

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 number, 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 $aH \cdot bH = abH$. But there's a potential problem of *well-definedness*. If $aH = a'H$ and $bH = b'H$ we need to be sure that $abH = a'b'H$.

Example 1:

Let $G = S_3$ and let $H = \{I, (12)\}$, the cyclic subgroup generated by (12) . The right cosets here are:

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

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

$$\begin{aligned} (123)H \times (132)H &= 1H = H \text{ while} \\ (123)H \times (132)H &= (23)H \times (13)H = (132)H \neq H. \end{aligned}$$

What's wrong isn't our definition so much as the subgroup H . For the right sort of subgroup this multiplication of cosets works perfectly.

§6.2. Normal Subgroups and Quotient Groups

Definition: A subgroup is **normal** if its left and right cosets are the same. **Notation:** $H \trianglelefteq G$.

Example 2: In the above example, the left cosets of $K = \{I, (123), (132)\}$ are

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

But these are also the right cosets of K

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)
--------	------------	------------

Theorem 1: If H is a normal subgroup of G then multiplication of right cosets is well-defined.

Proof: Suppose H is a normal subgroup of G and suppose $aH = a'H$ and $bH = b'H$. Then $a' = ah$ and $b' = bk$ for some $h, k \in H$. Thus $a'b' = ahbk$. Now $hb \in Hb = bH$ (this is where the normality of H comes in) so $hb = bh'$ for some $h' \in H$. Thus $a'b' = ahbk = abh'k \in abH$ and so $a'b'H = abH$.

It isn't difficult to check that if H is not 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 quotient group construction works.

Definition: If H is a normal subgroup of G , the corresponding **quotient group** G/H is the set of cosets with $aH \cdot bH$ defined to be abH .

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

Theorem 3: Subgroups of index 2 are normal.

Proof: A subgroup of index 2 is one that has two left cosets and two right cosets. But since one left coset is H 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 , A_n is a normal subgroup of S_n .

Proof: For $n \geq 2$ A_n has index 2. For $n = 1$ $A_n = S_n$.

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: $Hg = gH$ iff $g^{-1}Hg = H$.

Theorem 6: The order of gH in G/H divides the order of g in G .

Proof: If $n = |g|$ then $g^n = 1$ then $(gH)^n = g^nH = H$ so $|gH|$ divides n .

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

	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	b	c	1	e	f	g	d
b	b	c	1	a	f	g	d	e
c	c	1	a	b	g	d	e	f
d	d	e	f	g	1	a	b	c
e	e	f	g	d	a	b	c	1
f	f	g	d	e	b	c	1	a
g	g	d	e	f	c	1	a	b

The cosets are

1 b	a c	d f	e g
-----	-----	-----	-----

and the group table for G/H is:

	H	aH	dH	eH
H	H	aH	dH	eH
aH	aH	H	eH	dH
dH	dH	eH	H	aH
eH	eH	dH	aH	H

Now let $L = \{1, a, b, c\}$. The cosets are:

1 a b c	d e f g
---------	---------

and the group table for G/L is:

	L	dL
L	L	dL
dL	dL	L

Now let $K = \{1, d\}$. The cosets are:

1 d	a e	b f	c g
-----	-----	-----	-----

and the group table for G/K is:

	K	aK	bK	cK
K	K	aK	bK	cK
aK	aK	bK	cK	K
bK	bK	cK	K	aK
cK	cK	K	aK	bK

§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, which interact nicely with the algebraic operations. These are called “homomorphisms”. For groups with 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 $\theta: (G, *) \rightarrow (H, \bullet)$ is a **homomorphism** if $\theta(x * y) = \theta(x) \bullet \theta(y)$ for all $x, y \in G$. If the operations of both groups are written multiplicatively this simplifies to $\theta(xy) = \theta(x)\theta(y)$, but if both are written additively this would appear as $\theta(x + y) = \theta(x) + \theta(y)$. Other variations are $\theta(x + y) = \theta(x)\theta(y)$ and $\theta(xy) = \theta(x) + \theta(y)$.

There's a whole family of "morphisms" all with Latin names. If you've a good knowledge of Latin you might be able to guess their definitions. The basic one is the homomorphism, meaning something like "similar shape". The others are endomorphisms, epimorphisms, isomorphisms, monomorphisms and automorphisms.

Definition: 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 $H = G$.

Examples 5:

(1) If G is the group:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

the function $\theta: G \rightarrow \mathbf{R}^\#$ defined by $\theta(1) = \theta(a) = 1$ and $\theta(b) = \theta(c) = -1$ is a homomorphism.

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

(3) If $H \leq G$ the map $\theta: H \rightarrow G$ defined by $\theta(x) = x$ is a monomorphism.

(4) $G = GL(n, \mathbf{R}) = n \times n$ invertible real matrices, $H = \mathbf{R}^\#$ with $\theta: G \rightarrow H$ defined by $\theta(A) = |A|$ (determinant of A) is an epimorphism.

(5) The map $\theta: \mathbf{R}^+ \rightarrow \mathbf{R}$ defined by $\theta(x) = \log_e x$ is an isomorphism.

(6) The conjugation map $\theta: \mathbf{C} \rightarrow \mathbf{C}$ defined by $\theta(z) = \bar{z}$ is an automorphism.

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

(8) If H is a normal subgroup of G then $\theta: G \rightarrow G/H$ defined by $\theta(g) = gH$ is an epimorphism.

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

Theorem 7: If $\theta: G \rightarrow H$ is a homomorphism then

- (1) $\theta(1) = 1$
- (2) $\theta(g^n) = \theta(g)^n$ for all n
- (3) $|\theta(g)|$ divides $|g|$.

The particular significance of an isomorphism is that it relates two groups that are group-theoretically identical. 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, they're isomorphic. Isomorphic groups have the same group-theoretic properties. They differ only in notation.

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

Example 6:

If $\theta: \mathbf{R}^\# \rightarrow \mathbf{R}^\#$ is defined by $\theta(x) = x^2$ then $\ker\theta = \{\pm 1\}$ and $\text{im}\theta = \mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$.

1st ISOMORPHISM THEOREM

Theorem 9: If $\theta: G \rightarrow H$ is a homomorphism and $K = \ker\theta$ then

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

Proof:

(1) Let $a, b \in K$. Then $\theta(a) = \theta(b) = 1$ and so $\theta(ab) = 1$ and $\theta(a^{-1}) = 1$. Thus $\ker\theta \leq G$. If $k \in K$ and $g \in G$ then $\theta(g^{-1}kg) = \theta(g)^{-1}\theta(k)\theta(g) = \theta(g)^{-1}\theta(g) = 1$. Thus $\ker\theta \trianglelefteq G$.

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

(3) Define $\Phi: G/K \rightarrow \text{im}\theta$ by $\Phi(gK) = \theta(g)$. 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 $\Phi(aK) = \Phi(bK)$.

If $aK = bK$ then $b^{-1}a \in K$. Hence $\theta(b^{-1}a) = 1$ and so $\theta(b)^{-1}\theta(a) = 1$ and so $\theta(a) = \theta(b)$. The reverse calculation checks that Φ is 1-1. For if $\Phi(aK) = \Phi(bK)$ then $\theta(a) = \theta(b)$ and so $\theta(b^{-1}a) = 1$. Thus $b^{-1}a \in K$ and so $aK = bK$.

Finally, it is clear that Φ is onto. Hence Φ is an isomorphism and so $G/K \cong \text{im}\theta$.

2nd ISOMORPHISM THEOREM

Theorem 10: If $H \leq G$ and $K \trianglelefteq G$ then:

- (1) $H \cap K$ is $\trianglelefteq H$;
- (2) $HK \leq G$;
- (3) $HK/K \cong H/(H \cap K)$.

Proof: The map $h \rightarrow hK$ is a homomorphism with kernel = $H \cap K$ and image = HK . Now use the First Isomorphism Theorem.

3rd ISOMORPHISM THEOREM

Theorem 11: 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 $gH \rightarrow gK$ is a well-defined homomorphism with kernel = K/H and image G/K . Now use the First Isomorphism Theorem.

Examples 7:

(1) $\theta: \mathbf{C} \rightarrow \mathbf{R}$ where $\theta(x+iy) = y$. This is a homomorphism with $\ker\theta = \mathbf{R}$ and $\text{im}\theta = \mathbf{R}$. Hence $\mathbf{C}/\mathbf{R} \cong \mathbf{R}$.

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

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

$H =$ set of diagonal matrices in G ,

$L =$ set of scalar matrices

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

$H \cap K =$ 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, $H/(H \cap K) \cong G/K \cong \mathbf{R}^\#$ and $(G/L)/(K/L) \cong G/K \cong \mathbf{R}^\#$.

§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 8: In $D_8 = \langle A, B \mid A^4, B^2, BA = A^{-1}B \rangle$ 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 classes are called **conjugacy classes**.

Example 9: The conjugacy classes of D_8 are $\{1\}$, $\{A, A^3\}$, $\{A^2\}$, $\{B, BA^2\}$, $\{BA, BA^3\}$.

The **centraliser** of g in $G = \{x \mid gx = xg\}$. It's easy to check that it is a subgroup of G , though, as the next example shows, it needn't be a normal subgroup.

Notation: $C_G(g)$ or just $C(g)$.

Example 10:

The centraliser of $(12)(34)$ in $S_4 = \{I, (12), (34), (1324), (1423), (12)(34), (13)(24), (14)(23)\}$

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

Example 11: $Z(D_8) = \{1, A^2\}$.

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

The **class equation** of a finite group G is: $|G| = h_1 + h_2 + \dots + h_k$ where $1 = h_1 \leq h_2 \leq \dots$ are the sizes of the conjugacy classes. The number of h_i which equal 1 is $|Z(G)|$.

Example 12: The class equation for Z_4 is $4 = 1 + 1 + 1 + 1$.

Example 13: The class equation for S_3 is $6 = 1 + 2 + 3$ since the conjugacy classes are: $\{I\}, \{(123), (132)\}, \{(12), (13), (23)\}$.

Example 14: The class equation for S_4 is $24 = 1 + 3 + 6 + 6 + 8$ since the conjugacy classes correspond to the cycle structures: $I, (\times\times)$ of which there are $6 = 4 \cdot 3/2$, $(\times\times\times)$ of which there are $8 = 4 \cdot 3 \cdot 2/3$, $(\times\times\times\times)$ of which there are $6 = 4!/4$ and $(\times\times)(\times\times)$ of which there are $3 = \frac{4!}{2 \cdot 2 \cdot 2}$.

Example 15: The class equation for A_4 is $12 = 1 + 3 + 4 + 4$.

Let $G = S_4, H = A_4$. Classes in G may split in H . For example $x = (123)$ has 8 conjugates in S_4 so $|C_G(x)| = 3$. Thus $C_G(x) = \langle x \rangle$. All the elements of $\langle x \rangle$ are in H so $C_H(x) = \langle x \rangle$. Since $|H: C_H(x)| = 12/3 = 4$, x has only 4 conjugates in A_4 . Consequently the 8 cycles of length 3, though a single class in S_4 , split into two classes of 4 each in H .

Theorem 12: # conjugates of x in $G = |G:C_G(x)|$.

Proof: $x^g = x^h \Leftrightarrow xgh^{-1} = x \Leftrightarrow gh^{-1} \in C_G(x) \Leftrightarrow gC_G(x) = hC_G(x)$. 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 $C_G(x)$.

Example 16: Find the numbers of conjugates of (123) and (12345) in 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 S_5 is the number of permutations in S_5 with cycle structure $(\times\times\times)$, which is 20. The order of S_5 is 120, so by the above theorem the $|C_{S_5}(123)| = 120/20 = 6$. 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 A_5 ? Only the first 3. So $|C_{A_5}(123)| = 3$ and so the number of conjugates of (123) in A_5 is $60/3 = 20$.

In the case of (12345) , there are 24 conjugates in S_5 and so $|C_{S_5}(12345)| = 120/24 = 5$. These 5 elements that commute with (12345) are clearly its 5 powers, all of which are in A_5 . So $|C_{A_5}(12345)| = 5$ and so the number of conjugates of (12345) in A_5 is $60/5 = 12$.

So the conjugacy class containing all the 3-cycles in S_5 remains a single class in A_5 but the conjugacy class of size 24 containing all the 5-cycles in S_5 splits into two classes of

size 12 when we're considering classes in A_5 . In the latter case you need to conjugate by an odd permutation to take you from one lot of 12 to the other.

Theorem 13: 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 $(gZ(G))^r = g^rZ(G)$ and so every element of G has the form g^rz for some $z \in Z(G)$. Since g^rz_1 commutes with g^sz_2 for all integers r, s and all $z_1, z_2 \in Z(G)$, G is abelian.

If p is prime, a **finite p -group** is a group of order p^n for some n .

Theorem 14: The centre of a non-trivial finite p -group is non-trivial.

Proof: If $Z(G) = 1$ then G has only one conjugacy class of size 1. All the others are 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.

Corollary: 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 G is abelian.

Theorem 15: A finite p -group G has a subgroup of every order which divides $|G|$.

Proof: Let $|G| = p^n$. 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 $Z(G) > 1$ we may find an element $z \in Z(G)$ of order p and if $H = \langle z \rangle$ 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, which divides the order of the group.

§ 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 the elements of the form $a^{-1}b^{-1}ab$ are not all 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 $[a, b]$. So a, b commute if and only if $[a, b] = 1$.

Theorem 16: The following properties hold for commutators:

(1) $[b, a] = [a, b]^{-1}$ for all $a, b \in G$.

(2) $g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg]$ for all $a, b \in G$.

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 17: If $a = (123)$ and $b = (1423)$ are permutations in 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 are well on the way to proving that the commutators form a normal subgroup except ... the product of two commutators need not be a commutator. Instead of considering the *set* of all commutators we consider the *group generated by* all the commutators. Now indeed we have a normal subgroup.

The **derived subgroup (commutator subgroup)** of a group G is the subgroup G' generated by the commutators. Clearly it is a normal subgroup of G . G is abelian if and only if $G' = 1$, so in a certain sense G' (or perhaps its order) measures how close the group is to being abelian.

Example 18: $S_3' = A_3$.

It might appear that we must compute all 36 commutators $[a, b]$ where $a, b \in S_3$, 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 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 3 even permutations and we 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. Instead we use the following theorem.

Theorem 17: (1) G/G' is abelian.

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

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 19: We shall show that $S_4' = A_4$. By the parity argument of example 2 we easily see that $S_4' \leq A_4$. This can also be deduced from the above theorem and the fact that S_4/A_4 is abelian (after all it has order $24/12 = 2$, 2 is prime, groups of prime order are cyclic, and cyclic groups are abelian). But why can't S_4' be smaller?

Suppose S_4' was smaller than A_4 . Then $|S_4'|$ 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 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 this? Well groups of order 6 (twice a prime) are cyclic group or dihedral. But G/G' is abelian so it is not dihedral. It must be that G/G' is cyclic, of order 6. But this would require G itself

to contain elements of order 6, which it does not. So by patient detective work we obtain a contradiction to the assumption that $S_4' < A_4$. It follows that $S_4' = A_4$.

EXERCISES

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?

- (i) $f(1) = 2, f(2) = 3, f(3) = 4, f(4) = 5, f(5) = 6, f(6) = 1$;
- (ii) $f(1) = 1, f(2) = 2, f(3) = 1, f(4) = 2, f(5) = 1, f(6) = 2$;
- (iii) $f(1) = 1, f(2) = 3, f(3) = 1, f(4) = 5, f(5) = 1, f(6) = 3$;
- (iv) $f(1) = 1, f(2) = 2, f(3) = 3, f(4) = 4, f(5) = 5, f(6) = 6$;
- (v) $f(1) = 1, f(2) = 6, f(3) = 5, f(4) = 4, f(5) = 3, f(6) = 2$;
- (vi) $f(1) = 1, f(2) = 4, f(3) = 5, f(4) = 6, f(5) = 3, f(6) = 2$;
- (vii) $f(1) = 1, f(2) = 1, f(3) = 1, f(4) = 2, f(5) = 3, f(6) = 4$;
- (viii) $f(1) = 1, f(2) = 1, f(3) = 1, f(4) = 1, f(5) = 1, f(6) = 1$.

EXERCISE 3: Let $\mathbf{R}^\#$ denote the group of on-zero real numbers under multiplication and let \mathbf{R} denote the group of all real numbers under addition. Show $f: \mathbf{R}^\# \rightarrow \mathbf{R}$ defined by $f(x) = \log(|x|)$ is a homomorphism. Hence show that $\mathbf{R}^\#/\{\pm 1\} \cong \mathbf{R}$.

EXERCISE 4: Let $GL(n, \mathbf{R})$ denote the group of all invertible $n \times n$ real matrices under matrix multiplication and let $SL(n, \mathbf{R})$ denote all such matrices whose determinant is 1. Prove that $GL(n, \mathbf{R})/SL(n, \mathbf{R}) \cong \mathbf{R}^\#$.

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 $|Z(G)|$.

SOLUTIONS

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.

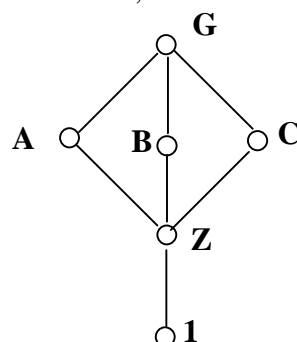
(f) G/H is abelian so $G' \leq H$. But $G' \neq 1$ since G is non-abelian. Hence $G' = H = Z(G)$.

(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 is 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 have 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 V_4 , or $C_2 \otimes C_2$ with 3 elements of order 2. Since G only has one element of order 2 there can be none 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 4: $\{1, 2, 3, 4\}$, $\{1, 2, 5, 7\}$ 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:

- (i) is NOT a homomorphism since the identity is not fixed.
- (ii) is a homomorphism. Even permutations map to 1 and odd permutations map to 2.
- (iii) is NOT a homomorphism. If it was then $\ker f = \{1, 3, 5\}$ and so $G/\ker f$ would have order 2. But $G/\ker f \cong \text{im } f$ and $\text{im } f$ has order 3.
- (iv) is a homomorphism. It is the identity automorphism.
- (v) is a homomorphism. We can see this by taking the group table for G , replacing each element by its image under f . 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

- (vi) is NOT a homomorphism. For example $f(2.3) = f(6) = 2$ while $f(2).f(3) = 4.5 = 6$.
- (vii) is NOT a homomorphism since $\text{im } f$ has order 4 and so cannot be a subgroup of G .
- (viii) is a homomorphism. It is the trivial homomorphism.

EXERCISE 3: $f(xy) = \log(|xy|) = \log(|x|.|y|) = \log(|x|) + \log(|y|) = f(x) + f(y)$ so f is a homomorphism. Its kernel is clearly $\{\pm 1\}$. So, by the First Isomorphism Theorem, $\mathbf{R}^\#/\{\pm 1\} \cong \mathbf{R}$.

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

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 $y = yx$. 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 ($p = 3$) $|Z(G)| \neq 1$. Since $G/Z(G)$ is not cyclic, $|Z(G)| \neq 9$. Hence $|Z(G)| = 3$.