Q 8

List all cyclic subgroups of $U(30)$

$U(30) = \{ x \in \mathbb{Z}_{30} : \gcd(x, 30) = 1 \}$

$U(30)$ is a group under multiplication modulo 30 $= 2 \cdot 3 \cdot 5$

$U(30) = \{ 1, 7, 11, 13, 17, 19, 23, 29 \}$

The cyclic subgroups are

$\langle 1 \rangle = \{ 1 \}$, the trivial subgroup.

$\langle 7 \rangle = \{ 1, 7, \underset{\underset{7^2}{\equiv}}{19}, \underset{\underset{7^3}{\equiv}}{13} \}$

$\langle 11 \rangle = \{ 1, 11 \}$

$\langle 13 \rangle = \{ 1, 13, 19, 7 \} = \langle 7 \rangle$, note that $7^{-1} = 13$

$\langle 17 \rangle = \{ 1, 17, 19, 23 \}$

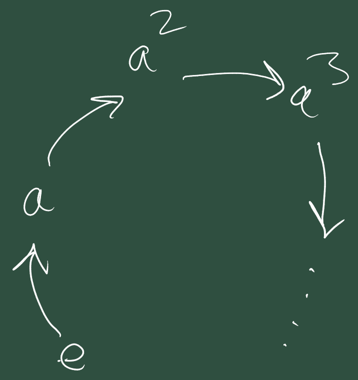
$17(23) \equiv 1$

$\langle 29 \rangle = \{1, 29\}$

<u>Q11</u> Suppose $a \in G$ and $a^{24} = e$

What are possibilities for $|a|$?

$|a| \in \{1, 2, 3, 4, 6, 12, \}$
24, 8



Q14. $G = GL_2(\mathbb{R})$

$=$ all invertible 2×2 real matrices under mat. mult.

$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$

$|A| = ?$, $|B| = ?$ orders of these group elements

$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$

$A^3 = AA^2 = A(-I) = -A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$A^4 = (A^2)^2 = (-I)^2 = I.$

Therefore $|A| = 4$.

$$B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

$$B^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

$$B^3 = BB^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Hence $|B| = 3$

But $AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$

$$= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$(AB)^2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$$

$$(AB)^3 = (AB)(AB)^2$$

$$= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$$

Conjecture

$$(AB)^k = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$$

<u>Proof</u>

$$(AB)(AB)^k = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -k-1 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -(k+1) \\ 0 & 1 \end{pmatrix}$$

So conjecture true by induction.

Therefore $|AB|$ is infinite.

Well suppose a group G is abelian

What $|BA|$?

$$\underbrace{AB\,AB \cdots\cdots AB}_{k \text{ pairs}} = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$$

$$A \underbrace{BA\,BA \cdots\cdots BA}_{k-1} B = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow (BA)^{k-1} = A^{-1} \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} B^{-1}$$

$$= A^{3} \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} B^{2}$$

I expect $|BA|$ will be infinite also.

$$\boxed{\text{Assume } G \text{ is abelian and } x, y \in G \text{ with finite order. conjecture: } |xy| \text{ is finite also.}}$$

Proof. Suppose $|x| = m$, $|y| = n$

FALSE

Then $|xy| = \overset{nm}{\mathrm{lcm}}(n, m)$

$\boxed{x = y^{-1}}$

$(xy)^k = e$?

$|x| = |y|$

$xy = e$

$(xy)^k = xyxyxy \cdots\cdots xy$

$= x^k y^k = e$?

Suppose $|x| = 6$, $|y| = 4$

$(xy)^{24} = e$

$(xy)^2 = x^2 y^2 = \dots$

$(xy)^{12} = x^{12} y^{12}$

$= (x^6)^2 (y^4)^3$

$= e^2 e^3 = e$

So if $k = \text{lcm}(|x|, |y|)$

then $(xy)^k = x^k y^k$

$= e \cdot e = e.$

more detail.

$$|xy| = \text{lcm}(|x|, |y|).$$

Contrast this with Q 14.

Continue 5:10.

$\underline{\text{Q31}}$ Let G be an abelian.

Define $T(G)$, the Torsion subgroup,

$$T(G) := \{ g \in G : |g| \text{ is finite} \}$$

Claim: $T(G)$ forms a subgroup of G.

<u>Proof</u> Use proposition 3.30

1. Is $e \in T(G)$? $|e| = 1$.

so $e \in T(G)$

2. Let $x, y \in T(G)$

so $|x|, |y|$ are finite.

If $|x| = n$, $|y| = m$

$$(xy)^{nm} = x^{nm} y^{nm}$$
$$= (x^n)^m (y^m)^n$$
$$= e^m e^n$$
$$= e.$$

So $|xy|$ is a divisor of nm,

and hence finite.

Therefore $xy \in T(G)$.

3. If $x \in T(G)$, $|x|$ is finite.

~~the~~ and $|x| = |x^{-1}|$

so $x^{-1} \in T(G)$.

So by the subgroup Theorem $T(G)$

forms a subgroup of G.

Chapter 5

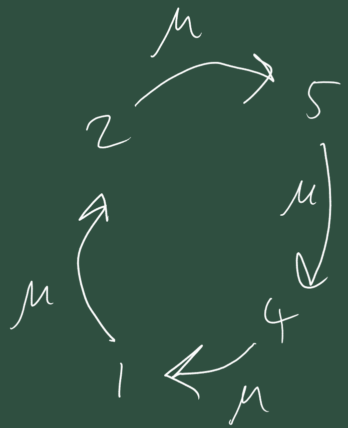
Prefered form of a permutation is its representation as a product of disjoint cycles.

Q2.

a) $\sigma = (1\ 3\ 4\ 5)(2\ 3\ 4)$

$= (1\ 3\ 5)(2\ 4)$

$= (2\ 4)(1\ 3\ 5)$



d) $\lambda = (1\ 2\ 5\ 4)^{100}$

So $\lambda(1) = 1$ $\qquad \lambda = \mu^{100}, \mu = (1254)$

and $\lambda(2) = 2$ and so on

ie $\lambda =$ identity permutation

$= (1)$

Transposition is a 2-cycle

eg $(x\ \ y)$

$$(a_1 \ldots a_m) = (a_{m-1}\, a_m) \ldots (a_2\, a_m)(a_1\, a_m)$$

$m-1$ transpositions

eg $(1\ 2\ 5\ 3) = (5\ 3)(2\ 3)(1\ 3)$

$\Rightarrow$ any permutation can be given as a composition of transpositions.

$\Rightarrow$ If σ can be written as a product of an <u>even</u> number of transpositions then it always requires an <u>even</u> number of transpositions

and the same for odd

— — — .

— — odd — — — .

S_n has an important subgroup A_n, called the Alternating group of index n.

$A_n := \{ \sigma \in S_n : \sigma \text{ is even} \}$.

<u>Q11</u> The possible cycle structures of elements of A_5 are.....

$\boxed{e} = (1)(2)(3)(4)(5)$

Five 1-cycles.

$(1\ 2\ 3) = (1\ 2)(2\ 3) \in A_5$

σ having one 3-cycle.

There are $\underline{\boxed{20}}$ $\boxed{\text{3-cycles in } S_5}$.

$(1\ 3\ 2) \neq (1\ 2\ 3)$

Any 5-cycle is ~~od~~ even and hence $\in A_5$

$(1\ 2\ 3\ 4\ 5)$

There are $\boxed{24}$ $\boxed{\text{5-cycles}}$ in S_5.

The structure of two 2-cycles

eg $(1\ 3)(2\ 4) \in A_5$

So $\frac{10 \times 3}{2} = \frac{30}{2}$ ways of choosing

2 pairs from 5 elements.

So there are $\boxed{15}$ perms in S_5 with cycle structure of $\boxed{\text{two 2-cycles}}$

$|S_5| = 5! = 120$

$|A_5| = \frac{|S_5|}{2} = 60$

$1 + 20 + 24 + 15 = 60$ ✓