LN VIII a

§4.4)

Group $(G, \cdot)$

- $a, b \in G \Rightarrow ab \in G$.
- $a, b, c \in G \Rightarrow (ab)c = a(bc)$ (associative)
- $\exists e$ (identity) $ea = ae \quad \forall a \in G$
- $\forall a \; \exists \bar{a}'$ (inverse) $a\bar{a}' = e = \bar{a}'a$.

- $(\mathbb{Z}, *)$ not a group. (No inverse)
- $F(X) = \{f : X \to X\}$. $fg = f \circ g$.
  If f is not invertible the f does not have an inverse

Definition Semi-group $(S, \cdot)$

- $a, b \in S \Rightarrow ab \in S$
- $a, b, c \in S \Rightarrow (ab)c = a(bc)$

$(F(X), \circ)$ Semi-group.

Ring $(R, +, \cdot)$

1) $(R, +)$ group, abelian. $(a+b = b+a)$

2) $(R, \cdot)$ semi-group

3) $\forall x, y, z \in R$

$$x(y+z) = xy + xz$$

$$(x+y)z = xz + yz$$

(distributive)

Examples

- $(\mathbb{Z}, +, \times)$ with 1. multiplicative identity.
- $(2\mathbb{Z}, +, \times)$ no 1.
- $M_2(\mathbb{R})$ 2x2 matrices.
  with 1.
  with zero-divisors

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

- $(\mathbb{Z}_n, +, \times)$ with 1.

Only when n is prime each non-zero elem has a multiplicative inverse.

- $(\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, +, \times)$

- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

Ring with multiplicative inverse. $(a,b) \neq (0,0)$

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

Field $(F, +, \times)$

1) Commutative ~~Ring~~ : $xy = yx$.

2) $\exists\ 1 \neq 0$ $\quad 1x = x = x1$.

3) Every $x \neq 0$ has inverse x^{-1}

$$xx^{-1} = 1 = x^{-1}x.$$

Ex) $\mathbb{Z}_p$ p prime.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $\mathbb{Q}[\sqrt{2}]$

$(F \setminus 0, \times)$ Abelian group

Lemma $(R,+,\cdot)$ Ring.

$\forall x \quad x0=0=0x.$

Pf) let $y=x0$.

$y+y = x0+x0 = x(0+0) = x0 = y.$

Add $-y$: $y=0$. □.

Similarly $0x=y$

Vector Space (V,F)

F field. (scalar)

V abelian group. (vector)

Scalar multiplication $\lambda\in F, v\in V$.

$\lambda v \in V$.

V1) $\lambda v \in V \quad \forall \lambda\in F \quad v\in V$

V2) $(\lambda\mu)v = \lambda(\mu v) \quad \forall \lambda,\mu\in F \quad v\in V.$

V3) $1v = v \quad \forall v\in V$

V4) $(\lambda+\mu)v = \lambda v+\mu v \quad \forall v\in V, \lambda,\mu\in F$

V5) $\lambda(v+w) = \lambda v+\lambda w \quad \forall v,w\in V \ \lambda\in F$

Ex) • $F = \mathbb{R}$ $V = \mathbb{R}^n$

• $V = M_n(\mathbb{R})$ $n \times n$ matrices

$F = \mathbb{R}$.

• $V = M_n(\mathbb{Z}_p)$ $n \times n$ matrices with entries in $\mathbb{Z}_p$

$F = \mathbb{Z}_p$.

Algebra: is a vectorspace (V, F) where V is also a ring.

Ex) $(M_n(\mathbb{Z}_p), \mathbb{Z}_p)$

§5.1 $(G, \cdot)$ group

- $a, b \in G \Rightarrow ab \in G$ (closed)
- $a, b, c, \in G \Rightarrow (ab)c = a(bc)$ associative
- $\exists e \quad \forall a \in G \quad ea = a = ae$
- $\forall a \exists \bar{a}' \quad a\bar{a}' = e = \bar{a}'a$.

Thm $(G, \cdot)$ group.

$\forall a, b \quad \exists! \, x, y \quad a = bx \quad a = yb$.

Pf) let $x = b^{-1}a$ $(y = ab^{-1})$

$bx = b(b^{-1}a) = (bb^{-1})a = ea = a$.

Uniqueness.. Suppose $a = bc$ $a = bd$.
Then $bc = bd$. Multiply both side by b^{-1}

$b^{-1}(bc) = b^{-1}(bd)$ $\Longleftrightarrow$ associativity.

$(b^{-1}b)c = (b^{-1}b)d \Longleftrightarrow ec = ed$

$\Longleftrightarrow c = d$. □

Ex) $a, b, c, \in G$

$\exists! x \quad xab\bar{a}^1 = c$

let $x = a\,b\,\bar{a}^1$

Uniqueness: $xab\bar{a}^{-1} = c \quad yab\bar{a}^{-1} = c$

Th $xab\bar{a}^1 = yab\bar{a}^1$

(xa on the right)

$xab\bar{a}^1 a = yab\bar{a}^1 a$

$xab = yab$

$x b^{-1}$ on the right

$xabb^{-1} = yabb^{-1}$

$xae = yae$

$xa = ya \qquad x a^{-1} \qquad x = y.$ □.

Ex) $a, b, c \in G$

$\exists! x \quad axb = b^{-1}c.$

let $x = \bar{a}^1 b^{-1} c \quad b^{-1}$

Lemma: identity is unique

inverse is unique.

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

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

Use Thm on pg 6

Pf) The equation $ax=a$ has a unique sol. : $x=e$.

The equation $ax=e$ has a unique sol. : $x=a^{-1}$.

$(a^{-1})^{-1}$ is a solution of $a^{-1}x=e$.

a is also a solution. Hence

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

$(ab)^{-1}$ is a solution of $(ab)x=e$.

$b^{-1}a^{-1}$ is also a sol.

So $(ab)^{-1}=b^{-1}a^{-1}$ □.

Definition powers $(G,\cdot)$ group $g\in G$

$$g^0=e$$

$$g^{k+1}=g\,g^k$$

$$g^{-k}=(g^{-1})^k$$

Thm $(G,\cdot)$

1) $g^r g^s = g^{r+s}$

2) $(g^r)^s = g^{rs}$

3) $g^{-r} = (g^r)^{-1} = (g^{-1})^r$

4) If $gh = hg$ then $(gh)^r = g^r h^r$

Claim: $hg^k = g^k h$, $k \geq 0$

Pf] First prove: If $hg = gh$ then $hg^k = g^k h$, $k \geq 0$

By Induction.

For $k=0$: ok.

$$hg^{k+1} = h(gg^k) = (hg)g^k = g(hg^k) \overset{IH}{=} g(g^k h)$$

$$= (gg^k)h = g^{k+1}h.$$

Proof of 4] By Induction $(r \geq 0)$

$r \geq 0$: ok.

$$(gh)^{r+1} = (gh)(gh)^r = (gh)(g^r h^r)$$

$$= g\,h(g\,g^r h^r) = h\,g^{r+1}h^r$$

$$= (g^{r+1}h)h^r = g^{r+1}h^{r+1}$$

$r = -k < 0$, $k > 0$

$$g^r h^r = (g^{-1})^k (h^{-1})^k = (g^{-1}h^{-1})^k$$

$$= ((hg)^{-1})^k = ((gh)^{-1})^k$$

$\uparrow$ $hg = gh$

$$= (gh)^{-k} = (gh)^r \qquad \square_4$$

Proof of 3|

$$e = e^r = (g\bar{g}^{-1})^r = g^r(\bar{g}^{-1})^r$$

So $(g^r)^{-1} = (\bar{g}^{-1})^r = \bar{g}^{-r}$

Uniquens of sol. $ax = e$

Proof of 1|

Case 1 $r, s \geq 0$ Induction $r+s=n$.

$r=s=0$: ok.

let $r+s=n>0$ at least one is positive

Say $s>0$.

$$g^{r+s} = g^{(r+s-1)+1}$$

$$\overset{\text{def}}{=} g\, g^{r+s-1} \overset{\text{Ind}}{=} g\left(g^{r} g^{s-1}\right)$$

$$= (g g^{r})\, g^{s-1} = (g^{r} g)\, g^{s-1}$$

↑ Claim page g

$$= g^{r}(g g^{s-1}) = g^{r} g^{s} \qquad \square.$$

Case 2) $r+s>0$

Say $r>0$ $s<0$ $(-s=k>0)$

Use Claim page g.

$$g^{-s}\, g^{s} = g^{k}\, g^{-k} = g^{k}(g^{-1})^{k} = (g g^{-1})^{k} = e.$$

Now $r+s>0$ $-s>0$. So from case 1.

$$g^{r+s}\, g^{-s} = g^{r+s-s} = g^{r}.$$

Multiply both sides by g^{s}.

$$(g^{r+s}\underbrace{g^{-s}}_{e})\, g^{s} = g^{r} g^{s} \quad \text{So } g^{r+s} = g^{r} g^{s} \qquad \square.$$

Case 3) $r+s=0$

Say $r>0 \quad -s=r>0$

$$g^r g^s = g^r g^{-r} = g^r (g^{-1})^r = (gg^{-1})^r = e^r = e.$$

Use Lemma 4) $= g^{r+s}$

Case 4) $r+s<0$

Then $-r+(-s)>0$. So from Case 2)

$$g^{-(r+s)} = g^{-s+(-r)} = g^{-s}\, g^{-r}.$$

(3) implies $\left(g^{-(r+s)}\right)^{-1} = g^{r+s}$

Lemma page 7 $(g^{-s}g^{-r})^{-1} = g^s g^r$

So $g^{r+s} = \left(g^{-(r+s)}\right)^{-1} = (g^{-s}g^{-r}) = g^s g^r$. □