Math 493 Lecture 1

Thomas Cohn

9/4/2019

Defn: Let S be a set. A **composition law** (or **binary operation**) on S is a function $S \times S \xrightarrow{f} S$. We typically write xy, $x \cdot y$, $x + y$, $x \star y$, etc. instead of $f(x, y)$ (f is implicit).

Ex:

- $S = \mathbb{Z}$, $x \cdot y = x + y$ (usual addition)
- $S = \mathbb{Z}$, $x \cdot y = xy$ (usual multiplication)
- $S = \mathbb{R}$, $x \cdot y = \frac{x+y}{2}$
- $S = \{f : X \to X\}$, $f \cdot g = f \circ g$
- $S = M_n(\mathbb{R})$, i.e., the set of $n \times n$ real matrices, with matrix addition or multiplication as the composition law.

This is very general, so it's not much to study.

Defn: A composition law is **associative** if $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall x, y, z \in S$.

All of the above examples (except the average one) are associative.

If we have an associative composition law, and $x_1, \ldots, x_n \in S$, we can make sense of $x_1 \cdot x_2 \cdot \ldots \cdot x_n$. We don't have to have parentheses.

Ex: $x_1 \cdot x_2 \cdot x_3 \cdot x_4 = x_1 \cdot (x_2 \cdot (x_3 \cdot x_4)) = (x_1 \cdot x_2) \cdot (x_3 \cdot x_4) = ((x_1 \cdot x_2) \cdot x_3) \cdot x_4$.

Defn: A composition law is **commutative** if $x \cdot y = y \cdot x$, $\forall x, y \in S$.

Defn: An element $e \in S$ is an **identity** for a composition law if $x \cdot e = e \cdot x = x$, $\forall x \in S$. e is often denoted 1 or 0 (depending on context).

All but the average example above have an identity. If an identity exists, it is unique – assume e and e' are identity elements. Then $e = e \cdot e' = e'$.

Defn: Suppose we have an identity element $e \in S$, and our composition law is associative. Given $x \in S$, we say $y \in S$ is an **inverse** to x if $x \cdot y = y \cdot x = e$. If such a y exists, we say x is **invertible**.

The inverse to x is unique if it exists. Assume y and y' are inverses of x. Then
$yxy' = y(xy') = ye = y$
$yxy' = (yx)y' = ey' = y'$
So $y = y'$.

We'll denote the inverse of x as x^{-1} or $-x$ if it exists, depending on context.

Prop: Suppose x and y are both invertible. Then so is xy, and $(xy)^{-1} = y^{-1}x^{-1}$.
Proof: $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$.
And $(y^{-1}x^{-1})xy = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$. $\square$

Defn: A **group** is a pair $(G, \cdot)$ where G is a set and $\cdot$ is a composition law on G s.t.

1. $\cdot$ is associative.
2. An identity element exists.
3. All elements are invertible.

Defn: A commutative group is also called an **abelian group**.

Ex:

- $(\mathbb{Z}, +)$ is an abelian group.
- $(\mathbb{Z}, \cdot)$ is not a group.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ is an abelian group.
- X set, $S = \{f : X \to X | f \text{ is a bijection}\}$. $(S, \circ)$ is a group.
- $\mathrm{GL}_n(\mathbb{R}) = \{\text{invertible matrices in } M_n(\mathbb{R})\}$ is a group under matrix multiplication.[1]

Defn: Let G be a group. A **subgroup** of G is a subset $H \subset G$ s.t.

1. H is closed under the composition law, i.e., $x, y \in H \Rightarrow xy \in H$.
2. H is closed under inverses, i.e., $x \in H \Rightarrow x^{-1} \in H$.
3. $e \in H$ (or equivalently, H is nonemepty).

Ex: $G = \mathbb{Z}$. Trivial subgroups $H = \mathbb{Z}$, $H = \{0\}$.
$H = \{\text{even integers}\} = 2\mathbb{Z} \subseteq G$ is a subgroup.
$H = m\mathbb{Z} = \{\text{all integers divisible by } m\}$ is a subgroup.
$H = \{n \geq 0 | n \in \mathbb{Z}\}$ is *not* a subgroup.

Prop: Every subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some $m \geq 0$, and if $H \subseteq \mathbb{Z}$ subgroup, $\exists! m \geq 0$ s.t. $H = m\mathbb{Z}$.
Proof: Given $H \subseteq \mathbb{Z}$. If $H = \{0\}$, then $m = 0$.
Assume now that $H \neq \{0\}$. So $\exists n \neq 0$ in H. Then either n or $-n$ is positive, and both are in H.
Let m be the minimal positive integer in H.
Claim: $H = m\mathbb{Z}$. Well, $m \in H$ by assumption, so $\forall k \geq 0$, $km \in H$. With inverse, we have $m\mathbb{Z} \subseteq H$. Suppose we have $n > 0 \in H$. We can write $n = qm + r$, with $q, r \geq 0$, $r < m$. Well, $n, qm \in H$, so $r = n + (-qm) \in H$. So $r = 0$. Thus, $H \subseteq m\mathbb{Z}$, so $H = m\mathbb{Z}$.
If $n < 0$, $-n \in m\mathbb{Z}$, so $n \in m\mathbb{Z}$. $\square$

[1] GL_n is the **General Linear Group**.

Observe: $H, K \subseteq \mathbb{Z}$ subgroups. $H + K = \{x + y | x \in H, y \in K\}$ is a subgroup.

Let $n, m > 0$. Then $n\mathbb{Z} + m\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. By the definition of subgroups, $\exists! d > 0$ s.t. $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$. d is in fact the GCD of n and m.

Defn: Let G be a group, $x \in G$. $H = \left\{\ldots, x^{-2}, x^{-1}, x^0 = e, x^1, x^2, \ldots\right\} = \{x^n | n \in \mathbb{Z}\}$ is a subgroup of G. H is the smallest subgroup of G containing x, and it is called the subgroup of G **generated** by x. A group that is generated by a single element is called **cyclic**.

Consider $K = \{n \in \mathbb{Z} | x^n = e\}$.

Lemma: K is a subgroup of $\mathbb{Z}$.
Proof:

1. $n, m \in K \Rightarrow x^{n+m} = x^n \cdot x^m = e \cdot e = e \Rightarrow n + m \in K$.
2. $n \in K \Rightarrow x^{-n} = (x^n)^{-1} = e^{-1} = e \Rightarrow -n \in K$.
3. $0 \in K$ because $x^0 = e$.

$\square$

Note: $x^n = x^m$ if and only if $x^{n-m} = e$ if and only if $n - m \in K$.

Two cases:

1. $K = 0$. Then $x^n = x^m$ if and only if $n = m$, so all pairs of x are distinct, so H is infinite.
2. $K \neq 0$. Then $k = d\mathbb{Z}$, for some $d > 0$. $x^n = x^m$ if and only if $n - m \in d\mathbb{Z}$ if and only if $n \equiv m \pmod{d}$.

Defn: G is a group. The **order** of G, denoted $|G|$ or $\#G$, is the cardinality of G.

Defn: G is a group, and $x \in G$. The **order** of x, denoted $\mathrm{ord}(x)$, is the order of the subgroup generated by x.

$\mathrm{ord}(x) = \infty \Leftrightarrow \forall n \neq 0, x^n \neq e$.
$\mathrm{ord}(x) = d \Leftrightarrow x^d = e$ and d is minimal.

Ex: $G = \mathrm{GL}_2(\mathbb{R})$, $x = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. So $x^2 = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$, $x^3 = xx^2 = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right]$. $x^n = \left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right]$, $\forall n \in \mathbb{Z}$.
$\langle x \rangle = \{x^n | n \in \mathbb{Z}\} = \{\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right] | n \in \mathbb{Z}\}$.
$\mathrm{ord}(x) = \infty$.

Ex: $G = \mathrm{GL}_3(\mathbb{R})$. $x = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, $x^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$, $x^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.
$\mathrm{ord}(x) = 3$.