Lec 9/27

Friday, September 27, 2019 11:31

let $\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$.

Then $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$.

<u>Prop</u> $\mathbb{H}$ is a division ring.

Pf Let $X = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \neq 0$. Write $a = \alpha_0 + \alpha_1 \sqrt{-1}$, $b = \alpha_2 + \alpha_3 \sqrt{-1}$.

Then $\Delta = \det x = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$.

Also, $X^{-1} = \Delta^{-1} \operatorname{adj} x = \begin{pmatrix} \bar{a}\Delta^{-1} & -b\Delta^{-1} \\ \bar{b}\Delta^{-1} & a\Delta^{-1} \end{pmatrix} \in \mathbb{H}$.

A set of "matrix coordinates" for $\mathbb{H}$ is

$$i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

in the sense that any Quaternion can be written as

$$X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k,$$

and this representation is unique.

Using this representation, the multiplication is determined by the laws

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k$$

$\mathbb{H}$ is a non-commutative division ring.

Quotient Rings & Ideals

<u>Def</u> Let $(M, \cdot, 1)$ be a monoid. a congruence $\equiv$ on M is an equivalence relation s.t. for $a, a', b, b' \in M$ w/ $a \equiv a'$, $b \equiv b'$, $ab \equiv a'b'$.

<u>Ex</u> the relation $\equiv \pmod{m}$, $m > 0$ is a congruence on $(\mathbb{Z}, +, 0)$ and on $(\mathbb{Z}, \times, 1)$.

<u>Prop</u> the quotient set $\overline{M} = M/\equiv$ is a monoid w/ $\overline{1} = \{a \in M \mid a \equiv 1\}$ and $\overline{a}\,\overline{b} = \overline{ab}$.

<u>Thm</u> Let G be a gp. There is a one-to-one correspondence between congruences & normal subgps.

$$\equiv \longleftrightarrow \overline{1}$$

<u>Def</u> Let R be a ring. A congruence $\equiv$ in R is an equiv. rel^n in R that is both a congruence on $(R, +, 0)$ and on $(R, \cdot, 1)$.

Prop The quotient set $\bar{R} = R/\equiv$ w/ additive gp $(\bar{R}, +, \bar{0})$ and mult monoid $(\bar{R}, \cdot, \bar{1})$.

By thm, congruences on $(R, +, 0)$ correspond to subgps I.
abelian
normal

Given I, we have the corresponding congruence $a \equiv b$ iff $a - b \in I$.

So a cong class $\bar{a} \in R/\equiv$ is a coset $a + I$.

If $\equiv$ is also a congruence for $(R, \cdot, 1)$, $\bar{a}\,\bar{0} = \bar{0}\,\bar{a} = \bar{0}$.

So $\boxed{\text{for } a \in R,\ b \in I,\ ab \in I \text{ and } ba \in I}$ $(*)$

Conversely, if $I \leq (R, +, 0)$ s.t. I satisfies $(*)$, then

If $a \equiv a' \bmod I$, $b \equiv b' \bmod I$, $ab \equiv a'b' \bmod I$

$$\left[ab - a'b' = ab - a'b + a'b - a'b' = \underbrace{(a - a')}_{\in I} b + a' \underbrace{(b - b')}_{\in I} \in I\right].$$

Def Let R be a ring. An ideal is a subgr of $(R, +, 0)$ satisfying $(*)$.

Def Let R be a ring, $I \subseteq R$ be an ideal. Then $\underset{R/I}{\overset{R/\equiv}{\shortparallel}}$ is the quotient ring.

Ex The elements of R/I are the cosets $a + I$.

$(a+I) + (b+I) = (a+b) + I$ ← this is a set equality.

$$\underbrace{(a+I)(b+I) =: ab + I}_{\text{this is not necessarily a set equality}}$$

Let $R = \mathbb{Z}$, $I = 10 \cdot \mathbb{Z}$

$(2 + 10\mathbb{Z})$ $\quad$ $(4 + 10\mathbb{Z})$

$\{2 + 10k\}$ $\quad$ $\{4 + 10\ell\}$

set-wise product is $\{8 + 20\ell + 40k + 100k\ell\} \subsetneq 8 + 10\mathbb{Z}$.

<u>Def</u> Let S be a subset of a ring R. The $\underbrace{\text{ideal gen by } S}_{= (S)}$, is the intersection of all ideals $\supseteq S$.

<u>Ex</u> Let $S = \{a_1, \dots, a_n\}$ be a finite subset of R.

Write $(a_1, \dots, a_n)$ for (S). This ideal contains all

$$x a_i y \quad \forall\, x, y \in R.$$

it also contains all finite linear combinations.

$$x_1 a_1 y_1 + \cdots + x_n a_n y_n.$$

Let I be the set of all elements of the form

$$\sum_{i_1} x_{1i_1} a_1 y_{1i_1} + \cdots + \sum_{i_n} x_{ni_n} a_n y_{ni_n} .$$

Then I is an ideal. Also, any element of I must be in $(a_1, \ldots, a_n)$, and $I \supset \{a_1, \ldots, a_n\}$.

So $I = (a_1, \ldots, a_n)$.