Group Lecture 1 Proofs

Zhang Liyan

1. By def, if G is a group, $\forall a,b,c\in G$:
$(ab)c=a(bc)$, $\exists e\in G: ea=ae=a$, $\exists a^{-1}\in G: aa^{-1}=e$
Then
$\alpha)$ $e^{-1}=e$ (let $x=e^{-1}$, then $x=ex=ee^{-1}=e$)
$\beta)$ $(a^{-1})^{-1}=a$ (let $x=(a^{-1})^{-1}$, then $a=ae=a(a^{-1}x)=(aa^{-1})x=ex=x$)
$\gamma)$ $a^{-1}a=e$ (let $b=a^{-1}$, then $a=b^{-1}$ by β and $a^{-1}a=bb^{-1}=e$)
$\delta)$ e is unique (if $\exists e_1,e_2$, then $e_1=e,e_2=e_2$)
$\varepsilon)$ a^{-1} is unique (if $ax=ay=e$, then by γ $xa=ya=e$, then $x=xay=y$)
$\zeta)$ $(ab)^{-1}=b^{-1}a^{-1}$ ($abb^{-1}a^{-1}=aa^{-1}=e$, then use ε)
$\eta)$ $ab=ac\Rightarrow b=c$ ($b=a^{-1}ab=a^{-1}ac=c$)
$\theta)$ $ba=ca\Rightarrow b=c$ ($b=baa^{-1}=caa^{-1}=c$) □

2. Subgroups: $(\mathbb{Z},+)\subset(\mathbb{R},+)$, $GL(n,\mathbb{R})\subset GL(n,\mathbb{C})$, $SL(n,\mathbb{R})\subset SL(n,\mathbb{C})\subset GL(n,\mathbb{C})$
$SU(n)\subset U(n)\subset GL(n,\mathbb{C})$, $SO(n)\subset O(n)\subset GL(n,\mathbb{R})$
C_n contains proper & non-trival subgroups iff n is not prime,
and then C_m is a subgroup of C_n iff m is a factor of n.

3. $Z(G):=\{a\in G \mid ab=ba\ \forall b\in G\}$ is an Abelian & normal subgroup of G.
Subgroup: $\forall x,y\in Z(G)$, $b\in G$: $xb=bx$, $yb=by$, and thus

$$\left.\begin{array}{lll} xyb= & xby & =bxy \\ eb= & b & =be \\ x^{-1}b=(b^{-1}x)^{-1}= & (xb^{-1})^{-1} & =bx^{-1}\end{array}\right\}\Rightarrow Z(G) \text{ is subgroup}$$

Abelian: by def of $Z(G)$
Normal $\Leftrightarrow \forall c\in G: cZ(G)c^{-1}=Z(G)\Leftrightarrow$ $\begin{cases} cZ(G)c^{-1}\subset Z(G) \\ cZ(G)c^{-1}\supset Z(G)\end{cases}$

$\forall c\in G\,\forall x\in Z(G): xc=cx\Rightarrow Z(G)\ni x=xcc^{-1}=cxc^{-1}\in cZ(G)c^{-1}$
$\Rightarrow cZ(G)c^{-1}\subset Z(G)\ \&\&\ cZ(G)c^{-1}\supset Z(G)$
$\Rightarrow cZ(G)c^{-1}=Z(G)$
$\Rightarrow Z(G)$ is normal □

4. $G_0[a]=[a]_{G_0}\Leftrightarrow G_0\lhd G$
$G_0[a]=[a]_{G_0}:\Leftrightarrow aG_0\subset G_0a\ \&\&\ aG_0\supset G_0a$
$:\Leftrightarrow \forall x\in G_0\,\exists p,q\in G_0: ax=pa,\ xa=aq$
$G_0\lhd G:\Leftrightarrow \forall c\in G, y\in G_0: cyc^{-1}\in G_0$ ($\Leftrightarrow cG_0c^{-1}\subset G_0\Rightarrow G_0=c^{-1}cG_0c^{-1}c\subset c^{-1}G_0c\Rightarrow G_0=cG_0c^{-1}$).
(i) $G_0\lhd G\Rightarrow \forall c\in G, n\in G_0: cnc^{-1}=:v\in G_0$, $c^{-1}nc=:v'\in G_0$
$\Rightarrow G_0c\ni vc=cnc^{-1}c=cn$, $cG_0\ni cv'=cc^{-1}nc=nc$
$\Rightarrow \forall c\in G$: $G_0c\supset cG_0$, $cG_0\supset G_0c$
$\Rightarrow \forall c\in G$: $[c]_{G_0}=G_0[c]$

4. (ii) $\forall a\in G: {}_{G_0}[a]=[a]_{G_0} \Leftrightarrow aG_0 = G_0a, \quad a^{-1}G_0 = G_0a^{-1}$

$\Rightarrow \forall a\in G, m\in G_0\ \exists u,u'\in G_0: am = ua, \quad a^{-1}m = u'a^{-1}$

$ama^{-1}=uaa^{-1}=u, \quad m=aa^{-1}m=au'a^{-1}$

$\Rightarrow \forall a\in G: \quad aG_0a^{-1} \subset G_0, \quad G_0 \subset aG_0a^{-1}$

$\Rightarrow \forall a\in G: \quad aG_0a^{-1} = G_0$

$\Rightarrow G_0 \lhd G$ □

5. $G_0\lhd G \Rightarrow [a]_{G_0}[b]_{G_0}=[ab]_{G_0}$

Assume $G_0\lhd G$, then $\forall c\in G: cG_0c^{-1}=G_0$, et après $\forall a,b\in G$:

$\forall x,y\in G_0=a^{-1}G_0a\ \exists n\in G_0: y=a^{-1}na$, et donc

$$xayb = xaa^{-1}nab = xnab$$

$\because x,y,n\in G_0 \ \therefore xa\in G_0a=[a]_{G_0}, yb\in G_0b=[b]_{G_0}, xn\in G_0, xnab=G_0ab\in[ab]_{G_0}$

$\Rightarrow \forall a,b\in G\,\forall x,y\in G_0: xayb\in[ab]_{G_0}$

$\Rightarrow \forall a,b\in G: \quad [a]_{G_0}[b]_{G_0}\subset[ab]_{G_0}$ ①

$\forall a,b\in G\ \forall z\in G_0: zab=zaeb$

$\because z,e\in G_0 \ \therefore zab\in G_0ab=[ab]_{G_0}, za\in G_0a=[a]_{G_0}, eb\in G_0b=[b]_{G_0}$

$\Rightarrow \forall a,b\in G\ \forall z\in G_0: zab\in[a]_{G_0}[b]_{G_0}$

$\Rightarrow \forall a,b\in G: \quad [ab]_{G_0}\subset[a]_{G_0}[b]_{G_0}$ ②

Parce que ①②, on a $\forall a,b\in G: [a]_{G_0}[b]_{G_0}=[ab]_{G_0}$ □

6. $|G|=:g<\infty$, $G_0\lhd G$ with $|G_0|=:g_0\le g \Rightarrow |G/G_0|=g/g_0$

Denote elements in G_0 by $a_1:=e, a_2, a_3, \cdots, a_{g_0}$;

elements in $G\backslash G_0$ by $b_1, b_2, b_3, \cdots, b_{g-g_0}$; $G/G_0=:Q$ and $|Q|=:q$.

(α) By def $[e]_{G_0}=G_0$.

$\forall i=2,3,\cdots,g_0,\ [a_i]_{G_0}=\{xa_i\in G\mid x\in G_0\}\subset G_0,\ G_0=\{xa_i^{-1}a_i\in G\mid x\in G_0\}\subset[a_i]_{G_0}$

$\Rightarrow [a_i]_{G_0}=G_0=[e]_{G_0}$

(β) $\forall j=1,2,\cdots,g-g_0\ \forall u\in[b_j]_{G_0}=G_0b_j: ub_j^{-1}\in G_0 \ \because b_j^{-1}\notin G_0 \ \therefore u\notin G_0$

$\Rightarrow [b_j]_{G_0}\cap G_0=\emptyset$

With the same settings of i and j,

(γ) $\because a_i\in G_0 \ \therefore a_ib_j\in[b_j]_{G_0} \ \therefore a_ib_j\notin G_0 \ \therefore \exists k=1,2,\cdots,g-g_0: a_ib_j=b_k$

$[a_ib_j]_{G_0}=\{xa_ib_j\in G\mid x\in G_0\}\subset[b_j]_{G_0}, [b_j]_{G_0}=[a_i^{-1}a_ib_j]_{G_0}\subset[a_ib_j]_{G_0}$

$\Rightarrow [a_ib_j]_{G_0}=[b_j]_{G_0}$

Denote all elements in Q by $[c_1]_{G_0}:=[e]_{G_0}, [c_2]_{G_0}, \cdots, [c_q]_{G_0}$ in which each pair are different

(δ) Since $\forall \text{æ}\neq\text{œ}$ and $\text{æ},\text{œ}\in\{1,2,\cdots,q\}: [c_{\text{æ}}]_{G_0}\neq[c_{\text{œ}}]_{G_0}$

$\overset{\gamma}{\Rightarrow} \forall i,j\in\{1,2,\cdots,g_0\}: c_{\text{æ}}\neq a_jc_{\text{œ}} \Rightarrow a_ic_{\text{æ}}\neq a_jc_{\text{œ}}$

$\Rightarrow G\supset G_0\{c_1,c_2,\cdots,c_q\}=:R$ with $|R|=|G_0|\cdot q=qg_0 \Rightarrow g\ge qg_0$ ①

(ε) $\forall d\in G: d=ed\in G_0d=[d]_{G_0}\in G/G_0=Q$

$\Rightarrow \exists n\in\{1,2,\cdots,q\}: [d]_{G_0}=[c_n]_{G_0}\subset\bigcup_{m=1}^{q}[c_m]_{G_0} \Rightarrow d\in\bigcup_{m=1}^{q}[c_m]_{G_0}$

$\Rightarrow G=\bigcup_{m=1}^{q}[c_m]_{G_0} \Rightarrow g\le\sum_{m=1}^{q}|[c_m]_{G_0}|=\sum_{m=1}^{q}|G_0c_m|=qg_0$ ②

From ①②, $g=qg_0 \Rightarrow \left|\frac{G}{G_0}\right|=q=\frac{g}{g_0}$ □

Group Lecture 1 Proof (continue)

Zhang Liyang

7. Let φ be a group homomorphism from G to G' ($\Leftrightarrow \varphi(ab)=\varphi(a)\,\varphi(b)$)

1) If G_0 is a subgroup of G, then $\varphi(G_0)$ is a subgroup of G'

2) $\varphi(e_G)=e_{G'}$, and $\varphi(a_G^{-1})=(\varphi(a))_{G'}^{-1}$

3) $\mathrm{Ker}(\varphi):=\{a\in G \mid \varphi(a)=e_{G'}\}\lhd G$

4) $G/\mathrm{Ker}(\varphi)$ is isomorphic (= has a bijective homomorphism) to $\varphi(G)$ with the isomorphism $\tilde{\varphi}([a]_{\mathrm{Ker}(\varphi)}):=\varphi(a)$

2) $\forall \alpha\in\varphi(G)\ \exists a\in G: \alpha=\varphi(a)$. And $\forall p\in G_0$

$\varphi(e_G)\alpha=\varphi(e_G)\varphi(a)=\varphi(e_G a)=\varphi(a)=\alpha$

$\Rightarrow \varphi(e_G)=e_{G'}$ (by the uniqueness of identity element)

$\varphi(p_G^{-1})\varphi(p)=\varphi(p_G^{-1}p)=\varphi(e_G)=e_G'=(\varphi(p))_{G'}^{-1}\varphi(p)$

$\Rightarrow \varphi(p_G^{-1})=(\varphi(p))_{G'}^{-1}$ (by $ac=bc\Rightarrow a=b$) □

1) $\forall \alpha,\beta\in\varphi(G_0)\ \exists a,b\in G_0: \alpha=\varphi(a),\ \beta=\varphi(b)$,

$\alpha\beta=\varphi(a)\varphi(b)=\varphi(ab)$. Since G_0 is a subgroup, then $ab\in G_0\Rightarrow \alpha\beta\in\varphi(G_0)$

Together with 2) $\Rightarrow \varphi(G_0)$ is a subgroup of G' □

3) H) $\varphi(e_G)=e_G'\Rightarrow e_G\in\mathrm{Ker}(\varphi)$

He) If $a\in\mathrm{Ker}(\varphi)$, then $\varphi(a_G^{-1})=(\varphi(a))_{G'}^{-1}=(e_{G'})_{G'}^{-1}=e_{G'}\Rightarrow a_G^{-1}\in\mathrm{Ker}(\varphi)$

Li) If $a,b\in\mathrm{Ker}(\varphi)$, then $\varphi(ab)=\varphi(a)\varphi(b)=e_{G'}e_{G'}=e_{G'}\Rightarrow ab\in\mathrm{Ker}(\varphi)$

$\Rightarrow \mathrm{Ker}(\varphi)$ is a subgroup of G.

Be) If $a\in\mathrm{Ker}(\varphi)$ and $c\in G$, then

$$\varphi(cac_G^{-1})=\varphi(c)\varphi(a)(\varphi(c))_{G'}^{-1}=\varphi(c)e_{G'}(\varphi(c))_{G'}^{-1}=\varphi(c)(\varphi(c))_{G'}^{-1}=e_{G'}$$

$\Rightarrow cac_G^{-1}\in\mathrm{Ker}(\varphi)$

$\Rightarrow \forall c\in G: c\mathrm{Ker}(\varphi)c^{-1}\subset\mathrm{Ker}(\varphi)\Rightarrow \mathrm{Ker}(\varphi)=c^{-1}c\mathrm{Ker}(\varphi)c^{-1}c\subset c\mathrm{Ker}(\varphi)c^{-1}$

$\Rightarrow c\mathrm{Ker}(\varphi)c^{-1}=\mathrm{Ker}(\varphi)$

$\Rightarrow \mathrm{Ker}(\varphi)\lhd G$ □

4) 1) $\forall m\in\mathrm{Ker}(\varphi),\ [m]_{\mathrm{Ker}(\varphi)}=\mathrm{Ker}(\varphi)=[e_G]_{\mathrm{Ker}(\varphi)}$ by proof of 6(α)

$\Rightarrow \{[m]_{\mathrm{Ker}(\varphi)}\mid \varphi(m)=e_{G'}\}=\{[e_G]_{\mathrm{Ker}(\varphi)}\}$

$\Rightarrow \mathrm{Ker}(\tilde{\varphi}):=\{[m]_{\mathrm{Ker}(\varphi)}\mid \tilde{\varphi}([m]_{\mathrm{Ker}(\varphi)})=e_{G'}\}=\{[m]_{\mathrm{Ker}(\varphi)}\mid \varphi(m)=e_{G'}\}=\{[e_G]_{\mathrm{Ker}(\varphi)}\}$

$=\{e_{\frac{G}{\mathrm{Ker}(\varphi)}}\}$ (as proved by Tsuzu)

$\Rightarrow \tilde{\varphi}$ is injective from $G/\mathrm{Ker}(\varphi)$ to $\varphi(G)$. ①

□) $\forall n\in[a]_{\mathrm{Ker}(\varphi)}=\mathrm{Ker}(\varphi)a\ \exists p\in\mathrm{Ker}(\varphi): n=pa$

$\Rightarrow \varphi(n)=\varphi(p)\varphi(a)=e_{G'}\varphi(a)=\varphi(a)$ for any $a\in G$

$\Rightarrow \varphi([a]_{\mathrm{Ker}(\varphi)})=\{\varphi(a)\}=\{\tilde{\varphi}([a]_{\mathrm{Ker}(\varphi)})\}\ \forall a\in G$

Denote all elements of $\frac{G}{\mathrm{Ker}(\varphi)}$ by $[c_1]_{\mathrm{Ker}(\varphi)}, [c_2]_{\mathrm{Ker}(\varphi)}\cdots, [c_q]_{\mathrm{Ker}(\varphi)}$

$\Rightarrow G=\bigcup_{i=1}^{q}[c_i]_{\mathrm{Ker}(\varphi)}$ by proof of 6(ε)

$\Rightarrow \varphi(G)=\varphi(\bigcup_{i=1}^{q}[c_i]_{\mathrm{Ker}(\varphi)})=\bigcup_{i=1}^{q}\varphi([c_i]_{\mathrm{Ker}(\varphi)})=\{\tilde{\varphi}([c_i]_{\mathrm{Ker}(\varphi)})\in G'\mid i=1,\cdots,q\}=:\mathrm{Im}(\tilde{\varphi})$

$\Rightarrow \tilde{\varphi}$ is surjective from $G/\mathrm{Ker}(\varphi)$ to $\varphi(G)$. ②

7. 4) $\forall [a]_{Ker(\varphi)}, [b]_{Ker(\varphi)} \in G/Ker(\varphi)$:

$$\tilde{\varphi}([a]_{Ker(\varphi)})\tilde{\varphi}([b]_{Ker(\varphi)}) = \varphi(a)\varphi(b) = \varphi(ab) = \tilde{\varphi}([ab]_{Ker(\varphi)})$$
$$= \tilde{\varphi}([a]_{Ker(\varphi)}[b]_{Ker(\varphi)}) \text{ by proof 5}$$

$\Rightarrow \tilde{\varphi}$ is homomorphism from $G/Ker(\varphi)$ to $\varphi(G)$. ③

From ①②③ one has

$\tilde{\varphi}$ is isomorphism from $G/Ker(\varphi)$ to $\varphi(G)$. □