MATH 403/503 L1

Groups → Fields ← Rings

Groups.
- Quotient Groups
- Group Actions.
- Counting.
- Sylow Theory.
- Abelian Groups.

Rings.
- Quotient Rings
- Maximal/prime ideals
- PIDs, UFDs, EDs

Fields
- Extensions
- Galois Theory
- Finite Fields.

Def A *binary operation* on a set A is a function $\mu : A \times A \to A$.

Usually we write $a \cdot b$ instead of $\mu(a, b)$.

Def A *monoid* (M, μ, e) is a set M with a binary op. μ and an element $e \in M$ s.t.

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\quad \forall a, b, c \in M$

$a \cdot e = a = e \cdot a$ $\quad \forall a \in M$

Def ~~An element a of a monoid M is a unit~~

Let x be an element of a monoid M.

$y \in M$ is a *left inverse* of x if

$yx = e$.

$y \in M$ is a *right inverse* of x if

$xy = e$

$y \in M$ is an inverse of x if y is both left and right inverse of x.

x is a unit if it has an inverse $y \in M$.

Def A group G is a monoid such that every $x \in G$ is a unit.

Notation $M^\times = \{x \in M \mid x \text{ is a unit}\}$

Exercise $M^\times$ is a group using the operation in M.

Examples. 1) $(\mathbb{Z}, \cdot, 1)$ is a monoid ($\cdot$ = mult. of integers)

and $\mathbb{Z}^\times = \{1, -1\}$

2) $(\mathbb{N}^*, +, 0)$ is a monoid, $\mathbb{N}^\times = \{0\}$

($\mathbb{N}^* = \{0, 1, \ldots\}$)

3) $(\mathbb{N}, \cdot, 1)$ is a monoid $\mathbb{N}^\times = \{1\}$

4) $(\mathbb{Z}, +, 0)$ is a group

5) Let X be a set and X^X the set of all functions $f: X \to X$.

Then $(X^X, \circ, Id_X)$ is a monoid ($\circ$: function comp.; Id_X: identity fcn on X).

Then $f \in X^X$ is a unit iff f is bijective. So the group of units of X^X is $S_X = \{f: X \to X \mid f \text{ is bij}\}$ called the symmetric group on X.

6) The set $M_n(\mathbb{R})$ of $n \times n$-matrices with real entries forms a monoid under matrix mult, and $e = I_n$.

The group of units is

$$GL_n(\mathbb{R}) = M_n(\mathbb{R})^\times = \{A \in M_n(\mathbb{R}) \mid A \text{ is invertible}\}$$

(general linear group.)

Def A monoid is commutative (or abelian) if $xy = yx \ \forall x, y \in M$

Exercise Determine when X^X is commutative.

Let $(M, \cdot, 1_M), (N, *, 1_N)$ be monoids.

Def A <u>monoid homomorphism</u>

$$\varphi : M \to N$$

is a function such that

1) $\varphi(m_1 \cdot m_2) = \varphi(m_1) * \varphi(m_2)$

($\cdot$: op. in M; $*$: op. in N)

2) $\varphi(1_M) = 1_N$

Remark If M, N are groups, then 2) holds automatically, and furthermore $\varphi(g^{-1}) = \varphi(g)^{-1}$ $\forall g \in M$.

Ex. $\exp : (\mathbb{R}, +, 0) \to (\mathbb{R}_{>}, \cdot, 1)$

$$\alpha \longmapsto e^{\alpha}$$

is a homomorphism of groups: $e^{\alpha} e^{\beta} = e^{\alpha+\beta}$

Ex $\cos(\alpha+\beta) \neq \cos(\alpha) + \cos(\beta)$ in general

However

$$\rho : (\mathbb{R}, +, 0) \longrightarrow GL_2(\mathbb{R})$$

$$\alpha \longmapsto \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

is a group homomorphism:

$$\rho(\alpha)\rho(\beta) = \begin{bmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta & \cdots \\ \cdots & \cdots \end{bmatrix} = \begin{bmatrix} \cos(\alpha+\beta) & \cdots \\ \cdots & \cdots \end{bmatrix}$$

$$= \rho(\alpha+\beta).$$

Def A submonoid of a monoid $(M, \cdot, e)$ is a subset $N \subseteq M$ s.t. $xy \in N \ \forall x, y \in N$ (closure) and $e \in N$.

Def The kernel of a monoid homomorphism $\varphi : M \to N$ is

$$\ker \varphi = \{ x \in M \mid \varphi(x) = e_N \}$$

Note If $x, y \in \ker \varphi$ then

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) = e_N \cdot e_N = e_N$$

so $x \cdot y \in \ker \varphi$. Also $\varphi(e_M) = e_N$ so $\ker \varphi$ is a submonoid of M.

Example Recall $\rho : \mathbb{R} \to GL_2(\mathbb{R})$ we have

$$\ker \rho = \{ \alpha \in \mathbb{R} \mid \rho(\alpha) = I_2 \} =$$

$$= \{ \alpha \in \mathbb{R} \mid \cos\alpha = 1, \sin\alpha = 0 \} =$$

$$= 2\pi\mathbb{Z} = \{ 2\pi n \mid n \in \mathbb{Z} \}.$$