Groups - Part 2 (12 pages; 23/10/16)

(A) Cyclic Groups - Examples

Notes

(a) All cyclic groups of order n (denoted C_n) are isomorphic.

(b) All groups of prime order are cyclic (but the converse is not true).

(1) $(\mathbb{Z},+)$

infinite order; $e = 0$; $a^{-1} = -a$

(2) $\{0,1,2, \dots , n-1\}$ under addition mod n (or 'modulo' n)

- commonly denoted $(\mathbb{Z}_n, +)$

Note: it is possible to write $a +_n b$, but $a + b$ is used when the modulus is understood.

For eg $(\mathbb{Z}_4, +)$, $\{0,2\}$ is a subgroup.

(3) $(\{1, -1\},\times)$

(4) $\{1, i, -1, -i\}$ under multiplication of complex numbers

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$i^2 = -1, i^3 = -i, i^4 = 1$, so i is of order 4

$(-1)^2 = 1$, so -1 is of order 2

$(-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$, so $-i$ is of order 4

Thus, i & $-i$ are generators of the group (being inverses of each other).

(5) {1,2,4,8} under multiplication mod 15

	1	2	4	8
1	1	2	4	8
2	2	4	8	1
4	4	8	1	2
8	8	1	2	4

(6) $\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\}$

under multiplication

[$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$: 90° rotation clockwise

$b = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$: 180° rotation

$c = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$: 90° rotation anti-clockwise]

[More generally, the group generated by the rotation of a plane through $\frac{360°}{n}$ about a fixed point.]

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

a & c are generators of the group

(7) $\{x, -\frac{1}{x}, \frac{x-1}{x+1}, \frac{1+x}{1-x}\}$

under composition of functions on $x \in \mathbb{R}, x \neq -1,0,1$

Let $a = -\frac{1}{x}$, $b = \frac{x-1}{x+1}$ & $c = \frac{1+x}{1-x}$

Then $a^2 = -\frac{1}{\left(-\frac{1}{x}\right)} = x = e$

and $b^2 = \frac{\left(\frac{x-1}{x+1}\right)-1}{\left(\frac{x-1}{x+1}\right)+1} = \frac{x-1-(x+1)}{x-1+(x+1)} = \frac{-2}{2x} = a$

So, if this is to be a group, it must be cyclic, rather than the Klein 4-group (since all elements are of order 2 for the latter).

As $a^2 = e$, it is worth relabelling the elements, so that $b = -\frac{1}{x}$

Then it doesn't matter how the other non-identity elements are labelled; eg $a = \frac{x-1}{x+1}$ & $c = \frac{1+x}{1-x}$, and the Cayley table is found to be:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(8) If $\omega = e^{2\pi i/3}$, $\{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$ under multiplication

(B) Non-Cyclic Groups - Examples

(1) $\{1,3,5,7\}$ under multiplication mod 8

Note: More generally, the positive integers less than n which have no factors in common with n (with 1 included) form a group under the operation of multiplication mod n.

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Klein 4-group (as not cyclic)

Note that the similar-looking group {1,2,4,8} under multiplication mod 15 was found to be cyclic.

(2) $\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}\}$

under multiplication

[$a = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$: reflection about x-axis

$b = \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$: reflection about y-axis

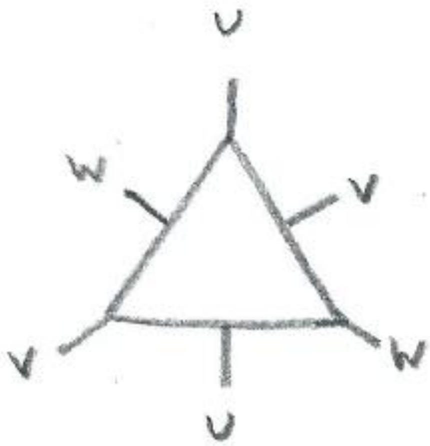
$c = \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$: 180° rotation]

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

ie the Klein 4-group

(3) The symmetry group of an equilateral triangle, D_3 has order 6. [D stands for 'dihedral' ("having or formed by 2 planes" - although that doesn't really explain much!)]

[More generally, D_n (the symmetry group of a regular n-sided polygon) is of order $2n$: in addition to the identity element, there will be $n-1$ rotations and n reflections.]



Let I be the identity transformation.

Let P be a rotation of 120° anticlockwise in the plane of the paper.

Let Q be a rotation of 120° clockwise in the plane of the paper.

Let U, V & W be reflections in the U, V & W axes respectively.

The Cayley table is found to be as follows:

(with the 1st transformation being along the top)

	I	P	Q	U	V	W
I	I	P	Q	U	V	W
P	P	Q	I	W	U	V
Q	Q	I	P	V	W	U
U	U	V	W	I	P	Q
V	V	W	U	Q	I	P
W	W	U	V	P	Q	I

The following observations can be made:

(i) The group is non-abelian.

(ii) U, V & W are of order 2.

(iii) $P^3 = P(P^2) = PQ = I$ and $Q^3 = Q(Q^2) = QP = I$, so that both P & Q are of order 3. And $\{I, P, Q\}$ is a subgroup.

(Note that, whilst U, V & W don't appear in the section of the table with rows and columns of I, P & Q, the reverse isn't true: P & Q do appear in the remainder of the table.)

(4) Permutations of $(1,2,3, \dots n)$

eg (for $n = 5$) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}$ is a possible permutation.

Denoted S_n (S stands for symmetric - though the origin of this isn't clear).

The order is $n!$ (n ways of choosing the 1st entry of the 2nd row,

$n - 1$ ways of choosing the 2nd entry etc)

(By convention, the top row is ordered.)

To find inverse permutations, simply swap the two rows and then order the top row.

For $n = 3$, the elements of the group are

$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \\ 1 & 2 & 3 \end{pmatrix} = e$, $b^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$

$c^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} = d$, $d^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} = c$

$f^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = e$

$$c^3 = c(c^2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = e \ , \ d^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = e$$

All groups of order 6 are either cyclic or isomorphic to D_3. As none of the elements has order 6, S_3 cannot be cyclic. Comparing with D_3, and relabelling, the two elements of order 3, c & d need to be P & Q (or the other way round); noting that c & d are the cyclic permutations of $(1,2,3)$.

Then, we can establish that $af = c$, so that we want a, b & f to become U, W & V, respectively (as $UV = P$).

(5) $\left\{x, 1-x, \frac{1}{x}, \frac{1}{1-x}, \frac{x-1}{x}, \frac{x}{x-1}\right\}$

under composition of functions on $x \in \mathbb{R}, x \neq 0,1$

Let $e = x, a = 1-x, b = \frac{1}{x}, c = \frac{1}{1-x}\ , d = \frac{x-1}{x}\ , f = \frac{x}{x-1}$

	e	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	c	e	a	f	d
c	c	b	f	d	e	a
d	d	f	a	e	c	b
f	f	d	c	b	a	e

This group is non-abelian.

$a^2 = e$, so a is of order 2

$b^2 = e$, so b is of order 2

$c^2 = d,\ c^3 = c(c^2) = cd = e$ so c is of order 3

[note that $c(c^2) = c(c)(c) = (c^2)c$, by associativity, so that $cd = dc$ (even though the group isn't abelian)]

$d^2 = c, d^3 = d(d^2) = dc = e$ so d is of order 3

$f^2 = e,$ so f is of order 2

Subgroups: $\{e, a\}, \{e, b\}, \{e, f\}, \{e, c, d\}$

By re-labelling, we can see that this group is isomorphic to D_3:

Rewrite $e\ as\ I, c\ as\ P, d\ as\ Q, a\ as\ U, f\ as\ V$ & $b\ as\ W$

(since $af = c$ & $UV = P$)

(6) Symmetries of a square (order 8), with the following subgroups:

4 reflections (each of order 2)

rotation through 180 (order 2)

rotations through $90°\ or -90°$ (each of order 4)

(C) Summaries of Results

Groups of Order 4

(1) All groups of order 4 are either cyclic or are the Klein 4-group.

(2) Cyclic groups of order 4 have the following structure:

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Alternative form:

	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e

a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

The only proper subgroup is: $\{e, a^2\}$

(3) The Klein 4-group has the following structure:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Alternative form:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

(4) Both these types are abelian.

Groups of Order 6

(1) All groups of order 6 are either cyclic (and therefore abelian) or isomorphic to D_3 (symmetries of an equilateral triangle) (and therefore non-abelian).

(2) Cyclic groups of order 6 have the following proper subgroups:

$\{e, a^2, a^4\}$ and $\{e, a^3\}$

(3) The D_3 group has the following structure:

	I	P	Q	U	V	W
I	I	P	Q	U	V	W
P	P	Q	I	W	U	V
Q	Q	I	P	V	W	U
U	U	V	W	I	P	Q
V	V	W	U	Q	I	P
W	W	U	V	P	Q	I

Cyclic Groups

(1) All groups of prime order are isomorphic to each other; being cyclic. Therefore they are isomorphic to $(\mathbb{Z}_n, +)$.

(2) All cyclic groups are abelian.

(3) A cyclic group of order n (whether n is prime or not) can always be created from $\{0,1,2, \dots, n-1\}$ under addition mod n.

(4) C_n is isomorphic to the group generated by the rotation of a plane though $\frac{2\pi}{n}$, and thus cyclic groups of all orders exist.

(5) A group of order n is cyclic if it contains an element of order n.

(6) Any subgroup of a cyclic group must also be cyclic.

(7) For each factor f of the order n of a cyclic group, there will be a subgroup of order f.

For example, the proper subgroups of the cyclic group of order 12 are: $\{e, a^2, a^4, a^6, a^8, a^{10}\}$, $\{e, a^3, a^6, a^9\}$, $\{e, a^4, a^8\}$, $\{e, a^6\}$

Abelian Groups

(1) A group that contains no elements of order greater than 2 (ie where every element is its own inverse) must be abelian.

(2) All cyclic groups are abelian.

(3) Klein 4-groups are abelian.

(4) All groups of order 4 are abelian.

Subgroups

(1) Lagrange's theorem: The order of a subgroup of a finite group is a factor of the order of the group.

(2) From Lagrange's theorem, groups of prime order have no subgroups.

(3) Let a be an element of a group G. Then $\{a^n : n \in \mathbb{Z}\}$ is a subgroup of G (referred to as the subgroup generated by a). This is an easy way of finding a subgroup.

(4) If H is a non-empty subset of G, then if $ab^{-1} \in H\ \forall a, b \in H$, then H is a subgroup of G

(5) Any subgroup of a cyclic group must also be cyclic.

Elements of Groups

(1) The order of an element divides the order of the group.

(2) Let a be an element of a group G. Then $\{a^n : n \in \mathbb{Z}\}$ is a subgroup of G (referred to as the subgroup generated by a). This is an easy way of finding a subgroup.

(3) If g is a generator of a group, then g^{-1} will be also.

(4) If g is a generator of a group of order n, then g^k will be also if and only if k and n are co-prime (ie have no common factors).

(5) Every element of a group of prime order is a generator of the group.

Isomorphisms

(1) All groups of prime order are isomorphic to each other; being cyclic. Therefore they are isomorphic to $(\mathbb{Z}_n, +)$.

(2) Groups of order 4 are either cyclic, or have 3 elements of order 2 (the Klein 4-group).

(3) Cayley's theorem: Any group of order n is isomorphic to a subgroup of S_n (the group of permutations of $(1,2,3, \ldots, n)$).

(D) Table of possibilities

Order	**Cyclic?**	**Abelian?**	**Proper Subgroups?**	**Notes**
4	Y	Y	Y	C_4
4	N	Y	Y	Klein 4-group
6	Y	Y	Y	C_6
6	N	N	Y	D_3 , S_3
Prime, p	Y	Y	N	C_p
Non-prime, n	Y	Y	Y	C_n
Non-prime, n	N	Y/N	Y/N	