II.I. Normal subgroups and quotient groups

In our discussion of conjugation, we defined the centralizer of an *element* $x \in G$: its elements are just those $g \in G$ with $gxg^{-1} = x$.

Suppose we replace x by a *subgroup* $H \leq G$. The new feature which arises is that $\imath_g(H) = gHg^{-1}$ ($:= \{ghg^{-1} \mid h \in H\}$) can equal H without our having $ghg^{-1} = h$ for each $h \in H$. So there are *two* natural generalizations of $C_G(x)$: the **centralizer** (of H in G)

(II.I.1) $$C_G(H) := \{g \in G \mid ghg^{-1} = h \ \ \forall h \in H\}$$

which we already encountered, and the **normalizer** (of H in G)

(II.I.2) $$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

Given $h \in H$ and $g \in N_G(H)$, we have *only* that $ghg^{-1} \in H$.

The orbit-stabilizer theorem (for conjugation) for an *element* $x \in G$ said that the number of conjugates (= size of orbit) of x equals the index of $C_G(x)$ in G. Similarly, recalling that the image of H under $\imath_g$ (also a subgroup of G) is called a *conjugate* of H, we have the

II.I.3. PROPOSITION. *The number of* (*distinct*) *conjugates of H in G is* $[G{:}N_G(H)]$.

PROOF. Let G act by conjugation *on the set* X *of subgroups of* G. We are interested in $|G(H)|$, where $G(H)$ means the orbit of H as an element in the set X. By the general orbit-stabilizer theorem, this is related to the stabilizer $G_H = N_G(H)$ of H in X by

$$|G(H)||N_G(H)| = |G|,$$

or equivalently $|G(H)| = |G|/|N_G(H)| = [G{:}N_G(H)]$. □

II.I.4. DEFINITION. If $N_G(H) = G$, H is *normalized* by all of G and we say H is a **normal subgroup** of G. We write $H \trianglelefteq G$ (or $H \triangleleft G$ if H is proper in G).

II.I.5. PROPOSITION. *For a subgroup $H \leq G$, the following properties are equivalent:*
(i) $N_G(H) = G$;
(ii)[16] $gHg^{-1} = H$ $(\forall g \in G)$;
(iii) $gH = Hg$ $(\forall g \in G)$; *and*
(iv) H *is a union of (entire) conjugacy classes.*

PROOF. (i) $\iff$ (ii) is obvious, as $N_G(H)$ is just those g for which $gHg^{-1} = H$.

(ii) $\iff$ (iii) looks clear, but let's write out the details for one direction: assume (ii), and let $gh \in gH$. We have $h' := ghg^{-1} \in H$, so that $gh = ghg^{-1}g = h'g \in Hg$. So $gH \subset Hg$; the reverse inclusion is similar.

(ii) $\implies$ (iv): If H is not a union of conjugacy classes, then H contains some but not all of a conjugacy class; i.e. there exist $y \notin H$ and $x \in H$ with $y \in \text{ccl}(x)$. But then for some $g \in G$, $gxg^{-1} = y \notin H \implies gHg^{-1} \not\subset H$.

(iv) $\implies$ (ii): Let $g \in G$ and $h \in H$. Since H is a union of conjugacy classes, $h \in H \implies \text{ccl}(h) \subset H \implies ghg^{-1} \in H$. We conclude that $gHg^{-1} \subseteq H$; moreover, every $h \in H$ is $g(g^{-1}hg)g^{-1}$ with $g^{-1}hg \in \text{ccl}(h) \subset H$, so the "$\subseteq$" is in fact an equality. $\square$

Note that if G is abelian, all its subgroups are normal. Here are some more interesting

II.I.6. EXAMPLES. (a) In $G = \mathfrak{S}_4$: The Klein 4-group V_4 is the union of two conjugacy classes of $\mathfrak{S}_3$: the identity $\{1\}$, and the set of all elements with cycle structure $(\cdot\cdot)(\cdot\cdot)$. Hence $V_4 \lhd \mathfrak{S}_4$.

Consider next the cyclic subgroup $\langle(123)\rangle = \{1, (123), (132)\}$. Since $(34)(123)(34)^{-1} = (124) \notin \langle(123)\rangle$, we find that $\langle(123)\rangle \ntriangleleft \mathfrak{S}_4$.

(b) In $G = D_5$: We have $\langle(h)\rangle = \{1, h\} \ntriangleleft D_5$, as $rhr^{-1} = r^2h \notin \langle(h)\rangle$. But $\langle r\rangle = \{1, r, r^2, r^3, r^4\} \lhd D_5$ since $hr^kh^{-1} = r^{-k} \in \langle(r)\rangle$.

[16] This is usually given as the definition of a normal subgroup.

(c) $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ for $n \geq 3$: Conjugacy classes in $\mathfrak{S}_n$ consist of all permutations with a given cycle-structure. $\mathfrak{A}_n$ consists of all permutations with "even" cycle-structures (i.e., $n - \#\{\text{disjoint cycles}\}$ is even). So $\mathfrak{A}_n$ is a union of ccl's in $\mathfrak{S}_n$, hence normal.

(d) $C(G) \trianglelefteq G$ for any group G: $x \in C(G) \implies gxg^{-1} = x\ \forall g \in G$, so $gC(G)g^{-1} = C(G)$ ($\forall g \in G$). Alternatively: the center consists of all 1-element ccl's.

(e) [HW] $[G, G] \trianglelefteq G$ for any G: here $[G, G]$ is the **commutator subgroup** generated by all *commutators* $[g_1, g_2] = g_1^{-1}g_2^{-1}g_1g_2$ of elements $g_1, g_2 \in G$.

II.I.7. EXAMPLE. Find

(a) all normal subgroups of $\mathfrak{S}_4$ other than $\{1\}$ and $\mathfrak{S}_4$, and

(b) all the normal subgroups of each such H.

(a) We know the conjugacy clases correspond to the cycle-structures: (i) $(\cdot\cdot\cdot\cdot)$, (ii) $(\cdot\cdot\cdot)(\cdot)$, (iii) $(\cdot\cdot)(\cdot\cdot)$, (iv) $(\cdot\cdot)(\cdot)(\cdot)$, and (v) $(\cdot)(\cdot)(\cdot)(\cdot)$ [identity]. All subgroups contain the identity. If H contains ccl (iv), then $H = \mathfrak{S}_4$: transpositions *generate* $\mathfrak{S}_4$ by II.B.5. If H contains ccl (ii) then $H = \mathfrak{A}_4$ or $\mathfrak{S}_4$: 3-cycles generate $\mathfrak{A}_4$ by II.C.6. If H contains ccl (i), then $H \ni (1234)$ hence $(1234)^2 = (13)(24)$; since it is normal, H then contains ccl (iii), and the element $(1234) \cdot (14)(23) = (24)$ $\implies$ H contains ccl (iv) $H = \mathfrak{S}_4$. (We are *not* saying that there is no proper subgroup of $\mathfrak{S}_4$ containing a 4-cycle, just that there are no proper *normal* subgroups!) Finally, if $H \supseteq$ ccl (iii), there are 2 options: contain also ccl (i), (ii), and/or (iv) (in which case we already know the outcome); or don't contain any of these. In the latter case, $H = V_4$. So the (proper) normal subgroups of $\mathfrak{S}_4$ are $\mathfrak{A}_4$ and V_4.

(b) In V_4, the order-2 cyclic subgroups (e.g. $\{1, (12)(34)\}$) are normal simply because V_4 is abelian. Note that these are *not* normal in $\mathfrak{S}_4$ since non-identity elements of V_4 can be conjugated into one another.

In $\mathfrak{A}_4 = \{1\} \cup \text{ccl(ii)} \cup \text{ccl(iii)}$, "ccl (ii)" [3-cycles] splits into 2 ccl's (with respect to conjugation by $\mathfrak{A}_4$) while "ccl (iii)" [$(\cdot\cdot)(\cdot\cdot)$] does not.

(Why? See II.G.19.) The 2 ccl's into which the 3-cycles split are

$$\{(123),(142),(134),(243)\} \quad \text{and} \quad \{(132),(124),(143),(234)\}.$$

Obviously, including one in a sub*group* forces inclusion of the other, since squaring the first set of elements gives the second set and vice-versa! But then you have included all 3-cycles and get all of $\mathfrak{A}_4$. The only option for a normal subgroup of $\mathfrak{A}_4$ (other than itself and $\{1\}$) is thus $V_4 = \{1\} \cup \text{ccl(iii)}$.

Here are two more ways to produce normal subgroups. The second is more important, and in fact characterizes *all* normal subgroups, as we will see.

II.I.8. PROPOSITION. *Any subgroup $H \leq G$ of index 2 is normal. (Here we need not assume G finite.)*

PROOF. For any $a \in G \backslash H$, $G = H \amalg aH$. Let $h \in H$ and $g \in G$; we must show that $ghg^{-1} \in H$ (cf. II.I.5(ii)). If $g \in H$, this is clear; so take $g = ax \in aH$.

Suppose $ghg^{-1} \notin H$. Then $ghg^{-1} \in aH$ and (for some $y \in H$) we have

$$ay = (ax)h(ax)^{-1} = a(\underbrace{xhx^{-1}}_{\in H})a^{-1} = ah'a^{-1}$$

$\Longrightarrow\ y = h'a^{-1} \ \Longrightarrow\ a = y^{-1}h' \in H$, contradicting the choice of a. So $ghg^{-1} \in H$ and we are done. □

II.I.9. PROPOSITION. *Let $\varphi\colon G \to H$ be a homomorphism. Then* $\ker(\varphi) \trianglelefteq G$.

PROOF. Let $k \in \ker(\varphi)$, i.e. $\varphi(k) = 1_H$. Then for $g \in G$

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)1_H\varphi(g)^{-1} = 1_H$$

$\Longrightarrow\ gkg^{-1} \in \ker(\varphi)$, done. □

II.I.10. EXAMPLES.

(a) Both II.I.8 and II.I.9 give quick proofs that $\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$:

- $\mathfrak{A}_n = \ker\{\text{sgn}\colon \mathfrak{S}_n \to \mathbb{Z}_2\}$ (identifying $(\{1,-1\},\bullet)$ with $(\mathbb{Z}_2,+)$)

- $[\mathfrak{S}_n{:}\mathfrak{A}_n] = 2$.

(b) $\mathrm{SL}_n(\mathbb{F}) = \ker\{\det\colon \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^*\} \lhd \mathrm{GL}_n(\mathbb{F})$, where $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(c) $\langle r \rangle \lhd D_n$ (index $= 2$).

As an application of normality we get a useful complement to our earlier result on decomposing a group into a direct product of subgroups II.E.11(iv). (Note that in (ii) below it isn't enough to have *one* of H or K normal in G — we need both.)

II.I.11. THEOREM. *Let $H, K \leq G$ (G finite) with $H \cap K = \{1\}$.*
(i) $|H||K| \leq |G|$.
(ii) *If also $H, K \trianglelefteq G$ and equality holds in* (i)*, then $G \cong H \times K$.*

PROOF. (i) Define a map *of sets*

$$\varphi\colon H \times K \to G$$
$$(h,k) \mapsto hk$$

This is 1-to-1: $\varphi(h,k) = \varphi(h',k') \implies hk = h'k' \implies (h')^{-1}h = k'k^{-1} \in H \cap K = \{1\} \implies (h')^{-1}h = 1 = k'k^{-1} \implies (h,k) = (h',k')$. Hence (by the pigeonhole principle) $|H||K| = |H \times K| \leq |G|$.

(ii) By II.E.11(iv) we are done if $(\forall h \in H,\, k \in K)$ $hk = kh$. (Recall in the proof of II.E.11 that this makes φ a homomorphism hence an isomorphism.) Now $K \trianglelefteq G \implies (hkh^{-1})k^{-1} \in K$, while $H \trianglelefteq G \implies h(kh^{-1}k^{-1}) \in H$. Hence $hkh^{-1}k^{-1} \in H \cap K = \{1\} \implies hk(kh)^{-1} = 1 \implies hk = kh$. □

II.I.12. DEFINITION. A group G is called **simple** if it contains no *normal* subgroups apart from $\{1\}$ and G.

II.I.13. EXAMPLE. Though we know that $\mathfrak{A}_4$ contains V_4 as a normal subgroup (hence is not simple), I claim that $\mathfrak{A}_\mathbf{n}$ **is simple for** $\mathbf{n} \geq \mathbf{5}$.

PROOF FOR $\mathfrak{A}_5$. (This gives an alternative approach to the method of II.I.7 used in your HW to see this.) Let $\{1\} \neq H \trianglelefteq \mathfrak{A}_5$, and

$\sigma \in H \backslash \{1\}$. Write

$$\sigma = \underset{\text{III}}{(123)}\ ,\quad \underset{\text{II}}{(12)(34)}\ ,\quad \underset{\text{I}}{(12345)}$$

for the three non-identity cycle-types in $\mathfrak{A}_5$.
Case I: Set $\rho := (132)$. Since $H \trianglelefteq \mathfrak{A}_5$, H contains

$$(\rho\sigma\rho^{-1})\sigma^{-1} = (31245)(15432) = (134).$$

Case II: Set $\tau := (12)(35)$. Since $H \trianglelefteq \mathfrak{A}_5$, H contains

$$(\tau\sigma\tau^{-1})\sigma^{-1} = (12)(54)(12)(34) = (354).$$

So in all cases (I, II, and III) H contains a 3-cycle. Since $H \trianglelefteq \mathfrak{A}_5$ and the 3-cycles form a ccl[17] in $\mathfrak{A}_5$, H contains all 3-cycles. But 3-cycles generate $\mathfrak{A}_5$, and so $H = \mathfrak{A}_5$. □

In light of this example and II.I.8, $\mathfrak{A}_n$ can have no subgroups of index 2 for $n \geq 5$ even though $2 \big| |\mathfrak{A}_n| \, (= \frac{n!}{2})$. This furnishes another example of how the "converse of Lagrange" fails.

Now recall that for $H \leq G$

$$G/H := \textit{set} \text{ of left cosets of } H \text{ in } G$$
$$\text{(with elements written } gH\text{)}.$$

We have $|G/H| = |G|/|H| = [G{:}H]$.

If $H \trianglelefteq G$, then left cosets equal right cosets, and we can make G/H into a group, called a **quotient group** (or "factor group" in some texts). Set

$$(aH)(bH) := \text{ all elements of the form } ahbh', \quad h, h' \in H.$$

II.I.14. Proposition. $H \trianglelefteq G \iff (aH)(bH){=}abH \ (\forall a, b \in G)$.

Proof. $(\implies)$: Using $gH = Hg$, one could write

$$(aH)(bH) = HabH = abHH = abH.$$

[17] Recall that this is false for $\mathfrak{A}_4$, and is true for $\mathfrak{A}_5$ because the stabilizer of a 3-cycle contains a transposition.

Alternatively, and more explicitly,

$$ahbh' = ab\underbrace{b^{-1}hb}_{\in H}h' = abh''h' \in abH$$

yields $aHbH \subset abH$; and conversely, $abH = a1bH \subset aHbH$ yields $aHbH \supset abH$.

$(\Longleftarrow)$: $(gH)(g^{-1}H) = gg^{-1}H = H$ implies $ghg^{-1} = (gh)(g^{-1}1) \in H$ for all $h \in H$, so that $gHg^{-1} \subset H$ (hence $= H$, by replacing g with g^{-1}). $\square$

II.I.15. REMARK. This last Proposition is equivalent to [**Jacobson**, Thm. 1.6], which states that the equivalence relation $a \equiv b \overset{\text{def}}{\equiv} a^{-1}b \in H$ being compatible with multiplication is equivalent to normality of H in G. Specifically, the "compatibility" requirement is that the pairing and inversion be well-defined on equivalence classes (i.e. the partition), and then "$\equiv$" is called a *congruence*.

II.I.16. COROLLARY. *If $H \trianglelefteq G$, then G/H, together with coset multiplication, $(aH)^{-1} := a^{-1}H$, and $1_{G/H} := (1)H$, forms a group.* (*The order of this group is $[G{:}H]$, and $\frac{|G|}{|H|}$ if G is finite.*)

PROOF. By II.I.14, the set of cosets is closed under multiplication; associativity is automatic from associativity of the product on G. Also, $(aH)(1H) = aH$ and $(aH)(a^{-1}H) = aa^{-1}H = 1H$. $\square$

II.I.17. EXAMPLES. (a) We have $n\mathbb{Z} \triangleleft \mathbb{Z}$ (since $\mathbb{Z}$ is abelian), and $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. (The elements of $\mathbb{Z}/n\mathbb{Z}$ are of the form $a + n\mathbb{Z}$, i.e. cosets written additively.)

(b) The quotient group associated to $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ is just $\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}_2$, with elements $\mathfrak{A}_n$ and $\tau\mathfrak{A}_n$, where τ is any transposition.

(c) $H \times \{1\}$ and $\{1\} \times K$ are both normal in $H \times K$. The quotient groups are K and H respectively.

(d) [HW] $G/[G, G]$ yields an abelian group, called the "abelianization" of G.

II.I.18. DEFINITION. Given $H \trianglelefteq G$, the **natural map**

$$\nu\colon G \twoheadrightarrow G/H$$

is the homomorphism obtained by sending $g \mapsto gH$. [To check that it is actually a homomorphism, write $\nu(g)\nu(g') = gHg'H = gg'H = \nu(gg')$.]

Here is the "converse" of II.I.9:

II.I.19. COROLLARY. *Every normal subgroup of a group G is the kernel of a homomorphism.*

PROOF. Given $H \trianglelefteq G$, we have the natural map $\nu\colon G \to G/H$. I claim that $H = \ker(\nu)$:

- $h \in H \implies \nu(h) = hH = H = 1_{G/H} \implies h \in \ker(\nu)$;
- $k \in \ker(\nu) \implies kH = \nu(k) = 1_{G/H}(= H) \implies k \in H$. □

II.I.20. FUNDAMENTAL THEOREM OF GROUP HOMOMORPHISMS. *Let $\varphi\colon G \to H$ be a group homomorphism, and write $K := \ker(\varphi)$. Then $K \trianglelefteq G$, and the map*

$$\bar{\varphi}\colon G/K \to \varphi(G) \ (\leq H)$$

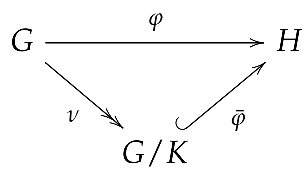
$$gK \overset{(*)}{\longmapsto} \varphi(g)$$

is an isomorphism of groups. (*In particular,* $\frac{|G|}{|K|} = |\varphi(G)|$.)

PROOF. We only need to check that $\bar{\varphi}$ is an isomorphism.

- $\bar{\varphi}$ is well-defined (as a map): Suppose $gK = g'K$. (We must show that $\bar{\varphi}(gK) = \bar{\varphi}(g'K)$.) Then $g' = gk$ for some $k \in K$, and $\bar{\varphi}(g'K) \overset{(*)}{=} \varphi(g') = \varphi(gk) = \varphi(g)\varphi(k) = \varphi(g) \overset{(*)}{=} \bar{\varphi}(gK)$.
- $\bar{\varphi}$ is a homomorphism: Since φ is one, $\bar{\varphi}((aK)(bK)) = \bar{\varphi}(abK) \overset{(*)}{=} \varphi(ab) = \varphi(a)\varphi(b) \overset{(*)}{=} \bar{\varphi}(aK)\bar{\varphi}(bK)$.
- $\bar{\varphi}$ surjects onto $\varphi(G)$: Any $\varphi(g) = \bar{\varphi}(gK)$.
- $\bar{\varphi}$ is injective: $\bar{\varphi}(aK) = 1_H \implies \varphi(a) = 1_H \implies a \in \ker(\varphi) = K \implies aK = K = 1_{G/H}$. □

The following diagram nicely describes the situation, namely that "φ factors through G/K":



It *commutes* (see the end of §I.A) in the sense that $\bar{\varphi} \circ \nu = \varphi$:

$$\bar{\varphi}(\nu(g)) = \bar{\varphi}(gK) \overset{(*)}{=} \varphi(g).$$

II.I.21. COROLLARY. *If* $\varphi\colon G \to H$ *is a* surjective *homomorphism, then* $G/\ker(\varphi) \cong H$. *(In particular,* $\frac{|G|}{|\ker(\varphi)|} = |H|$*.)*

II.I.22. EXAMPLES. (a) We obtain $\mathfrak{S}_n/\mathfrak{A}_n \cong \mathbb{Z}_2$ again by using $\mathrm{sgn}\colon \mathfrak{S}_n \twoheadrightarrow \mathbb{Z}_2$ with kernel $\mathfrak{A}_n$.

(b) The map $\psi\colon \mathbb{C}^* \twoheadrightarrow S^1 := \{z \in \mathbb{C}^* \mid |z| = 1\}$ sending $z \mapsto \frac{z}{|z|}$ has $\ker(\psi) = \mathbb{R}_{>0}$. So $\mathbb{C}^*/\mathbb{R}_{>0} \cong S^1$.

(c) Defining $\varphi\colon \mathbb{R} \twoheadrightarrow S^1$ by $\varphi(r) := e^{2\pi \mathbf{i} r}$, we have $\ker(\varphi) = \mathbb{Z}$, so that $\mathbb{R}/\mathbb{Z} \cong S^1$.

(d) There is a homomorphism $\Phi\colon Q \twoheadrightarrow V_4$ with kernel $\ker(\Phi) = C(Q) = \{\pm 1\}$; thus $Q/\{\pm 1\} \cong V_4$. [HW]

(e) We construct a homomorphism $\phi\colon \mathfrak{S}_4 \twoheadrightarrow \mathfrak{S}_3$ as follows: let $\mathfrak{S}_4$ act by conjugation on the ccl $\{(12)(34), (13)(24), (14)(23)\}$. Numbering its elements $1, 2, 3$ in the order shown, we obtain ϕ, and calculate that $\phi((12)) = (23)$ and $\phi((123)) = (132)$. Since $\phi(\mathfrak{S}_4) \leq \mathfrak{S}_3$ and $\langle (23), (132) \rangle = \mathfrak{S}_3$, we get surjectivity. By II.I.20 (or II.I.21),

$$\frac{|\mathfrak{S}_4|}{|\ker(\phi)|} = |\mathfrak{S}_3| \quad \Longrightarrow \quad \frac{24}{|\ker(\phi)|} = 6 \quad \Longrightarrow \quad |\ker(\phi)| = 4.$$

As $\ker(\phi) \trianglelefteq \mathfrak{S}_4$, the only possibility is now $\ker(\phi) = V_4$. Conclude that

$$\mathfrak{S}_4/V_4 \cong \mathfrak{S}_3. \qquad \text{(II.I.23)}$$

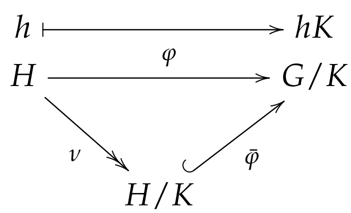
The following is immediate from II.I.20 and Lagrange, and is useful for ruling out homomorphisms between groups:

II.I.24. COROLLARY. *Let* $\varphi\colon G \to H$ *be a homomorphism, and* $|G|, |H|$ *finite. Then* $|\varphi(G)| \,\big|\, |G|, |H|$.

For a more serious application of the Fundamental Theorem, we turn to the two isomorphism theorems for groups.

II.I.25. FIRST ISOMORPHISM THEOREM. *Let* $K \trianglelefteq G$, $K \leq H \leq G$. *Then:*
(i) $K \trianglelefteq H$
(ii) $H/K \leq G/K$
(iii) $H \overset{(\dagger)}{\mapsto} H/K$ *induces a bijection:* $\left\{\begin{matrix}\text{subgroups of } G \\ \text{containing } K\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subgroups} \\ \text{of } G/K\end{matrix}\right\}$
(iv) $H \trianglelefteq G \iff H/K \trianglelefteq G/K$.
(v) *In case of* (iv), $G/H \cong \frac{G/K}{H/K}$.

PROOF. (i) is clear, and (ii) follows from II.I.20, viz.



(iii) injectivity of (†): Given $H_1/K = H_2/K$. Then for each $h_1 \in H_1$, there exists $h_2 \in H_2$ such that $h_1K = h_2K$. But then $h_2^{-1}h_1 \in K$, and so $h_1 = h_2k \in H_2$. That is, we have shown that $H_1 \subset H_2$. Similarly, one has $H_2 \subset H_1$; and so $H_1 = H_2$.

surjectivity of (†): Given $\bar{H} \leq G/K$, $\bar{H}$ is a collection of cosets. Define H to be the union of these cosets (hence $H \supset K$), so that

$$h_1, h_2 \in H \implies h_1K, h_2K \in \bar{H} \implies h_1h_2K = (h_1K)(h_2K) \in \bar{H}$$

$\implies h_1h_2 \in H$ (and similarly with inverses) $\implies H \leq G$.
(iv) If $H \trianglelefteq G$ (and $K \trianglelefteq H, G$), then

$$(gK)(hK)(g^{-1}K) \underset{K \trianglelefteq G}{=} ghg^{-1}K \underset{H \trianglelefteq G}{=} h'K \in H/K.$$

The converse is similar.
(v) The composition

$$\begin{array}{ccccc} & & \overset{\mu}{\frown} & & \\ G & \overset{\nu}{\twoheadrightarrow} & G/K & \overset{\bar{\nu}}{\twoheadrightarrow} & \frac{G/K}{H/K} \\ g & \longmapsto & gK & \longmapsto & (gK)(H/K) \end{array}$$

has $\ker(\mu) = \{g \in G \mid gK \in H/K\} = H$. [Check: $gK \in H/K$ means $gK = hK$ for some $h \in H$, hence $h^{-1}gK = K \implies h^{-1}g \in K \implies g = hk \in H$.] Now apply II.I.21: in a diagram,

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & \frac{G/K}{H/K} \\ & \searrow & \nearrow_{\cong} \\ & G/H & \end{array}$$

since $H = \ker(\mu)$. □

II.I.26. COROLLARY. *Given a homomorphism $\eta\colon G \twoheadrightarrow \mathfrak{G}$ with kernel K, let*

$$\Lambda := \{H \leq G \mid H \geq K\} \;\supseteq\; \Lambda' := \{H \trianglelefteq G \mid H \geq K\}.$$

Then
(i) *Sending $H \mapsto \eta(H)$ induces 1-to-1 correspondences*

$$\begin{array}{ccc} \Lambda & \longleftrightarrow & \{\textit{subgroups of } \mathfrak{G}\} \\ \cup & & \cup \\ \Lambda' & \longleftrightarrow & \{\textit{normal sgps. of } \mathfrak{G}\}. \end{array}$$

(ii) *For $H \in \Lambda'$, sending $gH \mapsto \eta(g)\eta(H)$ induces*

$$G/H \overset{\cong}{\longrightarrow} \mathfrak{G}/\eta(H).$$

PROOF. By II.I.21, $\mathfrak{G} \cong G/K$. Hence this is just parts (iii-iv) resp. (v) of II.I.25. □

II.I.27. SECOND ISOMORPHISM THEOREM. *Let $H \leq G$, $K \trianglelefteq G$. Then*
(i) $(K \trianglelefteq)\ HK \leq G$.

(ii) $H \cap K \trianglelefteq H$.

(iii) $h(K \cap H) \mapsto hK$ *induces* $H/(K \cap H) \overset{\cong}{\to} HK/K$.

PROOF. (i) $HK = \cup_{h\in H} hK = \cup_{h \in H} Kh = KH$ implies that $(HK)^2 = H^2K^2 = HK$, and also that (the set of all inverses of elements of HK) $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$. So HK is a subgroup of G.

(ii) Under $\nu \colon G \twoheadrightarrow G/K$,

$$\nu(H) = \{hK \mid h \in H\} = \{hkK \mid hk \in HK\} = HK/K.$$

This image is a subgroup of G/K. So we get by restriction a homomorphism of groups $\nu|_H : H \twoheadrightarrow HK/K$, with $\ker(\nu|_H) = \{h \in H \mid hK = K\} = H \cap K$.

(iii) The diagram

$$\begin{array}{ccc} H & \xrightarrow{\nu|_H} & HK/K \\ & \searrow \quad \nearrow_{\cong} & \\ & H/(H\cap K) & \end{array}$$

provides the desired isomorphism, courtesy of II.I.21. □

As an application, we finish off Example II.I.13:[18]

PROOF THAT $\mathfrak{A}_n$ IS SIMPLE FOR $n \geq 5$. Having done $n = 5$ (the base case) above, we induce on n (taking $n \geq 6$). Suppose $K \trianglelefteq \mathfrak{A}_n$, and consider (for each $i \in \{1, \ldots, n\}$) the subgroup $H_i \leq \mathfrak{A}_n$ of even permutations fixing i; clearly $H_i \cong \mathfrak{A}_{n-1}$, which is simple. By II.I.27(ii), we have $H_i \cap K \trianglelefteq H_i$, hence $H_i \cap K = \{1\}$ or H_i. If it is H_i for some i, then $H_i \leq K$ and so K contains a 3-cycle. But 3-cycles are a ccl in $\mathfrak{A}_n$ (since $n > 4$, by II.G.19), and these generate $\mathfrak{A}_n$, forcing $K = \mathfrak{A}_n$.

So suppose $K \cap H_i = \{1\}$ for all i. Then any $\sigma \in K \backslash \{1\}$ must be a product of r disjoint cycles of the same length k, with $rk = n$. (If there were cycles of different lengths $j < k$ in the decomposition of σ, then $\sigma^j \neq 1$ but fixes some i, so that $H_i \cap K \neq \{1\}$, a contradiction.)

[18] There are also direct (but lengthier) arguments in the style of that example or your HW.

Since $n \geq 6$, we can choose $\tau = (ab)(cd) \in \mathfrak{A}_n$ and i so that $i, \sigma(i)$ are distinct from a, b, c, d, and so that τ and σ do not commute.[19] Then $\sigma^{-1}(\tau\sigma\tau^{-1}) \in K$ since $K \trianglelefteq \mathfrak{A}_n$; but it also fixes i (hence belongs to $H_i \cap K$) and isn't the identity, a contradiction. Thus there is no $\sigma \in K \backslash \{1\}$ and $K = \{1\}$. $\square$

[19]This is easy, and left to you. Consider separately the cases $k = 2$ (which doesn't occur for $n = 6$) and $k > 2$.