(1) MATH 407

3/14/18

Groups

Def. (Binary operation) $*$ on a set S is a function $*: S \times S \to S$

$$*(s_1, s_2) = s_1 * s_2 \in S$$

Def. (Group) $(G, *)$ $*$ binary operation on G

1) $*$ Associative $a*(b*c) = (a*b)*c$

(contd. below)

Def. If $*$ is binary operation on G, then $e_\ell \in G$ is left identity for $*$, $e_\ell * g = g$ $\forall g \in G$ and $e_r \in G$ is right identity for $*$, $g * e_r = g$

Lemma: If $*$ is binary operation on G w/ both left and right identities they are the same.

Pf. $$\underset{e_\ell}{\overset{\shortparallel}{e_\ell}} * \underset{e_r}{\overset{\shortparallel}{e_r}}$$

2) $*$ has identity e

Cor. Identities are unique

Inverses: Let $*$ be an associative binary operation on G with an identity. Let $g \in G$

If $g_\ell^{-1} g = e$ (left identity), $g g_r^{-1} = e$ (right identity)

>>>

Lemma: If g_ℓ^{-1}, g_r^{-1} exist for g, then $g_\ell^{-1} = g_r^{-1}$

Pf. $(g_\ell^{-1} * g * g_r^{-1})$

$$g_r^{-1} = e * g_r^{-1} = g_\ell^{-1} * e = g_\ell^{-1}$$

>>> ☐ 3) g has an inverse g^{-1} for any $g \in G$.

Def. A group $(G, *)$ is commutative or Abelian iff $g_1 * g_2 = g_2 * g_1 \quad \forall \{g_1, g_2\} \subseteq G$

Def. Let $a \in G$.

$m_a^\ell : G \to G$ left multiplication by g

$m_a^\ell(g) = ag$

$m_a^r(g) = ga$ right multiplication by g

Lemma: m_a^ℓ, m_a^r are bijections.

Pf. $m_a^\ell(g_1) = m_a^r(g_2)$ left cancellation

$$ag_1 = ag_2$$
$$a^{-1}(ag_1) = a^{-1}(ag_2)$$
$$g_1 = g_2$$

If $g \in G$, solve $m_a^\ell(x) = g$

$$ax = g$$
$$x = a^{-1}g$$

③

⊛ <u>Thm.</u> $(g_1g_2)^{-1} = g_2^{-1}g_1^{-1}$

<u>Pf.</u> $(g_1g_2)(g_2^{-1}g_2^{-1}) = g_1(g_2g_2^{-1})g_1^{-1}$

$= g_1 E g_1^{-1}$

$= g_1g_1^{-1}$

$= e$

⊛ <u>Def.</u> $g \in G$, $g^0 = e$, $g^{-1} = g$, $g^{k+1} = g^1g^k$, $g^1 = m_g^l(e)$,
$g^{k+1} = m_g^l(g^k) = m_g^l(m_g^l)^k(e)$

$g^{k+l} = g^kg^l = g^{l+k} = g^lg^k$ (all powers commutative)

Example: If S is a set then $\mathrm{Sym}(S)$ is a group under composition.
Non-commutative. S_n, $n > 2$

⊛ 1) $(\mathbb{Z}, +)$ $(\mathbb{Z}_n, +)$
2) $(F, +)$ Field
3) $(V, +)$ Vector space
4) $(F_{n\times m}, +)$, $M_n(F)$ if $m=n$
5) $(F^\times, \times)$, $F^\times \setminus \{0\}$
6) $(\mathbb{Z}_n^\times, \times)$

7) $\mathbb{R}^{++} = (0, \infty)$ is group under $\times$.
$\mathbb{R}^+ = [0, \infty)$

8) $GL(n,F)$ = invertible elements A of $M_n(F)$

$= \{A : |A| = \det(A) \neq 0\}$

$S_1 \subseteq \mathbb{C} = \{z : |z| = \sqrt{x^2+y^2} = 1\}$, $z = x+iy$.

$(S, \times)$ is group $= \{e^{i\theta} : 0 \leq \theta < 2\pi\}$

$= \{\cos\theta + i\sin\theta, \pi\}$