Alg-6

$A \in GL(n, K)$

$a \in K^n$

$f_{A,a} : K^n \to K^n$ by

$f_{A,a}(x) = \underbrace{Ax}_{\in K^n} + a \in K^n$

$G = GL(n, K) \times K^n$

G is a group

$g \in G \quad g = (A, a)$

$h \in G \quad h = (B, b)$

$gh = (AB, a+b)$, coordinatewise

G is direct product of two groups

$\mathbb{R}$ is a group. where

$g \cdot h = gh = (AB, a+b)$

G_i, $i = 1 \ldots n$ are groups

$G = G_1 \times \ldots \times G_n = \{(g_1 \ldots g_n) : g_i \in G_i \ (i = 1 \ldots n)\}$

$gh = (g_1 h_1, \ldots, g_n h_n)$. Then G is a group $\Rightarrow g^{-1} = (g_1^{-1}, g_2^{-1} \ldots g_n^{-1})$

For $g = (g_1 \ldots g_n)$

Back to $G = GL(n, K) \times K^n$

↑ product

Back ...

semidirect product

$f_{A,a}(x) = Ax + b$

X

$ax = ay \implies x = y$

$a + x = a + y \implies x = y$

Thm G is a group. Then

1. e of G is unique:
2. $a \in G \implies b \in G \cdot ab = ba = e$ is unique
3. For each $a \in G$
   $(a^{-1})^{-1} = a$
4. For $a, b \in G$ $(ab)^{-1} = b^{-1}a^{-1}$
5. (i) The eqn $ax = b$ for $a, b \in G$ has a unique sol in G

   (ii) The eqn $xa = b$, for $a, b \in G$ has a unique sol.

Cor: (a) $ax = ay$ for $a \in G \implies x = y$ (called the left cancellation law)

(b) $xa = ya$ for $a \in G$ $\implies x = y$ (called the right cancellation law)

Proof. Have proved (1) & (2) earlier.

(3) $a \in G$. Then $aa^{-1} = e = a^{-1}a$

... inverse

(3) $a \in G$. Then $aa^{-1} = e = a^{-1}a$

So by uniqueness of inverse

$(a^{-1})^{-1} = a$

Recall the axiom of group is: $a \in G$, $\exists b \in G$ s.t. $ab = e = ba$

b is unique & called the inverse of a & write $b = a^{-1}$

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

(4) Let $a, b \in G$

Then $aa^{-1} = e = a^{-1}a$ and

$bb^{-1} = e = b^{-1}b$

Now to prove $(ab)^{-1} = b^{-1}a^{-1}$

& $(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1}$ by assoc

$= a(e)a^{-1}$

$= aa^{-1} = e$

and $(b^{-1}a^{-1})(ab) = e$ similar.

$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$.

5 (a) Given $ax = b$, $a, b \in G$

$a^{-1}(ax) = a^{-1}b$

and $x = ex = (a^{-1}a)x$
$= a^{-1}(ax)$
$= a^{-1}b \in G$

Similarly, $xa = b$
then $x = ba^{-1} \in G$

Is $\mathbb{Z}$ is a group under product?

Is $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ a group under product? No

---

Recall that $H \leq G$, G is a group is a subgroup of G, denoted $H \leq G$ iff
(1) $e \in H$
(2) $a, b \in H \Rightarrow ab \in H$
(3) $a \in H \Rightarrow a^{-1} \in H$

FACT: $H \leq G \iff ab^{-1} \in H$
$\forall\ a, b \in H$

Proof $\Rightarrow$. Assume H is a subgroup
let $a, b \in H$, $b^{-1} \in H$ as
H is a subgroup. $a \in H$ & $b^{-1} \in H$
$\Rightarrow ab^{-1} \in H$ as H is
a subgroup

$\Leftarrow$ Assume $ab^{-1} \in H$ $\forall\ a, b \in H$.

$\Leftarrow$ Assume $ab^{-1} \in H$ $\forall a, b \in H$.

Taking $a = b$. we get $e = aa^{-1} \in H$

Let $a, b \in H$, $eb^{-1} = b^{-1} \in H$

$b = (b^{-1})^{-1}$

$ab = a(b^{-1})^{-1} \in H$

$b^{-1} \in H$ for $b \in H$.

Ex 1 $H = \{e\}$ is a subgroup of G called the trivial subgroup

G itself is a subgroup of G

2. $\mathbb{Z} \subseteq \mathbb{Q}$ is a subgroup under addition, but $\mathbb{Z}^* \subseteq \mathbb{Q}^*$ is not a subgroup under product
3. $\mathbb{Q}^*$ is a subgroup of $\mathbb{R}^*$ w.r.t.
4. $\mathbb{R}^*$ - - - - - - $\mathbb{C}^*$ w.r.t product
5. $GL(n, \mathbb{R}) \subseteq M_{n \times n}(\mathbb{R})$ ↑ not a group under product
6. $O(n, \mathbb{R}) \subseteq GL(n, \mathbb{R})$

$A \in O(n, \mathbb{R}) \iff A^t = A^{-1}$

$SL(n, \mathbb{R}) \leq O(n, \mathbb{R}) \leq GL(n, \mathbb{R})$

|| special linear group

$\iff A \in O(n, \mathbb{R})$

special linear group

$A \in SL(n,\mathbb{R}) \iff A \in O(n,\mathbb{R})$ and $\det(A) = 1$

$SL(n,\mathbb{R})$ called the set of rotation matrices.

$\emptyset \neq S \subseteq G$, G is a group

Define $H = \{x_1 \cdots x_n : x_i \in S$ or $x_i^{-1} \in S$ for $i = 1 \cdots n\}$ $n \in \mathbb{N}$

$= \{y_1^{\varepsilon_1} \cdots y_m^{\varepsilon_m} : y_1 \cdots y_m \in S$, $\varepsilon_i = 1$ or -1 for each $i = 1 \cdots n\}$

H is a subgroup of G

$e \in H$ when $e = xx^{-1} \in H$ for $x \in S$

$a, b \in H$

$a = x_1 \cdots x_n$, $b = y_1 \cdots y_m$ where $x_i \in S$ & $x_i^{-1} \in S$ and $y_j \in S$ or $y_j^{-1} \in S$

$ab = x_1 \cdots x_n y_1 \cdots y_m \in H$

$a^{-1} = x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1} \in H$

H is a subgroup of G

& write $H = \langle S \rangle$ &

S is called generates of H

and H is generated by S

Def $S=\{a\}$, $H=\langle a\rangle$, is called a cyclic subgroup of G

If $G=\langle a\rangle$, G is called a cyclic group

G is finitely generated if $\exists\ S\subseteq G$ s.t. S is finite and $\langle S\rangle = G$.

Ex 1. $\mathbb{Z}=\langle 1\rangle$, $m\in\mathbb{Z}$

$m>0$ $\quad m=\underbrace{1+\cdots+1}_{m}$

$m<0$, $\quad -m=\underbrace{-1-\cdots-1}_{m\text{ times}}$

$0\cdot 1=0\in\mathbb{Z}$

2 Let G be a group Fix $a\in G$. $H=\{a^m : m\in\mathbb{Z}\}$

$=\langle a\rangle$

Prove that H is a subgroup of G

$e=a^0\in H$

Let $x,y\in H$, $x=a^n$, $n\in\mathbb{Z}$

$y=a^m$, $m\in\mathbb{Z}$

$xy=a^n\cdot a^m=a^{m+n}$, $m+n\in\mathbb{Z}$

$\in H$

$x\in H \Rightarrow x=a^n$, $n\in\mathbb{Z}$

$x^{-1} = (a^m)^{-1} = a^{-n}, -n \in \mathbb{Z}$

$\in H$

So H is a subgroup of G. H is called a cyclic subgroup generated by $a \in G$

Def If $G = \langle a \rangle = H$, then G is called a cyclic group

Ex 1. $\mathbb{Z}$ is cyclic

2. $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots [n-1]_n\}$

Is $\mathbb{Z}/6\mathbb{Z} = \{[0]_6, [1]_6, [2]_6, [3]_6, [5]_6\}$ cyclic?

Or Is $\mathbb{Z}/n\mathbb{Z}$ cyclic?

Yes $\mathbb{Z}/n\mathbb{Z} = \langle [1]_n \rangle$

Thm $H \leq \mathbb{Z} = \langle 1 \rangle$

Then $H = \langle a \rangle$ for some $a \in \mathbb{N}$

i.e. every subgroup of $\mathbb{Z}$, a cyclic group, is cyclic.

Proof. If $H = \{0\} = \langle 0 \rangle$, then done.

Suppose $H \neq \{0\}$

$S = H \cap \mathbb{N}$

Claim: $S \neq \phi$

Proof. Since $H \neq \{0\}$, $\exists\, m \in H$ s.t. $m \neq 0$. If $m > 0$, then $m \in S$. If $m < 0$ then $-m \in H$ & $-m \in \mathbb{N}$ $\Rightarrow -m \in S$. proved

$S \neq \phi$

By WOP $\exists\, d \in S$ s.t. $d \leq s \;\forall s \in S$

Claim $H = \langle d \rangle$

$d \in H$, $md \in H$, $\forall m \in \mathbb{Z}$

$\{md : m \in \mathbb{Z}\} \subseteq H$ ∴ To show $H \subseteq \langle d \rangle = \{md : m \in \mathbb{Z}\}$

$x \in H$, $x \in \mathbb{Z}$

$x = qd + r$ by Euclidean algorithm

$0 \leq r < d$

$r = x - qd \in H$. If $r > 0$ then $r \in H$, $d \leq r$, a contradiction

$r = 0$

$x = qd \in \langle d \rangle$.

Let $G = \langle a \rangle$, a cyclic group generated by a

Case 1. There is no $m \in \mathbb{N}$ s.t. $a^m = e$

i.e. $a^m \neq e \ \forall\ m \in \mathbb{N}$.

i.e. hence $a^m \neq e \ \forall\ m \in \mathbb{Z}$.

Then we say that G is infinite cyclic group (Ex $\mathbb{Z} = \langle 1 \rangle$ is cyclic & infinite.

$\{a^n\}, n \in \mathbb{Z}$ are all distinct

$n \neq m \quad a^n \neq a^m$

Suppose $a^n = a^m$

for $n, m \in \mathbb{Z}$

$$\Rightarrow a^{n-m} = a^n \cdot a^{-m}$$
$$= a^m \cdot a^{-m}$$
$$= a^{m-m}$$
$$= a^0$$
$$= e$$

$$\Rightarrow n - m = 0$$
$$\Rightarrow n = m$$

Case II. There $m \in \mathbb{N}$ s.t. $a^m = e$

In this case we say a has finite order & m is called an exponent of a, write $m = \text{Exp}(a)$

Let $J = \{n \in \mathbb{Z} : a^n = e\}$

then $m \in J \Rightarrow J \neq \{0\}$

then $n \in J \Rightarrow$ [illegible]

J is a subgroup of $\mathbb{Z}$

$0 \in J$ as $a^0 = e$

Suppose $n \in J \Rightarrow a^n = e$

$\Rightarrow e = e^{-1} = (a^n)^{-1} = a^{-n}, -n \in \mathbb{Z}$

$\Rightarrow -n \in J$

$n, m \in J$ to show $n+m \in J$

$\Downarrow$

$a^n = e = a^m$

Now $a^{n+m} = a^n \cdot a^m = e \cdot e = e$

$\Rightarrow n+m \in J$

By a theorem we proved today

$\exists\, d \in \mathbb{N}$ s.t. $J = \langle d \rangle$

d is smallest positive integer of J

s.t. $a^d = e$ and for any $n \in J = \langle d \rangle$

$n = qd$ for some $q \in \mathbb{Z}$

$a^n = a^{qd} = (a^d)^q$

Order of a group G is the number of elements $|G| = \#G$

Order of G is the number of elements in G & write $|G| = \#G$

$\mathbb{Z}$ is infinite group
$\mathbb{Z}/n\mathbb{Z}$ is finite order. $|\mathbb{Z}/n\mathbb{Z}| = n$.

Continuation of case II : $\exists m \in \mathbb{N}$ s.t. $a^m = e$

$\exists\ d \in \mathbb{N}$ s.t. $a^d = e$, & d is the smallest in its the book:

$a^k = e$, then $d \leq k$

If $a^k = e$ then $d \mid k$.

$k = qd + r$ by Euclidean $0 \leq r < d$.

If $\neq r$ integers. then

$a^r = a^{k-qd} = a^k \cdot (a^d)^{-q}$

$= e\ e = e$

$\Rightarrow d \leq r$, a contradiction

Hence $r = 0$ $k = qd \Rightarrow d \mid k$.

Thm Let G be a group. $a \in G$ suppose a is of finite order (This means $\exists m \in \mathbb{N}$ s.t. $a^m = e$). Let d be the period of a (which means $a^d = e$ and $a^r = e$

m.l.

... means $a^d = e$ and $a^r = e$
then $d \mid r$ (i.e. d is smallest such number). Then
the cyclic subgroup $H = \langle a \rangle$
is of order d i.e. $\#H = |H| = d$

$$H = \{e, a, a^2, \ldots a^{d-1}\}$$

Proof. Show $e, a, a^2, \ldots a^{d-1}$ are all distinct.

Suppose $a^r = a^s$ for $r, s \in \{0, 1, \ldots d-1\}$

then $a^{r-s} = a^r \cdot a^{-s} = a^s \cdot a^{-s} = e$

$\Rightarrow d \mid r-s \Rightarrow r-s = qd$

$d \leq r-s$

$\Rightarrow r-s = 0 \Rightarrow r = s$

$\text{Perm}(S) = \{f : S \to S \text{ bijective}\}$

where $S \neq \phi$. Then

Thm (1) $f, g \in \text{Perm}(S) \Rightarrow f \circ g \in \text{Perm}(S)$

(2) $f \in \text{Perm}(S) \Rightarrow f^{-1} \in \text{Perm}(S)$

That is $(\text{Perm}(S), \circ)$ is a group called a permutation group on S

$X \neq \phi$, $\text{Perm}(X) \equiv S_X$

$X \neq \phi$, $\text{Perm}(X) = S_X$

$X = \{1, \ldots n\}$, $S_X \equiv S_n$

$n = 3$, $X = \{1, 2, 3\}$

$(S_3, \circ)$ is a group & in general

$|S_n| = n!$, $|S_3| = 6$

$$S_3 = \{e, \alpha, \beta, \beta^2, \alpha\beta, \beta\alpha\}$$

where $\alpha(1) = 2$, $\alpha(2) = 1$, $\alpha(3) = 3$ and $\beta(1) = 2$, $\beta(2) = 3$, $\beta(3) = 1$

Check that $(\alpha\beta)(1) = 1$

$(\alpha\beta)(2) = 3$

$(\alpha\beta)(3) = 2$

and $(\beta\alpha)(1) = 3$

$(\beta\alpha)(2) = 2$

$(\beta\alpha)(3) = 1$

So $\alpha\beta \neq \beta\alpha$

$S_3 = \langle \alpha, \beta \rangle$, $\alpha^2 = id$, $\beta^3 = id$

$H_1 = \langle \alpha \rangle$

$H_2 = \langle \beta \rangle$ are two subgroups of S_3

$H_2 = \langle \beta \rangle$ subgp of S_3

$|H_1| = 2$, $|H_2| = 3$

$H_1 = \{id, \alpha\}$ period $\alpha = 2$

$H_2 = \{id, \beta, \beta^2\}$ period $\beta = 3$

FINITE ORDER OF $a \in G$ IS SOME $m \in \mathbb{N}$ s.t. $a^m = e$

$m = \text{Exp}(a)$.

Period of a is the smallest $d \in \mathbb{N}$ s.t. $a^d = e$.

---

① Group homomorphism $f: G \to G'$

② ker f, kernel of a homo

③ $f: G \to G'$ is homo

f is injective $\iff \ker f = \{e\}$