Q3.

Hint: First prove $\boxed{a_n \mid a_{n+1} - 2}$

then use to prove that

$$\gcd(a_n, a_{n+1}) = 1 \quad \text{ie.}$$

a_n, a_{n+1} are coprime

then extend this

Chap 5.

(d). $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} \in S_5$

Decompose σ into a product of disjoint cycles

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

$$= (2\ 4)$$

(a) $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$

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

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

Q2. Find the disjoint cycle representation for each permutation.

(d') $\pi = (1\,4\,2\,3)(3\,4)(5\,6)(1\,2\,3\,4)$

$= (1\,3)(5\,6)(2)(4)$

$= (1\,3)(5\,6) \in S_6$

(h) $\mu = (1\,2\,5\,4)^2(1\,2\,3)(4\,5)$

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

g^{-2}

$= g^{-1} \cdot g^{-1}$

(j) $(1\,2\,5\,4)^{100} = id.$

$(1\,2\,5\,4\,7\,6)^{100} = (1\,2\,5\,4\,7\,6)^4$

$= (1\,7\,5)(4\,2\,6)$

(i) $(1\,2\,3)(4\,5)(1\,2\,5\,4)^{-2}.$

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

(k) $\underbrace{|(1\ 2\ 5\ 4)|}_{\text{length of cycle}}$ = least positive int. k s.t. $(1\ 2\ 5\ 4)^k = id$

$= 4$

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

$|\pi| = 6$, the $\mathrm{lcm}(2,3)$, $2,3$ being the orders of disjoint cycles

$\boxed{\text{Q7}}$ What element orders do we see in S_7, A_7?

Think about the different possible disjoint cycle representations of elements in S_7, A_7. A_7 = all the even permutations.

order	element
1.	id.
2.	$(1\ 2) \in S_7$, $(1\ 2)(3\ 4) \in A_7$
3.	$(1\ 2\ 3) \in A_7 = (1\ 3)(1\ 2)$
4	$(1\ 2\ 3\ 4) \in S_7$, $(1\ 2\ 3\ 4)(5\ 6) \in A_7$
5.	$(1\ 2\ 3\ 4\ 5) \in A_7$.
6.	$(1\ 2\ 3\ 4\ 5\ 6) \in S_7$

$(1\ 2\ 3)(4\ 5)(6\ 7) \in A_7$

7. $(1\ 2\ 3\ 4\ 5\ 6\ 7) \in A_7$

~~8~~ Nothing.

~~9~~ "

10 $(1\ 2\ 3\ 4\ 5)(6\ 7) \in S_7$

12 $(1\ 2\ 3\ 4)(5\ 6\ 7) \in S_7$, not A_7.

Q8 For example. 3-cycle $\circ$ 5-cycle.

$$\pi = (1\ 2\ 3)(4\ 5\ 6\ 7\ 8) \in A_{10}$$

Q10

<u>Cyclic Groups</u> under addition mod 60

Q11 "All generators of $\mathbb{Z}_{60} = \{0, 1, 2, \dots, 59\}$ are prime".

$|\mathbb{Z}_{60}| = 60$. $\mathbb{Z}_{60} = \langle 1 \rangle$, 1 is not prime.

<u>theorem 4.13</u>

n will generate $\mathbb{Z}_{60}$ provided $\gcd(n, 60) = 1$.

So any prime p from $1, \dots, 59$ will generate $\mathbb{Z}_{60} = \langle p \rangle$

$60 = 2^2 \cdot 3 \cdot 5$

$\gcd(49, 60) = 1$ so $\mathbb{Z}_{60} = \langle 49 \rangle$

(b) "$U(8)$ is cyclic" FALSE

$U(8) = \{1, 3, 5, 7\}$ under mult. mod 8.

$\langle 3 \rangle = \{3^0 = 1, 3^1 = 3, 3^2 = 9 \equiv 1\} = \{1, 3\}$

$\langle 5 \rangle = \{1, 5\}$, $\langle 7 \rangle = \{1, 7\}$

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

$H = \{1, 3, 5, 7\} = U(8)$

d) is FALSE, $U(8)$ is a counterexample

D_3 is also a counter-example.

e) infinite groups include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$,

$\mathbb{Q}^*$, $\mathbb{R}^*$

considering cyclic subgroups $\langle x \rangle$, we can construct infinite lists of subgroups

Q2 $|5|$ within $(\mathbb{Z}_{12}, +)$

$|5| = k$, where k is the least positive multiple such that

$k \cdot 5 \equiv 0 \pmod{12}$

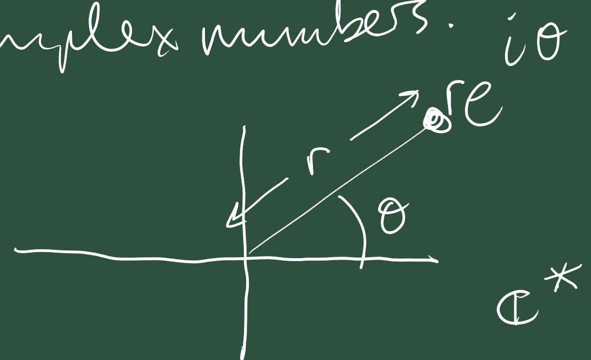
i.e. $12 \mid k \cdot 5$

Note 5 is coprime to 12

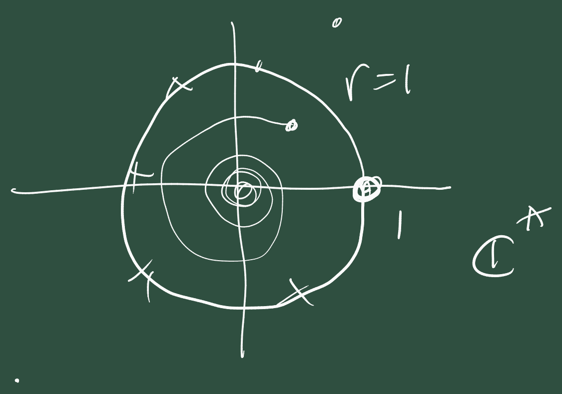
$\Rightarrow k = 12$.

So $|5| = 12$, i.e. $\mathbb{Z}_{12} = \langle 5 \rangle$.

(d) $|-i|$ in $\mathbb{C}^*$ = multiplicative group of non-zero complex numbers.



$$(re^{i\theta})^n = r^n e^{in\theta}$$



$|-i| =$

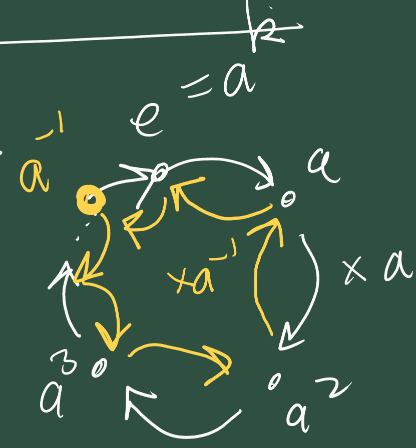
$(-i)^1 = -i$, $(-i)^2 = i^2 = -1$

$(-i)^3 = -i \cdot (-i)^2 = -i(-1) = i$

$(-i)^4 = ((-i)^2)^2 = (-1)^2 = 1$

So $|-i| = 4$

<u>Q23</u> A general group G.



Let $a, b \in G$.

a) $|a| = |a^{-1}|$.

<u>Proof</u> Note that if

$$a^k = e.$$

$$\iff (a^k)^{-1} = e^{-1}$$

$$\iff a^{-k} = e$$

$$\iff (a^{-1})^k = e$$

Therefore $|a| = |a^{-1}|$

b). $\forall\ g \in G$ $\quad |\overbrace{g^{-1}ag}^{\text{"conjugation of } a \text{ by } g\text{"}}| = |a|$

<u>Pf</u>:

$$(g^{-1}ag)^k = \overbrace{g^{-1}ag\ g^{-1}ag\ g^{-1}ag \cdots g^{-1}ag}^{k \text{ brackets}}$$

$$= g^{-1}aeaeae \cdots eag$$

$$= g^{-1} a^k g$$

$$(g^{-1} a g)^k = e.$$

$$\iff g^{-1} a^k g = e.$$

$$\iff \underbrace{g g^{-1}} a^k \underbrace{g g^{-1}} = g e g^{-1} = e$$

$$\iff a^k = e.$$

Therefore $|g^{-1} a g| = |a|$.

(c) $|ab| = |ba|$

<u>Proof</u> Note. we can't assume G is abelian.

~~If G is abelian~~ $ab = ba$

$$(ab)^k = (ba)^k$$

$$\Rightarrow |ab| = |ba| \checkmark$$

If we can't use commutativity.

Well $(ab)^k = ababab \ldots\ldots ab$

$$= a(ba)^{k-1}b$$

Consider $\boxed{(ab)^k = e.}$

$$\Leftrightarrow a(ba)^{k-1}b = e.$$

$$\Leftrightarrow (ba)^{k-1} = a^{-1}b^{-1}$$

$$\Leftrightarrow (ba)(ba)^{k-1} = ba\,a^{-1}b^{-1}$$

$$\Leftrightarrow \boxed{(ba)^k = e.}$$

Therefore $|ab| = |ba|$

$+$ $\quad \mathbb{Z}, +$ $\quad \cancel{n * m}$ $\quad n+m$

$\cancel{n^k}$ $\quad \underbrace{n+n+\cdots\cdots+n}_{k}$

$= k \cdot n$

$\mathbb{Q}, +$

$\mathbb{R}, +$ $\quad (\mathbb{Z}_n, +)$

$\mathbb{Q}^*$, $\mathbb{R}^*$