$a_0, a_1, a_2, a_3, \ldots$

$\gcd(a_i, a_j) = 1$

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

Once you've proven this try and prove then that $\gcd(a_n, a_{n+1}) = 1.$

and then try and generalise this to any pair.

$$a_{n+1} - 2 = 10^{2^{n+1}} + 1 - 2$$

$$= 10^{2^{n+1}} - 1$$

$$= (\underline{\quad ? \quad}) a_n$$

$$= (\quad ? \quad)(10^{2^n} - 1)$$

Investigate $n = 1, 2, 3, 4, 5, \ldots$

Also look at the exercise.
Chap 3 Q 10, 11

where we used.

$$\left(a^m - b^m\right) = (a-b)\left(\sum_{j=0}^{m-1} a^{m-1-j} b^j\right)$$

$$a_{n+1} - 2 = q\, a_n$$

<u>Q15</u> $\sigma \in S_9$

$$\sigma = (1\ 2)(3\ 4\ 5)(7\ 8)(9)$$

This σ has cycle structure/type

$[1, 2, 2, 3]$

<u>Claim</u> $\alpha, \beta \in S_n$

α, β have the same cycle type iff α, β are conjugate.

ie. $\exists\ \gamma \in S_n \quad \beta = \underline{\gamma \alpha \gamma^{-1}}$

<u>Proof</u>: We will prove that if β contains a cycle of length m, then so does α.

So suppose β has the cycle

$$(a_0, a_1, a_2, \dots, a_{m-1})$$

so $\beta(a_j) = a_{j+1 \pmod m}$

Assume $\beta = \gamma \alpha \gamma^{-1}$, for some $\gamma \in S_n$.

so also $(\gamma \alpha \gamma^{-1})(a_j) = a_{j+1 \pmod m}$

Let's define. $\boxed{x_j = \gamma^{-1}(a_j),\ j = 0, \dots, m-1}$

$$(\gamma \alpha \gamma^{-1})(a_j) = a_{j+1}$$

$$\Rightarrow \gamma(\alpha(\gamma^{-1}(a_j))) = a_{j+1}$$

$$\Rightarrow \gamma(\alpha(x_j)) = a_{j+1}$$

$$\Rightarrow \gamma^{-1}(\gamma(\alpha(x_j))) = \gamma^{-1}(a_{j+1})$$

$$\Rightarrow \boxed{\alpha(x_j) = x_{j+1}.}$$

This means α contains the cycle.

$(x_0, x_1, x_2, \ldots, x_{m-1})$

---

eg. $\sigma = (6)(1\ 2)(3\ 4\ 5)(7\ 8)(9)$

Consider the conjugate

$\gamma \sigma \gamma^{-1}$ where γ is the permutation

$\gamma = (1\ 2\ 3\ 4\ 5)(6\ 7\ 8\ 9)$

Let's write down the disjoint cycle decomposition of $\gamma \sigma \gamma^{-1}$

$\gamma \sigma \gamma^{-1} = (1\ 4\ 5)(2\ 3)(6)(7)(8\ 9)$

Q20] Let H, K be subgroups of G.

Relation $\sim$ on G defined by

$a, b \in G$ $a \sim b$ iff $\exists\, h \in H, k \in K$ $b = hak$

Claim: $\sim$ is an $\underbrace{\text{equivalence relation}}$.

① reflexive i.e. $\forall x \in G$ $x \sim x$

② symmetric i.e. $\forall x, y \in G$ $x \sim y \Rightarrow y \sim x$

③ transitive, i.e. $\forall x, y, z \in G$ $(x \sim y \;\&\; y \sim z) \Rightarrow x \sim z$

①. Let $x \in G$.

we have to find $h \in H$, $k \in K$ such that

$$x = h x k$$

this is achieved when $h = e$, $k = e$.

$$x = e x e = x \quad \checkmark$$

So $\sim$ is reflexive.

②. Let $x, y \in G$ and suppose $x \sim y$.

$\Rightarrow \exists\, h, k \in K$ $x = hyk$

$$\Rightarrow y = \underset{\in H}{\underline{h^{-1}}}\, x\, \underset{\in K}{\underline{k^{-1}}} \quad \checkmark$$

$$\Rightarrow y \sim x.$$

So $\sim$ is symmetric.

③ Let $x, y, z \in G$. Suppose $x \sim y$ & $y \sim z$

$\Rightarrow \exists\, h_1, h_2 \in H$, $k_1, k_2 \in K$ such that

$x = h_1 y k_1$, $y = h_2 z k_2$

$\Rightarrow x = \underbrace{h_1 h_2}_{\in H} z \underbrace{k_2 k_1}_{\in K.}$, note $h_1 h_2 \in H$ and $k_1 k_2 \in K$ since H, K are subgroups.

$\Rightarrow x \sim z$

So $\sim$ is transitive.

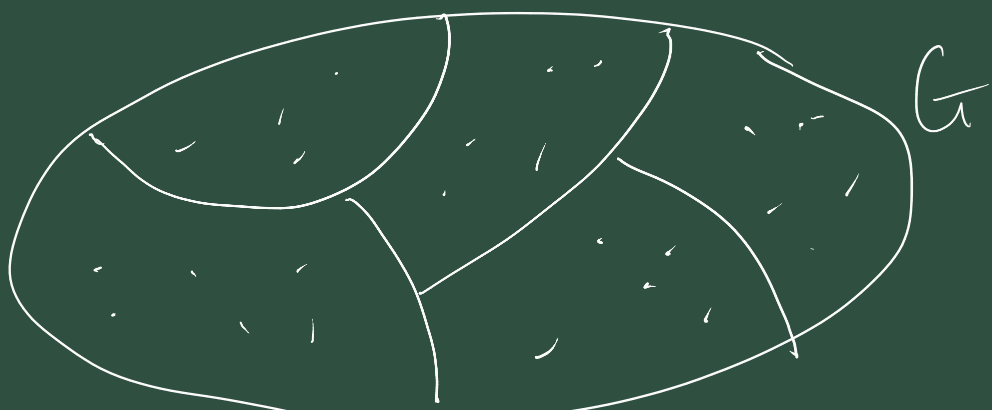
So $\sim$ is an equivalence relation on G.

There is an equivalence relation that goes hand in hand with cosets concept.

Given a subgroup H of G.

Define relation $\sim$ on G by.

$x \sim y$ iff $xH = yH$., i.e. x, y are in the same coset.



Q53) Chap 3

Let H be a subgroup of G.
Define the centralizer of H in G as $C(H)$.

$$C(H) = \{ g \in G : \forall h \in H \; gh = hg \}.$$

Claim: $C(H)$ is a subgroup of G.

Proof Check the conditions of Prop 3.30

1. $e \in C(H)$ since $\forall h \in H$ $\boxed{eh = h = he}$

2. Let $x, y \in C(H)$. Let $h \in H$.
$xyh = xhy = hxy$, since $x, y \in C(H)$.

$\Rightarrow \forall h \in H \; (xy)h = h(xy)$
$\Rightarrow xy \in C(H)$

3. Let $x \in C(H)$
$\Rightarrow \forall h \in H \; xh = hx$
$\Rightarrow \forall h \in H \; xh^{-1} = h^{-1}x$, since $h^{-1} \in H$.
$\Rightarrow (xh^{-1})^{-1} = (h^{-1})^{-1}x^{-1} = hx^{-1} = (h^{-1}x)^{-1} = x^{-1}(h^{-1})^{-1}$
$= x^{-1}h$

$\Rightarrow \forall h \in H \; x^{-1}h = hx^{-1}$
$\Rightarrow x^{-1} \in C(H)$.

So by Prop 3.30 $C(H)$ is a subgroup of G.

$\boxed{Q42}$ $G = M_2(\mathbb{R})$ = group of 2×2 matrices with real entries under addition.

Consider the subset $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a+d=0 \right\}$

Claim: H is a subgroup of G.

Proof: Using additive notation in G.

1. Well the identity of G is the matrix

$Z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $Z \in H$ ✓ since trace $Z = 0$

2. Let $X, Y \in H$

$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $Y = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, $\quad a+d=0$, $e+h=0$

$\Rightarrow X + Y = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$

and $\operatorname{trace}(X+Y) = a+e+d+h = (a+d)+(e+h) = 0$

$\Rightarrow \quad X + Y = H$

3. Let $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$, ie $a+d=0$

well $-X = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$

$\text{trace}(-X) = -a-d = -(a+d) = -0 = 0$

So by prop 3.30 H is a subgroup of G.
subgroup theorem.

$\boxed{\text{Q14}}$ Example of a general construction called (external) direct product of groups.

Consider the two known groups

$\mathbb{R}^* =$ non-zero reals under $\times$

$\mathbb{Z} =$ integers under $+$.

Consider the Cartesian product.

$$G = \mathbb{R}^* \times \mathbb{Z} = \left\{ (r, z) : \begin{array}{l} r \in \mathbb{R}^* \\ z \in \mathbb{Z} \end{array} \right\}$$

Claim: G is a group under the operation $\circ$ defined by

$$(a,m)\circ(b,n) = (ab, m+n) \in G$$

$\therefore$ G is closed under $\circ$ since.

$ab \in \mathbb{R}^*$, $m+n \in \mathbb{Z}$ so $(ab, m+n) \in \mathbb{R}^* \times \mathbb{Z}$

Associativity

$$\big((a,m)\circ(b,n)\big)\circ(c,p)$$

$$= (ab, m+n)\circ(c,p) \quad \text{, def of } \circ$$

$$= \big((ab)c, (m+n)+p\big) \quad \text{, def of } \circ.$$

$$= \big(a(bc), m+(n+p)\big) \quad \text{, using associativity of } \mathbb{R}^* \text{ and } \mathbb{Z}.$$

$$= (a, m)\circ(bc, n+p) \quad \text{, def of } \circ.$$

$$\downarrow$$

$$= (a,m)\circ\big((b,n)\circ(c,p)\big) \quad \text{, def of } \circ.$$

So $\circ$ is associative on G.

Does G have an identity? Yes

It is $(1, 0)$

$1 \to$ id. of $\mathbb{R}^*$, $0 \to$ id of $\mathbb{Z}$.

$$(a, n) \circ (1, 0) = (a \cdot 1, n + 0)$$
$$= (a, n)$$

Does G contain inverses for all its elements? Yes.

$$(a, n)^{-1} = \left(\frac{1}{a}, -n\right) \in G.$$

inv. from $\mathbb{R}^*$, inv from $\mathbb{Z}$.

$$(a, n) \circ \left(\frac{1}{a}, -n\right) = \left(a \cdot \frac{1}{a}, n + (-n)\right)$$
$$= (1, 0)$$

the identity from G.

Hence G is a group under $\circ$.

In fact this all generalizes to a general group theory construction.

If G_1, G_2 are groups then $G_1 \times G_2$ is a group with the operation: $x_1, y_1 \in G_1$, $x_2, y_2 \in G_2$

$$(x_1, x_2) \circ (y_1, y_2) = (x_1 y_1, x_2 y_2)$$

and also extends to a direct product of any number of factors.