Math 493 Lecture 4

Thomas Cohn

9/16/2019

Defn: Let G be a group, $A, B \in G$ subsets. We define $AB = \{ab | a \in A, b \in B\}$. If $A = \{a\}$, then we write it aB instead of $\{a\} B$.

Warning: If A, B are subgroups, AB is not always a subgroup. If $ab \in AB$, $a'b' \in AB$, then $(ab)(a'b') \neq aa'bb'$ in general.

Ex: $G = S_3$, $A = \langle (1\ 2) \rangle = \{1, (1\ 2)\}$, $B = \langle (1\ 3) \rangle = \{1, (1\ 3)\}$. Then $AB = \{1, (2\ 3), (1\ 2), (1\ 2)(2\ 3)\} = \{1, (2\ 3), (1\ 2), (1\ 3\ 2)\}$. So AB is not a subgroup by Lagrange's Theorem.

Prop: $A, B, C \subseteq G$ subsets. Then $(AB)C = A(BC)$.
Proof: Say $x \in (AB)C$. Then $x = (ab)c$ for some $a \in A, b \in B, c \in C$. So $x = a(bc)$, so $x \in A(BC)$. $\square$

Recall: a subgroup N of G is normal if $\forall g \in G, n \in N$, we have $gng^{-1} \in N$. This is true
$\Leftrightarrow gNg^{-1} \subseteq N, \forall g \in G$
$\Leftrightarrow gNg^{-1} = N, \forall g \in G$ because given $n \in N$, $g^{-1}ng \in N$, $g(g^{-1}ng)g^{-1} = n \in gNg^{-1}$
$\Leftrightarrow gN = Ng$, $\forall g \in G$ because $(gNg^{-1})g = gN(g^{-1}g) = gN$

Fix a normal subgroup $N \subset G$. Define G/N to be the set of all cosets of N, $\{gN | g \in G\}$. Define a composition law on G/N using product of subsets.

Verify: $(gN)(hN) = gNhN = ghNN = ghN$. So it's a composition law. It's associative because multiplication of subsets is associative. N is the identity, because $(gN)N = g(NN) = gN$, and $N(gN) = NgN = gNN = gN$.

Inverses: $(gN)(g^{-1}N) = gg^{-1}N = N$, and $(g^{-1}N)(gN) = g^{-1}gN = N$. So $g^{-1}N$ is the inverse of gN.

Thus, G/N is a group!

We have a function $\begin{aligned} \pi : G &\to G/N \\ g &\mapsto gN \end{aligned}$ and it is a group homomorphism (and surjective).
$\pi(g)\pi(h) = (gN)(hN) = (gh)N = \pi(gh)$.

Prop: $\ker(\pi) = N$.
Proof: If $n \in N$, then $\pi(n) = nN = N$. So $N \subset \ker(\pi)$.
Let $\pi(g) = N$. Then $gN = N$. So $g \in N$. So $\ker(\pi) \subset N$. $\square$

Given $g \in G$, put $\bar{g} = \pi(g) = gN$. Every element of G/N has the form $\bar{g}$ for some g.
Warning: $\bar{g} = \bar{h} \Leftrightarrow gh^{-1} \in N$.

Ex: $G = \mathbb{Z}$, $N = n\mathbb{Z}, G/N = \mathbb{Z}/n\mathbb{Z} = \left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}$.
$\#G/N = n$. $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} = \bar{b}$ iff $a \equiv b \pmod{n}$.

Mapping Property for Quotients

$$\begin{tikzcd} G \arrow[d, "\pi"] \arrow[dr, "\psi"] & \\ G/N \arrow[r, "\varphi"] & H \end{tikzcd}$$

Given φ, we get ψ by $\psi = \varphi \circ \pi$. If $n \in N$, then $\psi(n) = \varphi(\pi(n)) = 1$, so $N \subset \ker(\psi)$.

Prop: Given a group homomorphism $\psi : G \to H$ s.t. $N \subset \ker(\psi)$, $\exists! \varphi : G/N \to H$ s.t. $\psi = \varphi \circ \pi$. Moreover, φ is surjective iff ϕ is surjective;
in fact $\operatorname{im}(\varphi) = \operatorname{im}(\psi)$, and φ is injective iff $\ker(\psi = N)$.
Proof: attempt to define $\varphi(\bar{g}) = \psi(g)$. Check that this is well defined:
If $\bar{g} = \bar{h}$, then $\varphi(\bar{g}) = \psi(g) \stackrel{?}{=} \psi(h)$. Well, $\bar{g} = \bar{h} \Leftrightarrow g = hn$ for some $n \in N$. So $\psi(g) = \psi(hn) = \psi(h)\psi(n) = \psi(h)$, because $n \in \ker(\psi)$.
Verify that φ is a group homomorphism:

$$\varphi(\bar{g} \cdot \bar{h}) = \varphi(\overline{gh}) = \psi(gh) = \psi(g)\psi(h) = \varphi(\bar{g})\varphi(\bar{h})$$

φ is unique because π is surjective. Suppose $\varphi : G/N \to H$ s.t. $\psi = \varphi \circ \pi$. Evaluate at g: $\varphi(\bar{g}) = \psi(g)$. So all values of φ are determined.

$\operatorname{im}(\varphi) = \operatorname{im}(\psi)$:
Say $x \in \operatorname{im}(\varphi)$. Then $x = \varphi(\bar{g}) = \psi(g) \Rightarrow x \in \operatorname{im}(\Psi)$.
Say $x \in \operatorname{im}(\psi)$. Then $x = \psi(g) = \varphi(\bar{g}) \Rightarrow x \in \operatorname{im}(\varphi)$.

Suppose $\ker(\psi) = N$. Say $\varphi(\bar{g}) = 1$. Then $\psi(g) = 1$, so $g \in \ker(\psi) = N$. Thus, $\bar{g} = 1$ in G/N. $\ker(\varphi) = 1 \Rightarrow \varphi$ is injective.

Suppose φ is injective, $g \in \ker(\psi)$. $\psi(g) = 1$, so $\varphi(\bar{g}) = 1$, so $\bar{g} \in \ker(\varphi)$. Thus, $\bar{g} = \mathrm{id}$ in G/N, so $\bar{g} = N$. Thus, $\ker(\psi) \subseteq N$. $\square$

Cor: (First Isomorphism Theorem) Suppose $\psi : G \to H$ is a homomorphism. Then we have a natural isomorphism $G/\ker(\psi) \xrightarrow{\sim} \operatorname{im}(\psi)$.
Proof: Let $N = \ker(\psi)$ (a normal subgroup). Because $N \subseteq \ker(\psi)$, $\exists! \varphi : G/N \to H$ s.t. $\psi = \varphi \circ \pi$. Then because $\operatorname{im}\varphi = \operatorname{im}\psi$ and φ is injective, φ is a bijection between G/N and $\operatorname{im}\varphi = \operatorname{im}\psi$. $\square$

Ex: Let G be a group and let $g \in G$ of order $1 \leq n < \infty$. We have a group homomorphism $\begin{aligned} \psi : \mathbb{Z} &\to G \\ m &\mapsto g^m \end{aligned}$.
$\operatorname{im}(\psi) = \langle g \rangle$, $\ker(\psi) = n\mathbb{Z}$. So according to the first isomorphism theorem, we have $\begin{aligned} \varphi : \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} \langle g \rangle \\ \bar{m} &\mapsto g^m \end{aligned}$.

Cor: Any two cyclic groups of the same order are isomorphic.
Proof: Any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Furthermore, any cyclic group of order ∞ is isomorphic to $\mathbb{Z}$.

Ex: Define $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ (the unit circle in the complex plane).
Observe:

- S_1 is a group under multiplication.
- $|1| = 1$, so $1 \in S^1$.
- $z, w \in S^1 \Rightarrow |zw| = 1 \Rightarrow |z|\,|w| = 1$.
- $z \in S^1 \Rightarrow \left|z^{-1}\right| = |z|^{-1} = 1$.

We have a group homomorphism $\begin{array}{c} \psi : \mathbb{R} \to S^1 \\ x \mapsto e^{2\pi i x} \end{array}$.

- $|\psi(x)| = \left|e^{2\pi i x}\right| = 1$.
- $\psi(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x} e^{2\pi i y} = \psi(x)\psi(y)$.
- $\ker(\psi) = \mathbb{Z}$.

Thus, by the first isomorphism theorem, $\begin{array}{c} \mathbb{R}/\mathbb{Z} \xrightarrow{\sim} S^1 \\ \bar{x} \mapsto e^{2\pi i x} \end{array}$.

Ex: $S_n/A_n \cong \mathbb{Z}/n\mathbb{Z}$ if $n \geq 2$. We have $\mathrm{sgn} : S_2 \to \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$. sgn is surjective if $n \geq 2$.
So by the first isomorphism theorem, $S_n/\underbrace{\ker(\mathrm{sgn})}_{=A_n} \cong \mathrm{im}(\mathrm{sgn}) \cong \mathbb{Z}/2\mathbb{Z}$.

Fact: $\#G/N = [G : N]$. If G is finite, then $\#G/N = \frac{\#G}{\#N}$.

Product Groups

Let G, H be groups. Define $G \times H$ as a group (the direct product). Elements are ordered pairs (g, h) for $g \in G, h \in H$. We have the composition law $(g, h)(g', h') = (gg', hh')$.

Exer: Check that this is a group.

Defn: Suppose K is a group, and we have two subgroups $\bar{G}, \bar{H} \subseteq K$. Then K is the **internal product** (or **direct product**) of $\bar{G}$ and $\bar{H}$ if

1. $x \in \bar{G}, y \in \bar{H} \Rightarrow xy = yx$.
2. $\bar{G} \cap \bar{H} = \{1\}$.
3. $K = \bar{G}\bar{H}$.

$K = G \times H$. Let $\bar{G} = \{(g, 1) \mid g \in G\} \subseteq K$ and $\bar{H} = \{(1, h) \mid h \in H\} \subseteq K$ subgroups.