II.E. Homomorphisms and isomorphisms

In §II.A it was mentioned that from the assumption

$$\varphi(ab) = \varphi(a)\varphi(b)$$

on the map $\varphi\colon G \to H$ (i.e., the defining property of a homomorphism) follow other properties:

- $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) \underset{\varphi(1)}{\overset{\text{cancel}}{\Longrightarrow}} 1 = \varphi(1)$
- $1 = \varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) \implies \varphi(x^{-1}) = \varphi(x)^{-1}$
- $\varphi(x^n) = \varphi(x)^n$ etc.

You can also use a homomorphism to construct subgroups of G and H, called the **kernel** and **image** of φ:

- $\ker(\varphi) := \{g \in G \mid \varphi(g) = 1_H\} \subset G$;
- $\text{im}(\varphi) := \{h \in H \mid h = \varphi(g) \text{ for some } g \in G\} \subset H$.

(The image is also denoted $\varphi(G)$.)

II.E.1. PROPOSITION. (i) $\ker(\varphi) \leq G$; *and* (ii) $\text{im}(\varphi) \leq H$.

PROOF. (i) $\varphi(g) = 1 = \varphi(g') \implies \varphi(gg') = \varphi(g)\varphi(g') = 1$.
(ii) $h = \varphi(g), h' = \varphi(g') \implies hh' = \varphi(g)\varphi(g') = \varphi(gg')$. □

II.E.2. EXAMPLES. (a) $\mathfrak{A}_n = \ker\{\text{sgn}\colon \mathfrak{S}_n \to \{1, -1\}\}$.
(b) $SL_n(\mathbb{C}) = \ker\{\det\colon GL_n(\mathbb{C}) \to \mathbb{C}^*\}$.
(c) $\langle e^{\frac{2\pi\mathbf{i}}{n}} \rangle = \text{im}\{\zeta_n\colon \mathbb{Z}_n \to \mathbb{C}^*\}$, where ζ_n sends $\bar{a} \mapsto e^{\frac{2\pi\mathbf{i}a}{n}}$.
(d) $\langle r \rangle = \text{im}\{\varphi_n\colon \mathbb{Z}_n \to D_n\}$, where φ_n sends $\bar{a} \mapsto r^a$.
(e) $\Gamma(N) := \ker\{SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})\}$. (The target of the map means 2×2 matrices with entries in $\mathbb{Z}_m$ and determinant $\bar{1}$. The kernel can be thought of as integer matrices with determinant 1 and equivalent to the identity matrix mod N, entry by entry.)
(f) $2\pi\mathbb{Z} = \ker\{(\mathbb{R}, +, 0) \to (\mathbb{C}^*, \bullet, 1)\}$, where the homomorphism sends $\theta \mapsto e^{\mathbf{i}\theta}$.
(g) $C(G) = \ker\{\imath\colon G \to \text{Aut}(G)\}$. Here $\text{Aut}(G)$ is the group of **automorphisms** of G, or isomorphisms[7] from G to itself, under the binary operation of composing maps. The homomorphism $\imath$ sends $g \mapsto \imath_g$,

[7] see II.E.3 just below

where $\imath_g(x) := gxg^{-1}$ is the automorphism called *conjugation by g*. (These are also written Ψ and Ψ_g.) If G is abelian, then $C(G) = G$ and all $\imath_g$ are just the identity map (sending $g \mapsto g$).

Note that if G is a cyclic group $\langle \alpha \rangle$, a homomorphism $\varphi\colon G \to H$ is completely determined by the image of α. (Why?)

II.E.3. DEFINITION. A homomorphism $\varphi\colon G \to H$ is called

- **trivial** if $\mathrm{im}(\varphi) = \{1\}$ (or $\{0\}$ if the operation is "+"); equivalently, $\ker(\varphi) = G$.
- **surjective** (or "onto"), and written $G \twoheadrightarrow H$, if $\mathrm{im}(\varphi) = H$; an example is the *reduction mod n* homomorphism $\mathbb{Z} \to \mathbb{Z}_n$ sending $a \mapsto \bar{a}$.
- **injective** (or "1-to-1"), and written $G \hookrightarrow H$, if $\ker(\varphi) = \{1\}$ (or $\{0\}$ if the operation is "+"); an example is the map $\mathbb{Z}_n \hookrightarrow \mathbb{Z}_{mn}$ sending $\bar{a} \mapsto \overline{ma}$.
- an **isomorphism**, and written $G \overset{\cong}{\to} H$, if it is both injective and surjective; the conjugation map $\imath_g\colon G \overset{\cong}{\to} G$ (for any $g \in G$) is an example, as is the identity map. Another would be the map $\mathbb{Z}_n \to \langle e^{\frac{2\pi \mathbf{i}}{n}} \rangle$ sending $\bar{a} \mapsto e^{\frac{2\pi \mathbf{i} a}{n}}$.

On one hand, a non-identity automorphism of a group (like conjugation by a non-central element in a non-abelian group) should be thought of as a structural *symmetry*. On the other, given two groups G and H, *a priori* differently presented and/or labeled, the existence of an isomorphism φ between them reveals that they are really the same group. We then say that G and H are **isomorphic**. Along these lines there is the

II.E.4. PROPOSITION. *If $G \cong H$ then G, H have:*
(a) the same order (if finite);
(b) the same orders of subgroups and elements; and
(c) are either both abelian or both nonabelian.[8]

[8]One could also add (say) that G and H have the same minimal number of generators.

We will first prove two lemmas. The start with, we should justify calling injective homomorphisms "1-to-1".

II.E.5. LEMMA. *For a homomorphism $\varphi\colon G \to H$, the following are equivalent:*
(A) φ injective in the sense of II.E.3;
(B) φ is 1-to-1, i.e. injective in the set-theoretic sense; and
(C) φ is an isomorphism onto its image.

PROOF. (A) $\iff$ (C): clear, since φ is always "surjective onto its image".
(A) $\implies$ (B): suppose $\varphi(x) = \varphi(y)$. Then $1 = \varphi(y)\varphi(x)^{-1} = \varphi(yx^{-1})$; since the kernel is trivial, this gives $yx^{-1} = 1$ hence $x = y$.
(B) $\implies$ (A): $\varphi(1_G) = 1_H$; since φ is 1-to-1, no other element of G goes to 1_H, so $\ker(\varphi) = \varphi^{-1}(1_H) = \{1\}$. □

Part (ii) of the next lemma is useful for producing isomorphisms.

II.E.6. LEMMA. (i) *Any $\varphi\colon G \xrightarrow{\cong} H$ is invertible: "$\varphi^{-1}\colon H \to G$" is well-defined, a homomorphism and an isomorphism, with $\varphi \circ \varphi^{-1} = \mathrm{id}_H$ and $\varphi^{-1} \circ \varphi = \mathrm{id}_G$.*
(ii) *If homomorphisms $\varphi\colon G \to H$ and $\eta\colon H \to G$ are such that $\varphi \circ \eta = \mathrm{id}_H$ and $\eta \circ \varphi = \mathrm{id}_G$, then φ and η are isomorphisms.*

PROOF. (i) Let $h \in H$. Since φ is 1-to-1 [resp. onto], $\varphi^{-1}(h)$ is ≤ 1 [resp. ≥ 1] element; i.e. $\varphi^{-1}(h) \in G$ is exactly one element. Writing $h = \varphi(g)$ and $h' = \varphi(g')$, applying φ^{-1} to $\varphi(g)\varphi(g') = \varphi(gg')$ gives $\varphi^{-1}(hh') = gg' = \varphi^{-1}(h)\varphi^{-1}(h')$. Finally, since φ is everywhere defined (on G) [resp. well-defined], φ^{-1} is onto [resp. 1-to-1].
(ii) We check this for φ. For surjectivity: given $h \in H$, we have $h = \mathrm{id_H}(h) = \varphi(\eta(h))$. For injectivity: if $\varphi(g) = 1$, then $1 = \eta(1) = \eta(\varphi(g)) = \mathrm{id}_G(g) = g$. □

PROOF OF II.E.4. We have some $\varphi\colon G \xrightarrow{\cong} H$.
(a) By II.E.6(i), φ is a bijection of sets; so the orders are the same.
(b) φ is a bijection, and for any $G' \leq G$, we have $\varphi(G') \leq H$ (by II.E.1(ii)) and $G' \cong \varphi(G')$ (given by restricting φ to G'). Similarly,

taking $H' \leq H$, $\varphi^{-1}(H') \leq G$ and $H' \cong \varphi^{-1}(H')$. So orders of subgroups (in particular, the cyclic groups generated by elements) are the same.
(c) Applying φ to $xy = yx$ yields $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$; and any pair of elements of H can be written as $\varphi(x)$, $\varphi(y)$. So G abelian $\implies H$ abelian; and the converse holds by using φ^{-1} in the same way. □

Here is a very useful way to construct isomorphisms for finite groups (which saves work involved in II.E.6(ii)).

II.E.7. PROPOSITION. *If $\varphi\colon G \to H$ is an injective homomorphism and $|G| = |H| < \infty$, then φ is an isomorphism.*

PROOF. To get surjectivity, apply the "pigeonhole principle": you have a map from an n-element set G to an n-element set H; no 2 elements of G go to the same element of H, and so every element of H gets "hit". □

The contrapositive of II.E.4 says: if any of the structural properties (a), (b), (c) of 2 groups differ, they *cannot be isomorphic*. This will be our first *main* application — telling groups apart (cf. (ii), (iii), (iv) below). But let's start with an isomorphism:

II.E.8. EXAMPLES. (i) The symmetries of a regular n-gon yield permutations of the vertices (numbered 1 to n), which produces a homomorphism $\varphi\colon D_n \to \mathfrak{S}_n$. If vertices stay in place then clearly there is no motion, and so φ is injective. (By II.E.5(c), you can think of this as saying: *there is* $(\forall n)$ *a subgroup of* $\mathfrak{S}_n$ *isomorphic to* D_n.) For $n = 3$, $|D_3| = 6 = |\mathfrak{S}_3| \implies \varphi$ is an isomorphism (by II.E.7); numbering the vertices of the triangle counterclockwise, with "1" fixed by the reflection h, we have $\varphi(h) = (23)$ and $\varphi(r) = (123)$.

(ii) $|D_6| = 12 = |\mathfrak{A}_4|$. An isomorphism doesn't "feel" natural, so instinct tells us to look for a difference in structure: D_6 has 2 elements of order 3: r^2 and r^4; while $\mathfrak{A}_4$ has 8 elements of order 3: the 8 3-cycles $(123), (132), (124), (142), (134), (143), (234), (243)$. So $D_6 \not\cong \mathfrak{A}_4$.

(iii) $|D_{12}| = |\mathfrak{S}_4| = |\mathbb{Z}_{24}| = 24$. $\mathbb{Z}_{24}$ is abelian; the other two are not: in $\mathfrak{S}_4$, $(12)(23) = (123) \neq (132) = (23)(12)$, while in D_{12}, $hr = r^{-1}h \neq rh$. So $\mathbb{Z}_{24} \ncong D_{12}, \mathfrak{S}_4$.

Now write out the cycle types for $\mathfrak{S}_4$:

form of decomp. into disjoint cycles	order	how many such elements?
$(\cdot\cdot\cdot\cdot)$	4	6
$(\cdot\cdot\cdot)(\cdot)$	3	8
$(\cdot\cdot)(\cdot\cdot)$	2	3
$(\cdot\cdot)(\cdot)(\cdot)$	2	6
$(\cdot)(\cdot)(\cdot)(\cdot)$	1	1

The last row is just the identity element; the two rows above it indicate that there are $3 + 6 = 9$ elements of order 2 in $\mathfrak{S}_4$. Now D_{12} has 13 elements of order 2: the 12 reflections $\{hr^a \mid a = 0, 1, \ldots, 11\}$, and one 180°-rotation r^6. So $D_{12} \ncong \mathfrak{S}_4$.

(iv) $|V| = |\mathbb{Z}_4| = 4$. The orders of elements are $1, 2, 2, 2$ for V, and $1, 4, 2, 4$ for $\mathbb{Z}_4$. So $V \ncong \mathbb{Z}_4$.

(v) All cyclic groups of order N are isomorphic to $(\mathbb{Z}_N, +)$. Just write down the homomorphism from $\mathbb{Z}_N \to \langle \alpha \rangle$ sending $\bar{1} \mapsto \alpha$ hence $\overline{m} \mapsto \alpha^m$.

We now formalize a construction touched on in II.C.3(iv):

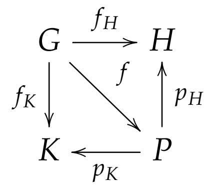
II.E.9. Definition. The **direct product** of two groups H and K is (a group)

$$H \times K := \{(h, k) \mid h \in H,\ k \in K\}$$

with $(h, k) \cdot (h', k') := (hh', kk')$, $(h, k)^{-1} = (h^{-1}, k^{-1})$, and $1_{H\times K} = (1_H, 1_K)$. [If H, K are abelian, we will frequently write this additively: $(h, k) + (h', k') = (h + h', k + k')$, $-(h, k) = (-h, -k)$, and $0_{H\times K} = (0_H, 0_K)$.]

II.E.10. Alternate Definition. A group P is a **direct product** of groups H and K if *there exist homomorphisms* $p_H \colon P \to H$ *and*

$p_K\colon P \to K$ such that for all groups G and homomorphisms $f_H\colon G \to H$ and $f_K\colon G \to K$, there exists a unique homomorphism $f\colon G \to P$ which makes



commute.

This kind of characterization of direct products is called *universal*, and the italicized statement their *universal property*. In the HW, you will check that $P = H \times K$ (from II.E.9) indeed is a direct product in this sense (of II.E.10).

Now clearly $|H \times K| = |H| \cdot |K|$, which brings us to the

II.E.11. DIRECT PRODUCT THEOREM. *Let $H, K \leq G$. Put $HK := \{hk \mid h \in H,\ k \in K\}$.* (*This is not necessarily a group!*) *Consider the possible assumptions*

$$\text{(A)} \quad hk = kh \quad (\forall h \in H, k \in K)$$
$$\text{(B)} \quad H \cap K = \{1_G\}.$$

Then
(i) (A) $\implies HK \leq G$
(ii) (A) + (B) $\implies HK \cong H \times K$
(iii) (A) + (B) + $HK{=}G \implies G \cong H \times K$
(iv) (A) + (B) + $|G| < \infty$ + $|H||K|{=}|G| \implies G \cong H \times K$.

PROOF. *(i)* We only need to check that $1 \in HK$, $(hk)(h'k') = hh'kk' \in HK$ (by (A)), and $(hk)^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$ (again by (A)).

(ii) Define $\varphi\colon H \times K \to HK$ by $\varphi(h,k) := hk$. This is a homomorphism since $\varphi(h,k)\varphi(h',k') = hkh'k' = hh'kk' = \varphi(hh',kk') = \varphi((h,k)\cdot(h',k'))$ (by (A)), injective because $1 = \varphi(h,k) = hk \implies k^{-1} = h \in H \cap K = \{1\} \implies (h,k) = (1,1)$ (by (B)), and obviously surjective by the description of HK.

(iii) is clear from *(ii)*.

(iv) By *(i)*, $G \geq HK$, so

$$|G| \geq |HK| \overset{(ii)}{=} |H \times K| = |H||K| = |G|$$

forces $|G| = |HK|$. Hence $G = HK$, whence (by *(iii)*) $G \cong H \times K$. $\square$

II.E.12. EXAMPLE. Given $r, s \in \mathbb{N}$, let $\ell := \mathrm{lcm}(r,s)$, $g := \gcd(r,s)$. Put $\tilde{s} := s/g \in \mathbb{N}$ and $G := \mathbb{Z}_r \times \mathbb{Z}_s$. Now let H denote the isomorphic image of $\mathbb{Z}_\ell \hookrightarrow \mathbb{Z}_r \times \mathbb{Z}_s$ (via[9] $\bar{a} \mapsto (\bar{a}, \bar{a})$), and K denote the isomorphic image of $\mathbb{Z}_g \hookrightarrow \mathbb{Z}_r \times \mathbb{Z}_s$ (via[10] $\bar{b} \mapsto (\bar{0}, \overline{b\tilde{s}})$). Since $\ell g = rs$, we get $|H||K| = |G|$.

Now in II.E.11, (A) holds since G is abelian. To see (B), we need $H \cap K = \{(\bar{0}, \bar{0})\}$. Take $(\bar{a}, \bar{a}) \equiv (\bar{0}, \overline{b\tilde{s}}) \in H \cap K \subset \mathbb{Z}_r \times \mathbb{Z}_s$. It's enough to show that the left-hand side is zero, i.e. $a \equiv 0$ mod r *and* mod s. We already have $a \underset{(r)}{\equiv} 0$ and $a \underset{(s)}{\equiv} b\tilde{s}$, which yield $r|a$ and $\tilde{s}|s|(a - b\tilde{s})$. Hence $r, \tilde{s}|a$; and since r and $\tilde{s}$ are relatively prime, we get $\ell = r\tilde{s}|a$. But $r, s|\ell$, and so $r, s|a$ as desired. At this point, by II.E.11*(iv)* we obtain $H \times K \cong G$, or

$$\mathbb{Z}_\ell \times \mathbb{Z}_g \cong \mathbb{Z}_r \times \mathbb{Z}_s.$$

II.E.13. EXAMPLE. The special case $\mathbb{Z}_{rs} \overset{\cong}{\to} \mathbb{Z}_r \times \mathbb{Z}_s$ for $(r,s) = 1$ is also valid for multiplicative groups:

$$\varphi \colon \mathbb{Z}_{rs}^* \overset{\cong}{\to} \mathbb{Z}_r^* \times \mathbb{Z}_s^*$$
$$\bar{a} \longmapsto (\bar{a}, \bar{a}).$$

[This is clearly also a multiplicative homomorphism, and so invertible congruence classes (mod rs) go to pairs of such. For surjectivity, the point is to use the surjectivity of $\mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ that we already know. Given $(\bar{b}, \bar{c}) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$, there is $(\bar{\beta}, \bar{\gamma}) \in \mathbb{Z}_r^* \times \mathbb{Z}_s^*$ with $\overline{\beta b} = \bar{1}$ and $\overline{\gamma c} = \bar{1}$; and that surjectivity yields $\bar{a}, \bar{\alpha} \in \mathbb{Z}_{rs}$ with $(\bar{a}, \bar{a}) = (\bar{b}, \bar{c})$

[9] In more detail, this sends a mod ℓ to (a mod r, a mod s). Since $r, s|\ell$, this makes sense. The map is injective because if $\bar{a}$ goes to $(\bar{0}, \bar{0})$, this means that $r, s|a$, so that their lcm $\ell|a$ and the original $\bar{a}$ was $\bar{0}$.

[10] Here $g|b \implies s = g\tilde{s}|b\tilde{s}$, so it is well-defined.

and $(\bar{\alpha}, \bar{\alpha}) = (\bar{\beta}, \bar{\gamma})$. So we get $\overline{a\alpha} \overset{\varphi}{\mapsto} (\overline{b\beta}, \overline{c\gamma}) = (\bar{1}, \bar{1})$. Since φ is injective on a set-theoretic level, $\overline{a\alpha}$ must be $= \bar{1}$, hence $\bar{a} \in \mathbb{Z}_{rs}^*$.]

This example has a beautiful number-theoretic application.

II.E.14. PROPOSITION. *The Euler phi-function*

$$\phi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} (1 - \tfrac{1}{p}).$$

PROOF. Write the prime factorization of n

$$n = p_1^{e_1} \cdots p_t^{e_t}.$$

Inductively applying II.E.13,

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{{p_1}^{e_1}}^* \times \cdots \times \mathbb{Z}_{{p_t}^{e_t}}^*,$$

and taking orders on both sides gives

$$\phi(n) = \prod_i \phi(p_i^{e_i}).$$

Now, for a prime p, everything in $\{0, 1, \ldots, p^e - 1\}$ is relatively prime to p^e except for multiples of p. As there are p^{e-1} such multiples,

$$\phi(p^e) = p^e - p^{e-1} = p^e(1 - \tfrac{1}{p}),$$

so $\phi(n) = \prod_i p_i^{e_i} \prod_i (1 - \frac{1}{p_i}) = n \prod_i (1 - \frac{1}{p_i})$. □

II.E.15. EXAMPLES. (i) $D_6 \cong D_3 \times \mathbb{Z}_2$: apply II.E.11(iv) to $G = D_6$, $H = \langle r^3 \rangle \cong \mathbb{Z}_2$, and $K = \langle r^2, h \rangle \cong D_3$. (Think of a regular triangle inside a regular hexagon, sharing 3 of its vertices.) Since $H = \{1, r^3\}$ and $K = \{1, r^2, r^4, h, hr^2, hr^4\}$, we have $H \cap K = \{1\}$; $|H||K| = 2 \cdot 6 = 12 = |D_6|$; and r^3 commutes with powers of r, and also with h (in general, $r^i h = hr^{-i}$, but $r^3 = r^{-3}$ in D_6).

(ii) $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$: use $H = \langle (12)(34) \rangle$ and $K = \langle (14)(23) \rangle$, same idea as above.