6. A SECOND ROUND OF THEORY

§6.1. Groups of Cosets

If H is a subgroup of G we have a set of right cosets $\{gH \mid g \in G\}$ whose size, if G is finite, is $|G|/|H|$. It would be nice if we could make this set into a group, for if we denoted this group by G/H we would have, in a certain sense, decomposed G into the two groups H and G/H. But to do this we'd need to define the product of two right cosets. A very natural definition is simply $aH.bH = abH$. But there's a potential problem of *well-definedness*.

If $aH = a'H$ and $bH = b'H$ it needn't be that $a = a'$ and $b = b'$. So we would need to check that, in all cases, $abH = a'b'H$.

Example 1:

Let $G = \mathbf{S}_3$ and let $H = \{I, (12)\}$, the cyclic subgroup generated by (12). The right cosets here are:

$$H = \{I, (12)\} = (12)H,$$
$$(123)H = \{(123), (23)\} = (23)H,$$
$$(132)H = \{(132), (13)\} = (13)H.$$

If our multiplication of cosets was valid we'd have the contradiction:

$$(123)H \times (132)H = 1H = H \text{ while}$$

$$(23)H \times (13)H = (132)H \neq H.$$

What's wrong isn't our definition so much as the subgroup H itself. If H was the right sort of subgroup this multiplication of cosets would have worked perfectly.

§6.2. Normal Subgroups and Quotient Groups

Évariste Galois, in his quest to find a way of deciding whether a given polynomial was soluble by radicals, invented groups and subgroups and he noticed that only certain subgroups were suitable. He called these 'normal' subgroups.

A subgroup is **normal** if its left and right cosets are the same. **Notation: $\mathbf{H \trianglelefteq G}$**. Clearly every group is normal in itself because in that case there is only one left coset and only one right coset, namely the whole group in each case. Also the identity subgroup {1} is a normal subgroup of any group because the left and right cosets all have the form {g} for $g \in G$. Some groups have no other normal subgroups and for this reason they play a special role in group theory, as we'll see in a later chapter.

At the other extreme there are groups where every subgroup is normal. Clearly these include all the abelian groups but, interestingly, there are also certain non-abelian groups with this property. But usually a non-abelian group will have some non-normal subgroups.

Example 2: If $G = \mathbf{S}_3$ and K = {I, (123), (132)} the left cosets of K in G are:

I (123) (132)	(12) (13) (23)

But these are also the right cosets of K in G. So the left and right cosets of K are the same and hence K is a normal subgroup of G.

But for H = {I, (12)} this isn't so. The left cosets are:

I (12)	(123) (23)	(132) (13)

while the right cosets are:

I (12)	(123) (13)	(132) (23)

A natural way to define multiplication of cosets is:

$$a\mathrm{H}.b\mathrm{H} = ab\mathrm{H}$$

with a similar definition for left cosets. As indicated earlier, the problem with this definition is that it depends on the choice of representative. Remember that for any $b \in a\mathrm{H}$ we have $b\mathrm{H} = a\mathrm{H}$. Any element of the coset can be used as the representative. It's important that our definition be *well-defined*, that is, the answer shouldn't depend on our choice of representative. Only for normal subgroups does this work.

Theorem 1: If $\mathrm{H} \trianglelefteq \mathrm{G}$ then multiplication of right cosets is well-defined.

Proof: Suppose $\mathrm{H} \trianglelefteq \mathrm{G}$ and suppose $a\mathrm{H} = a'\mathrm{H}$ and

bH = b'H.
Then $a' = ah$ and $b' = bk$ for some $h, k \in$ H.
Thus $a'b' = ahbk$. Now $hb \in$ H$b = b$H (this is where the normality of H comes in) so $hb = bh'$ for some $h' \in$ H.
Thus $a'b' = ahbk = abh'k \in ab$H and so $a'b'$H = abH. ☺👋

It isn't difficult to check that if H isn't a normal subgroup of G then coset multiplication is not well-defined and so we don't have a quotient group. Normal subgroups are precisely those subgroups for which the multiplication of cosets works.

If H is a normal subgroup of G, the corresponding **quotient group G/H** is the set of (left or right) cosets with aH.bH defined to be abH. The following are easily checked.

Theorem 2:
(1) The identity element of G/H is the coset H itself.
(2) If G is finite |G/H| = |G|/|H|.
(3) Every subgroup of an abelian group is normal.
(4) Every group is a normal subgroup of itself.
(5) The trivial subgroup is a normal subgroup of any group. ☺

Example 3: Let G = $\mathbb{Z}_9^{\#}$ = {1, 2, 4, 5, 7, 8} under multiplication modulo 9 and let H = {1, 8} be the cyclic subgroup generated by 8. Since G is abelian, H is a normal subgroup of G.

The cosets are H = {1, 8}, 2H = {2, 7} and 4H = {4, 5} and the group table for G/H is:

	H	**2H**	**4H**
H	H	2H	4H
2H	2H	4H	H
4H	4H	H	2H

The **index** of a subgroup H of a group G is the number of right cosets. (This will be the same as the number of left cosets). If this is finite we denote it by |G:H|. If H is normal in G this is the same as |G/H| and if G is finite we can write |G:H| as |G|/|H|.

But you can have subgroups of finite index even in infinite groups. For example, under addition, the group of integers has a subgroup of index 2, namely the even integers. The two cosets are the even integers and the odd integers. The case of index 2 is interesting, especially in non-abelian groups, as the next theorem shows.

Theorem 3: Subgroups of index 2 are always normal.
Proof: A subgroup of index 2 is one that has two left cosets and two right cosets. But since one left coset is the subgroup itself the other must be the complement. The same is true for the right cosets and so left cosets and right cosets are identical. ☺✋

Theorem 4: For all n, $\mathbf{A}_n$ is a normal subgroup of $\mathbf{S}_n$.
Proof: For $n \geq 2$ $\mathbf{A}_n$ has index 2 in $\mathbf{S}_n$. For $n = 1$ $\mathbf{A}_n = \mathbf{S}_n$. ☺✋

Theorem 5: A subgroup H of G is normal if and only if $g^{-1}hg \in H$ for all $g \in G$, $h \in H$.
Proof: $Hg = gH$ if and only if $g^{-1}Hg = H$. ☺✋

Theorem 6: The order of gH in G/H divides the order of g in G.
Proof: If $n = |g|$ then $g^n = 1$ and so $(g\mathrm{H})^n = g^n\mathrm{H} = \mathrm{H}$. ☺✋

Example 4: Let G be the following group of order 8 and let H = {1, 3}.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	2	3	4	5	6	7	8
2	2	3	4	1	6	7	8	5
3	3	4	1	2	7	8	5	6
4	4	1	2	3	8	5	6	7
5	5	8	7	6	3	2	1	4
6	6	5	8	7	4	3	2	1
7	7	6	5	8	1	4	3	2
8	8	7	6	5	2	1	4	3

The cosets are

1 3	2 4	5 7	6 8

and the group table for G/H is:

	H	**2H**	**5H**	**6H**
H	H	2H	5H	6H
2H	2H	H	6H	5H
5H	5H	6H	H	2H
6H	6H	5H	2H	H

For example 5H.2H = 8H = 6H. We multiply the representatives in the original group, and then look to see which coset it is in. We must not write the product as 8H, even though this is correct, because in a group table every element in the body of the table must be written exactly as it is at the top and the left-hand side.

Usually we save space by just writing down the representatives. This is OK so long as we remember that 5 here represents 5H = {5, 7} and not just the single element 5. So in the above example we could write:

G/H	**1**	**2**	**5**	**6**
1	1	2	5	6
2	2	1	6	5
5	5	6	1	2
6	6	5	2	1

§6.3. Homomorphisms

Abstract algebra studies algebraic systems, but not in isolation. Just as important as the structures themselves are functions between them, though not just any old function. The ones of interest are those that interact nicely with the algebraic operations. These are called ‘homomorphisms’. In linear algebra, for example, the homomorphisms are called ‘linear transformations’.

For groups, having just one operation of multiplication, we require homomorphisms to take products to products. But to state the definition in its

greatest generality we must be conscious of the fact that the operations in the two groups may be different.

A map f: (G, $*$) $\rightarrow$(H, $\bullet$) is a **homomorphism** if

$$f(x * y) = f(x) \bullet f(y) \text{ for all } x, y \in G.$$

If the operations of both groups are written multiplicatively this simplifies to

$$f(xy) = f(x)\, f(y).$$

But if both are written additively this would appear as

$$f(x + y) = f(x) + f(y).$$

Other variations are

$$f(x + y) = f(x)\, f(y) \text{ and}$$
$$f(xy) = f(x) + f(y).$$

This last version may remind you of the property of logarithms – the log of a product is the sum of the logs. In fact the logarithm function is indeed a homomorphism.

Example 5: Let G = ($\mathbb{R}^+$, $\times$) be the group of positive real numbers under multiplication and H = ($\mathbb{R}$, +), the group of all real numbers under addition. Then $f(x) = \log(x)$ is a homomorphism from G to H.

There's a whole family of 'morphisms' all with Latin names. If you have a good knowledge of Latin you might be able to guess their definitions. The basic one is the *homo*morphism, meaning something like 'similar shape'. The others are *endo*morphisms, *epi*morphisms, *iso*morphisms, *mono*morphisms and *auto*morphisms.

A homomorphism f: G$\rightarrow$ H is:

an **epimorphism** if it is onto;
a **monomorphism** if it is 1-1;
an **isomorphism** if it is both 1-1 and onto;
an **endomorphism** if H = G;
an **automorphism** if it is 1-1 and onto and H = G.

So in example 5, $f(x)$ is an isomorphism from G to H.

Example 6:
(1) If G is the group:

	1	**2**	**3**	**4**
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

the function f: G$\rightarrow \mathbb{R}^{\#}$ defined by $f(1) = f(2) = 1$ and $f(3) = f(4) = -1$ is a homomorphism.

(2) For all *groups* G, H the map f: G$\rightarrow$H defined by $f(x) = 1$ is a homomorphism. It's called the **trivial homomorphism**.

(3) If H $\leq$ G the map f: H$\rightarrow$G defined by $f(x) = x$ is a monomorphism, called the **identity homomorphism**.

(4) f: GL(n, $\mathbb{R}$)$\rightarrow \mathbb{R}^{\#}$ defined by f(A) = |A| (determinant of A) is an epimorphism.

(5) The exponential function f: $\mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^x$ is an isomorphism since

$$e^{x+y} = e^x.e^y.$$

It is the inverse of the log function.

(6) The conjugation map f: $\mathbb{C} \to \mathbb{C}$ defined by $f(z) = \bar{z}$ is an automorphism.

(7) For any group G the map f: G $\to$ G defined by $f(x) = x$ is an automorphism.

(8) If H is a normal subgroup of G then f: G $\to$ G/H defined by $f(x) = x$H is an epimorphism.

(9) If $g \in$ G the map f: G$\to$G defined by f(x) = $g^{-1}xg$ is an automorphism.

Theorem 7: If f: G$\to$H is a homomorphism then

(1) $f(1) = 1$

(2) $f(a^n) = f(a)^n$ for all $a \in$ G and all $n \in \mathbb{Z}$.

(3) $|f(a)|$ divides $|a|$ for all $a \in$ G. ☺

The significance of an isomorphism is that it relates two groups that are group-theoretically the same. They may look quite different. They may use different notation and involve quite different operations. But if there's an isomorphism between them they're structurally equivalent, or as we say, isomorphic. Isomorphic groups

have the same group-theoretic properties. They differ only in notation.

If there exists an isomorphism f: G $\rightarrow$ H we say that G is **isomorphic** to H. **Notation:** G $\cong$ H.

Theorem 8: Isomorphism is an equivalence relation.
Proof: *Reflexive:* The identity map is an isomorphism.
Symmetric: The inverse of isomorphism is an isomorphism.
Transitive: The product of two isomorphisms is an isomorphism. ☺✋

§6.4. Isomorphism Theorems

Associated with any homomorphism are two very important subgroups, the kernel and the image. The kernel is a subgroup (in fact a normal subgroup) of the group being mapped out of and the image is a subgroup of the group being mapped into.

If f:G$\rightarrow$H is a homomorphism, the **kernel** of f is the set of elements which map to the identity. That is, **ker(f)** = $\{g \in G \mid f(g) = 1\}$.

The **image** is **im(f)** = $\{f(g) \mid g \in G\}$. [Recall that for a linear transformation between vector spaces the kernel is the set of vectors that map to the zero vector, this being the identity element of the additive part of the vector space.]

Example 7:
If f: $\mathbb{R}^{\#} \to \mathbb{R}^{\#}$ is defined by $f(x) = x^2$ then $\ker(f) = \{\pm 1\}$ and $\text{im}(f) = \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$.

1st ISOMORPHISM THEOREM

Theorem 9: If f:G→H is a homomorphism and K = ker(f) then

(1) $K \trianglelefteq G$;
(2) $\text{im(f)} \leq H$;
(3) $G/K \cong \text{im}(f)$.

Proof:
(1) Let $a, b \in K$. Then $f(a) = f(b) = 1$ and so $f(ab) = 1$ and $f(a^{-1}) = 1$. Thus $\ker(f) \leq G$.

If $k \in K$ and $g \in G$ then $f(g^{-1}kg) = f(g)^{-1}f(k)f(g)$
$= f(g)^{-1}f(g) = 1.$

Thus ker(f) is a normal subgroup of G.

(2) Let $f(a), f(b) \in \text{im}(f)$.
Then $f(b)^{-1}f(a) = f(b^{-1}a) \in \text{im}(f)$ and $f(a)^{-1} = f(a^{-1}) \in \text{im}(f)$.

(3) Define Φ:G/K $\to$ im(f) by $\Phi(gK) = f(g)$. Since $\Phi(gK)$ is defined in terms of a representative of the coset we must first check that this is well-defined, that is, if $aK = bK$ then $\Phi(aK) = \Phi(bK)$.
Suppose $aK = bK$. Then $b^{-1}a \in K$. Hence $f(b^{-1}a) = 1$ and so $f(b)^{-1}f(a) = 1$ and so $f(a) = f(b)$.
The reverse calculation checks that Φ is 1-1. For if $\Phi(aK) = \Phi(bK)$ then $f(a) = f(b)$ and so $f(b^{-1}a) = 1$.

Thus $b^{-1}a \in K$ and so $aK = bK$.
Finally, it's clear that Φ is onto. Hence Φ is an isomorphism and so $G/K \cong \text{im}\theta$. ☺👋

If H, K are subgroups of a group G there are three important ways in which we could combine them:

$$H \cap K,\ H \cup K \text{ and } HK.$$

You already know what the first two are.
We define $HK = \{hk \mid h \in H, k \in K\}$.
Are these subgroups? The following can be easily shown:

	Is it a subgroup?
$H \cup K$	never (unless one is a subset of the other)
HK	sometimes
$H \cap K$	always

I have left it as an exercise to prove the statements about $H \cup K$ and $H \cap K$. We will soon explore situations when HK is a subgroup. But because the union of two subgroups is virtually never a subgroup it has no significance in group theory.

The following are easily shown and are left as exercises.

neither H, K normal	$H \cap K$ is a subgroup
one of H, K normal	$H \cap K$ is a subgroup but may not be normal
both H, K normal	$H \cap K$ is a normal subgroup

We will now show the following:

neither H, K normal	HK may not be a subgroup
one of H, K normal	HK is a subgroup
both H, K normal	HK is a normal subgroup

Example 8: HK may not be a subgroup: Let $G = S_3$ and let $H = \{I, (12)\}$ and $K = \{I, (13)\}$. Then, since $(12)(13) = (123)$, $HK = \{I, (12), (13), (123)\}$. This has 4 elements and G has 6. Since 4 does not divide 6 HK can't be a subgroup of G. Indeed $(123)(123) = (132)$ so HK is not closed.

Theorem 10: If H, K are subgroups of G and at least one of them is a normal subgroup of G then HK is a subgroup of G.

Proof: Suppose that K is normal in G.

Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Then $(h_1k_1)(h_2k_2) = h_1h_2(h_2^{-1}k_1h_2)k_2$.

Since $h_1h_2 \in H$ and $h_2^{-1}k_1h_2 \in K$, by normality and $(h_2^{-1}k_1h_2)k_2 \in K$ by closure, the above product is in HK.

Clearly $1 = 1.1 \in HK$.

Let $h \in H$ and $k \in K$.

Then $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}) \in HK$.

If H is a normal subgroup then a similar proof shows that HK is a subgroup of G. ☺✋

Theorem 11: If both H and K are normal subgroups of G then HK is a normal subgroup of G.

Proof: By the above theorem we only need to check normality.

Let $h \in H$, $k \in K$ and $g \in G$.

Then $g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$. ☺✋

2nd ISOMORPHISM THEOREM

Theorem 12: If H and K are normal subgroups of G then:

(1) $H \cap K$ is a normal subgroup of G;

(2) HK is a normal subgroup of G;

(3) $HK/K \cong H/(H \cap K)$.

Proof: The map $h \to hK$ is a homomorphism with kernel $H \cap K$ and image HK.

Now use the First Isomorphism Theorem. ☺✋

3rd ISOMORPHISM THEOREM

Theorem 13: If $H \leq K \leq G$ with both H, K being normal in G then:

(1) $K/H \trianglelefteq G/H$;

(2) $(G/H)/(K/H) \cong G/K$.

Proof: The map $gH \to gK$ is a well-defined (why?) homomorphism with kernel K/H and image G/K. Now use the First Isomorphism Theorem. ☺✋

Examples 9:

(1) $f: \mathbb{C} \to \mathbb{R}$ where $f(x + iy) = y$.

This is a homomorphism with $\ker(f) = \text{im}(f) = \mathbb{R}$.

Hence $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$.

(2) G = GL(n, $\mathbb{R}$) is the set of $n \times n$ invertible real matrices, f: G$\to \mathbb{R}^{\#}$ where f(A) = |A|.

K = SL(n, $\mathbb{R}$) is the set of those matrices with determinant 1,

H = set of diagonal matrices in G,

L = set of scalar matrices in G.

ker(f) = K and im(f) = $\mathbb{R}^{\#}$ since for all $x \in \mathbb{R}^{\#}$, the determinant of the diagonal matrix
diag(x, 1, 1, ...) is x. Hence G/K $\cong \mathbb{R}^{\#}$.

H $\cap$ K is the set of matrices of form $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ and HK = G (because every invertible matrix can be transformed to a diagonal matrix using elementary matrices with determinant 1.)
Hence, by the 2nd and 3rd Isomorphism Theorems,
H/(H $\cap$ K) $\cong$ G/K $\cong \mathbb{R}^{\#}$ and (G/L)/(K/L) $\cong$ G/K$\cong \mathbb{R}^{\#}$.

§6.5. Conjugacy Classes

The **conjugate** of x by g is defined to be

$$x^g = g^{-1}xg.$$

The exponential notation is justified by the following properties of conjugation, which are analogous to powers.

(1) $x^{gh} = (x^g)^h$

(2) $(xy)^g = x^g\, y^g$

But note that $g^g = g$ for all g, something which has no counterpart for powers.

Example 10: In $\mathbf{D}_8 = \langle A, B \mid A^4, B^2, BA = A^{-1}B \rangle$ the conjugate of A by B is

$B^{-1}AB = BAB$

$= A^{-1}BB$

$= A^{-1}$

$= A^3$.

The relation 'is a conjugate of' is an equivalence relation and the equivalence classes are called **conjugacy classes**.

Example 11: The conjugacy classes of $\mathbf{D}_8$ are:

$\{1\}, \{A, A^3\}, \{A^2\}, \{B, BA^2\}, \{BA, BA^3\}$.

The **centraliser** of g in $G = \{x \in G \mid gx = xg\}$. It's easy to check that it's a subgroup of G, though, as the next example shows, it needn't be a normal subgroup.
Notation: $\mathbf{C_G(g)}$ or just $\mathbf{C(g)}$.

Example 12:
The centraliser of (12)(34) in $\mathbf{S}_4$ = {I, (12), (34), (1324), (1423), (12)(34), (13)(24), (14)(23)}

The **centre** of G is $\mathbf{Z(G)}=\{x \mid \forall g\ [xg = gx]\}$. It's the intersection of all the centralisers of the elements of G and is therefore subgroup. But in fact, as is easily seen, it's a normal subgroup of G.

Example 13: $Z(\mathbf{D}_8) = \{1, A^2\}$.

Note that $g \in Z(G)$ if and only if $\{g\}$ is a conjugacy class, of size 1.

The **class equation** of a finite group G is:

$$|G| = h_1 + h_2 + ... + h_k$$

where $1 = h_1 \leq h_2 \leq ...$ are the sizes of the conjugacy classes. The number of h_i which equal 1 is $|Z(G)|$.

Example 14: The class equation for $\mathbb{Z}_4$ is:

$$4 = 1 + 1 + 1 + 1.$$

Example 15: The class equation for $\mathbf{S}_3$ is:

$$6 = 1 + 2 + 3$$

since the conjugacy classes are:

$$\{I\}, \{(123), (132)\}, \{(12), (13), (23)\}.$$

Example 16: The class equation for $\mathbf{S}_4$ is:

$$24 = 1 + 3 + 6 + 6 + 8$$

since the conjugacy classes correspond to the cycle structures. There are 6 permutations with cycle structure $(\times\times)$, 6 with cycle structure $(\times\times\times)$, 8 with cycle structure $(\times\times\times\times)$ and 3 with cycle structure $(\times\times)(\times\times)$.

The next example shows how important counting is in finite group theory. In this case, the fact that normal subgroups are made up of entire conjugacy classes can help us find normal subgroups.

Example 17: Suppose $H \leq \mathbf{S}_4$ with $|H| = 12$.
Since $|\mathbf{S}_4:H| = 2$, H is normal and so must be made up of complete conjugacy classes. One of them must consist of the identity so we have to be able add some of the numbers 3, 6, 6 and 8 to get 11. Clearly 3 + 8 is the only possibility. So H must contain all the elements with cycle structures I, (××)(××), and (×××) in which case $H = \mathbf{A}_4$. Hence $\mathbf{A}_4$ is the only subgroup of order 12 in $\mathbf{S}_4$.

Theorem 14: The number of conjugates of x in G is:
the index of its centraliser in G .

Proof: $x^g = x^h$ if and only if $xgh^{-1} = x$ if and only if $gh^{-1} \in C_G(x)$ if and only if $gC_G(x) = hC_G(x)$. So $f(x^g) = gC_G(x)$ is a well-defined 1-1 and onto map between the conjugacy class of x and the set of right cosets of the centraliser $C_G(x)$. ☺✋

$$\textbf{\#conjugates of } x \textbf{ in G} = \frac{|\mathbf{G}|}{|\mathbf{C_G}(x)|}.$$

Example 18: The class equation for $\mathbf{A}_4$ is:

$$12 = 1 + 3 + 4 + 4.$$

The conjugacy classes for $\mathbf{S}_4$ that contain elements of $\mathbf{A}_4$ are I, (××)(××) and (×××) with sizes 1, 3 and 8 respectively. But the class containing all the 3-cycles splits into two conjugacy classes within $\mathbf{A}_4$.

To see this, consider the centralizer of one of these 3-cycles such as (123). Since there are 8 conjugates in $\mathbf{S}_4$

there must be 24/8 = 3 elements in its centralizer. Clearly these must be I, (123) and (132).

These are all in $\mathbf{A}_4$ so in $\mathbf{A}_4$ the centralizer has order 3. The number of conjugates must therefore be 12/3 = 4. So if each 3-cycle has only 4 conjugates in $\mathbf{A}_4$ the 8 3-cycles must form 2 conjugacy classes of size 4 in S_4.

How can this be? Well, if you conjugate (123) by only the even permutations you only get 4 conjugates. To get across to the other 4 you need to conjugate by an odd permutation.

Example 19: Find the numbers of conjugates of (123) and (12345) in $\mathbf{A}_5$.

Proof: Doing this by actually finding the conjugacy class is a lot of work, but the above theorem can help. The number of conjugates of (123) in $\mathbf{S}_5$ is the number of permutations in $\mathbf{S}_5$ with cycle structure (×××), which is 20. The order of $\mathbf{S}_5$ is 120, so by the above theorem $|C_{\mathbf{S}_5}(123)| = 120/20 = 6$.

Now it's clear that these 6 elements that commute with (123) are its 3 powers and its 3 powers times (45). How many of these are in $\mathbf{A}_5$? Only the first 3. So $|C_{\mathbf{A}_5}(123)| = 3$ and so the number of conjugates of (123) in $\mathbf{A}_5$ is 60/3 = 20. This time the conjugacy class doesn't split when we consider conjugates in $\mathbf{A}_5$.

In the case of (12345), there are 24 conjugates in S_5 and so $|C_{\mathbf{S}_5}(12345)| = 120/24 = 5$. These 5 elements that commute with (12345) are clearly its 5 powers, all of

which are in $\mathbf{A}_5$. So $|C_{\mathbf{A}_5}(12345)| = 5$ and so the number of conjugates of (12345) in $\mathbf{A}_5$ is 60/5 = 12.

So the conjugacy class containing all the 3-cycles in $\mathbf{S}_5$ remains a single class in $\mathbf{A}_5$ but the conjugacy class of size 24 containing all the 5-cycles in $\mathbf{S}_5$ splits into two classes of size 12 when we're considering classes in $\mathbf{A}_5$. In the latter case you'd need to conjugate by an odd permutation to take you from one lot of 12 to the other.

Theorem 15: If G/Z(G) is cyclic then G is abelian (and so G = Z(G)).
Proof: Suppose G/Z(G) is generated by gZ(G). Then every element of G/Z(G) has the form $(g\mathrm{Z}(\mathrm{G}))^r = g^r\mathrm{Z}(\mathrm{G})$ and so every element of G has the form g^rz for some integer r and some z ∈ Z(G).
Since $g^r u$ commutes with $g^s v$ for all integers r, s and all u, $v \in$ Z(G), it follows that G is abelian. ☺👋

If p is prime, a **finite *p*-group** is a group of order p^n for some n. Whenever we say that a group is a p-group we are assuming that p is prime.

Example 20: The dihedral group of order 8 is a p-group for $p = 2$.

Theorem 16: The centre of a non-trivial finite p-group G is non-trivial.
Proof: Suppose that Z(G) = 1. Then G has only one conjugacy class of size 1. All the others must be proper

powers of p, and hence multiples of p. Thus the sum of the sizes of the conjugacy classes would be of the form $kp + 1$ yet $|G|$ is a multiple of p, contradicting the class equation. In fact $|Z(G)| \geq p$. ☺✋

Theorem 17: Groups of order p^2 (where p is prime) are abelian.
Proof: Suppose $|G| = p^2$ where p is prime. Since $Z(G)$ is non-trivial, $|Z(G)| = p$ or p^2. Thus $|G/Z(G)| = p$ or 1 and so is cyclic. Hence, by Theorem 15, G is abelian. ☺✋

Theorem 18: A finite p-group G has a subgroup of every order that divides $|G|$.
Proof: Let $|G| = p^n$ and let $1 \leq r \leq n$. We prove the result by induction on n. It is clearly true if $n = 1$ so suppose that $n \geq 2$. Let $r \leq n$.

Since $Z(G) > 1$ there is an element $z \in Z(G)$ of order p. Let $H = \langle z \rangle$ then $H \trianglelefteq G$.

By induction G/H has a subgroup of order p^{r-1} and so G has a subgroup of order p^r. ☺✋

In fact all finite groups have at least one subgroup of every prime power order that divides the order of the group, as we will see later.

§ 6.6. Commutators

In an abelian group G, $ab = ba$ for all $a, b \in G$. Now the equation $ab = ba$ can be written as $a^{-1}b^{-1}ab = 1$. In a non-abelian group, on the other hand, not all the elements of the form $a^{-1}b^{-1}ab$ are equal to the identity. They generate an important non-trivial subgroup.

A **commutator** in a group is an element of the form $a^{-1}b^{-1}ab$. We denote such an element by $\mathbf{[a, b]}$. So a, b commute if and only if $[a, b] = 1$.

Theorem 19: The following properties hold for commutators:

(1) $[b, a] = [a, b]^{-1}$.

(2) $g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg]$.

Proof: (1) $[b, a] = b^{-1}a^{-1}ba$

$= (a^{-1}b^{-1}ab)^{-1}$

$= [a, b]^{-1}$.

(2) $g^{-1}[a, b]g = g^{-1}a^{-1}b^{-1}abg$

$= g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg$

$= (g^{-1}ag)^{-1}(g^{-1}bg)^{-1}(g^{-1}ag)(g^{-1}bg)$

$= [g^{-1}ag, g^{-1}bg]$. ☺✋

Example 21: If $a = (123)$ and $b = (1423)$ are permutations in $\mathbf{S}_4$ then:

$[a, b] = (123)^{-1}(1423)^{-1}(123)(1423)$
$= (132)(1324)(123)(1423)$
$= (243)$.

§ 6.7. The Derived Subgroup

So the inverse of a commutator is a commutator and a conjugate of a commutator is a commutator. We're well on the way to proving that the commutators form a normal subgroup except that the product of two commutators needn't be a commutator. So, instead of considering the *set* of all commutators we consider the *group generated by* all the commutators – that is, we consider all products of commutators. Now indeed we do have a normal subgroup.

The **derived subgroup** (**commutator subgroup**) of a group G is the subgroup $\mathbf{G'}$ generated by the commutators. Clearly it's a normal subgroup of G. It is also obvious that G is abelian if and only if $G' = 1$, so in a certain sense G' (or perhaps its size) measures how close the group is to being abelian.

Example 22: $\mathbf{S}_3' = \mathbf{A}_3$.

It might appear that we must compute all 36 commutators $[a, b]$ where $a, b \in \mathbf{S}_3$, which would be a lot of work. But after computing just the one commutator $[(12), (13)] = (12)(13)(12)(13) = (132)$ we conclude that G' must contain (132), and hence all its powers. Thus far we obtain {I, (132), (123)}, which is $\mathbf{A}_3$, the group of even permutations. Could there be any more? No, because

clearly in groups of permutations all commutators are even permutations.

We get all the 3 even permutations and we certainly can't get any odd ones. So the question is settled with a minimum of computation. In finding the derived subgroup we almost never have to compute the commutators themselves. Usually we use the following theorem.

Theorem 20: (1) G/G' is abelian.

(2) If G/H is abelian then $G' \leq H$.

Proof: (1) Let aG', bG' be two elements of G/G'.

Then $[aG', bG'] = (aG')^{-1}(bG')^{-1}(aG')(bG')$

$= a^{-1}b^{-1}abG'$

$= [a, b]G'$

$= G'$ since $[a, b] \in G'$.

(2) Suppose G/H is abelian.

Then for all $a, b \in G$, $[aH, bH] = H$ (the identity element of G/H).

Thus $[a, b]H = H$ so $[a, b] \in H$.

Hence H contains all the commutators, and being a subgroup, it contains all products of commutators.

Hence G' lies inside H. ☺👋

A simple way of stating the above theorem is to say that:

The derived subgroup is the smallest normal subgroup for which the quotient is abelian.

Example 23: I'll show that $\mathbf{S}_4' = \mathbf{A}_4$. By the parity argument of example 2 we easily see that $\mathbf{S}_4' \leq \mathbf{A}_4$. This can also be deduced from the above theorem and the fact that $\mathbf{S}_4/\mathbf{A}_4$ is abelian (after all it has order 2, 2 is prime, groups of prime order are cyclic, and cyclic groups are abelian). But why can't $\mathbf{S}_4'$ be smaller?

Suppose $\mathbf{S}_4'$ was smaller than $\mathbf{A}_4$. Then $|\mathbf{S}_4'|$ would have to properly divide 12. The possibilities are 1, 2, 3, 4 and 6. Now we know that the sizes of the conjugacy classes in S_4 are 1, 3, 6, 6 and 8 (these are the numbers of elements of each cycle structure – remember that two permutations are conjugate in $\mathbf{S}_n$ if and only if they have the same cycle structure). And a normal subgroup, such as G', must be made up of entire conjugacy classes. The only possibility would be for G' to have order 4 and be made up of the classes of sizes 1 and 3.

So why can't G' have order 4? Because then G/G' would have order 6. And what's wrong with that? Well groups of order 6 (twice a prime) are cyclic group or dihedral. But G/G' is abelian so it isn't dihedral. And why can't G/G' be the cyclic group of order 6? Why then it would have to have elements of order 6 and yet $\mathbf{S}_4$ doesn't contain any such permutations. So by patient detective work we get a contradiction to the assumption that S_4' is smaller than $\mathbf{A}_4$. It follows therefore that $\mathbf{S}_4'$ is equal to $\mathbf{A}_4$.

EXERCISES FOR CHAPTER 6

EXERCISE 1: Let *G* be the following group:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	1	2	3	4	5	6	7	8
2	2	1	4	3	7	8	5	6
3	3	4	2	1	6	7	8	5
4	4	3	1	2	8	5	6	7
5	5	7	8	6	2	3	1	4
6	6	8	5	7	4	2	3	1
7	7	5	6	8	1	4	2	3
8	8	6	7	5	3	1	4	2

(a) Find the elements of H, the cyclic subgroup generated by 2.
(b) Write down the left and right cosets of H and show that H is a normal subgroup of G.
(c) Representing each coset of H by one of its elements (say the smallest) write out the group table for G/H.
(d) Find Z(G).
(e) Explain why G/H is not cyclic.
(f) Show that $G' = Z(G)$.
(g) Show that every subgroup of G is a normal subgroup.
(h) Find all the subgroups of G.

EXERCISE 2: G is a group with the following group table:

	1	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	4	5	6	1	2
4	4	3	2	1	6	5
5	5	6	1	2	3	4
6	6	5	4	3	2	1

Which of the following functions from G to G are homomorphisms?

x	**1**	**2**	**3**	**4**	**5**	**6**
***a*(*x*)**	2	3	4	5	6	1
***b*(*x*)**	1	2	1	2	1	2
***c*(*x*)**	1	3	1	5	1	3
***d*(*x*)**	1	2	3	4	5	6
***e*(*x*)**	1	6	5	4	3	2
***f*(*x*)**	1	4	5	6	3	2
***g*(*x*)**	1	1	1	2	3	4
***h*(*x*)**	1	1	1	1	1	1

EXERCISE 3: Let $\mathbb{R}^+$ denote the group of positive real numbers under multiplication, let $\mathbb{R}$ denote the group of all real numbers under addition and let $H = \{\pm 1\}$.
Use the fact that f: $\mathbb{R}^+ \to \mathbb{R}$ defined by $f(x) = \log(x)$ is a homomorphism to show that

$$\mathbb{R}^{\#}/H \cong \mathbb{R}.$$

EXERCISE 4: Prove that $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^{\#}$.
[**HINT:** Think of a homomorphism from $GL(n, \mathbb{R})$ to $\mathbb{R}^{\#}$.]

EXERCISE 5: Prove that if $f(x) = x^{-1}$ is an automorphism from a group G to itself then G is abelian.

EXERCISE 6: G is a non-abelian group of order 27. Find |Z(G)|.

EXERCISE 7: Show that $H \cup K$ is never a subgroup of a group G unless one of H, K is inside the other.

EXERCISE 8: Prove that if H, K are subgroups of G then so is $H \cap K$.

EXERCISE 9: Prove that if H, K are normal subgroups of G then so is $H \cap K$.

SOLUTIONS FOR CHAPTER 6

EXERCISE 1: (a) H = {1, 2}.
(b) The left cosets are: H = {1, 2}, 3H = {3, 4}, 5H = {5, 7}, 6H = {6, 8}. These are also the right cosets. Since the left and right cosets are the same H is normal in G.
(c)

	1	**3**	**5**	**6**
1	1	3	5	6
3	3	1	6	5
5	5	6	1	3
6	6	5	3	1

(d) Z(G) = H = {1, 2}.
(e) From (d) we can see that every non-trivial element of G/H has order 2 so G/H has no element of order 4. Alternatively we could appeal to the theorem that for a non-abelian group G/Z(G) can never be cyclic.
(f) G/H is abelian so $G' \leq H$. But $G' \neq 1$ since G is non-abelian. Hence $G' = H = Z(G)$.
(g) We need to systematically find all the subgroups of G. By Lagrange's Theorem the possible orders of subgroups are 1, 2, 4 and 8 and there's only one subgroup, {1} of order 1 and only one of order 8, the group *G* itself. Both of these are clearly normal.

Subgroups of order 2 are cyclic, generated by an element of order 2. Looking down the diagonal of the group table for *G* we see that the only candidate is 2. As we've seen, this generates H and this is a normal subgroup. This leaves subgroups of order 4. Since these

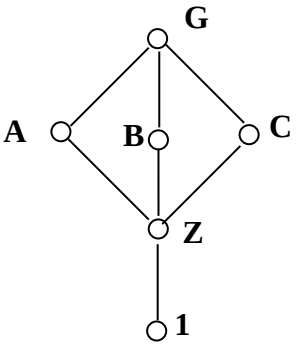
are of index 2, and subgroups of index 2 are normal, these subgroups are normal.

(h) It remains to find the subgroups of order 4. Now there are only two types of group of order 4 – the cyclic group of order 4 and the group known as $\mathbf{V}_4$, or $\mathbf{C}_2 \otimes \mathbf{C}_2$ with 3 elements of order 4. Since G only has one element of order 2 there can't be any of the latter type. So the subgroups of order 4 are cyclic, generated by an element of order 4. There are 6 elements of order 4 but, as pairs of these generate a single cyclic subgroup there are just 3 subgroups of order 3: {1, 2, 3, 4}, {1, 2, 5, 7} and {1, 2, 6, 8}.

The subgroups of G are thus:

G = {1, 2, 3, 4, 5, 6, 7, 8}, A = {1, 2, 3, 4},
B = {1, 2, 5, 7}, C = {1, 2, 6, 8}, Z = {1, 2} and the trivial subgroup {1} that we always denote by the symbol 1.

We can draw a picture of these, known as a lattice of subgroups, as follows:



EXERCISE 2:

$a(x)$ is a NOT a homomorphism since the identity is not fixed.

$b(x)$ is a homomorphism. Even permutations map to 1 and odd permutations map to 2.

$c(x)$ is NOT a homomorphism.
If it was then $\ker(c) = \{1, 3, 5\}$ and so $G/\ker(c)$ would have order 2.
But $G/\ker(c) \cong \text{im}(c)$ and $\text{im}(c)$ has order 3.

$d(x)$ is a homomorphism.
It's the identity automorphism.

$e(x)$ is a homomorphism. We can see this by taking the group table for G, replacing each element by its image under e. We then rearrange the rows and columns and check that we get back to the original group table.

	1	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	1	6	5	4	3
3	3	4	5	6	1	2
4	4	3	2	1	6	5
5	5	6	1	2	3	4
6	6	5	4	3	2	1

	1	**6**	**5**	**4**	**3**	**2**
1	1	6	5	6	3	2
6	6	1	2	3	4	5
5	5	4	3	2	1	6
4	4	5	4	1	2	3
3	3	2	1	6	5	4
2	2	3	4	5	6	1

	1	**2**	**3**	**4**	**5**	**6**
1	1	2	3	6	5	6
6	6	5	4	3	2	1
5	5	6	1	2	3	4
4	4	3	2	1	4	5
3	3	4	5	6	1	2
2	2	1	6	5	4	3

	1	**2**	**3**	**4**	**5**	**6**
1	1	2	3	6	5	6
2	2	1	6	5	4	3
3	3	4	5	6	1	2
4	4	3	2	1	4	5
5	5	6	1	2	3	4
6	6	5	4	3	2	1

$f(x)$ is NOT a homomorphism.
For example $f(2 \times 3) = f(6) = 2$ while $f(2).f(3) = 4.5 = 6$.

$g(x)$ is NOT a homomorphism since im(g) has order 4 and so cannot be a subgroup of G.

$h(x)$ is a homomorphism. It's the trivial homomorphism.

EXERCISE 3: $\ker(f) = \{\pm 1\} = H$ so, by the First Isomorphism Theorem, $\mathbb{R}^{\#}/H \cong \mathbb{R}$.

EXERCISE 4: The map f:GL(n, $\mathbb{R}$) $\rightarrow \mathbb{R}^{\#}$ defined by f(A) = |A| is a homomorphism. Its kernel is SL(n, $\mathbb{R}$) and its image is $\mathbb{R}^{\#}$. Hence, by the First Isomorphism Theorem, GL(n, $\mathbb{R}$)/SL(n, $\mathbb{R}$) $\cong \mathbb{R}^{\#}$.

EXERCISE 5: Let $x, y \in G$. Then $(xy)^{-1} = x^{-1}y^{-1}$. But $(xy)^{-1} = y^{-1}x^{-1}$ so $x^{-1}y^{-1} = y^{-1}x^{-1}$. This equation can be rearranged to give $xy = yx$. So every pair of elements commute and so G is abelian.

EXERCISE 6: By Lagrange's Theorem, $|Z(G)| = 1, 3, 9$ or 27.
Since G is non-abelian, $|Z(G)| \neq 27$. Since G is a p-group (for $p = 3$), $|Z(G)| > 1$.
Since G/Z(G) is not cyclic, $|Z(G)| \neq 9$. Hence $|Z(G)| = 3$.

EXERCISE 7: Suppose neither of these subgroups lies inside the other and that $H \cup K$ is a subgroup of G. Choose $g \in H$ so that $g \notin K$ and $h \in K$ so that $h \notin H$. Then, since both g, h belong to $H \cup K$, so does gh. Thus $gh \in H$ or $gh \in K$. If $gh \in H$ then $h = g^{-1}(gh) \in H$, a contradiction.
Similarly, if $gh \in K$ we get a contradiction.

EXERCISE 8: Let $a, b \in H \cap K$. Since $a, b \in H$ we have $ab \in H$. Similarly $ab \in K$, so $ab \in H \cap K$.
Clearly $1 \in H, K$. And a^{-1} is in both H, K so it belongs to $H \cap K$.

EXERCISE 9: By exercise 8 we only need to check normality. Let $h \in H \cap K$ and $g \in G$. Then since $h \in H$, $g^{-1}hg \in H$. Similarly $g^{-1}hg \in K$, so it belongs to $H \cap K$.