Lectures 11–13: groups and subgroups.

Wednesday, November 05, 2014
11:59 PM

Here is the summary of the topics discussed in these lectures.

Lemma In a group the identity element is unique.

Pf. Suppose $\forall g \in G$, $g * e = e * g = g$ (I)

and $g * e' = e' * g = g$. (II)

Then $e \underbrace{=}_{\text{because of (II)}} e * e' \underbrace{=}_{\text{because of (I)}} e'$ ∎

Lemma In a group, any element has a unique "inverse".

Pf. For $g \in G$, suppose $g * g' = g' * g = e$ (I)

and $g * g'' = g'' * g = e$. (II)

Then $g' = g' * e$

$= g' * (g * g'')$ (because of (II))

$= (g' * g) * g''$

$= e * g''$ (because of (I))

$= g''$. ∎

$= g''.$ ∎

Def. $\forall g \in G, \exists!\, g' \in G$ s.t. $g * g' = g' * g = e.$

g' is called the inverse of g, and it is usually denoted by g^{-1}.

Remark / Warning. When the group operation is denoted by $+$, the identity element of the group is denoted by 0, and the inverse of g is denoted by $-g$.

Lemma. $\forall g_1, g_2 \in G,\ (g_1 \cdot g_2)^{-1} = g_2^{-1} \cdot g_1^{-1}.$

Pf. To show this, it is enough to check

$$(g_1 \cdot g_2) \cdot (g_2^{-1} \cdot g_1^{-1}) = e$$

and $$(g_2^{-1} \cdot g_1^{-1}) \cdot (g_1 \cdot g_2) = e.$$

$$\begin{aligned}(g_1 \cdot g_2) \cdot (g_2^{-1} \cdot g_1^{-1}) &= g_1 \cdot (g_2 \cdot g_2^{-1}) \cdot g_1^{-1} \\ &= g_1 \cdot e \cdot g_1^{-1} \\ &= g_1 \cdot g_1^{-1} \\ &= e.\end{aligned}$$

$= e.$

The other one is similar. ∎

<u>Cor.</u> $(g_1 \cdot \cdots \cdot g_n)^{-1} = g_n^{-1} \cdot g_{n-1}^{-1} \cdot \cdots \cdot g_1^{-1}$ and

$(g^n)^{-1} = (g^{-1})^n$ for any $n \in \mathbb{Z}^+$

where $g^n := \underbrace{g \cdot g \cdot \cdots \cdot g}_{n \text{ times}}$.

<u>Pf.</u> Both parts can be proved by induction on n. ∎

<u>Warning</u>. When the group operation is denoted by $+$, instead of writing $\underline{g^n}$ for $\underbrace{g + \cdots + g}_{n \text{ times}}$ we write $n g$.

<u>Def.</u> In $(G, \cdot)$, let $g^n := \begin{cases} \underbrace{g \cdot g \cdot \cdots \cdot g}_{n \text{ times}} & \text{if } n > 0 \\ e & \text{if } n = 0 \\ \underbrace{g^{-1} \cdot \cdots \cdot g^{-1}}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$

When the group operation is denoted by $+$, we write it this way

$$n g := \begin{cases} \underbrace{g + g + \cdots + g}_{n \text{ times}} & \text{if } n > 0 \\ \cdots & \text{if } n = 0 \end{cases}$$

$$\begin{cases} \underbrace{\quad\quad}_{n \text{ times}} & \\ 0 & \text{if } n=0 \\ \underbrace{(-g)+(-g)+\cdots+(-g)}_{-n \text{ times}} & \text{if } n<0 \end{cases}$$

Lemma. $\forall g \in G$, $\forall m,n \in \mathbb{Z}$, $(g^m)(g^n) = g^{m+n}$.

Pf. Case 1. $m,n \geq 0$.

$$(g^m)(g^n) = (\underbrace{g \cdot \cdots \cdot g}_{m \text{ times}}) \cdot (\underbrace{g \cdot \cdots \cdot g}_{n \text{ times}})$$

(Convention: 0 times means e.)

$$= \underbrace{g \cdot \cdots g}_{m+n \text{ times}}$$

$$= g^{m+n}.$$

So $(g^m)(g^n) = g^{m+n}$ if $m,n \geq 0$.

$$\Rightarrow (g^m)(g^n)(g^n)^{-1} = (g^{m+n})(g^n)^{-1}$$

$$\Rightarrow g^m = g^{m+n} \cdot g^{-n}$$ (by the definition and previous corollary)

Hence $g^{m'} \cdot g^{n'} = g^{m'+n'}$ if $m'+n' \geq 0$ and $m' \geq 0 \geq n'$.

Using similar arguments we can show other cases. ∎

Lemma. $\forall g \in G$, $\forall\, m,n \in \mathbb{Z}$, $(g^m)^n = g^{mn}$.

Pf. For $n \in \mathbb{Z}^{\geq 0}$, one can show this by induction on n.

For $n<0$, notice that
$$(g^m)^n = \left[(g^m)^{(-n)}\right]^{-1} = \left(g^{m(-n)}\right)^{-1} = \left(g^{-mn}\right)^{-1} = g^{mn}.$$
∎

Subgroup Criteria $\emptyset \neq H \subseteq G$. Then

$$H \text{ is a subgroup} \iff \forall\, a,b \in H,\ a \cdot b^{-1} \in H.$$

Pf. $(\Rightarrow)$ $\left.\begin{array}{l} b \in H \Rightarrow b^{-1} \in H \\ a \in H \end{array}\right\} \Rightarrow a \cdot b^{-1} \in H.$

$(\Leftarrow)$ We have to show (i) $e \in H$.

(ii) $x \in H \Rightarrow x^{-1} \in H$.

(iii) $x, y \in H \Rightarrow x \cdot y \in H$.

(i) Since $H \neq \emptyset$, $\exists\, h \in H$. So $h \cdot h^{-1} \in H$

$\Rightarrow e \in H$.

(ii) $e \in H$ and $x \in H \Rightarrow e \cdot x^{-1} \in H \Rightarrow x^{-1} \in H$.

(iii) $\left.\begin{matrix} y \in H \Rightarrow y^{-1} \in H \\ x \in H \end{matrix}\right\} \Rightarrow x (y^{-1})^{-1} \in H$.

$\Rightarrow xy \in H$.

$\boxed{(y^{-1})^{-1} = y^{(-1)(-1)} = y}$

■

Cor. Let G be a group, and $\{H_i\}_{i \in I}$ be a family of subgroups of G. Then

$$\bigcap_{i \in I} H_i \leq G.$$

Pf. $\forall\, i \in I$, $H_i \leq G \Rightarrow \forall\, i \in I$, $e \in H_i$

$$\Rightarrow e \in \bigcap_{i \in I} H_i.$$

$$\Rightarrow \bigcap_{i \in I} H_i \neq \emptyset.$$

So we can use subgroup criteria.

$a, b \in \bigcap_{i \in I} H_i \Rightarrow \forall\, i \in I$, $a, b \in H_i$ and $H_i \leq G$

$\Rightarrow \forall\, i \in I$, $a \cdot b^{-1} \in H_i$

$\Rightarrow a \cdot b^{-1} \in \bigcap H_i$. ■

$$\Rightarrow a \cdot b^{-1} \in \bigcap_{i \in I} H_i .$$ ∎

Def. / Lemma. For any $X \subseteq G$, there is a smallest subgroup of G which contains X. It is called the group generated by X, and it is denoted by $\langle X \rangle$.

Pf. We have to show that there is a subgroup H_0 s.t.

① $X \subseteq H_0$

② If $H \leq G$ and $X \subseteq H$, then $H_0 \subseteq H$.

Let $H_0 := \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$. Then by the previous Corollary $H_0 \leq G$. Since $X \subseteq H$ for any term H of the above intersection, $X \subseteq H_0$. On the other hand, if $H \leq G$ and $X \subseteq H$, then H is one of the terms in the above intersection. And so $H_0 \subseteq H$. ∎

Def. A group G is called cyclic if $\exists a \in G$ s.t.

$$G = \langle a \rangle .$$

<u>Lemma</u>. $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ for any $a \in G$.

<u>Pf.</u> Let $H_0 = \{ a^n \mid n \in \mathbb{Z} \}$. We have to show

(i) $H_0 \leq G$ and $a \in H_0$.

(ii) $H \leq G$ and $a \in H \Rightarrow H_0 \subseteq H$.

(i) $a^1 = a \in H_0$. In particular, $H_0 \neq \emptyset$. So we can use Subgroup Criteria:

$x, y \in H \Rightarrow \exists\, m, n \in \mathbb{Z}$ s.t. $x = a^m$ and $y = a^n$

$$\Rightarrow x \cdot y^{-1} = (a^m) \cdot (a^n)^{-1}$$

$$= a^m \cdot a^{-n} = a^{m-n} \in H.$$

(ii) By induction on $\underline{n}$, we show that $a^n \in H$ for any $n \in \mathbb{Z}^{\geq 0}$.

<u>Base</u>. $a^0 = e \in H$ (as $H \leq G$).

<u>Induction Step</u>. $a^k \in H \overset{?}{\Rightarrow} a^{k+1} \in H$.

$a^k \in H$ and $a \in H \Rightarrow (a^k) \cdot a \in H$

$$\Rightarrow a^{k+1} \in H.$$

$a^n \quad (a^{-n})^{-1}$

$\Rightarrow a^n \in H.$

<u>For $n<0$</u> : $a^n = (a^{-n})^{-1} \in H$

$\boxed{a^{-n} \in H \text{ and } H \leq G}$ ∎

<u>Exp.</u> $\forall a,b \in \mathbb{Z}$, $a \neq 0 \Rightarrow \langle a,b \rangle = \langle \gcd(a,b) \rangle$.

<u>Pf.</u> $\langle a,b \rangle \supseteq \langle a \rangle$ and $\langle b \rangle$

By the previous lemma, $\langle a \rangle = a\mathbb{Z}$ and $\langle b \rangle = b\mathbb{Z}$

$$\Rightarrow \left.\begin{array}{l} a\mathbb{Z} \subseteq \langle a,b \rangle \\ b\mathbb{Z} \subseteq \langle a,b \rangle \end{array}\right\} \Rightarrow a\mathbb{Z} + b\mathbb{Z} \subseteq \langle a,b \rangle$$

$$\Rightarrow \gcd(a,b)\,\mathbb{Z} \subseteq \langle a,b \rangle . \qquad \text{I}$$

On the other hand, $\gcd(a,b) \mid a$ and b

$$\Rightarrow \{a, b\} \subseteq \gcd(a,b)\,\mathbb{Z}$$

$$\Rightarrow \langle a,b \rangle \subseteq \gcd(a,b)\,\mathbb{Z} \qquad \text{II}$$

I and II $\Rightarrow \langle a,b \rangle = \gcd(a,b)\,\mathbb{Z}$

$= \langle \gcd(a,b) \rangle$ (again previous lemma.)

∎