Content:

Theorem	Cayley's Theorem, Every group G is isomorphic to a subgroup of S_G. In particular, if $\|G\| = n$, then G is isomorphic to a subgroup of S_n.
Theorem	Representation on Cosets, Let G be a group and $H \leq G$ such that $[G:H] = n$. Then there is a homomorphism $\phi: G \to S_n$ with $\ker \phi \leq H$.
Proposition	If G is a group, $\|G\| = 6$, then $G \cong \mathbb{Z}_6$ or $G \cong S_3$.
Proposition	$\ker \phi$ (from Representation on Cosets Theorem) is the largest normal subgroup of G contained in H.
Corollary	Let G be a finite group. Let H be a proper subgroup of G with $[G:H] = n$. If $\|G\| \nmid n!$, then G contains a normal, nontrivial subgroup.
Definition	simple
Theorem	Index Factorial Theorem, Let G be a finite group such that $\|G\| > 1$. If G contains a proper subgroup H where $[G:H] = n$ and $\|G\| \nmid n!$, then G is not simple.
Definition	G acts on X.

Question was asked regarding homework problem 4(a). Response:
Let $x \in HK$.
$\phi: H \cap K \to \{(h', k') \in H \times K \mid \underbrace{h'k' = x}\}$. $\phi(d) = (hd, d^{-1}k)$.

all the different ways I can write x.

correction

HW: 2.7 #81, 83, 84, 85, 89, 90, 94, 98, 99

Theorem Cayley's Theorem
Every group G is isomorphic to a subgroup of S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof:
Let $a \in G$. Define $\tau_a: G \to G$ by $\tau_a(x) = ax$.

(Note that τ_a is not a homomorphism. $\tau_a(x)\tau_a(y) = axay \neq axy = \tau_a(xy)$.)

$(*)$ $\tau_a\tau_b(x) = \tau_a(bx) = a(bx) = (ab)x = \tau_{ab}(x)$.

$\tau_a^{-1} = \tau_{a^{-1}}$. Thus τ_a is a permutation.

$\tau_a^{-1} = \tau_{a^{-1}}$ gives us that τ_a is a permutation because depending on how you look at it, you get 1-1 or onto. (i.e. If $f^{-1}(f(A)) = A$, then f is 1-1, and if $f(f^{-1}(B)) = B$, then f is onto.)

Or, to show 1-1 and well-defined, let $x, y \in G$ such that $\tau_a(x) = \tau_a(y)$. Then since $\tau_a(x) = \tau_a(y) \Leftrightarrow ax = ay \Leftrightarrow x = y$. $\therefore$ τ_a is 1-1 and well-defined.

To show onto, let $y \in G$, then, since $a^{-1}y \in G$, $\tau_a(a^{-1}y) = aa^{-1}y = y$.

$\therefore$ τ_a is onto.

Define $\phi: G \to S_G$ by $\phi(a) = \tau_a$. By $(*)$, ϕ is a homomorphism.

We know $G/\ker \phi \cong \phi(G)$.

(I don't see the connection between this and $G \cong \phi(G) \leq S_G$.)

So we only need to show ϕ is 1-1.

(We already have onto since ϕ is always onto $\phi(G)$.)

Assume $\phi(a) = \phi(b)$.

$$\tau_a = \tau_b.$$
$$\tau_a(e) = \tau_a(e).$$
$$ae = be.$$
$$a = b.$$

So $G \cong \phi(G) \leq S_G$.

If $|G| = n$, then $S_G \cong S_n$.

Theorem Representation on Cosets
Let G be a group and $H \leq G$ such that $[G:H] = n$.
Then there is a homomorphism ϕ: $G \rightarrow S_n$ with $\ker \phi \leq H$.
(Note: If $H = \{e\}$, this is Cayley's Theorem.)

Proof:
Define G/H as the set of left cosets (even if G/H is not a group).

Let $a \in G$. Define τ_a: $G/H \rightarrow G/H$ by $\tau_a(xH) = axH, x \in G$.

Since $\forall\ xH \in G/H, \tau_a^{-1}(\tau_a(xH)) = \tau_a^{-1}(axH) = \tau_{a^{-1}}(axH) = xH$,

then τ_a is 1-1.

Since $\forall\ xH \in G/H, \tau_a(\tau_a^{-1}(xH)) = \tau_a(\tau_{a^{-1}}(xH)) = \tau_a((a^{-1}xH)) = xH$, then τ_a is onto.

So thus τ_a is a bijection, hence a permutation of G/H.

Define ϕ':$G \rightarrow S_{G/H}$ by $\phi'(g) = \tau_g$.

Then ϕ' is a homomorphism as

$\tau_a\tau_b(xH) = \tau_a(bxH) = a(bxH) = (ab)xH = \tau_{ab}(x)$.

Let $a \in \ker \phi'$. Then $\phi'(a) = I_{G/H} = \tau_a$. So $\tau_a(H) = aH = H$, hence $a \in H$.

Thus, $\ker \phi \leq H$.

So we have ϕ: $G \rightarrow S_n$ with $\ker \phi \leq H$.

Proposition If G is a group, $|G| = 6$, then $G \cong \mathbb{Z}_6$ or $G \cong S_3$.
(Read this in the book, p. 98)

Proof:

By Lagranges' theorem, the only possible orders of nonidentity elements are 2, 3, and 6. Of course, $G \cong \mathbb{Z}_6$ if G has an element of order 6. Now Exercise 2.27, p. 62 (If G is a group with an even number of elements, the number of elements in G of order 2 is odd. In particular, G must contain an element of order 2.) shows that G must contain an element of order 2, say, t. We now consider the cases G Abelian and G nonabelian separately.

Case 1. G is Abelian.

If there is a second element or order 2, say, a, then it is easy to see, using $at = ta$, that $H = \{1, a, t, at\}$ is a subgroup of G. This contradicts Langrange's themorem, because 4 is not a divisor of 6. It follows that G must contain an element b of order 3. But tb has order 6, by Proposition 2,82 (Let G be a group, and let $a, b \in G$ be commuting elements of order m and n respectively. If $(m, n) = 1$, then ab has order mn.) Therefore, G is cyclic if it is Abelian. Hence $G \cong \mathbb{Z}_6$.

Case 2. G is not Abelian.

If G has no elements of order 3, then $x^2 = 1$ for all $x \in G$, and G is abelian, by Exercise 2.26 on p. 62 (If G is a group in which $x^2 = 1$ for every $x \in G$, G must be abelian.) Therefore, G contains an element s of order 3 as well as the element t of order 2.

Now $|\langle s\rangle| = 3$, so that $[G:\langle s\rangle] = |G|/|\langle s\rangle| = 6/3 = 2$, and so $\langle s\rangle$ is a normal subgroup of G, by Proposition 2.62(ii) (If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G.) Since $t = t^{-1}$, we have $tst \in \langle s\rangle$; hence, $tst = s^i$ for $i = 0$, 1, or 2. Now $i \neq 0$, for $tst = s^0 = 1$ implies $s = 1$. If $i = 1$, then s and t commute, and this gives st of order 6, as in Case 1 (which forces G to be cyclic, hence abelian, contrary to our present hypothesis). Therefore, $tst = s^2 = s^{-1}$.

We now use the Theorem 2.88 (If $H \leq G$, $[G:H] = n$, $\exists$ homomorphism $\phi: G \to S_n$ with $\ker \phi \leq H$.) to construct an isomorphism $G \to S_3$. Let $H = \langle t\rangle$ and consider the homomorphism ϕ: $G \to S_{G/t}$ given by $\phi(g)$: $x\langle t\rangle \to gx\langle t\rangle$. (Choose x in G first.)

By the theorem, $\ker \phi \leq \langle t\rangle$, so that either $\ker \phi = \{1\}$ (ϕ is injective) (by Proposition 2.56(iii) f is an injection iff $\ker f = \{1\}$), or $\ker \phi = \langle t\rangle$.

Now $G/\langle t\rangle = \{\langle t\rangle, s\langle t\rangle, s^2\langle t\rangle\}$, and, in two-rowed notation,

$$\varphi(t) = \begin{pmatrix} \langle t\rangle & s\langle t\rangle & s^2\langle t\rangle \\ t\langle t\rangle & ts\langle t\rangle & ts^2\langle t\rangle \end{pmatrix}$$

If $\phi(t)$ is the identity permutation, then $ts\langle t\rangle = s\langle t\rangle$, so that

$s^{-1}ts \in \langle t\rangle = \{1, t\}$, by Lemma 2.40 ($H \leq G$, $a, b \in G$. $aH = bH$ iff $b^{-1}a \in H$). But now $s^{-1}ts = t$ (it cannot be 1), hence $ts = st$, contradicting t and s not commuting.

Therefore, $t \notin \ker \phi$, and $\phi: G \to S_{G/t} \cong S_3$ is an injective homomorphism. Since both G and S_3 have order 6, ϕ must be a bijection, and so $G \cong S_3$.

It is clear that $\mathbb{Z}_6$ and S_3 are not isomorphic, for one is Abelian and the other is not.

Proposition $\ker \phi$ (from Representation on Cosets Theorem) is the largest normal subgroup of G contained in H.

Proof:
Suppose $K \triangleleft G$ such that $\ker \phi \leq K \leq H \leq G$.
We want to show $\ker \phi = K$.
Let $k \in K$. So $\phi(k) = \tau_k = I$.
Let $gH \in G/H$. Then $\tau_k(gH) = kgH$.
Since K is normal, $Kg = gK$. Thus $kg = gk'$ for some $k' \in K$.
So $kgH = gk'H$, since $k' \in K \subseteq H$.
Thus $\tau_k = I_{G/H}$. So $k \in \ker \phi$. $\therefore$ $K = \ker \phi$.

Corollary Let G be a finite group. Let H be a proper subgroup of G with $[G:H] = n$. If $|G| \nmid n!$, then G contains a normal, nontrivial subgroup.

Proof:
$|G| \nmid n! \Rightarrow |G| \nmid |S_n| \Rightarrow G \not\leq S_n$ by Lagrange's Theorem.
If ϕ (from Representation on Cosets Theorem) were 1-1, then $\ker \phi = \{e\}$ and G "$\leq$" S_n, (actually $\phi(G) \leq S_n$.) So $\ker \phi \neq \{e\}$.
So $\ker \phi \triangleleft G$ and $\ker \phi \neq \{e\}$.
Since $\ker \phi \leq H \neq G$, then $\ker \phi \neq G$.
$\therefore$ $\ker \phi$ is a nontrivial, normal subgroup of G.

Definition A group $G \neq \{e\}$ is called *simple* if G has no nontrivial normal subgroups.

Example Is $\mathbb{Z}_6$ simple? No. Is $\mathbb{Z}_2$ simple? Yes.

Theorem Index Factorial Theorem
Let G be a finite group such that $|G| > 1$. If G contains a proper subgroup H where $[G:H] = n$ and $|G| \nmid n!$, then G is not simple.
(This is the corollary we just proved, but with new vocabulary "simple" inserted.)

Example Suppose $|G| = 45$. Suppose $H \leq G$, $|H| = 9$, then $[G:H] = 5$.
Since $45 \nmid 5!$, G is not simple.

Before today, we knew everything there is to know about groups of order
1 (the identity)
2 ($\cong \mathbb{Z}_2$)
3 ($\cong \mathbb{Z}_3$)
4 ($\cong \mathbb{Z}_4$ or Klein 4)
5 ($\cong \mathbb{Z}_5$)
7 ($\cong \mathbb{Z}_7$)

And, today we know :
6 ($\cong \mathbb{Z}_6$ or S_3)

Definition If X is a set and G is a group then *G acts on X* if there is a function $G \times X \to X$ denoted $(g, x) \mapsto g \bullet x$ such that
(1) $(gh) \bullet x = g \bullet (g \bullet x)$ $\forall$ $gh \in G$, $\forall$ $x \in X$.
(2) $e \bullet x = x$ $\forall$ $x \in X$.