14. DIHEDRAL GROUPS

§14.1. Subgroups

If G is a group and H is a subset of G then H is a **subgroup** if

(i) $xy \in G$ for all $x, y \in G$
(ii) $1 \in G$
(iii) $x^{-1} \in G$ for all $x \in G$.

A subgroup H is a group in its own right. Every group is a subgroup of itself.
All other subgroups are called **proper subgroups**.
The set {1} is a subgroup in any group and is called the **trivial subgroup**.
We write $\mathbf{H \leq G}$ if H is a subgroup of G and $\mathbf{H < G}$ if H is a **proper subgroup** of G, that is, if H is a subgroup but is not G itself.

Example 1: $2\mathbb{Z}$ (the group of even integers) is a subgroup of $\mathbb{Z}$ (under +).

WARNING: G and H must have the same binary operation before one can say $H \leq G$. For example $\mathbb{R}^{\#}$ (the group of non-zero real numbers under multiplication) is not a subgroup of $\mathbb{R}$ (the group of all real numbers under addition) even though it is a subset.

Theorem 1: For all $\boldsymbol{g} \in G$, $\langle \boldsymbol{g} \rangle$ is a subgroup of G.
Proof: (1) For all r, s we have $g^r g^s = g^{r+s} \in \langle \boldsymbol{g} \rangle$.
(2) $1 = g^0 \in \langle g \rangle$.
(3) For all r, $(g^r)^{-1} = g^{-r} \in \langle g \rangle$. ✋☺

§14.2. Cosets

Suppose $H \leq G$. We define a relation $\equiv$ on G by defining $x \equiv y$ if $x = yh$ for some $h \in H$.

Theorem 2: $\equiv$ is an equivalence relation.
Proof:
Reflexive: Let $a \in G$. Then $a = a1$. Since $1 \in H$, $a \equiv a$.
Symmetric: Suppose $a \equiv b$. Then $a = bh$ for some $h \in H$ and so $ah^{-1} = b$. Since $h^{-1} \in H$, $b \equiv a$.
Transitive: Suppose $a \equiv b$ and $b \equiv c$. Then $a = bh$ for some $h \in H$ and $b = ck$ for some $k \in H$.
Thus $a = (ck)h = c(kh)$. Since $kh \in H$, $a \equiv c$. ✋☺

NOTE: Each of the three properties of an equivalence relation comes from one of the three closure properties of a subgroup.

The equivalence classes under $\equiv$ are called the **right cosets** of H in G. The coset containing g is denoted by **gH**. We define left cosets similarly, writing them as **Hg**.

The **right coset** containing g is

$$\boldsymbol{g}\mathbf{H} = \{gh \mid h \in \mathrm{H}\}$$

and the **left coset** containing g is

$$\mathbf{H}\boldsymbol{g} = \{hg \mid h \in \mathrm{H}\}.$$

NOTES: (1) Many books define left and right cosets in the opposite manner. However the notation gH and Hg always mean what we have stated above.
(2) Just because aH = bH does not mean that a = b. It merely means that they are in the same right coset, or equivalently that $b^{-1}a \in \mathrm{H}$.

Example 2: (1) G = $\mathbb{R}^{\#}$, H = {±1} under the operation of multiplication. The cosets are all of the form $\{\pm x\}$.

(2) G = $\mathbb{C}^{\#}$, the group of non-zero complex numbers under multiplication and let

$$\mathrm{H} = \{\mathrm{z} \in \mathbb{C} \mid |\mathrm{z}| = 1\}.$$

The right (or left) cosets of H in G are the concentric circles with the origin as centre.

(3) G = the Symmetry Group of a square:

	1	**r**	**r^2**	**r^3**	**a**	**b**	**c**	**d**
1	1	r	r^2	r^3	a	b	c	d
r	r	r^2	r^3	1	b	c	d	a
r^2	r^2	r^3	1	r	c	d	a	b
r^3	r^3	1	r	r^2	d	a	b	c
a	a	d	c	b	1	r^3	r^2	r
b	b	c	d	a	r^2	1	r	r^3
c	c	b	a	d	r^3	r	1	r^2
d	d	a	b	c	r	r^2	r^3	1

Let H = {1, *a*}. The right and left cosets of H in G are:

H1 = {11, *a*1} = {1, *a*} 1H = {11, 1*a*} = {1, *a*}

H*b* = {1*b*, *ab*} = {*b*, r^3} *b*H = {*b*1, *ba*} = {*b*,r^2}

H*c* = {1*c*, *ac*} = {*c*, r^2} *c*H = {*c*1,*ca*} = {*c*,r^3}

H*d* = {1*d*, *ad*} = {*d*, *r*} *d*H = {*d*1, *d*a} = {*d*,*r*}

Theorem 3:

(1) The subgroup H is itself one of the cosets of H in G.

(2) Two elements *a*, *b* belong to the same coset (of H in G) if and only if $b^{-1}a \in$ H.

Proof:

(1) H = 1H.

(2) *a*, *b* belong to the same coset

$\Leftrightarrow a$H = *b*H

$\Leftrightarrow a = bh$ for some $h \in$ H

$\Leftrightarrow b^{-1}a = h$ for some $h \in$ H

$\Leftrightarrow b^{-1}a \in$ H. ✋☺

Generally, equivalence classes can be of different sizes. But in the case of cosets, they all have the same size.

Theorem 4: If $H \leq G$ then every coset of H in G has |H| elements.
Proof: There is a natural 1-1 correspondence between any coset aH and H itself viz. $ah \leftrightarrow h$. Hence the number of elements in each is the same. ✋☺

§14.3. Lagrange's Theorem

Theorem 5 (Lagrange): The order of a subgroup (of a finite group) divides the order of the group.
Proof: Suppose there are m cosets of H in G. Since G is the disjoint union of them and each coset has |H| elements, it follows that |G| = m.|H| and so |H| divides |G|. ✋☺

This is a very powerful result. It shows that the number of elements in a group greatly affects its structure.

Example 3: If |G| = 14 , the only possible orders for a subgroup are 1, 2, 7 and 14.

Theorem 6: Groups of prime order are cyclic.
Proof: Suppose $|G| = p$ where p is prime.
Since $p \geq 2$ we may choose $g \in G$ such that $g \neq 1$.
Let $H = \langle g \rangle$.
Let $|H| = n$. Now n divides p and $n > 1$ so $n = p$.
Hence G = H and so is cyclic. ✋☺

Corollary: The order of an element of a finite group divides the order of the group.

§14.4. Euler's Theorem

Recall that if m is any positive integer $\mathbb{Z}_m^{\#}$ denotes the group of all numbers from 1 to $m - 1$ which are coprime with m, under the operation of multiplication modulo m. [The coprimeness is what ensures the existence of inverses]

For example $\mathbb{Z}_7^{\#} = \{1, 2, 3, 4, 5, 6\}$;

$\mathbb{Z}_8^{\#} = \{1, 3, 5, 7\}$;

$\mathbb{Z}_{10}^{\#} = \{1, 3, 7, 9\}$.

The order of $\mathbb{Z}_m^{\#}$ is denoted by $\varphi(m)$. The function φ is called the **Euler φ function** [N.B. you pronounce Euler as 'Oiler'].

For example, $\varphi(7) = 6$; $\varphi(8) = 4$; $\varphi(10) = 4$.

It's all very well to find $\varphi(m)$ for small values of m by counting the elements of $\mathbb{Z}_m^{\#}$. What do we do for large m? Is there a formula?

If a and b are coprime integers (i.e. have no common factors) it can be shown that:
$\varphi(ab) = \varphi(a)\,\varphi(b)$. For example, $\varphi(70) = \varphi(7)\,\varphi(10) = 6.4 = 24$. This means that $\varphi(m)$ can be computed provided we have a formula for prime powers.

Theorem 7: If p is prime, $\varphi(p^n) = p^{n-1}(p-1)$.
Proof: Of the p^n numbers from 0 to $p^n - 1$ there are precisely p^{n-1} multiples of p. The remaining $p^n - p^{n-1} = p^{n-1}(p-1)$ numbers will be precisely the ones with no factor in common with p^n. Hence $\varphi(p^n) = p^{n-1}(p-1)$. ✋☺

Example 4: $\varphi(200) = \varphi(2^3.5^2)$
$= 2^2(2-1) \,.\, 5^1(5-1)$
$= 4.1.5.4$
$= 80.$

Theorem 8(EULER): If a is coprime with m then:
$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$
Proof: Suppose that a is coprime with m. Then $a \in \mathbb{Z}_m^{\#}$. Suppose it has order n.
By Lagrange's Theorem n divides $\varphi(m)$.
Thus $\varphi(m) = nq$ for some $q \in \mathbb{Z}$.
Now $a^{\varphi(m)} = (a^n)^q = 1^q = 1$. ✋☺
Corollary (FERMAT): If p is prime and doesn't divide a, then $a^{p-1} \equiv 1 \pmod{p}$.

Euler's theorem can be used to calculate the remainders of certain very large numbers.
Example 5: What is the remainder on dividing 2^{1000} by 42?
Solution: $\varphi(42) = \varphi(2.3.7) = 12$ so $2^{12} \equiv 1 \pmod{42}$.

Dividing 1000 by 12 we get a remainder of 4. [$1000 = 12.83 + 4$]
So $2^{1000} \equiv (2^{12})^{83}.2^4 \equiv 1^{83}.2^4 \equiv 16$.
Hence 2^{1000} leaves a remainder of 16 when divided by 42.
NOTE: To work this out directly, by calculating 2^{1000} first, would need vast amounts of computing power.

§14.5. Generators and Relations

A finite group can be described by means of a multiplication table but its structure is hidden in a mass of details. A more compact way of representing a group structure is in terms of generators and relations.

A set of **generators** for a group is a set of elements such that every element can be expressed in terms of them. A **relation** is an equation that holds between the generators. The notation

$$\langle g_1, g_2, \ldots, g_m \mid R_1, R_2, \ldots, R_n \rangle$$

represents a group generated by the elements $g_1, g_2, \ldots, g_m$ where the relations $R_1, R_2, \ldots, R_n$ hold.
A typical example is:

$$\langle A, B, C \mid A^7 = 1, B^4 = 1, C^5 = 1, BA = A^{-1}B, CA = AC, CB = BC \rangle$$

or more simply as:

$$\langle A, B, C \mid A^7 = B^4 = C^5 = 1, BA = A^{-1}B, CA = AC, CB = BC \rangle$$

where the elements are strings of A's, B's and C's and where the six relations can be used to simplify such strings. To multiply two strings you just write one following the other and simplify where possible using the relations.

For example if $X = A^4BC^3$ and $Y = A^2B^3C^4$ in the above group then $XY = A^4BC^3A^2B^3C^4$.
This can be simplified as follows:

$$\begin{aligned}
A^4BC^3A^2B^3C^4 &= A^4BA^2C^3B^3C^4 \text{ (since CA = AC)} \\
&= A^4BA^2B^3C^7 \text{ (since CB = BC)} \\
&= A^4BA^2B^3C^2 \text{ (since } C^5 = 1) \\
&= A^4(BA)AB^3C^2 \\
&= A^4(A^{-1}B)AB^3C^2 \text{ (since } BA = A^{-1}B) \\
&= A^3(BA)B^3C^2 \\
&= A^3(A^{-1}B)B^3C^2 \\
&\qquad \text{(again, since } BA = A^{-1}B) \\
&= A^2B^4C^2 \\
&= A^2C^2 \text{ (since } B^4 = 1).
\end{aligned}$$

In this case we could have done this simplification more easily by observing that C an move freely across A's and B's and that every time the letter B crosses the letter A the A gets inverted.

All the C's can slip down to the end with no change. If we bring all the B's to the right of all the A's then the A^4 gets inverted 4 times, so stays as A^4 and the A^2 gets inverted 3 times so becomes A^{-2}.

Hence $A^4BC^3A^2B^3C^4 = B^4A^4A^{-2}C^7 = B^4A^2C^7 = A^2C^2$.

This example is rather more complicated than those we shall encounter. A much simpler example is $\langle A \mid A^n = 1\rangle$ which denotes the cyclic group of order n (there's essentially only one such group since all cyclic groups of the same order are isomorphic).

The infinite cyclic group, an example of which is $(\mathbb{Z},+)$, is denoted by $\langle A \mid \rangle$, with an empty set of relations.

Not every relation that holds in a group needs to be listed. Only enough so that any other relation can be deduced from those that are given.

For example in the group $\langle A \mid A^4 = 1\rangle$ the relation $A^{12} = 1$ must hold but it is just a consequence of the one which is listed.

§14.6. Dihedral Groups

The family of cyclic groups contain those groups with the simplest possible group structure. A closely related family is the family of dihedral groups. The **dihedral group** of order $2n$ is the group:

$$D_{2n} = \langle A, B \mid A^n = B^2 = 1, BA = A^{-1}B\rangle.$$

Dihedral groups occur naturally in many different guises. D_{2n} is, for example, the Symmetry Group of a regular n-

sided polygon. The symmetry operations consist of the rotation R through $2\pi/n$, and its powers plus the 180° rotations about the n axes of symmetry. But if Q denotes any one of these, the others can be expressed in the form R^kQR^{-k}.

If, for example, there is a vertical axis of symmetry and Q denotes the 180° degree rotation about it, any other 180° symmetry operation can be achieved by rotating the axis until it becomes vertical (R^k), carrying out Q about the vertical axis, and then rotating the axis back to its original position (R^{-k}).

Now $R^n = 1$ (n successive rotations through $2\pi/n$);
$Q^2 = 1$ (two successive 180° rotations) and
$QR = R^{-1}Q$ (try it!).
So this symmetry group is $\langle R, Q \mid R^n = Q^2 = 1, QR = R^{-1}Q\rangle$, that is, it's the dihedral group of order $2n$. In particular D_8 is the symmetry group of a square.

§14.7. Dihedral Arithmetic

The dihedral group $D_{2n} = \langle A, B \mid A^n = B^2 = 1, BA = A^{-1}B\rangle$ has its relations built up from the basic three relations in the list. Let's examine their implications.

$A^n = 1$: This means that any expression involving A's and B's needn't have any string of successive A's longer than

$n - 1$, because any block of n successive A's is A^n which, because it is equal to the identity, can be removed.

For example in $D_8 = \langle A, B \mid A^4 = B^2 = 1, BA = A^{-1}B \rangle$, an element such as A^2BA^7BA can be simplified to A^2BA^3BA by removing an A^4 from the middle.

$B^2 = 1$: This means that it's never necessary to have two successive B's. For example in D_8 an expression such as $AB^3A^3\ B^2A^2$ can be simplified to ABA^5 by using $B^2 = 1$, twice. This can be further reduced to ABA by use of the relation $A^4 = 1$.

Another consequence of $B^2 = 1$ is $B = B^{-1}$ (just multiply both sides on the left by B^{-1}).
This means that there is never any need to have B^{-1} in any expression.

$BA = A^{-1}B$: It is this third relation that makes dihedral groups non-abelian (except for the trivial cases of D_4 and D_2 where $A^{-1} = A$). Expressing this relation in words, we can say that every time each B passes across each A it inverts it innverts it.

Consequently if we have an expression involving a mixture of A's and B's we can move all the A's up to the front and all the B's down to the back just as we would if the commutative law was in force. The difference is that

the A's get inverted every time a B crosses over them. This is the dihedral 'twist'.

Example 6: The expression ABA^3BA^2BAB can be written as:
$AA^{-3}BBA^2AB = A^{-2}BBA^2AB = A^{-2}A^2AB = AB.$

Theorem 9: The elements of D_{2n} are:

1	A	A^2	A^3	...	A^{n-1}
B	AB	A^2B	A^3B	...	$A^{n-1}B$

Proof: Because of the relation $BA = A^{-1}B$ we can express every element in the form A^rB^s.
But because $A^n = 1$ and $B^2 = 1$, we may assume that $r = 0, 1, 2, \ldots, n-1$ and $j = 0$ or 1. ✋☺

Notice that the first row consists of the cyclic subgroup, H, generated by A, and the second row is the left coset HB.

Theorem 10: The elements of the form A^kB all have order 2.
Proof: $(A^kB)^2 = A^kBA^kB = A^kA^{-k}BB = B^2 = 1.$ ✋☺

§14.8. Groups of Order 2*p*

Recall that as a consequence of Lagrange's Theorem we showed that groups of prime order are cyclic. This is an example of a **classification theorem**. A classification theorem says, in effect, "tell me a little about a group and I will tell you everything". Here, just by knowing that the order of the group is prime, we essentially know everything about the structure of the group.

Constructing classification theorems is one of the goals of a group-theorist. Many of these classification theorems exist. There is a classification theorem for finite abelian groups which says, in effect, "tell me the orders of the elements of a finite abelian group and I will tell you all you want to know about the group's structure". This is a big theorem but not too big to present in a full course on group theory. The proof might take two or three pages to write out but that is not for us here.

The biggest classification theorem in the whole subject is the famous Classification of Finite Simple Groups. It doesn't take too much to explain what a simple group is. A **simple group** is one where there is no subgroup H (other than 1 and the group itself) for which the left and right cosets are the same. In a certain sense simple groups are the building blocks of all finite groups. They are to finite groups what primes are to integers,l and chemical elements are to all matter.

The theorem, essentially lists all finite simple groups. There are a few infinite lists of simple groups where those in each list have a similar structure, plus a finite list of sporadic simple groups, which are one-offs.

It would take a couple of pages to write out this list. But the proof has never been assembled in one place for it's been estimated that it would occupy about 20,000 pages! Thousands of group-theorists worked for decades and they have gradually dealt with more and more cases until finally the last piece was fitted into the jig-saw. It's an achievement that is surely worthy of a place in the *Guiness Book Of Records*. Indeed for a number of years it was listed, along with Pythagoras' Theorem. Pythagoras' Theorem holds the record for the theorem with the largest number of different proofs. The classification theorem for finite simple groups holds the record for the theorem with the longest proof.

The next big classification theorem may be the classification of finite *p*-groups, groups whose orders are powers of a prime.

But to conclude our brief excursion into group theory we present a much more modest classification theorem, the classification of groups of order 2*p* (where p is prime). We'll show that all such groups are either cyclic or dihedral.

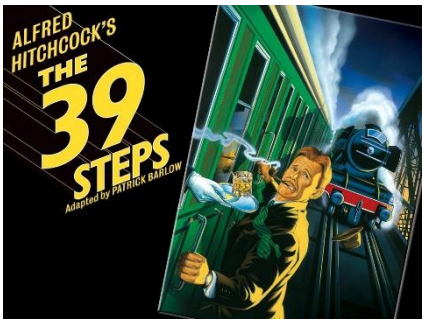
Modest though it may be in comparison with the Finite Simple Group Classification Theorem, it still probably represents one of the longest and most sustained pieces of reasoning you will have encountered so far in mathematics.

The result is not one you are likely to use. Nor will you ever be likely to need to make use of a knowledge of the proof. But then this could be said of the vast amount of mathematics you learn. It's the mode of reasoning, the way it shows how a problem can be clearly and logically attacked by a sustained piece of reasoning, that will benefit you.

So take a packed lunch, for this will be a long journey. You may have heard of the thriller called *The Thirty-nine Steps*. Well here they are!

§14.9. The Thirty Nine Steps

Theorem 11: If $|G| = 2p$ for some prime p, G is cyclic or dihedral.



Proof:

(1) Suppose that $|G| = 2p$ where p is prime

(2) Suppose that p is odd.

(2) By Lagrange's theorem the order of every element is 1, 2, p or $2p$.

(3) Suppose G contains an element of order $2p$.

(4) Hence G is cyclic. ☺

(5) Since |G| is even, G must contain an element, b, of order 2.

(6) Suppose that all the elements of G, except 1, have order 2.

(7) Then G is abelian.

(8) Choose $a, b \in$ G of order 2 with $a \neq b$.

(9) Hence H = {1, a, b, ab} is a subgroup of G of order 4.

(10) Since 4 does not divide $2p$ we get a contradiction.

(11) So G must have an element, a, of order p.

(12) Let H = $\langle a \rangle$.

(13) Since 2 doesn't divide p, we must have $b \notin$ H.

(14) The right cosets of H in G must be H and bH.

(15) Similarly the left cosets are H and Hb.

(16) Since bH and Hb consist of all the elements outside H, they must be equal, i.e. Hb = bH.

(17) Now $ba \in b$H so $ba \in$ Hb.

(18) Hence $ba = a^r b$ for some integer $r = 0, 1, \ldots, p - 1$.

(19) Hence $b^2 a = ba^r b$

(20) $= baa \ldots ab$ (where there are r factors of a).

(21) $= a^r a^r \ldots a^r b^2$ (where there are r factors of a^r).

(22) $= a^{r^2}$ (since $b^2 = 1$).

(23) So $a^{r^2} = a$,

(24) Hence p divides $r^2 - 1$.

(25) Since p is prime and $r^2 - 1 = (r-1)(r+1)$,
p divides $r - 1$ or $r + 1$.
(26) Thus $ba = ab$ or $a^{-1}b$.
(27) Suppose $ba = ab$.
(28) Now the order of ab must be 1, 2 or p.
(29) Suppose $ab = 1$.
(30) Then $a = b^{-1} = b$, a contradiction.
(31) Suppose ab has order 2.
(32) Then $1 = (ab)^2 = a^2b^2 = a^2$,
a contradiction.
(33) Hence ab has order p.
(34) Then $1 = (ab)^p = a^pb^p = b^p$, a contradiction.
(35) So $ba = a^{-1}b$ and so $G = \langle a, b \mid a^p = b^2 = 1, ba = a^{-1}b \rangle$
$= D_{2p}$. ☺
(36) Suppose that $p = 2$.
(37) Then every element of G (except 1) has order 2.
(38) Hence G is abelian.
(39) Hence $G = \langle a, b \mid a^2 = b^2 = 1, ba = ab \rangle = \langle a, b \mid a^2 = b^2 = 1, ba = a^{-1}b \rangle = D_4$. ✋☺

SUMMARY

Subgroup: $H \leq G$ means H is a subset of G which is closed under $\times$, 1 and inverse.
Includes cyclic subgroups $\langle g \rangle$ consisting of all powers of a single generator, g.
Cosets: Right cosets are $gH = \{gh \mid h \in H\}$. They include H itself and all have the same size viz. $|H|$. (Left cosets, Hg, similarly.)

Lagrange's Theorem: If $H \leq G$, $|H|$divides $|G|$.
Euler's Theorem: $\varphi(m) = |Z_m^{\#}|$ = the number of integers from 1 to $m - 1$, coprime with m.
If a, b are coprime $\varphi(ab) = \varphi(a)\varphi(b)$ and

$$\varphi(p^n) = p^{n-1}(p - 1).$$

If a, m are coprime $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Fermat's Theorem: If the prime p doesn't divide a then $a^{p-1} \equiv 1 \pmod{p}$.
Generators and Relations: $\langle A, B, ... \mid R_1, ... \rangle$ is the group generated by A,B,... subject to the relations R_1, ...
Cyclic Groups: $C_n = \langle A \mid A^n = 1 \rangle$ is the cyclic group of order n.
Dihedral Groups: $D_{2n} = \langle A, B \mid A^n = B^2 = 1, BA = A^{-1}B \rangle$ is the dihedral group of order $2n$.
If $n > 2$, D_{2n} is non-abelian. Moving each B past an A inverts the A.
The elements are: 1, A, A^2 , ... , A^{n-1} (a cyclic subgroup of order n) and

$$B, AB, A^2B, ... , A^{n-1}B$$

(each one having order 2)
Groups of Order p: are cyclic.
Groups of Order 2p: are cyclic or dihedral.

EXERCISES FOR CHAPTER 14

Exercise 1: If G = ($\mathbb{Z}$, +), which of the following subsets are subgroups of G?

A = the set of even integers;
B = the set of odd integers;
C = the set of non-negative integers;
D = {0}
E = the set of integers which are expressible as 42m + 1023n for integers m,n.

Exercise 2: If G = ($\mathbb{C}^{\#}$, ×), the set of non-zero complex numbers under multiplication, which of the following subsets are subgroups of G?

A = the set of non-zero rational numbers;
B = the set of positive integers;
C = {1, –1, i, –i};
D = {1, ½, 2};
E = {a + bi | a > 0};
F = {1, π, π^2, π^3, ... }.

Exercise 3: If G is the group whose table is given below, show that H = {1, c, d} and
K = {1, b} are both subgroups of G. Find all the left and right cosets of each subgroup.

	1	**a**	**b**	**c**	**d**	**e**
1	1	a	b	c	d	e
a	a	1	c	b	e	d
b	b	d	1	e	a	c
c	c	e	a	d	1	b
d	d	b	e	1	c	a
e	e	c	d	a	b	1

Exercise 4:
If $G = \langle A,B \mid A^4 = B^3 = 1, AB = BA \rangle$ and H is the cyclic subgroup generated by B, find the left and right cosets of H in G.

Exercise 5: In the dihedral group $D_{10} = \langle A, B \mid A^5 = B^2 = 1, BA = A^{-1}B \rangle$, simplify

$$A^7B^3A^{-2}BABA^3BA^2A^7B^2A \, .$$

Exercise 6: Simplify $A^{13}B^5A^2B^{-7}A^2BA$ in the above group D_{10}.

Exercise 7: Find the order of H given the following clues:

(a) H is a proper subgroup of a group of order 68
(b) H is non-cyclic

Exercise 8: Find the order of H given the following clues.

(a) H is a subgroup of some group of order 100.

(b) H contains no element of order 2.

(c) H is not cyclic.

Exercise 9: Find the order of H given the following clues:

(a) H is a subgroup of some group G of order 168.

(b) H is a subgroup of another group K of order 112.

(c) H is not cyclic or dihedral.

(d) H contains an element of order 7.

(e) H has more than two left cosets in K.

Exercise 10: If G is a group, the **centre** (*zentrum* in German) of G is defined to be
$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$. In other words, it is the set of all elements which commute with everything.
(a) Prove that Z(G) is a subgroup of G.
(b) Find $Z(D_{2n})$. **[HINT:** You will need to consider odd and even values of *n* separately.]

Exercise 11: If $G = (\mathbb{R}, +)$, which of the following subsets are subgroups of G?

A = the set of integers;

B = the set $\{x \mid -10 < x < 10\}$;

C = the set of numbers of the form $a + b\sqrt{2}$ where a, b are integers;

D = the set of real numbers whose decimal expansions are finite.

Exercise 12: If $G = (\mathbb{C}^{\#}, \times)$, which of the following subsets are subgroups of G?

A = the set of complex numbers whose modulus is 1;

B = the set of complex numbers whose modulus is an integer;

C = the set of complex numbers whose modulus is a rational number;

D = the set of solutions to the equation:

$$z^9 + z^8 - z - 1 = 0.$$

Exercise 13: G is the group whose table is given below. Show that H = {1, a, d, f} and K = {1, d} are both subgroups of G. Find all the left and right cosets of each subgroup.

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

Exercise 14:

Find the left and right cosets of {1, b} in the dihedral group $D_{12} = \langle a, b \mid a^6 = b^2 = 1, ba = a^{-1} b \rangle$.

Exercise 15: In the dihedral group
$D_{14} = \langle a, b \mid a^7 = 1, b^2 = 1, ba = a^{-1}b \rangle$, simplify $a^9b^7a^{-4}baba^2ba^3a^{12}ba$.

Exercise 16: Find the order of H given the following clues:

(a) H is a proper subgroup of a group of order 52.
(b) H is non-cyclic

Exercise 17: Find the order of H given the following clues:
(a) H is a subgroup of some group G of order 100.
(b) H is a subgroup of another group K of order 40.
(c) H is not cyclic or dihedral.

Exercise 18: Find the order of H given the following clues:
(a) H is a subgroup of some group G of order 20.
(b) H is non-abelian.
(c) G contains an element g of order 2 and an element h of order 5.
(d) H contains h but not g.

Exercise 19: If G is a group, the **derived subgroup** of G is defined to be the subgroup generated by all the elements of the form $x^{-1}y^{-1}xy$ as x, y range over the elements of the group. Find the derived subgroup of D_{2n}. [**HINT:** You will need to consider odd and even values of n separately.]

SOLUTIONS FOR CHAPTER 14

Exercise 1:
A is a subgroup since the sum of two even integers is even, 0 (the identity of G) is even, and the additive inverse, $-n$ of any even integer is even.

B is not a subgroup. In fact the sum of two odd integers is never odd. As well as not being closed under addition, B doesn't contain the identity of G.

C is not a subgroup. It *is* closed under addition and it *does* contain the identity, 0. But it is *not* closed under inverses. If $n \geq 0$ it is *not* true that $-n \geq 0$.

D is a subgroup as is easily verified. It is always the case for any group that the set consisting of just the identity is a subgroup.

E is a subgroup. Closure under addition comes from checking that:

$(42a + 1023b) + (42c + 1023d)$

$= 42(a + c) + 1023(b + d)$.

Since $a + c$ and $b + d$ will be integers if a, b, c, d are, this sum has the required form. Zero can be expressed as $42\times 0 + 1023\times 0$ and so is in the subset, and $-(42m + 1023n) = 42(-a) + 1023(-\underline{b})$ which has the required form.

Exercise 2:

A is a subgroup since the product of two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$ is the rational number $\frac{ac}{bd}$, the integer 1 is rational and the inverse of every rational number $\frac{a}{b}$ is the rational number $\frac{b}{a}$.

B is not a subgroup because although it is closed under multiplication and contains the identity, it is not closed under inverses. For example, 2 is an integer but not its multiplicative inverse ½ .

C is a subgroup.

D is not a subgroup. It contains the identity and is closed under inverses, but it is not closed under multiplication. For example 2 is in the subset but not 2×2.

E is likewise not a subgroup, for much the same reasons as D. The set E consists of all complex numbers which lie

to the right of the imaginary axis, and that set certainly contains 1 and is closed under inverses. But it fails to satisfy the most fundamental property of subgroups – it is not closed under multiplication. For example, $e^{\pi i/4}$ lies to the right of the imaginary axis but its square is i and lies on that axis, and its cube, $e^{3\pi i/4}$ lies to the left.

F is a subgroup because it is the cyclic subgroup generated by π.

Exercise 3:
The fact that H and K are subgroups of G can be most easily seen by extracting their group tables from the main table:

H	**1**	**c**	**d**
1	1	c	d
c	c	d	1
d	d	1	c

K	**1**	**b**
1	1	b
b	b	1

Since every entry in each table belongs to the subset in each case each subset is closed under multiplication. Clearly each contains the identity and, since 1 appears in each row and column, every element has an inverse within the respective subset.

The right cosets of H in G are H = {1, c, d} and aH = (a1, ac, ad} = {a, b, e}.
The left cosets of H in G are H = {1, c, d} and Ha = {1a, ca, da} = {a, e, b}.

NOTE: that in this example the left and right cosets are the same, even though the group is non-abelian.

The right cosets of K in G are K = {1, *b*}, *a*K = {*a*1, *ab*} = {*a*, *c*} and *d*K = {*d*1, *db*} = {*d*, *e*}.

NOTE: that we didn't waste our time with *b*K or *c*K because those elements were already included and we would have simply repeated the first two cosets.For example *b*K = {*b*1, *bb*} = {*b*, 1} = {1, *b*}. So always use as a representative for a new coset, an element which has not yet been included.

The left cosets of K in G are K = {1, *b*},
K*a* = {1*a*, *ba*} = {*a*, *d*} and K*c* = {1*c*, *bc*} = {*c*, *e*}

NOTE: that in this case the left cosets and the right cosets give two different subdivisions of the group. Thus K is not one of these normal subgroups.

Exercise 4:

The elements are: $1, \quad a, \quad a^2, \quad a^3,$
$b, \quad ab, \quad a^2b, \quad a^3b,$
$b^2, ab^2, a^2b^2, a^3b^2.$

The right cosets are $\mathrm{H} = \{1, b, b^2\}$

$$a\mathrm{H} = \{a, ab, ab^2\}$$
$$a^2\mathrm{H} = \{a^2, a^2b, a^2b^2\}$$
$$\text{and } a^3\mathrm{H} = \{a^3, a^3b, a^3b^2\}$$

Of course since this group is abelian the left cosets are the same as the right cosets.

Exercise 5:

Using $b^2 = 1$ this becomes $a^7ba^{-2}baba^3\mathrm{b}a^2ba^7a$, and combining powers of a we get $a^7ba^{-2}baba^3ba^{10}$.

Using $a^5 = 1$ we get $a^2ba^3baba^3\mathrm{b}$. Now we need to make use of the relation $ba = a^{-1}b$.

Moving each b past an a, inverts the a. Moving the second last b to the back we get:

$$a^2ba^3baa^{-3}b^2 = a^2ba^3ba^3.$$

Moving the next b down gives $a^2ba^3a^{-3}b = a^2bb = a^2$.

Exercise 6:

The expression can be successively simplified as follows:

$$a^{13}b^5a^2b^{-7}a^2ba \to a^3ba^2ba^2ba \to a^3ba^2ba^2a^{-1}b$$
$$\to a^3ba^2bab \to a^3ba^2a^{-1} \to a^3ba \to a^2b.$$

Exercise 7:
By Lagrange's Theorem divides 68. Since H is not cyclic and groups of prime order are cyclic, |H| is not prime. Similarly it is not 1 (groups of order 1 contain just the identity and are cyclic). So we're looking for a divisor of 68 which is neither 1 nor a prime. Since the prime factorisation of 68 is $2^2.17$, the only possibilities are 4 and 68. However since H is a *proper* subgroup, this means it is not the whole of G and so 68 is ruled out. Thus, by a process of elimination, |H| = 4.

Exercise 8:
By Lagrange's Theorem |H| divides 100. H being non-cyclic rules out 1 and the primes 2 and 5, leaving 4, 5, 10, 20, 25, 50 and 100. Now groups of even order must contain an element of order 2. Since H doesn't, it must have odd order, leaving 25 as the only possibility.

Exercise 9:
By Lagrange, |H| divides both $168 = 8\times3\times7$ and $112 = 16\times7$ and therefore must divide their greatest common divisor, which is 56. Since H contains an element of order 7, |H| must be divisible by 7. This limits the possibilities to 7, 14, 28 and 56. Now since H is neither cyclic nor dihedral, |H| cannot be prime or twice a prime. This narrows down the possibilities to 28 and 56. Now if |H| was 56 there would be exactly 2 left cosets in K which has order 112. By clue (e) this is not so, and hence 56 is ruled out. Therefore |H| must be 28.

Exercise 10:

(a) This is easily verified. Note that $gx = xg$ implies that $xg^{-1} = g^{-1}x$.

(b) $D_{2n} = \langle a, b \mid a^n = b^2 = 1, ba = a^{-1}b \rangle$.

If $a^r \in Z(G)$ then $a^r b = ba^r = a^{-r}b$, so $a^{2r} = 1$ which means that n divides $2r$.

If n is odd this means n divides r and so $a^r = 1$.

If n is even a^r is 1 or $a^{n/2}$.

Similarly one can check that no element of the form $a^r b$ commutes with a.

So $Z(D_{2n}) = \{1\}$ if n is odd and $\{1, a^{n/2}\}$ if n is even.

coopersnotes.net
LIST OF TITLES

GENERAL

- The Mathematics At The Edge Of The Rational Universe

ELEMENTARY

- Basic Mathematics
- Concepts of Algebra
- Concepts of Calculus
- Elementary Algebra
- Elementary Calculus

1st YEAR UNI

- Techniques of Algebra
- Techniques of Calculus
- Matrices

2nd YEAR UNI

- Linear Algebra
- Languages & Machines
- Discrete Mathematics

3rd YEAR UNI

- Group Theory volume 1
- Group Theory volume 2
- Galois Theory
- Graph Theory
- Number Theory
- Geometry
- Topology
- Set Theory

POSTGRADUATE

- Ring Theory
- Representation Theory
- Quadratic Forms
- Group Tables vol 1
- Group Tables vol 2