Groups:

Today: Review basics, including Sylow theorems
+ go over basic notions / notations

$\mathbb{R}, \mathbb{C}, \mathbb{Z}, \mathbb{Q}, \mathbb{Z}[\frac{1}{n}], \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \middle| \begin{array}{l} a, b \in \mathbb{Z} \\ \gcd(b, p) = 1 \end{array} \right\}$

a prime number

rings: all contain 1

algebras A over a commutative ring R

= a ring homom $R \to A$
such that $\mathrm{Im}(R) \subseteq Z(A)$

$\mathbb{Z}/n\mathbb{Z}$
- cyclic group of (finite) order n
- a finite ring.

G: a group
$\begin{array}{c} G \\ \text{\rotatebox{90}{$\leq$}} \\ H \end{array} \rightsquigarrow N_G(H) = \{ g \in G \mid gHg^{-1} = H \}$

a special case in the general context of group actions.

* left action of G on a set S

$\mu : G \times S \to S$ satisfying <u>unity</u>, associativity.

$S \supseteq T \rightsquigarrow \mathrm{Fix}_G(T) = \{ x \in G \mid \underset{\mu(x,t)}{\underset{\shortparallel}{x \cdot t}} = t \ \forall t \in T \}$

$G \geq \mathrm{stab}_G(T) = \{ x \in G \mid x \cdot T = T \}$

$$\mathrm{Stab}_G(T) = \text{the stabilizer subgroup of the element } T \in 2^S$$
$$= \mathrm{Stab}_G(\{T\}), \quad \{T\} \subseteq 2^S$$

G: a group

$$\begin{array}{rccc} \mathrm{Ad}: & G & \longrightarrow & \mathrm{Aut}_{grp}(G) \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ & x & \longmapsto & \mathrm{Ad}(x): y \longmapsto \mathrm{Ad}(x)y = xyx^{-1} \end{array}$$

$Z(G)$ = the center of G = $\mathrm{Ker}(\mathrm{Ad})$

$\mathrm{Im}(\mathrm{Ad}) = \{$ inner automorphisms of $G \}$

A left action of G on S

$\xleftrightarrow{1-1}$ a homomorphism $G \longrightarrow \mathrm{Perm}(S) = \left\{ \begin{array}{l} \text{bijective maps} \\ \text{from } S \text{ to } S \end{array} \right\}$

a right action of G on S

$\longleftrightarrow$ a homomorphism $G^{opp} \longrightarrow \mathrm{Perm}(S)$

the opposite group of G

$$\begin{array}{ccc} G & \xrightarrow{\sim} & G^{opp} \\ x & \longmapsto & x^{-1} \end{array}$$

Can always turn a right action to a left action, and vice versa.

Given a right action of G on S, define a left action of G on S by

$$\underset{\text{new}}{x * s} \stackrel{\text{def}}{=} s \cdot x^{-1}$$

old right action

<u>Matrices</u> $M_{m\times n}$, M_n

square matrices

R: ring $\rightsquigarrow$ $M_n(R)$ is a ring.

$\det: M_n(R) \longrightarrow R$ for R <u>commutative</u>

R: ring $\rightsquigarrow$ $R^\times$ = invertible elements in R: a group
= units in R

$\rightsquigarrow$ $M_n(R)^\times =: GL_n(R) = \{ A \in M_n(R) \mid \det(A) \in R^\times \}$

R commutative

<u>cofactor</u>!

What is $GL_n(\mathbb{Z})$?

$$A \cdot \left(\begin{matrix}\text{cofactor} \\ \text{matrix of } A\end{matrix}\right) = \det(A) \cdot I_n.$$

<u>Exer</u>: Prove <u>this</u>. (Treat case R = a field) as known

(R = a general commutative ring.)

Sylow theorems:

G: a finite group, p: a prime nber.

$p^a \| G \qquad a \geq 1$

1) $\exists$ a p-Sylow subgroup $P \leq G$

2) P, Q: p-Sylows,

$\Rightarrow \exists\, x \in G$ s.t. $xPx^{-1} = Q$

3) $\#\{p\text{-Sylow subgps of } G\} \equiv 1 \pmod p$

2, 3: easy consequences of the following "counting lemma":

If G is a finite p-group

S is a finite set, $\mu: G \times S \to S$ left action

then $\#\underbrace{(S^G)}_{\{s \in S \mid x \cdot s = s\}} \equiv \# S \pmod p$

For 1): Apply this to:

$S = \{ T \subseteq G \mid \#(T) = p^a \}$

Vector spaces

Modules R: a ring

- a left R module is:
  - an abelian group M.
  - a map $\mu : R \times M \longrightarrow M$

    s.t. $\mu(x, \mu(y,m)) = \mu(x \cdot y, m)$ $\forall x,y \in R$, $\forall m \in M$

    $\mu(x, m_1+m_2) = \mu(x, m_1) + \mu(x, m_2)$ $\forall x \in R$ $\forall m_1, m_2 \in M$

    $\mu(x+y, m) = \mu(x,m) + \mu(y,m)$ $\forall x,y \in R$ $\forall m \in M$

  equiv: a ring homom

$$R \longrightarrow \mathrm{End}_{grp}(M)$$

a right R-module M

$\longleftrightarrow$ a ring homom $R^{opp} \longrightarrow \mathrm{End}_{grp}(M)$

(Exer!)

Question Is it true that R^{opp} is isomorphic to R for every ring R?

Extra problem for assignment.

Remark

1) commutative rings —— numbers
functions
(e.g. all $\mathbb{C}$-valued function on $\mathbb{R}^n$)

2) non-commutative rings
—— operators e.g. $M_n(\mathbb{C})$
$\parallel$
$\mathbb{C}$-linear operators on $\mathbb{C}^n$

$\mathrm{End}_R(M)$ M: module over R
[R commutative]

3) groups are more difficult than rings.
$\updownarrow$
symmetry

modules $\longleftrightarrow$ linear alg. over rings

Example of modules

Ex 1 V: a vector space over a field k
T: a k-linear oper. on V. i.e. $T \in \mathrm{End}_k(V)$
$\rightsquigarrow$ define a $k[x]$-module structure on V by

$$\underset{\substack{\uparrow \\ k[x]}}{f(x)} \cdot \underset{\substack{\uparrow \\ V}}{v} :\overset{\text{def}}{=} f(T)(v)$$

$\longrightarrow$ Canonical forms, using the fact that $k[x]$ is a PID and the structure theorem of finitely generated modules over a PID.

Ex. Is the statement also true for $\mathcal{O}_K$

Extra Credit

$[K:\mathbb{Q}]=2$ quadratic ext'n field

$\mathcal{O}_K = \left\{ z \in K \;\middle|\; \begin{array}{l} \exists \text{ a monic quad. poly } f(x) \in \mathbb{Z}[x] \\ \text{s.t. } f(z)=0 \end{array} \right\}$

$\mathbb{C} \geq K \geq \mathbb{Q}$ field

Let G be a finite group

k: a field, V: a vector space over k

Several ways to look at the same notion

- a left action of G on V through linear endomorphisms
- a group homomorphism
  $\rho: G \longrightarrow \mathrm{End}_k(V)^\times =: GL_k(V) =: \mathrm{Aut}_k(V)$
- a ring homom
  $\rho: k[G] \longrightarrow \mathrm{End}_k(V)$

where $k[G]$ = the group ring of G over k
with underlying set a vector space
over k with basis $\{[x] \mid x \in G\}$

and $\displaystyle\sum_{x\in G} \underset{\overset{\uparrow}{k}}{a_x}[x] + \sum_{x\in G} \underset{\overset{\uparrow}{k}}{b_x}[x] = \sum_{x\in G}(a_x+b_x)[x]$

$$\sum_{x\in G} a_x[x] \cdot \sum_{y\in G} b_y[y] = \sum_{x,y\in G} a_x b_y [x\cdot y]$$

<u>Exer.</u> : Show that these 3 concepts are <u>equiv.</u>