Math 113, Fall 2019
Lecture 4, Tues, 9/10/2019

Topics Today:

- Identity elements and inverse elements, Groups
- Reading for Thurs: Up to (and including) §6

1 Clicker Questions

Which of the following is **not** a part of the definition for $\langle G, * \rangle$ to be a group? Answer: $*$ is commutative.
A group $\langle G, * \rangle$ is said to be **abelian** if (and only if): Answer: $*$ is commutative.

2 Lecture

Definition: identity element -

An **identity element** of a binary structure $\langle S, * \rangle$ is an element $e \in S$ such that $e * s = s * e = s, \forall_{s \in S}$. Hence having an identity element is a **stuctural property**.

Remark: In fact, if $\langle S, * \rangle$ has an identity element e and $\phi : S \to S'$ is an isomorphism, then $\phi(e)$ is an identity element of S'.

Proof. $\forall_{s' \in S'} \exists_{s \in S} : s' = \phi(s)$, so that

$$s' * \phi(e) = \phi(s) * \phi(e) = \phi(s * e) = \phi(s) = s',$$

and similarly $\phi(e) * s' = s'$. □

Additionally, if a binary structure has an identity element, then the identity element e is unique.

Proof. Consider:

$$e_1 = e_1 * e_2 = e_2,$$

where first equality follows from that e_2 is an identity, and the second equality follows from e_1 as the identity. □

Also, another thing: $\langle \mathbb{Z}^+, + \rangle$ is NOT isomorphic to $\langle \mathbb{N}, + \rangle$, where the latter has identity element 0, whereas the former does not have an identity element. Recall that in order to show two binary structures are isomorphic, it suffices to show that they differ in a structural property. That is, one fails the structural property whereas the other satisfies that same property.

Definition: Inverse -

Let $\langle S, * \rangle$ be a binary structure with identity element e, and let $s \in S$. Then an **inverse** of s is an element s' such that

$$s * s' = s' * s = e.$$

Example: In $\langle \mathbb{Z}, + \rangle$, 0 is the identity and n has inverse $-n$.
In $\langle \mathbb{C}, \cdot \rangle$, z has the inverse $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$ if $z \neq 0$, where 0 has no inverse. And 1 is the identity element.
In $\langle \mathbb{Z}, \cdot \rangle$, only 1 and -1 have inverses.
In $\langle U, \cdot \rangle$, all elements have inverse.

2.1 Matrices

Let $n \in \mathbb{Z}^+$. Define $M_n(\mathbb{R})$ as the set of $n \times n$ matrices with entries in $\mathbb{R}$. In $\langle M_n(\mathbb{R}), \text{matrix mult} \rangle$, I_n (the identity matrix) is the identity element and a matrix M has an inverse (M^{-1}) if and only if $\det M \neq 0$.

2.2 Clicker Question

Let $\langle S, * \rangle$ be the binary structure with $S = \{e, a, b\}$ and $*$ given by:

$$\begin{bmatrix} * & e & a & b \\ e & e & a & b \\ a & a & e & e \\ b & b & e & b \end{bmatrix}$$

(so it has an identity element e). How many elements of S have inverses?
Answer: 3.

3 Groups

Definition: Group -

A group $\langle G, * \rangle$ is a binary structure $\langle G, * \rangle$ such that :
(1) $*$ is associative. That is,

$$a * (b * c) = (a * b) * c, \forall_{a,b,c \in G}.$$

(2) $\langle G, + \rangle$ has an identity element, and

$$\exists_{e \in G} : a * e = e * a = a, \forall_{a \in G}$$

(3) every element of G has an inverse.

$$\forall_{a \in G} \exists_{a' \in G} : a * a' = a' * a = e.$$

Remark: Let $\langle G, * \rangle$ be a group and let $a \in G$. Then the inverse a' of a is **unique**.

Proof. If a' and a'' are inverses of a, then associativity gives:

$$a' * (a * a'') = (a' * a) * a''$$
$$a' * e = e * a''$$
$$a' = a'',$$

□

Example:
- $\langle \mathbb{Z}, + \rangle$ is a group
- $\langle \mathbb{N}, + \rangle$ is NOT a group (only 0 has an inverse)
- $\langle \mathbb{R}, \cdot \rangle$ is NOT a group (0 has no inverse)
- $\langle \mathbb{R} \setminus \{0\}, \dot{} \rangle$ is a group
- $\langle V, + \rangle$ is a group, where V is ANY vector space.
- $\langle \{e\}, e * e = e \rangle$ is a group (this is called the 'trivial group')
- $\{\}$ is NOT a group (no inverse)

Definition: $GL_n(\mathbb{R})$ **-**

Let $n \in \mathbb{Z}^+$ and let $GL_n(\mathbb{R})$ be the set of **invertible** $n \times n$ matrices with entries in $\mathbb{R}$. Then

$$\langle GL_n(\mathbb{R}), \text{mat. mult.} \rangle$$

is a group. We check that $I_n \in GL_n(\mathbb{R})$ (the identity matrix) is the identity element. If $M \in GL_n(\mathbb{R})$ then so is M^{-1}. If $A, B \in GL_n(\mathbb{R})$, then $AB \in GL_n(\mathbb{R})$.

Definition: Abelian -

A group is **abelian** if it is commutative. It is **non-abelian** if it is not abelian.

All groups in the preceding examples are abelian, except $GL_n(\mathbb{R})$ for all $n \geq 2$.

4 Properties of Groups:

(Property 1) We can left-cancel or left-cancel. That is,

$$a * b = a * c \implies b = c.$$

Proof.

$$a * b = a * c$$
$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
$$(a^{-1} * a) * b = (a^{-1} * a) * c$$
$$e * b = e * c$$
$$b = c$$

□

Caution:
Notice that

$$a * b = c * a$$

does NOT imply $b = c$ (unless the group is **abelian**). For example, take A, B nonsingular similar $n \times n$ matrices with $A + B$. Notice that $A, B, P \in GL_n(\mathbb{R})$.

(Property 2): Solve for x in equations $a * x = b \implies x = a^{-1} * b$ or $x * a = b \implies x = b * a^{-1}$.

5 Useful Facts:

(1) Notice that e is its own inverse. That is, $e^{-1} = e$ because $e^{-1} = e^{-1} * e = e$, where first equality follows from e as identity, and the second equality follows from the definition of e^{-1} as inverse.
(2)

$$(x^{-1})^{-1} = x \forall_{x \in G}$$

because

$$(x^{-1})^{-1} * x^{-1} = e = x * x^{-1}.$$

Now cancel $* x^{-1}$.
(3) $x * y = e$ implies $y = x^{-1}$ and $x = y^{-1}$ because $x * y = e = x * x^{-1}$. Cancel $x*$ similarly to get $x = y^{-1}$.
(4) As with matrices, $(x * y)^{-1} = y^{-1} * x^{-1}$ gives

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e.$$

Theorem 5.1. General Associative Law
Let $\langle S, * \rangle$ be a binary structure in which $*$ is associative. Let $n \in \mathbb{Z}^+$, and let $x_1, \ldots, x_n \in S$. Then the result of $x_1 * x_2 * \cdots * x_n$ is the same regardless of how we place parenthesis to evaluate.

Proof. To prove this, we use strong induction. Taking the base cases $n = 1, 2, 3$, there is nothing to prove (regular associative law). Suppose we put parentheses in the expression in some way:
Let $E = \underbrace{(x_1 * x_2 * \cdots * x_m)} * \underbrace{(x_{m+1} * \cdots * x_n)}$ with $1 \leq m \leq n - 1$, where the parentheses in these do not matter.

Case 1: $m < n - 1$. Write $x_{m+1} * \cdots * x_n = (x_{m+1} * \cdots * x_{m-1}) * x_n$ (by the $n - m$ case; note $n - m < n$). Then

$$\begin{aligned} E &= (x_1 * \cdots * x_m) * ((x_{m+1} * \cdots * x_{n-1}) * x_n) \\ &= ((x_1 * \cdots * x_m) * (x_{m+1} * \cdots * x_{n-1})) * x_n \\ &= ((\cdots (x_1 * x_2) * \cdots) * x_{n-1}) * x_n, \end{aligned}$$

where the first equality follows from the regular associativity law, and the second equality follows from the $n - 1$ case (strong induction).

Case 2: $m = n - 1$. Then

$$E = (x_1 * \cdots * x_{n-1}) * x_n = ((\cdots (x_1 * x_2) * \cdots) * x_{n-1}) * x_n$$

by the $n-1$ case. So they're equal to the result we get when we multiply left to right, completing our proof.

□

6 Another Example of a Group:

Let $n \in \mathbb{Z}^+$. Recall that $\equiv_n$ (stands for congruence $\mod n$) is an equivalence relation. That is, $x \equiv_n y$ means $x \equiv y \pmod n$, which shows $x - y = qn$ for some $q \in \mathbb{Z}$.

Define $+'$ on $\tilde{\mathbb{Z}}_n$ by:

$$x +' y = \overline{a + b},$$

where $a, b \in \mathbb{Z}$ are chosen so that $x = \overline{a}$ and $y = \overline{b}$.

Recall that $\overline{a} = \{m \in \mathbb{Z} \mid m \equiv a \pmod n\}$ (equivalence class of a). We choose a way to write x, y in terms of their eqiuvalence classes, we add thoses, then take the equivalence class of that. We check that the answer does NOT depend on the choice of a, b (that is, the answer is well-defined).

Proof. Suppose $x = \overline{a} = \overline{a}_1$ and $y = \overline{b} = \overline{b}_1$ (property of equivalence class). Then $a \equiv_n a_1$, so $a_1 = a + cn$ for some $c \in \mathbb{Z}$. Similarly, $b \equiv_n b_1$, so $b_1 = b + dn$ for some $d \in \mathbb{Z}$. Therefore $a_1 + b_1 = a + cn + b + dn = (a + b) + (c + d)n$, which gives

$$\begin{aligned} a_1 + b_1 &\equiv a + b \pmod n \\ \overline{a_1 + b_1} &\equiv_n \overline{a + b}. \end{aligned}$$

□

Then we conclude that $\langle \tilde{\mathbb{Z}}_n, +' \rangle$ is a well-defined binary structure. Moreover, it is also a group. We check the requirements. To see associativity, consider:

$$(\overline{a} +' \overline{b}) +' \overline{c} = \overline{a + b} +' \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} +' (\overline{b} +' \overline{c}).$$

Now $\overline{0}$ is an identity element. To see this, consider:

$$\overline{a} +' \overline{0} = \overline{a + 0} = \overline{a},$$

and $\overline{0} +' \overline{a} = \overline{a}$, similarly. Finally, $\overline{n}$ has inverse $\overline{-n}$ because

$$\overline{n} +' \overline{-n} = \overline{n + (-n)} = \overline{0},$$

and similarly for $\overline{-n} +' \overline{n}$. Its elements are $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$, and these are all **different**.

Proof. We use the division algorithm for $\mathbb{Z}^{-1}$ (p. 60). For all $m \in \mathbb{Z}$, $\exists!_{q,r \in \mathbb{Z}}$: $m = qn + r$, and $0 \leq r < n$. Then there is a unique $r \in \{0, 1, \ldots, n-1\}$ such that $m \equiv r \pmod n$. That is, $\overline{m} = \overline{r}$. Vojta leaves showing that these are different as an exercise, but this really follows easily. □

Lecture ends here.