way to see this is by example. Consider the bijection $\varphi$ sending 1 to 3, 2 to 4, 3 to 2, and 4 to 1. If $e_j$ is the jth standard basis vector in 4 space, with all zeroes except a 1 in the jth entry, then the first column of $[\varphi]$ is $e_3$, the second is $e_4$, the third is $e_2$, and the fourth is $e_1$ If we multiply this matrix by the

column $e_1$, we get $e_3$, i.e. $[\varphi]e_1 = e_3$. If we multiply $[\varphi]$ by $e_2$, we get $[\varphi]e_2 = e_4$. Similarly, $[\varphi]e_3 = e_2$, and $[\varphi]e_4 = e_1$. Thus $[\varphi]$ permutes the vectors $\{e_1,...,e_n\}$ exactly as $\varphi$ permutes the integers $\{1,...,n\}$, $[\varphi]e_j = e_{\varphi(j)}$.

Moreover our definition makes matrix multiplication the same as composition in the usual (right to left) order. That's the whole point: the permutation matrices are isomorphic to $Bij(\{e_1, ..., e_n\})$ which is isomorphic to $Bij(\{1,...,n\}) = S_n$. QED.

**Definition**: The sign of a permutation is the *determinant* of its corresponding permutation matrix, either 1 or -1. If $n \geq 2$, "sign" is a surjective homomorphism from $S_n$ to the group $\{1, -1\}$, and its kernel is called $A_n$ , the "alternating group". The elements of $A_n$ are called "even" permutations, and the remainder of the elements of $S_n$ are called "odd". Obviously the even permutations form a normal subgroup of index 2, while the odd permutations do not form a subgroup, but a coset of the subgroup of even ones. $S_n$ has n! elements for $n \geq 1$, and $A_n$ has $(1/2)n!$ elements for $n \geq 2$.

[For an element $\sigma$ of the opposite group $S_n^{op}$, the sign is exactly the same, i.e. the determinant of the element $\sigma$ of $S_n$. Since a permutation matrix and its inverse have the same determinant, the same elements are even in $S_n$ as in $S_n^{op}$, and $sign: S_n^{op} \to \{1,-1\}$ is still a homomorphism with kernel = the even permutations.]

The usual characterization of even permutations by transpositions, is a corollary of properties of determinants.
**Theorem**: A permutation is even if and only if it can be written as a product of an even number of 2-cycles, and is odd if and only if it can be written as a product of an odd number of 2-cycles.
**proof**: This all follows from usual properties of determinants (proved in the Appendix), i.e. a determinant changes sign if you transpose two rows, or columns, and the determinant of a matrix product is the product of the determinants. So if a permutation is a product of r transpositions, then its permutation matrix is a product of r transposition matrices, so the determinant is $(-1)^r$. QED.

**Remark**. The non obvious corollary of the previous theorem is that although the same permutation can be written as a product of 2-cycles in many ways, the number of 2-cycles is *always* either an

odd number, or always an even number. If we had attempted to define an even permutation as one which can be written as a product of an even number of 2-cycles, we would have had to figure out some way to prove that an even permutation could never be written differently as an odd number of 2-cycles.

**Theorem**: An r cycle is an even permutation if and only if the integer r is odd. The order of an r cycle is r. The order of any permutation is the l.c.m. of the lengths of the cycles in its unique disjoint cycle decomposition. Every permutation of odd order, i.e. whose disjoint cycle decomposition involves only cycles of odd length, is an even permutation. In general a permutation is even if and only if its disjoint cycle decomposition involves an even number of cycles of even length, [for example none].
**proof**: These are good exercises for you. About all you need to notice is that disjoint cycles commute with each other. "QED".

**Exercises on the symmetric group $S_n$**, [these three exercises and the following argument that $A_n$ is simple when $n \geq 5$, are from Lang, Algebra].
Remember we compose permutations from right to left. Thus fg means first g then f, and (123)(16) sends 3 to 1, and sends 6 to 2.

**Exercise #33)**
**(a)** Let $\sigma = (i_1\ i_2\ \ldots\ i_m)$ be a cycle, and $\gamma$ any element of $S_n$. Show that $\gamma\sigma\gamma^{-1} = (\gamma(i_1)\ \gamma(i_2)\ \ldots\ \gamma(i_m))$.
**(b)** Assume a permutation $\sigma$ in $S_n$, can be written as a product of r disjoint cycles, and let $d_1 \leq \ldots \leq d_r$ be the lengths of the cycles, in increasing order. Let $\tau$ be another permutation in $S_n$, and let the lengths of the cycles in its disjoint decomposition, in increasing order, be $e_1 \leq \ldots \leq e_s$. Prove that $\sigma$ is conjugate to $\tau$ in $S_n$ iff $r = s$ and for each $j = 1\ \ldots\ r$, $d_j = e_j$.

**Exercise #34)**
**a)** Let $\sigma = (123\ldots n)$ in $S_n$. Show that the conjugacy class of $\sigma$ has $(n-1)!$ elements.
**b)** Show the "centralizer" of $\sigma$ is the subgroup of powers of $\sigma$, i.e. the only elements of $S_n$ that commute with $\sigma$ are its own powers.

**Exercise #35)**
a) Show that $S_n$ is generated by (12), (13),....,(1n).
b) Show that $S_n$ is generated by (1 2), (2 3), (3 4),.... , ([n-1] n).
c) Prove that $S_n$ is generated by (12), (123....n).
d) Prove that (12), and (234....n) generate $S_n$.
e) Prove that if p is prime and $1 < i \leq p$, then $S_p$ is generated by (1 i) and (123.....p).
f) Show that if p is prime, then $S_p$ is generated by any permutation of period p, and any transposition.

**Theorem:** If $n \geq 3$, then every 3-cycle belongs to $A_n$, and $A_n$ is generated by the 3-cycles.
**proof:** Since (abc) = (ac)(ab), where a,b,c are distinct integers, every 3 cycle is an even permutation. For the second statement, since every element of $A_n$ can be written as a product of an even number of 2-cycles, we need only show that a non trivial product of two 2-cycles is a product of 3-cycles. Case (i): the two 2-cycles are the same. (ab)(ab) = id, so this is the trivial product case. case (ii) the two 2 cycles are different but not disjoint: [we just did this case above], i.e. (ac)(ab) = (abc). case (iii) the two 2-cycles are disjoint: (ab)(cd) = (dca)(abc). QED.

**Theorem:** Any two r - cycles are conjugate in $S_n$, (where $n \geq r$).
**proof:** Since conjugacy is an equivalence relation, it suffices to show any r cycle $\sigma = (a_1a_2a_3.....a_r)$ is conjugate to (12....r). Let $\varphi$ be a permutation of {1,2,3...,n} with $\varphi(1) = a_1, ...., \varphi(r) = a_r$. Then with the usual "right to left" convention on composition, $\varphi^{-1}\sigma\varphi$ = (12...r), as you should be able to check. Remember to check the equality also on integers greater than r. QED.

**Theorem:** If $n \geq 5$, then any two 3-cycles are conjugate in $A_n$.
**proof:** Given (abc) and (123), choose any $\varphi$ such that $\varphi(1) = a$, $\varphi(2) = b$, $\varphi(3) = c$, and of course $\varphi$ takes the integers greater than 3 to the integers different from a, b, c, in some way. Now $\varphi^{-1}\sigma\varphi$ = (123) as above, but $\varphi$ may not belong to $A_n$. If it does, stop, but if it does not, then just change what it does to 4 and 5. I.e. say $\varphi(4) = x$, $\varphi(5) = y$. Then change it so that $\varphi(4) = y$, and $\varphi(5) = x$. This changes $\varphi$ by composing it with one transposition, and hence changes it from odd to even. [Notice we needed $n \geq 5$ to do this.] QED.

**Theorem:** If $n \geq 5$, then a non trivial normal subgroup N of $A_n$ must contain a 3-cycle.
**proof:** Let N be a normal non trivial subgroup of $A_n$, and let $\sigma$ be a non trivial element of N which fixes at least as many integers as any other element of N. We claim $\sigma$ is a 3-cycle.

**Temporary convention: Just for this one proof let's work in $S_n$ ^ P, i.e. we will compose cycles from left to right.**
**case (i)** The disjoint cycle decomposition of $\sigma$ consists entirely of 2-cycles. Then since $\sigma$ is even, there must be more than one 2-cycle, and so $\sigma = (a_1a_2)(a_3a_4)(\ldots\ldots)$. Then $\sigma$ moves at least the four integers $a_1, a_2, a_3, a_4$. Let $a_5$ be any other integer, and suppose $\sigma$ fixes exactly k integers other than $a_1, a_2, a_3, a_4, a_5$. Since $\sigma$ may fix also $a_5$, but not $a_1, a_2, a_3, a_4$, $\sigma$ has at most k+1 fix points.

Define $\tau = (a_3a_4a_5)$, and consider $\gamma = (\tau\sigma\tau^{-1})\sigma^{-1}$. You may convince yourself that this element belongs to N, and fixes all k of the integers different from $a_1, a_2, a_3, a_4, a_5$ which are fixed by $\sigma$, and also fixes the two other integers $a_1, a_2$. Hence this $\gamma$ has at least k+2 fix points. Since you can also check that $\sigma\tau$ and $\tau\sigma$ do not do the same thing to $a_3$, we see that $\sigma\tau \neq \tau\sigma$, and hence their commutator $\gamma$ is a non trivial element of N with more fix points than $\sigma$, contradicting the choice of $\sigma$.

**case (ii)** The disjoint cycle decomposition of $\sigma$ contains at least one r cycle with $r \geq 3$. In this case, since the disjoint cycles commute, we may write them in descending order as to size, i.e. with the longest ones first. Then we have $\sigma = (a_1a_2a_3\ldots\ldots)(\ldots\ldots)$. Of course if $\sigma$ moves only three integers, then $\sigma = (a_1a_2a_3)$ is a 3-cycle, and we are finished, so we may assume that $\sigma$ moves either 4 or 5 integers. But $\sigma$ cannot move only four integers since then $\sigma = (a_1a_2a_3a_4)$ which is odd, hence not in $A_n$. So we must have $\sigma = (a_1a_2a_3\ldots\ldots)(\ldots\ldots)$ where $\sigma$ moves at least 5 integers, $a_1, a_2, a_3$ and at least two more, $a_4$ and $a_5$. Thus either there are more than two cycles in the decomposition of $\sigma$, or else the first cycle has length at least 5, or perhaps both happen.

Either way, the rest of the argument is the same. I.e. define again $\tau = (a_3a_4a_5)$, and consider $(\tau\sigma\tau^{-1})\sigma^{-1}$. Again this is a non

trivial element, since $\sigma\tau$ and $\tau\sigma$ differ on the integer $a_2$, and again it belongs to N [why?]. However, $\gamma$ fixes every element fixed by $\sigma$ [why?], and also fixes $a_1$ [why?]. This contradicts the choice of $\sigma$, and the only option is that in fact $\sigma$ moves only three integers and $\sigma = (a_1a_2a_3)$ is a 3-cycle. **QED.**

**Corollary**: Although we proved it in $S_n{}^{op}$, the same theorem holds for $S_n$.
**proof**: We remarked that the map $\varphi: x \mapsto x^{-1}$ is an isomorphism from $S_n$ to $S_n{}^{op}$. This map takes every subgroup to itself, [and every 3-cycle to a 3-cycle]. Hence if N is a normal subgroup in $S_n$, then N is also a normal subgroup in $S_n{}^{op}$, hence N contains a 3-cycle; or you can just copy the proof in the other direction. **QED.**

**Corollary**: If $n \geq 5$, $A_n$ is simple.
**proof**: If N is a non trivial normal subgroup of $A_n$, N contains a 3-cycle, hence all the $A_n$ conjugates of that 3-cycle, hence all 3 cycles. Thus N contains a set of generators for $A_n$, hence $N = A_n$. **QED.**

**Remarks**: We now have an infinite collection of simple groups, $\{A_n\}$ $n \geq 5$, but they seem rather sparsely distributed in the collection of all groups. E.g. $A_5$ has order 60, $A_6$ has order 360, and $A_7$ has order 2520. We also have met the simple group $G_{168}$ of collineations of the seven point plane. This naturally makes us wonder whether there are other simple groups, and if so what are they?

There are in fact four other non abelian simple groups of order less than 2520, all analogous to the collineation group $G_{168}$. Since we now know two simple groups of order 60, the icosahedral group I and $A_5$, we want to know whether they are isomorphic. We will show that in fact they are, and that moreover any simple group of order 60 must be isomorphic to $A_5$.

We will prove that the only possible non-prime orders up to 168, for simple groups, are 60 and 168. There is also exactly one simple group of order 168, and there are nice ways to represent it as a matrix group over a finite field.

After about 150 years of work, group theorists have determined *all* simple finite groups. Aside from the prime order groups, and the simple $A_n$'s, most of them are, or are analogous to,

matrix groups. For example $G_{168}$ is isomorphic to the group of 3×3 matrices of determinant one, with entries in the field $\mathbb{Z}_2$ of two elements. In addition to these matrix-like groups, which form the 16 infinite families of groups "of lie type" after Sophus Lie, there are 26 "sporadic" finite simple groups that don't fit into any pattern.

Some of those are quite large, and have names like "monster" and "baby monster". The importance of simple groups for the analysis of more general groups is indicated below, in the concept of the "simple components" of an arbitrary finite group. In a sense simple groups have the same relation to all finite groups as do prime numbers to all integers; i.e. simple groups are fundamental building blocks for other finite groups. They are also the key to Galois' criterion for solvable polynomials.

**Lemma**: If a simple group G of order 60 admits a non trivial homomorphism $\varphi: G \to S_5$ then $G \cong A_5$.
**Proof**: Pulling back the normal subgroup $A_5$, we get a normal subgroup $\varphi^{-1}(A_5) \subset G$, which must be either G or {e}. If $\varphi^{-1}(A_5) = \{e\}$, then the induced map $G \to S_5/A_5 \cong \mathbb{Z}_2$ is injective, an impossibility. Hence $\varphi^{-1}(A_5) = G$, and $\varphi: G \to A_5$ is an isomorphism. **QED**.

**Proposition**: Icos $\cong A_5$, where Icos is the group of rotations of the isocahedron.
**proof**: We want to find a subgroup of Icos of index 5, or a subgroup with 5 conjugates. Since Icos is simple of order 60, there is no non trivial homomorphism to $S_n$ for $n \leq 4$, so no proper subgroup has index $\leq 4$, nor fewer than 5 conjugates. [I.e. there are no subgroups of orders 15, 20 or 30, and we seek a subgroup of order 12, or one whose normalizer has order 12.] Since the number of Sylow 2-subgroups is odd and divides 60, and must be greater than 4, there are either 5 or 15 of them.

Now let x be an element of order two. Since all 15 elements of order 2 are conjugate, the orbit of x under the action of Icos by conjugation has orbit of order 15 and isotropy group of order 4, i.e. $\#(N(x)) = 4$. Since all Sylow 2-subgroups have order 4, but Icos has no elements of order 4, if P is a Sylow 2-subgroup containing x then $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian, so $P = N(x)$. Thus each x of order two belongs to only one Sylow 2-subgroup.

Since there are 15 elements of order two, and each Sylow 2-

subgroup contains 3 of them, there are 5 Sylow 2-subgroups. Since Icos acts transitively on them by conjugation, the normalizer N(P) of a Sylow 2-subgroup P is a subgroup of order 12 and index 5 in Icos| Thus we get an embedding Icos$\rightarrow S_5$, via the translation action on cosets of N(P), and thus an isomorphism $I \cong A_5$, by the previous lemma. QED.

**Exercise #36)** Adapt the argument above to prove any simple group G of order 60 is $\cong$ to $A_5$. [Hint: If there are more than 5 Sylow 2-subgroups, prove some element x of order two lies in at least two of them, and then show the subgroup N(x) would have index 5 in G.]

**Challenge:** Find a geometric proof that $I \cong A_5$ by finding 5 objects permuted by the elements of I, or the dodecahedral group. [For example, there are 5 ways to embed a cube in a dodecahedron, such that each edge of the cube is a diagonal of one face of the dodecahedron. Also the 15 axes bisecting the pairs of edges of an icosahedron, (the axes of the 15 elements of order 2 in I), can be divided into 5 disjoint triples of mutually perpendicular axes, such that these triples are permuted by the elements of I.

**Exercise #37)** **(i)** If G is a finite cyclic group of order n, then there exists a sequence of subgroups $\{e\} = N_k \subset N_{k-1} \subset \ldots\ldots \subset N_0 = G$ such that each quotient $N_{j-1} / N_j$ has prime order $p_j$, where the primes $\{p_j\}$ occurring are precisely the prime factors of n, i.e. $n = \Pi_j\, p_j$ .
**(ii)** Prove the same statement for any finite abelian group G of order n.

**Exercise #38)** If G is a group with a simple normal subgroup N such that G/N is simple, and M is any other normal subgroup,
**(i)** prove $M \cap N$ and MN are normal subgroups different from M, N.
**(ii)** prove $M \cong G/N$, and $N \cong G/M$.

If G is any group with a simple normal subgroup N such that G/N is simple, it follows from the previous exercise that the two simple groups {N, (G/N)} are determined by G up to isomorphism and reordering. They are called the "simple components" of G. We wish to generalize this notion to every finite group.

**Definitions:** (i) If G is a non trivial group, a sequence of distinct

subgroups $\{e\} = N_k \subset N_{k-1} \subset \ldots\ldots \subset N_1 \subset N_0 = G$, with each $N_j$ normal in $N_{j-1}$, is called a normal tower (of length k) for G.
(ii) A normal tower obtained by inserting more normal subgroups into another tower is called a refinement of that tower.
(iii) A normal tower in which each quotient group $N_{j-1}/N_j$ is simple, is called a composition series for G.
(iv) The k simple quotient groups $\{N_{k-1}/N_k\ ,\ N_{k-2}/N_{k-1},\ \ldots\ldots\ ,\ G/N_1\}$, unordered but not necessarily all different, associated to a given composition series is called a system of simple components for G.
(v) Two composition series for G are equivalent if up to isomorphism and reordering they have the same system of simple components; in particular equivalent composition series have the same length.

**Exercise #39)** (i) If $f: G \to H$ is a surjective homomorphism of groups, and G has a composition series of length two, then H is isomorphic either to G, $\{e\}$, or to one of the two simple constituents of G.
(ii) For any normal tower of a finite group G, prove the order of G is the product of the orders of the successive quotients of the tower.

**Examples of composition series**

The group $G = S_2 \cong \mathbf{Z}_2$ is simple, hence $\{id\} \subset S_2$ is a composition series with one simple component $\{\mathbf{Z}_2\}$.
If $G = S_3$, then $\{id\} \subset \langle(123)\rangle \subset S_3$ is a composition series of length 2, with corresponding system $\{\mathbf{Z}_3, \mathbf{Z}_2\}$ of simple components.
We know $G = S_4$ is isomorphic to the full isometry group of the tetrahedron, with normal subgroup $A_4$ isomorphic to the rotation group of the tetrahedron, which in turn has a normal subgroup of order 4 generated by rotations of order 2. Hence there is a composition series equivalent to $\{id\} \subset \mathbf{Z}_2 \subset \mathbf{Z}_2 \times \mathbf{Z}_2 \subset A_4 \subset S_4$, with simple quotients $\{\mathbf{Z}_2, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_2\}$.

Since $A_5 \cong$ Icos is simple, the only composition series for $G = S_5$ is $\{id\} \subset$ Icos $\subset S_5$, with simple quotients $\{$Icos, $\mathbf{Z}_2\}$. This is the first time we have seen a group whose simple quotients are not cyclic, but this phenomenon continues from here on for the symmetric groups. E.g. for $n \geq 5$, the only composition series is $\{id\} \subset A_n \subset S_n$, and the system of simple components is $\{A_n, \mathbf{Z}_2\}$. It will turn out later this is why polynomials of degree $\geq 5$ do not have a general solution formula in terms of radicals, as made clear by Galois.

Our next goal, the Jordan - Hölder theorem, says any two composition series for the same group are equivalent. We need this to conclude that the system of simple components is intrinsically determined by the group. This is trivial for simple groups, i.e. groups having a Jordan Holder series of length one, and exercise #38 proves it for groups having a composition series of length two. Using that result, we will complete the proof by induction.

**Theorem**: If G has one composition series, then every normal tower can be refined to a composition series equivalent to the given one.

**Corollary**: If G has one composition series of length n, then every normal tower has length ≤ n, every composition series has length n, and any two composition series are equivalent. In particular, G determines a well defined system of simple component groups.

**Proof**: Assume the theorem for groups having a composition series of length < k, and let $\{e\} \subset N_{k-1} \subset \ldots\ldots \subset N_1 \subset G$ be a composition series for G of length k. By the induction hypothesis no composition series of length less than k exists, so every normal tower can be refined until it has length at least k. Thus it suffices to show that every normal tower of length k is a composition series equivalent to the composition series above.

So assume $\{e\} \subset M_{k-1} \subset \ldots\ldots \subset M_1 \subset G$ is a normal tower of length k and consider $M_1 \cap N_1$. If $N_1 = M_1$ we are done by the induction hypothesis applied to the group $N_1 = M_1$, so assume $N_1$ and $M_1$ are different subgroups of G. Since $G/N_1$ is simple, $M_1$ does not properly contain $N_1$. Also, by the induction hypothesis, $N_1$ cannot properly contain $M_1$ since then $N_1$ would have a composition series $\{e\} \subset N_{k-1} \subset \ldots\ldots \subset N_1$ of length k-1 and also a normal tower $\{e\} \subset M_{k-1} \subset \ldots\ldots \subset M_1 \subset N_1$ of length $k > k-1$.

Hence the subgroups $M_1 \cap N_1$ and $M_1 N_1$ are both different from $N_1$ and $M_1$, and moreover both are normal in G. Thus we can consider this normal tower for $N_1$: $\{e\} \subset M_1 \cap N_1 \subset N_1$, and refine it by the induction hypothesis to a composition series for $N_1$ of length k-1: $\{e\} \subset \{*\} \subset M_1 \cap N_1 \subset \{**\} \subset N_1$, where the number of subgroups in the two families $\{*\}$ and $\{**\}$ add up to k-3.

Now extend the analogous normal tower for $M_1$: $\{e\} \subset M_1 \cap N_1 \subset M_1$, by adding the subgroups $\{*\}$, getting: $\{e\} \subset \{*\} \subset M_1 \cap N_1 \subset$

$M_1$. This is a composition series for $M_1$ except possibly at the top stage. But since $M_1N_1$ is a normal subgroup strictly larger than $N_1$, and $G/N_1$ is simple, we have $M_1N_1 = G$. Hence $M_1/(M_1 \cap N_1) \cong (M_1N_1)/N_1 \cong G/N_1$, which is simple

Hence $\{e\} \subset \{*\} \subset M_1 \cap N_1 \subset M_1$ is a composition series for $M_1$ of length $\leq k-1$. Since we were initially given a normal tower $\{e\} \subset M_{k-1} \subset \ldots\ldots \subset M_1$ of length $k-1$ for M, by the induction hypothesis, the original normal tower of length $k-1$: $\{e\} \subset M_{k-1} \subset \ldots\ldots \subset M_1$ is also a composition series, and the composition series $\{e\} \subset \{*\} \subset M_1 \cap N_1 \subset M_1$ must have length exactly $k-1$. In particular the sequence of groups $\{*\}$ contains exactly $n-3$ groups, and the sequence $\{**\}$ contains no groups. Hence the sequence $\{e\} \subset \{*\} \subset M_1 \cap N_1 \subset N_1$, is a composition series for $N_1$, and the quotient $N_1/(M_1 \cap N_1)$ is simple.

Thus the quotient group $G/(M_1 \cap N_1)$ has a composition series of length 2, namely $\{e\} \subset N_1/(M_1 \cap N_1) \subset G/(M_1 \cap N_1)$. By exercise #38, this implies that the normal tower $\{e\} \subset M_1/(M_1 \cap N_1) \subset G/(M_1 \cap N_1)$ is an equivalent composition series for $G/(M_1 \cap N_1)$, and in particular $\{G/(M_1 \cap N_1)\} / \{M_1/(M_1 \cap N_1)\} \cong G/M_1$ is simple.

Therefore the normal tower $\{e\} \subset M_{k-1} \subset \ldots\ldots \subset M_1 \subset G$ is a composition series, and we now have four composition series for G as follows

(I): $\{e\} \subset N_{k-1} \subset \ldots\ldots \subset N_1 \subset G$,
(II): $\{e\} \subset \{*\} \subset M_1 \cap N_1 \subset N_1 \subset G$,
(III): $\{e\} \subset \{*\} \subset M_1 \cap N_1 \subset M_1 \subset G$, and
(IV): $\{e\} \subset M_{k-1} \subset \ldots\ldots \subset M_1 \subset G$.

Series (I) is equivalent to (II), and also (II) is equivalent to (IV), by the induction hypothesis applied to $N_1$, while series (II) is equivalent to (III) by exercise #38. Thus (I) is equivalent to (IV). **QED**.

**Definitions**: (i) A finite group is <u>solvable</u> if it has a composition series whose simple components are all cyclic of prime order.
(ii) A normal tower is called <u>cyclic</u>, <u>abelian</u>, or <u>solvable</u>, if all the quotient groups are cyclic, abelian, or solvable, respectively.

**Remark**: By problem #37, all abelian groups are solvable.

**Exercise #40)** (i) Prove a group with a solvable normal tower is

solvable.
(ii) Prove $S_n$ is solvable iff $n \leq 4$.
(iii) Prove all semi direct products of solvable groups are solvable.
(iv) Prove a group of order $< 335$ is solvable if its order is not a multiple of 60.
(v) Find non solvable groups of order 60n, for every $n \geq 1$.
(vi) Find the simple components of a group of order 288.
(vii) Find the simple components of a solvable group of order n.

**Remark**: By problem #40(i), for a finite group the following properties are all equivalent: to have a solvable normal tower, to have an abelian normal tower, to have a cyclic normal tower, to have a cyclic composition series, i.e. to be solvable.

**Exercise #41)**: (i) If G has a composition series, and $f:G \to H$ is a surjective homomorphism, then H has a composition series whose simple components form a subsystem of the simple components of G
(ii) What does this say for finite abelian groups G, H?
(iii) If G is simple, $\#(G) \geq 3$, a homomorphism $f:G \to S_n$ maps $f(G) \subset A_n$.
(iv) If G acts transitively on a set of n elements and #(G) does not divide (n!/2), then G is not simple.
(v) There is no simple group of order 112.

Now we finish the list of possible orders $< 168$ for simple groups.
**Exercise #42)** (i) A Sylow 3-subgroup in a simple group G of order 90 cannot be cyclic.

[Show the intersection of two distinct such Sylow groups cannot contain a generator of either group, hence the group G contains at least 60 elements of order 9, 2 elements of order 3, and 24 elements of order 5, hence at most 3 elements of order 2. Then what?]
(ii) The non trivial elements of a Sylow 3-subgroup of a simple group of order 90 cannot consist entirely of elements of order three.

[If so, either any two Sylow 3-subgroups intersect trivially and hence there are at least 80 elements of order three in G, or else some element x of order three belongs to more than one Sylow 3-subgroup whence the normalizer of the subgroup generated by x has order at least 18.]
(iii) There is no simple group of order 90.

**Theorem:** If G simple and $60 < \#(G) < 168$, then $\#(G)$ is prime.
**proof:** (The harder ones are 90, 112, 120, 144, and 105, 132 are not entirely trivial). The efficient way of organizing the following proof was suggested by Ken Berenhaut.

We know if $\#(G) = p^k n$, where $p > n$, then G is not simple, so no prime greater than 11 can occur in $\#(G)$
Moreover, if $\#(G) = 11n$, then $60 < \#(G) < 167$ implies that $11 < n < 15$. We need consider only n such that 12 divides n by Sylow III, so only $\#(G) = 132 = 11(3)(4)$.

But then G simple means there are 12 $P_{11}$'s, hence 120 elements of order 11, and at least 4 $P_3$'s hence at least 8 elements of order 3, leaving only 4 elements for a unique group of order 4; hence G is not simple after all.

If $p = 7$ is the highest prime occurring, and $\#(G) = 7n$, then $8 < n < 23$, and by Sylow III we need only consider cases with 8 or 15 dividing n, hence $n = 15$ or 16, i.e. $\#(G) = 112$ or 105.
If $\#(G) = 112 = 7(16)$, see ex. 43 above.

If $\#(G) = 105 = 7(3)(5)$, and G simple we have 15 $P_7$'s, hence 90 elements of order 7, and 21 $P_5$'s, hence 84 elements of order 5, too many for G to hold.

If 5 is the largest prime dividing $\#(G)$, not all factors can be 5 so we have $\#(G) = 5^k n$, $5 < n < 34$, and 6 or 16 must divide n by Sylow III (since other candidates 11, 21, 25, 31, have prime factors greater than 5, already handled above). Thus we consider
$\#(G) = 5(32) = 160$, so index of $P_2$ is 5, and 160 does not divide (5!)
$\#(G) = 5(16) = 80$, same argument.
$\#(G) = (25)(2)(3) = 150$, index of $P_5$ is 6, and 150 does not divide (6!).

$\#(G) = 5(18) = 90$. This proof is due to Ken Berenhaut.

Look at the homomorphism of G into $S_{90}$, given by G acting on itself by left multiplication. Note that left multiplication by a non trivial element of G does not fix any element of G. Hence the image in $S_{90}$ of a non trivial element of G is a permutation with a disjoint cycle decomposition with no singleton cycles of form (n). By Sylow's theorem G contains an element of order 2, whose image in $S_{90}$ is thus a permutation $\sigma$ of order 2.

Then the disjoint cycle decomposition of $\sigma$ has no singleton

cycles, and the l.c.m. of the lengths of its cycles is 2. Hence the decomposition of $\sigma$ must be a product of 45 disjoint 2-cycles, whence $\sigma$ is an odd element of $S_{90}$, (it is a product of an odd number of 2 cycles). Hence $\sigma$ does not belong to $A_{90}$. Since G has order > 2, G is not simple by exercise #27 above

#(G) = 120. This solution is due to Gang Yu.

Note 120 = 15(8) = (3)(5)$(2^3)$, so consider the groups $P_3$, $P_5$, $P_2$. If G is simple there are 10 $P_3$'s, and 6 $P_5$'s, and 15 $P_2$'s. First we prove there is an element of order 6 in G. Since there are 10 groups conjugate to $P_3$, the index of the normalizer of $P_3$ is 10, so the order of the normalizer N is 12. Now conjugation of elements of $P_3$ by elements of N carries them back into $P_3$, hence gives an automorphism of $P_3$. I.e. taking each element of N to conjugation of elements of $P_3$ by that element, gives a map from N to the group $Aut(P_3) = Aut(\mathbb{Z}_3) = \mathbb{Z}_2$.

Hence the kernel of this map, the elements of N that conjugate every element of $P_3$ trivially, has order either 6 or 12. Now an element of N conjugates elements of $P_3$ trivially iff it commutes with all of them. So if we take an element of order 2 that commutes with all elements of $P_3$, we can multiply it by an element of order 3 in $P_3$ and get an element of order 6 in G Thus we have our element of order 6 in G.

Since there are 6 $P_5$'s, if we operate on them by conjugation we get a non constant map of G into $S_6$, which is injective if G is simple, hence our element of order 6 from G goes to an element of order 6 in $S_6$. Now we know also that this map goes entirely into $A_6$. It only remains to show that $A_6$ does not contain any elements of order 6.

The disjoint cycle decomposition of an element of order 6, must be into disjoint cycles such the l.c.m. of their lengths is 6. Since there are only 6 letters to use, either there is one cycle of length 6, or two cycles, one of length 2 and one of length 3. But neither of these elements can be even. QED.

If 3 is the highest prime occurring in #(G), and #(G) > 60, then #(G) cannot divide $n!$ when n = 2, 3, or 4, so we must have $\#(G) = 2^r3^s$, with both r > 2, s >1. But r > 2, implies s < 3, and s > 1 implies r < 5. So we have to consider s = 2, and r = 3,4.

$\#(G) = 2^3 3^2 = 72$, a case done in the class notes above.

$\#(G) = 2^4 3^2 = 144$. This one can be done by the same method outlined in the exercises for 90, i.e. find a subgroup of small index which has form N(H) for some appropriate subgroup H of $P_3$. If there is more than one $P_3$, there are 4 or 16 of them, and 4 is out since 144 does not divide (4!). If there are 16 of them, each of order 9, and if any two of them meet only in the identity, then the union of all 16 $P_3$'s contains at least 128 elements of orders $3^k$.

This leaves exactly 16 more elements, hence only one $P_2$. So there must be two $P_3$'s, say P' and P'' that meet in a subgroup H of order 3. Moreover, since $\#(P_3) = 3^2$, we know all $P_3$'s are abelian. Hence the 3 elements in H commute with the other 6 elements in each of P', P''. Hence $P' \cup P'' \subset N(H)$, so $\#(N(H)) > 14$, and 9 divides $\#(N(H))$

If $\#(N(H)) = 18$, then P' is normal in N(H) of index 2, N(H)/P' has order 2, so any element of order 3 in N(H) is in P', i.e. then P'' would not be there So $\#(N(H))$ is at least 36, and thus has index no more than 4, so since 144 does not divide 4! we are done. (I.e. if the normalizer is G we are done, since then H is a normal subgroup, and if N(H) is a proper subgroup of index less than 5 we are done by our usual argument permuting its cosets by translation).
We have them all!

**§10) Categories, functors, and natural transformations**

We have encountered several natural constructions which replace one mathematical object with another, not always of the same type. For example, we can forget the group structure on a group and regard it merely as a set, thus replacing a group by a set The other aspect of this construction is that a homomorphism of groups can be regarded as a set map on the underlying sets.

The fact that the construction replaces not only one type of *object* with another, but also a *map* of the first type of object with a map of the new type of objects, is part of what we mean by saying the forgetful construction is a "functor" from groups and homomorphisms, to sets and set maps.

The rest of the axioms for a functor say that identity maps go to identity maps and compositions go to compositions. As an example of a functor in the other direction, from sets to groups, we

can replace a set by the group of bijections of that set. Not every function between sets S, T yields a homomorphism between Bij(S) and Bij(T), but if we consider only bijective functions between S and T, composition with such bijections does yield homomorphisms between Bij(S) and Bij(T).

More precisely, if $f:S \to T$ is a bijection of sets, then we get a homomorphism $f_*:Bij(S) \to Bij(T)$, by setting $f_*(\sigma) = (f \circ \sigma \circ f^{-1})$. Thus "Bij" is a functor, from sets and bijections, to groups and (isomorphic) homomorphisms.

There is another important functor from sets to groups that associates a homomorphism to *every* set function, namely the "free group" functor. Let S be any set, {a,b,c....}, thought of as an "alphabet" of letters, finite or infinite. Consider all finite "words" spelled with those letters and with their "inverse letters" $\{a^{-1},b^{-1},c^{-1},....\}$. A word then is a finite sequence such as $bbb^{-1}aac$. We multiply two words by juxtaposing them, e.g. $(acbb^{-1})(cbdac^{-1}) = acbb^{-1}cbdac^{-1}$. The identity is the "empty word". Since we want $xx^{-1}$ and $x^{-1}x$ to equal the identity, we allow canceling of such pairs of symbols. We call a word "reduced" if there are no adjacent symbols of form $xx^{-1}$ or $x^{-1}x$, i.e. if no cancellation is possible. (We agree that $(x^{-1})^{-1} = x$.)

Obviously any word can be transformed into a reduced word by repeatedly canceling any pairs of form $xx^{-1}$ that occur in the word. The free group Fr(S) will consist of all reduced words, with the operation being juxtaposition followed by reduction. Although juxtaposition of words is clearly associative, it is not so clear that this holds for reduced words, since cancellation can often be done in more than one way. The following nice argument is from M. Artin, Algebra.

**Lemma:** Every word has exactly one reduced form.
**proof:** (By induction on the length of the word). If a word is reduced there is nothing to prove. If not, there is at least one pair of form $xx^{-1}$ occurring in the word. We claim every reduction of the word can be obtained by canceling this pair first. (The result then follows by induction applied to the length of the resulting shorter word.) Any reduction of this word must involve elminating this pair at some time, by canceling at least one of the symbols. If the

pair itself is at any time, the same reduction is achieved by canceling this pair first and then proceeding with the other cancellations

If on the other hand the first cancellation involving this pair cancels only one of the symbols, say the symbol x, then at that point the word must look like $..x^{-1}xx^{-1}.....$, where the first two symbols are canceled. But the same result is obtained at this stage by canceling instead the second two symbols, i.e. by canceling the original pair. This is the previous case. QED.

**Corollary**: Fr(S) is a group.
**proof**: We have inverses and an identity and the previous lemma implies associativity. QED.

Equivalently a word can be represented by a finite sequence of the symbols $a_j{}^r j$, where $a_j$ is an element of S and $r_j$ is a non zero integer. Here the word is reduced iff whenever $a_j{}^r j\ a_k{}^r k$ are adjacent letters then $j \neq k$. For example $(a_3)^2(a_1)^{-1}(a_3)^{-6}(a_4)^3$ is a reduced word. Reduction is performed by applying the usual laws of exponents to adjacent occurrences of powers of the same letter.

Given any set map $f:S \to T$ of two sets, the associated group homomorphism between their free groups $f_*:Fr(S) \to Fr(T)$ is defined by sending a word spelled with letters from S to the word spelled with the corresponding letters from T For example $f_*((a_3)^2(a_1)^{-1}(a_3)^{-6}(a_4)^3) = [f(a_3)]^2[f(a_1)]^{-1}[f(a_3)]^{-6}[f(a_4)]^3$.

The free group has a very nice property: it is extremely easy to define a homomorphism from it to any other group. In fact any set map from S to a group G extends uniquely to a group homomorphism from Fr(S) to G, using exactly the same definition as just given for the homomorphism to Fr(T).

**Theorem**: If G is any finite group, there is a surjective homomorphism from a free group onto G.
**proof**: Let the set S = G, [actually S = the "underlying set" of G]. The identity function $S \to G$ extends to a unique homomorphism which is surjective, since S already maps onto G. QED.
**Cor**: Every finite group is a quotient of a free group on a finite set.
**proof**: This follows from the theorem above by the "first

fundamental homomorphism theorem". **QED**.

**Remark**: In this theorem we only need to take for S a set large enough to map onto a generating set for G. For example if p is prime we can take a two element set {a,b} for S, and map Fr({a,b}) onto $S_p$ by sending a to (12) and b to (123....p), according to our homework problem that these generate the symmetric group $S_p$. To appreciate how large and complex the free group Fr({a,b}) on two generators is, note that every finite group in the world embeds inside one of the groups $S_p$. That means that the different quotients of the one group Fr({a,b}) contain subgroups isomorphic to *every* finite group.

We also don't need to assume G is finite in the previous theorem, or even finitely generated, if we consider free groups on infinite sets. This shows the potential of using free groups to study arbitrary groups The method of expressing groups as quotients of free groups is called the method of "generators and relations". It is quite analogous to the relationship between finite field extensions and polynomial rings which we will use presently in our study of Galois theory.

As mentioned above, the three constructions we have given (and all functors) satisfy two properties that are crucial to their usefulness, namely they preserve both identity maps and compositions Thus for the forgetful functor, the set map associated to the identity homomorphism of a group G, equals the identity map on the underlying set, and the set map associated to the composition of two homomorphisms, is the composition of the two set maps.

In the case of the bijections functor, if $f:S \to S$ is the identity map of S, then $f_*:Bij(S) \to Bij(S)$ is also the identity homomorphism of Bij(S), [since $id \circ \sigma \circ id^{-1} = \sigma$ for every $\sigma$ in Bij(S)]. Moreover, if $f:S \to T$, and $g:T \to U$, are two set maps that can be composed, then $(g \circ f)_* = g_* \circ f_*:Bij(S) \to Bij(U)$, since $(g \circ f)_*(\sigma) = (g \circ f) \circ \sigma \circ (g \circ f)^{-1} = (g \circ f) \circ \sigma \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ \sigma \circ f^{-1}) \circ g^{-1} = g_*(f_*(\sigma))$, for all $\sigma$ in Bij(S). You can also check readily that the free functor from sets to groups satisfies these two fundamental properties.

These two axioms yield the following very important result, (and trivial to prove), but first we must be very clear about the definition of the word "isomorphism".

**Definition**: In any category, an isomorphism from X to Y, is a morphism $f:X \to Y$ that has an inverse morphism $g:Y \to X$. I.e. $f:X \to Y$ is an isomorphism iff there is a morphism $g:Y \to X$ such that the two compositions $fg:Y \to Y$ and $gf:X \to X$ are both identity maps.

**Theorem**: Any functor always takes isomorphisms (of one type) to isomorphisms (of possibly another type).
**proof**: If f is an isomorphism, say of sets, then f has an inverse map g with the properties that $f \circ g = id$, and $g \circ f = id$. If $f_*$ and $g_*$ are the maps, say of groups, associated to f,g by some functor, then by the two axioms we have $f_* \circ g_* = (f \circ g)_* = id_* = id$, and $g_* \circ f_* = (g \circ f)_* = id_* = id$. Thus $f_*$ and $g_*$ are also mutually inverse group homomorphisms, and hence both are isomorphisms. **QED**.

**Warning**: This theorem is not true without the correct definition of isomorphism, as given above. In topology for instance, a continuous map can be bijective without being an isomorphism.

For instance there is a continuous bijection from the half open interval [0,1) to the unit circle taking x to $e^{2\pi ix}$, but this map will not induce an isomorphism of fundamental groups. Thus a "homeomorphism" (topological isomorphism) is defined as a continuous map with a continuous inverse, *not* as a bijective continuous map.

**Cor**: Isomorphic groups always have the same number of elements.
**proof**: The forgetful functor takes a group isomorphism to a bijection on the underlying sets **QED.**

**Cor**: Two bijectively equivalent sets have isomorphic groups of bijections.
**proof**: The Bij functor takes a set bijection to a group isomorphism of their groups of bijections. QED.

**Cor**: The group of bijections of a finite set S is isomorphic to some symmetric group $S_n$.
**proof**: A bijection from S to a set of form {1,2,....,n} yields a group isomorphism from Bij(S) to $Bij(\{1,2,....,n\}) = S_n$. **QED.**

**Cor**: Two free groups on the same number of letters are isomorphic.
**proof**: Applying the free group functor to a bijection between their

sets of letters yields an isomorphism of the corresponding free groups. QED.

Another functor, this time from groups and isomorphism, to groups and isomorphisms, is the "automorphism" functor. This associates to a group G the group Aut(G) of group automorphisms from G to itself. As with the bijection functor of sets, not every group homomorphism $G \to H$ yields a group homomorphism $Aut(G) \to Aut(H)$, but isomorphisms $f:G \to H$ do. I.e. if $f:G \to H$ is a group isomorphism, we get, again by conjugation, an [isomorphic] homomorphism $Aut(G) \to Aut(H)$ taking $\sigma$ to $\sigma_* = (f \circ \sigma \circ f^{-1})$. As before, if $id:G \to G$ is the identity homomorphism of G, then $id_* =$ the identity homomorphism of Aut(G), and $(f \circ g)_* = f_* \circ g_*$.

**Cor**: Isomorphic groups have isomorphic automorphism groups.
**proof**: The functor Aut takes an isomorphism f between G and H to an isomorphism $f_*$ between Aut(G) and Aut(H). QED.

**Cor**: The groups $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_2$ are not isomorphic.
**proof**: Check as exercise that $Aut(\mathbf{Z}_4) \cong \mathbf{Z}_2$, and $Aut(\mathbf{Z}_2 \times \mathbf{Z}_2) \cong S_3$. Since these automorphism groups have different numbers of elements, they are not isomorphic, and thus the original groups are not isomorphic either. QED.

**Remark**: Even when G is abelian, Aut(G) may not be.

**Challenge**: Compute $Aut(\mathbf{Z}_n)$ for every n. Is it always abelian?

In order to speak precisely about constructions taking one type of mathematical object and map, and changing them into (possibly) another type, a word has been coined for the collection of all mathematical objects of a given type, a "category". The collection of all groups and their homomorphisms is called the category of groups, and the collection of all sets and set maps is called the category of all sets. So a category consists of two collections, first the collection of all "objects" in the category, and secondly the collection of all "morphisms" or "maps" in the category.

Each group G constitutes one object in **G**, the category of groups, and for each ordered pair (G,H) of objects in **G**, there is one

set of maps $\mathrm{Hom}_{\mathcal{G}}(G,H)$ = { all group homomorphisms $f:G \to H$}. Similarly, in the category $\mathcal{S}$ of sets, the collection of objects consists of all sets S, and for each pair of sets S, T, there is one set of maps, $\mathrm{Hom}_{\mathcal{S}}(S,T)$ = {all functions $f:S \to T$}.

In topology, one considers the category $\mathcal{T}$ of all topological spaces and continuous maps, i.e. the objects are the topological spaces X, and there is one set of morphisms $\mathrm{Hom}_{\mathcal{T}}(X,Y)$ = {all continuous maps $f:X \to Y$}, for each pair X,Y of objects.

There are also two axioms for categories, namely for every object X there must be an identity morphism $1_X$ in Hom(X,X), and whenever three objects X, Y, Z exist in a category, composition must be defined for the morphisms as follows: $\mathrm{Hom}(X,Y) \times \mathrm{Hom}(Y,Z) \to \mathrm{Hom}(X,Z)$. I.e. you must be able to compose a morphism from X to Y with a morphism from Y to Z to get a morphism from X to Z, and of course composition must be associative

**Remarks**: (i) Although the definition of a category may seem somewhat trivial, containing no new ideas, remember that even when a definition only awards a name to a concept which already exists, it serves notice that the concept has been found to be important. The definition of category suggests that it is useful to consider a whole collection of objects of a similar type, that it is important to consider simultaneously their morphisms, and suggests the correct definition of isomorphism. We have really only defined categories in order to talk about how to relate different categories, i.e. to discuss functors.

(ii) We are particularly interested in comparing functors, via certain homomorphisms of functors, called "natural transformations", and isomorphisms of functors called "natural equivalences" as we will discuss in more detail in the final third of these notes. For instance each group G can be made abelian, by modding out by the smallest normal subgroup containing all "commutators" [products of form $aba^{-1}b^{-1}$].

Doing this to any group valued functor turns it into an abelian group valued functor, and defines a natural transformation between the two functors. In topology, it is proved that the "first homology" functor is equivalent to the "fundamental group functor made abelian", i.e. $H_1 \cong \pi_1/\{\text{commutators}\}$. The free abelian group functor

defined below is equivalent to the free group functor made abelian.

The famous result in topology, due to Brouwer, that a disc cannot be retracted onto its boundary circle, is a favorite for illustrating the use of functors in topology. Suppose one could "retract" a disc onto its boundary circle continuously. That would mean the existence of a continuous function $g:D^2 \to S^1$ (where $D^2$ = unit disc, $S^1$ = unit circle) such that the restriction of g to the unit circle is the identity. Thus the composition $(g \circ f):S^1 \to D^2 \to S^1$ is the identity where $f:S^1 \to D^2$ is the inclusion map of the circle as the boundary of the disc. Applying to this composition any functor F from topological spaces to groups, implies that the composition $(g \circ f)_* :F(S^1) \to F(D^2) \to F(S^1)$, must be the identity group homomorphism of the group $F(S^1)$.

Hence if there were a functor F such that $F(S^1) \neq \{0\}$, while $F(D^2) = \{0\}$, we would have a contradiction, since you cannot factor the identity map of a non zero group through the zero group! Indeed those of you who have studied topology know several functors with these properties, such as the fundamental group functor $\pi_1$, and the first homology group functor $H_1$, both of which take $D^2$ to $\{0\}$, and $S^1$ to $\mathbf{Z}$.

**Summary**: To recap, a functor F, say from groups to sets, associates to each group G in $\mathbf{G}$, a set F(G) in $\mathbf{S}$, and to any two groups G, H in $\mathbf{G}$, a map from the collection of homomorphisms $\mathrm{Hom}_{\mathbf{G}}(G,H)$ to the collection of set maps $\mathrm{Hom}_{\mathbf{S}}(F(G), F(H))$. Moreover, if we have three groups G, H, K, and two homomorphisms $f:G \to H$, and $g:H \to K$, which can be composed to yield a homomorphism $(g \circ f):G \to K$, then the two corresponding set maps $F(g \circ f)$: $F(G) \to F(K)$, and $F(g) \circ F(f)$: $F(G) \to F(K)$, must be the same. Further, if $1_G:G \to G$, is the identity homomorphism on G, then $F(1_G)$ must equal $1_{F(G)}:F(G) \to F(G)$, the identity set map on F(G).

That's all there is to functors: objects go to objects, and maps go to maps, so that identities go to identities, compositions go to compositions, and hence isomorphisms go to isomorphisms.

**Remark**: Some functors change the direction of maps, so that if $f:X \to Y$, then $F(f):F(Y) \to F(X)$, and $F(g \circ f) = F(f) \circ F(g)$. Such functors are called "contravariant", while functors that do not change direction

are called "covariant".

Let's look at one more commonly used "free" functor to groups, the "free abelian group" on a given set. We approach it backwards: instead of giving the construction and then stating the properties it has, we first state the desired properties, and then give two possible constructions. The moral is that the properties a thing has are more important than the particular choice of construction, provided some construction is possible.

**Definition**: Let S be a set, such as a finite set $S = \{a_1, a_2, ..., a_n\}$. By analogy with the mapping property satisfied by the previous free group construction, a "free abelian group on the set S" should be an abelian group Frab(S) containing the set S, and such that every set function $S \to G$, from S to an *abelian* group G, should extend uniquely to a group homomorphism $Frab(S) \to G$.

More generally, we require only an injection $S \to Frab(S)$, and that for any set map $f: S \to G$ there is a unique group homomorphism $Frab(S) \to G$ such that the composition $S \to Frab(S) \to G$ equals f.

**Exercise #43)** If a construction exists satisfying the (more general) property above of a free abelian group, prove it satisfies the axioms of a functor from sets and functions to (abelian) groups and homomorphisms.

**Theorem**: Free abelian groups Frab(S) exist for any set S.
**proof sketch**: Assume for simplicity $S = \{a_1, a_2, ..., a_n\}$ is finite. We can give a construction analogous to the previous one, and then make it abelian. I.e. we can consider words of form $(a_1)^{r_1} (a_2)^{r_2} ... (a_n)^{r_n}$, and multiply by rearranging the letters until all of the same letters are adjacent, and then using the exponent law to simplify. For example, $\{(a_1)^{r_1} (a_2)^{r_2} ... (a_n)^{r_n}\} \cdot \{(a_1)^{s_1} (a_2)^{s_2} ... (a_n)^{s_n}\} = (a_1)^{r_1+s_1} (a_2)^{r_2+s_2} ... (a_n)^{r_n+s_n}$. End of sketch.

As an exercise we give a second construction of free abelian groups, using product groups.
**Exercise #44)**: If $S = \{a_1, a_2, ..., a_n\}$, prove that the product $\mathbf{Z}^n = \mathbf{Z} \times \mathbf{Z} \times ... \times \mathbf{Z}$, (of n factors), together with the injection $f: S \to \mathbf{Z}^n$, (taking $a_j$ to the n tuple $e_j = (0,...,0,1,0,...,0)$ having 1 in the jth position, and

0's elsewhere), is a free abelian group on S. I.e. check the mapping property for free abelian groups is satisfied. [that is, show how to define the group homomorphism $\varphi_* : \mathbf{Z}^n \to G$, associated with a set map $\varphi: S \to G$ to an abelian group G, and show your $\varphi_*$ is the unique group map with $\varphi_* \circ f = \varphi$.]

**Exercise #45):** If S is any set, possibly infinite, let F be the set of those functions $\alpha: S \to \mathbf{Z}$ which have non zero values only at a finite number of points of S. Show that F, with pointwise addition of functions, is a free abelian group on the set S **QED. for theorem.**

**Terminology**: A subset on which an abelian group is free, is called a basis of the (free abelian) group. In particular, the set $\{e_j\}$ in $\mathbf{Z}^n$ in Ex. #46 is called the "standard basis" of $\mathbf{Z}^n$.

**Remark**: If $S = \{a_1, a_2, \ldots, a_n\}$, note that the "exponential map" taking $(r_1, \ldots, r_n)$ to the "word" $(a_1)^{r1}\,(a_2)^{r2} \ldots (a_n)^{rn}$ is an isomorphism from $\mathbf{Z} \times \mathbf{Z} \times \ldots \times \mathbf{Z}$ to Frab(S) as it was defined in the first sketch of proof of the Theorem given above.

**Looking ahead**: As we begin our study of "solvability" of polynomial equations by formulas involving radicals, we study the structure of "fields" generated by the roots of polynomials. We will use an automorphism functor associating to a nested pair of fields their "Galois group", automorphisms of the larger field which restrict to the identity on the smaller field Since groups are simpler than field extensions, we will gain an advantage in our study of fields and the polynomials which give rise to them.

The amazing triumph of this tool, due to Galois himself, is its complete success in resolving the question of solvability of polynomial equations by radicals. The Galois group of a polynomial, i.e. of the field generated by its roots, determines completely whether there is an expression for the roots of the polynomial in terms of the coefficients of the polynomial, using only radicals and rational arithmetic. Next we discuss how this works.