Content:

Definition	G/H "G mod H"
Definition	direct product
Definition	normal subgroup
Theorem	If $H \lhd G$, then G/H is a group.
Theorem	Let G be a group, $H \leq G$. The following are equivalent. 1) $H \lhd G$; 2) $gHg^{-1} = H, \forall\, g \in G$; 3) $ghg^{-1} \in H, \forall\, h \in H, g \in G$. 4) $gHg^{-1} \subseteq H, \forall\, g \in G$.
Theorem	If $H \leq G$, $[G:H] = 2$, then $H \lhd G$.

Warm-up:

1) True or False:

If $H, K \leq G$, then $H \cup K \leq G$. False.

Counterexample: $\langle a \rangle \leq V, \langle b \rangle \leq V$, but $\sim[(\langle a \rangle \cup \langle b \rangle) \leq V]$.

However, this proof cannot be extended to more than 2 subgroups without proof by induction.

For example, $V = \{e, a, b, c\} = \langle a \rangle \cup \langle b \rangle \cup \langle c \rangle$.

2) $G = GL_2(\mathbb{R})$, $H = SL_2(\mathbb{R})$, $A = \begin{pmatrix} 1 & 1 \\ 4 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 7 \\ 2 & 4 \end{pmatrix}$. Does $AH = BH$?

Is $A^{-1}B \in H$? Or, equivalently, is $A^{-1}B \in SL_2(\mathbb{R})$? And this is asking, is $\det(A^{-1}B) = 1$?

Recall that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Well, $\det(A^{-1}B) = \frac{\det B}{\det A} = \frac{12 - 14}{2 - 4} = \frac{-2}{-2} = 1$.

So, yes $A^{-1}B \in SL_2(\mathbb{R})$. But, we still need to prove AH, BH are equivalence classes.

(Does she mean we need to show $\begin{pmatrix} 1 & 1 \\ 4 & 2 \end{pmatrix} SL_2(\mathbb{R}) = \{A \in GL_2(\mathbb{R}) \mid A^{-1}\begin{pmatrix} 1 & 1 \\ 4 & 2 \end{pmatrix} \in SL_2(\mathbb{R})\}$

and $\begin{pmatrix} 3 & 7 \\ 2 & 4 \end{pmatrix} SL_2(\mathbb{R}) = \{B \in GL_2(\mathbb{R}) \mid B^{-1}\begin{pmatrix} 3 & 7 \\ 2 & 4 \end{pmatrix} \in SL_2(\mathbb{R})\}$? Something else?)

2.5/2.6

Definition Let G be a group, $H \leq G$.
$G/H = \{aH \mid a \in G\}$ is the set of left cosets of H in G, read "G mod H".

Example Let $G = \mathbb{Z}$, $H = \langle 6 \rangle$.
Then $G/H = \mathbb{Z}/\langle 6 \rangle = \{n + \langle 6 \rangle \mid n \in \mathbb{Z}\}$
$= \{0 + \langle 6 \rangle, 1 + \langle 6 \rangle, \ldots, 5 + \langle 6 \rangle\}$
$= \mathbb{Z}_6$. (and thus we eliminate redundancy)

Example Let $G = Q = \{\pm 1, \pm i, \pm j, \pm k\}$, and $H = \{\pm 1, \pm i\}$.
Recall that $|G| = [G:H]|H| \Leftrightarrow [G:H] = |G|/|H|$. So, $[Q:H] = |Q|/|H| = 8/4 = 2$.
$G/H = \{H, jH\}$. This is saying that $kH = jH$. We can verify this by noting that $i = -kj = k^{-1}j \in H$, hence $kH = jH$.

Example Let $G = \mathbb{Q}$ and $H = \mathbb{Z}$.
Then $\mathbb{Q} / \mathbb{Z} = \{q + \mathbb{Z} \mid q \in \mathbb{Q}\}$ (but this is overkill).
$= \{ q + \mathbb{Z} \mid q \in \mathbb{Q}$ and $0 \le q < 1\}$.
To show $\mathbb{Q} / \mathbb{Z} = \{ q + \mathbb{Z} \mid q \in \mathbb{Q}$ and $0 \le q < 1\}$, we need to show $\subseteq$ and $\supseteq$.
Is $13/8 + \mathbb{Z} = 5/8 + \mathbb{Z}$? Yes, because $-5/8 + 13/8 + \mathbb{Z} = 8/8 + \mathbb{Z} = \mathbb{Z}$.
Proof:
Let $a \in \mathbb{Q} / \mathbb{Z}$. Then $a = q + \mathbb{Z}$ for some $q \in \mathbb{Q}$.
But $\exists\ q'$ such that $q + \mathbb{Z} = q' + \text{int}[q] + Z =$
$q' + \mathbb{Z} \in \{ q + \mathbb{Z} \mid q \in \mathbb{Q}$ and $0 \le q < 1\}$.
If $b \in \{ q + \mathbb{Z} \mid q \in \mathbb{Q}$ and $0 \le q < 1\}$, then clearly $b \in \{q + \mathbb{Z} \mid q \in \mathbb{Q}\}$.
$\therefore \mathbb{Q} / \mathbb{Z} = \{ q + \mathbb{Z} \mid q \in \mathbb{Q}$ and $0 \le q < 1\}$. (Is this what she means?)

Direct Products

Definition Let G_1 and G_2 be groups, with binary operations $*_1$ and $*_2$, respectively.
Then, the *direct product* $G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_1\}$.
$(a_1, b_1) \times (a_2, b_2) = (a_1 *_1 a_2, b_1 *_2 b_2)$.
Check that this is a group on your own.
Proof:
We first show associativity holds.
$[(a_1, b_1) \times (a_2, b_2)] \times (a_3, b_3) = (a_1 *_1 a_2, b_1 *_2 b_2) \times (a_3, b_3)$
$= ([a_1 *_1 a_2] *_1 a_3, [b_1 *_2 b_2] *_2 b_3) = (a_1 *_1 [a_2 *_1 a_3], b_1 *_2 [b_2 *_2 b_3])$
$= (a_1, b_1) \times [(a_2 *_1 a_3), (b_2 *_2 b_3)] = (a_1, b_1) \times [(a_2, b_2) \times (a_3, b_3)]$.

Let $(a, b) \in G_1 \times G_2$.
Then $(e_1, e_2) \times (a, b) = (e_1 *_1 a, e_2 *_2 b) = (a *_1 e_1, b *_2 e_2) = (a, b) \times (e_1, e_2)$.
$\therefore$ The identity of $G_1 \times G_2$ is (e_1, e_2).

$\forall\ (a, b) \in G_1 \times G_2$, $(a, b) \times (a^{-1}, b^{-1}) = (a *_1 a^{-1}, b *_2 b^{-1}) = (e_1, e_2)$.
And $(a^{-1}, b^{-1}) \times (a, b) = (a^{-1} *_1 a, b^{-1} *_2 b) = (e_1, e_2)$.
$\therefore G_1 \times G_2$ is a group.

Let $G = G_1 \times G_2$. Let $H = \{e\} \times G_2$.
Then $G/H = \{(a, b)H \mid (a, b) \in G_1 \times G_2\}$.
We want to know if $(a, b)H = (c, d)H$,
or equivalently, if $(c, d)^{-1}(a, b) \in H$,
or if $(c^{-1}a, d^{-1}b) \in H$.
Since $H = \{e\} \times G_2$, then $(c^{-1}a, d^{-1}b) \in H \Leftrightarrow a = c$.

Is G/H always a group?

Define the operation on G/H as $(aH)(bH) = (ab)H$. Is this well-defined? In order to answer this question, we needed to understand the meaning of $aH = bH$.

Suppose $aH = cH$ and $bH = dH$. We want to show $abH = cdH$.
We know $c^{-1}a \in H$ and $d^{-1}b \in H$. We want to show $(cd)^{-1}(ab) \in H$.
Since $c^{-1}a = h$ for some $h \in H$, $(cd)^{-1}(ab) = d^{-1}c^{-1}ab = d^{-1}hb$.
We would like $d^{-1}hb = d^{-1}bh'$ for some $h' \in H$.
For then we'd have the product of two elements of H, $d^{-1}b$ and h', hence $(cd)^{-1}(ab) \in H$.
This is our motivation for the definition of normal subgroups.

Definition Let $H \leq G$, then H is a *normal subgroup* if $aH = Ha$, $\forall\ a \in G$. This is denoted $H \lhd G$.

Theorem If $H \lhd G$, then G/H is a group.

Proof:

1) We have proven we have a well-defined binary operation above.
2) Associativity follows from the associativity in G.
3) To show we have an identity, let $aH \in G/H$. Then $eHaH = eaH = aH = aeH = aHeH$.
$\therefore\ eH = H$ is the identity for G/H.
4) To show each element has an inverse, let $aH \in G/H$.
Note that $a^{-1}HaH = a^{-1}aH = eH = aa^{-1}H = aHa^{-1}H$. $\therefore\ (aH)^{-1} = a^{-1}H$.

Theorem Let G be a group, $H \leq G$. The following are equivalent.

1) $H \lhd G$.
2) $gHg^{-1} = H$, $\forall\ g \in G$.
3) $ghg^{-1} \in H$, $\forall\ h \in H, g \in G$.
4) $gHg^{-1} \subseteq H$, $\forall\ g \in G$.

Proof:

(3) ⇒ (2): Assume $ghg^{-1} \in H$, $\forall\ h \in H, g \in G$.
We will first show $gHg^{-1} \subseteq H$. Let $a \in gHg^{-1}$.
Then $a = ghg^{-1}$ for some $h \in H$, $g \in G$, and by assumption, $a \in H$.
$\therefore\ gHg^{-1} \subseteq H$.
To show containment in the other direction we let $h \in H$ and note that $g^{-1} \in G$ and our assumption give us that $g^{-1}hg \in H$. So $g^{-1}hg = h'$ for some $h' \in H$.
Thus $h = gh'g^{-1} \in gHg^{-1}$. So $H \subseteq gHg^{-1}$.

You should do (1) ⇔ (2) on your own.

Proof:

(1) ⇒ (2): Assume $H \triangleleft G$. Then $gH = Hg$, $\forall\ g \in G$.

$\therefore\ \{gh \mid h \in H\} = \{hg \mid h \in H\}$.

We'll use this to show $gHg^{-1} \subseteq H$.

Let $a \in gHg^{-1}$. Then $a = ghg^{-1}$ for some $h \in H$, $g \in G$.

But our assumption gives us that $gh = h'g$ for some $h' \in H$,

hence $a = hgg^{-1} = h \in H$ as desired.

To show $H \subseteq gHg^{-1}$, let $h \in H$ and g ∈ G.

Since $gh = h'g$, for some $h' \in H$, then $g^{-1}h = h'g^{-1}$, hence $h = gh'g^{-1}$.

$\therefore\ h \in gHg^{-1}$. And we are done.

(2) ⇒ (1): Assume $gHg^{-1} = H$, $\forall\ g \in G$. Let $a \in gH$.

Then $a = gh$ for some $h \in H$.

By our assumption we have $h = g^{-1}h'g$ for some $h' \in H$.

$\therefore\ gh = g\ g^{-1}h'g = h'g$.

$\therefore\ a \in Hg$ and we have $gH \subseteq Hg$.

Suppose $b \in Hg$. Then $b = hg$ for some $h \in H$.

Our assumption gives us that $h = gh'g^{-1}$ for some $h' \in H$,

hence $hg = gh'g^{-1}g = gh' \in gH$. Thus $gH \subseteq Hg$.

And we have shown $H \triangleleft G$.

Example $H \leq G$, $[G:H] = 2$ (this means there are only 2 cosets).
Than $G/H = \{H, aH\}$. To prove H is normal, we need to show $aH = Ha$.
The set of right cosets is $\{H, Ha\}$ because $a \notin H$, so Ha must be the other coset.

Theorem If $H \leq G$, $[G:H] = 2$, then $H \triangleleft G$.
Proof is above.
(Or, by Mark's comment, "If $c \in aH$, then $c \notin H$, and if $c \notin H$, then $c \in Ha$.")

Example Recall $[S_n : A_n] = 2$. So $A_n \triangleleft S_n$.

Example Show A_4 has no subgroup of order 6. (This shows Lagrange's Theorem only goes one way.)

Proof:
Suppose $H \leq A_4$ and $|H| = 6$. $[A_4:H] = |A_4|/|H| = 12/6 = 2$, so $H \triangleleft A_4$.
(Aside: $\alpha\beta\alpha^{-1} \in S_n$. If H is normal in G then all conjugates of elements in H must live in H. But in S_n we know all conjugates have the same cycle structure and if permutations have the same cycle structure, then they're conjugates. If α is 3-cycle in H, then all 3-cycles in A_n must be in H. There are 8 of them $(4 \bullet 3 \bullet 2) / 3 = 8$. (123), (132), (124), (142), (134), (143), (234), (243). So, if there is a 3-cycle in H, this would be a problem since $|H| = 6$ and there are 8 3-cycles in A_4.)

Cycle Structure (S_4)	Number	Even (A_4)	Odd $S_4 - A_4$
(1)	1	1	
(12)	6		6
(123)	8	8	
(1234)	6		6
(12)(34)	3	3	
Total	24	12	12

Let $\alpha \in A_4$ and $\alpha \notin H$, then $\alpha^2 H = H$ or $\alpha^2 H = \alpha H$ (since we only have 2 cosets). If $\alpha^2 H = \alpha H$, then $(\alpha H)^2 = \alpha H$, which implies $\alpha H = H$, hence $\alpha \in H$, contradicting our assumption. (Alternatively, we could have multiplied both sides of $\alpha^2 H = \alpha H$ by α^{-1} to get $\alpha H = H$.)
So, it must be that $\alpha^2 H = H$, hence $\alpha^2 \in H$.
Suppose α is a 3-cycle. If α is a 3-cycle, then α^2 is a 3-cycle.
So there is a 3-cycle in H.
And we have shown H cannot be a subgroup of A_4.

Example Let Q_8 = Quaternions, $H = \{\pm 1, \pm i\}$.
Q_8 / H is a group. $|Q_8 / H| = 2$. So $Q_8 / H \cong \mathbb{Z}_2$.

Example $\mathbb{Q}/\mathbb{Z}$ is a group. Pick $(5/8 + \mathbb{Z}) \in \mathbb{Q}/\mathbb{Z}$.
Then $\circ(5/8 + \mathbb{Z}) \mid 8$ since $8(5/8 + \mathbb{Z}) = 5 + \mathbb{Z} = \mathbb{Z}$.
$\therefore$ Every element of $\mathbb{Q}/\mathbb{Z}$ has finite order, however the group is infinite.