UCSD, Fall 2019.

LECTURE NOTES:

"MODERN ALGEBRA I"
(MATH 103A)

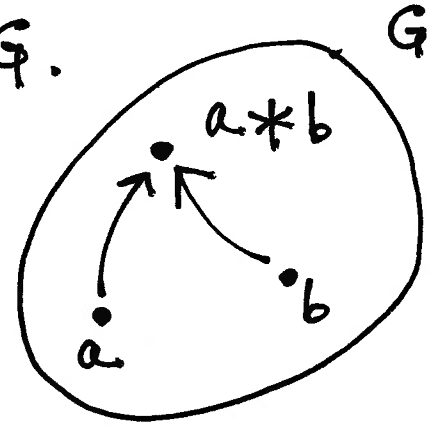
CLAUS M. SORENSEN

LECTURE 1

(Friday SEP. 27, 2019)

— What is a group?

A set G with a specified way of "combining" two elements $a, b \in G$.
(satisfying three conditions...)



More precisely G is endowed with a function:

$$
\begin{aligned}
G \times G &\longrightarrow G \\
(a, b) &\longmapsto a * b
\end{aligned}
$$

known as the "composition law".

GROUP AXIOMS:

(1) The associative law: $\forall a, b, c \in G$,

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

(2) Existence of a neutral element:
There's some $e \in G$ with the property

$$a * e = a = e * a$$

for all $a \in G$.

[LATER: Such an e is necessarily unique.]

(3) Every element has an <u>inverse</u>: $\forall a \in G$ there's some $b \in G$ with the property

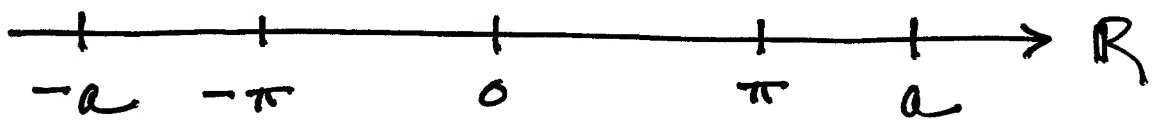
$$a * b = e = b * a.$$

[LATER: Such b is necessarily uniquely determined by a. We denote it by a^{-1}.]

<u>Examples:</u>

<u>Note:</u> Not requiring that $a*b = b*a$ — say G is <u>abelian</u>.

(i) $\mathbb{R} = \{\text{real numbers}\}$ with <u>addition</u>:



$(\mathbb{R}, +)$ is an <u>additive</u> group:

- $(a+b)+c = a+(b+c)$
- $a+0 = a = 0+a$ $\qquad (e=0)$
- $a+(-a) = 0 = (-a)+a$

$\quad$ ↖ the <u>inverse</u> of a. (additive)

(it's even <u>abelian</u>:

$a+b = b+a$)

(ii) $\mathbb{R}$ with <u>multiplication</u> is <u>not</u> a group,

but $\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\} = \{$<u>nonzero</u> real numbers$\}$

<u>is</u> a (multiplicative) group:

- $(ab)c = a(bc)$
- $1a = a = a1$ $\qquad (e = 1)$
- $a\frac{1}{a} = 1 = \frac{1}{a}a$

the (multiplicative) inverse of a.
— only defined when $a \neq 0$.

(it's again <u>abelian</u>: $ab = ba$)

(iii) $GL_N(\mathbb{R}) = \{$invertible $N \times N$-matrices$\}$.
with <u>matrix multiplication</u>.

1st note this <u>is</u> a composition law on $GL_N(\mathbb{R})$. I.e.,

A, B invertible $\Longrightarrow$ AB invertible.
(so <u>lies</u> in $GL_N(\mathbb{R})$)

Why? "Shoes and Socks"

$$(AB)^{-1} = B^{-1}A^{-1}$$

- Linear Algebra:

  - $(AB)C = A(BC)$
  - $AI = A = IA$ $\qquad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ identity matrix. $(N=3)$
  - $AA^{-1} = I = A^{-1}A$.

    (A^{-1}:) inverse matrix.

This is NOT abelian: (for $N > 1$)

$N=2$ counterexample:

$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Here

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

$BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

- invertible ones:

  $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ don't commute.

Finite groups: $|G|$ = cardinality $< \infty$.
(# of elements)

(iv) $|G| = 1$.

Here $G = \{e\}$ and $e * e = e$.

(v) $|G| = 2$.

Here $G = \{e, a\}$. There are $16 \; (= 2^4)$ composition laws

$*$	e	a
e	e	a
a	a	e

(composition table)

— but only one gives a group!

$a * a$ must be e.

(otherwise: $a * a = a \Rightarrow a = e$) cancel factor a.

(vi) $|G| = 3$.

$G = \{e, a, b\}$. Now there are 19683 ($= 3^9$) composition laws. Only <u>one</u> group!

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

check $a * b = e$
(by ruling out a, b)

Say there's only one group of size 3
— up to "ISOMORPHISM".
($\sim$ renaming the elements)

<u>LATER</u>: There are <u>two</u> G with $|G| = 4$.

cyclic   Klein.