GROUP HOMOMORPHISM

L. MARIZZA A. BAILEY

0.1. **Homomorphisms.**

Definition 1. Let G and H be a groups.

A *group homomorphism* is a function $\phi : G \to H$ such that

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \text{ for any } g_1, g_2 \in G.$$

Proposition 1. *Let $\phi : G \to H$ be a homomorphism. Then*

(a) $\phi(1_G) = 1_H$*;*

(b) $\phi(g^{-1}) = \phi(g)^{-1}$ *for every $g \in G$.*

Proof. We have $\phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G)\phi(1_G)$. Multiplying both sides by $\phi(1_G)^{-1}$ in H, we have $1_H = \phi(1_G)$.

Let $g \in G$. Then $1_H = \phi(1_G) = \phi(g^{-1}g) = \phi(g)\phi(g^{-1})$. Multiplying both sides by $\phi(g)^{-1}$ in H yields $\phi(g)^{-1} = \phi(g^{-1})$. □

For example,

$\phi(n) : \mathbb{R} \to \mathbb{R}^*$ defined by $\phi(x) = e^x$ is a group homomorphism from the group of real numbers under addition, to the group of nonzero real numbers under multiplication.

By the properties of exponentiation, we get $\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$. Note that $\phi(0) = 1$, so the identity under addition is sent to the identity under multiplication.

Also, we see that $\phi(-x) = e^{-x} = \dfrac{1}{e^x}$. So the additive inverse of x is sent to the multiplicative inverse of e^x.

Proposition 2 (The restriction of a homomorphism onto a subgroup is still a homomorphism)**.** *Let $\phi : G \to H$ be a homomorphism and let $K \leq G$.*
Then $\phi \restriction_K : K \to H$ is a homomorphism.

The proof to this is very simple, and should be a mental exercise.

Date: September 29, 2006.

Proposition 3 (The image of a subgroup is a subgroup)**.** *Let $\phi : G \to H$ be a homomorphism and let $K \leq G$.*
Then $\phi(K) \leq H$.

Proof 1. *Recall, to prove $\phi(K) \leq H$, we need to verify*

(IDENT) *Since $1_G \in K$, by definition of $K \leq G$, then $\phi(1_G) \in \phi(K)$ by definition of the image of K. By lemma, $\phi(1_G) = 1_H \in \phi(K)$. Therefore, the identity is in $\phi(K)$.*

(INV) *Let $h \in \phi(K)$. Then $h = \phi(k)$ for some $k \in K$. Therefore, by definition of $K \leq G$, we get $k^{-1} \in K$. Hence, $\phi(k^{-1}) \in \phi(K)$, and finally, $\phi(k^{-1}) = h^{-1} \in \phi(K)$ by lemma.*

(CLOS) *Let $h_1, h_2 \in \phi(K)$. Then there exists $k_1, k_2 \in K$ such that $\phi(k_1) = h_1$ and $\phi(k_2) = h_2$. By definition of subgroup $k_1 k_2 \in K$ which implies $\phi(k_1 k_2) \in \phi(K)$. By definition of group homomorphism, $\phi_(k_1 k_2) = \phi(k_1)\phi(k_2) = h_1 h_2$.*

Proposition 4 (The Preimage of a subgroup is a subgroup)**.** *Let $\phi : G \to H$ be a homomorphism and let $K \leq H$.*
Then $\phi^{-1}(K) \leq G$.

Proof. Note that $\phi^{-1}(K)$ is closed under multiplication and inverses since K is and because ϕ is a homomorphism. □

Proposition 5 (The composition of homomorphisms is a homomorphism)**.** *Let $\phi : G \to H$ and $\psi : H \to K$ be homomorphisms.*
Then $\psi \circ \phi : G \to K$ is a homomorphism.

Proposition 6 (The order of the image divides the order of the original element)**.** *Let $\phi : G \to H$ be a homomorphism and let $g \in G$ be an element of finite order.*
Then $\operatorname{ord}(\phi(g)) \mid \operatorname{ord}(g)$.

Proof. Let $\operatorname{ord}(g) = n$. Then $\phi(g)^n = \phi(g^n) = \phi(1_G) = 1_H$. Thus n is an multiple of the order of $\phi(g)$. □

Proposition 7 (Generators are mapped to generators)**.** *Let $\phi : G \to H$ be a homomorphism and let $X \subset G$.*
Then $\langle \phi(X) \rangle = \phi(\langle X \rangle)$.

Proof. Let $\mathcal{X}$ be the collection of subgroups in G which contain X. If $K \in \mathcal{X}$, then $\phi(K)$ is a subgroup of H which contains $\phi(X)$. On the other hand, if $M \leq H$ is a subgroup of H which contains $\phi(X)$, then $\phi^{-1}(M) \in \mathcal{X}$. Thus $\langle \phi(X) \rangle = \cap \phi(\mathcal{X})$, and

$$\phi(\langle X \rangle) = \phi(\cap \mathcal{X}) = \cap \phi(\mathcal{X}) = \langle \phi(X) \rangle.$$

□

Corollary 1. *The homomorphic image of a cyclic group is cyclic.*

Definition 2. An injective homomorphism is called a *monomorphism*. A surjective homomorphism is called an *epimorphism*. A bijective homomorphism is called an *isomorphism*. If there exists an isomorphism between the groups G and H, we say that G and H are *isomorphic*, and write $G \cong H$.

Proposition 8. *Let G be a group. Then $\mathrm{id}_G : G \to G$ is an isomorphism.*

Proposition 9. *Let $\phi : G \to H$ be an isomorphism.*
Then $\phi^{-1} : H \to G$ is an isomorphism.

Proof. By definition, ϕ is bijective, so it is invertible. Let $h_1, h_2 \in H$. Since ϕ is bijective, there exist unique $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$. Thus $\phi^{-1}(h_1 h_2) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$.
□

Proposition 10. *Let $\mathcal{G}$ be a collection of groups.*
Then isomorphism is an equivalence relation on $\mathcal{G}$.

Proof. The identity map on a group establishes the reflexivity of isomorphism. The symmetry relation is estabilished by the fact that bijective maps are invertible. The transitivity relation is given by the fact that the composition of homomorphisms is a homomorphism, and the composition of bijections is a bijection. □

Definition 3. Let $\phi : G \to H$ be a homomorphism. The *kernel* of ϕ is the subset of G denoted by $\ker(\phi)$ and defined by

$$\ker(\phi) = \{g \in G \mid \phi(g) = 1_H\}.$$

This is easily seen to be a subgroup.

Proposition 11. *Let $\phi : G \to H$ be a homomorphism.*
Then ϕ is injective if and only if $\ker(\phi) = \{1_G\}$.

Proof.
($\Rightarrow$) Suppose the ϕ is injective. Since the identity of G maps to the identity of H, no other element of G may map to the identity of H.

($\Leftarrow$) Suppose that $\ker(\phi)$ is trivial. Then

$$\begin{aligned}\phi(g_1) = \phi(g_2) &\Leftrightarrow \phi(g_1)\phi(g_2)^{-1} = 1_H \\ &\Leftrightarrow \phi(g_1)\phi(g_2^{-1}) = 1_H \\ &\Leftrightarrow \phi(g_1 g_2^{-1}) = 1_H \\ &\Leftrightarrow g_1 g_2^{-1} = 1_G \\ &\Leftrightarrow g_1 = g_2.\end{aligned}$$

□

0.2. **Cosets.**

Definition 4. Let G be a group and $H \leq G$. Let $g \in G$.

The *left coset* at g of H in G is the set

$$gH = \{gh \mid h \in H\}.$$

The *right coset* at g of H in G is the set

$$Hg = \{hg \mid h \in H\}.$$

Proposition 12. *Let G be a group and $H \leq G$. Let $g, g_1, g_2 \in G$. Then*

(a) $g \in gH$;
(b) $g \in Hg$;
(c) $gH = H \Leftrightarrow g \in H$;
(d) $Hg = H \Leftrightarrow g \in H$;
(e) $g_1 H = g_2 H \Leftrightarrow g_1^{-1} g_2 \in H$;
(f) $Hg_1 = Hg_2 \Leftrightarrow g_2 g_1^{-1} \in H$.

Proof. First note that since $1 \in G$, H is a coset of H in G, specifically, $H = 1H$. Also $g \in gH$ since $g = g \cdot 1$. This proves **(a)**.

Thus if $gH = H$, then $g \in H$.

If $g \in H$, then $gH \subset H$ by closure, because H is a group. Since g^{-1} is also in H, we have $g^{-1}H \subset H$, so $H \subset gH$; thus $gH = H$. This proves **(c)**.

If $g_1 H = g_2 H$, then $H = g_1^{-1} g_2 H$, so $g_1^{-1} g_2 \in H$. If $g_1^{-1} g_2 \in H$, then $g_1^{-1} g_2 H = H$, so $g_2 H = g_1 H$. This proves **(e)**.

The proofs for right cosets are analogous. □

Definition 5. Let G be a group and let $H \leq G$. Let $g_1, g_2 \in G$.

We say that g_1 and g_2 are *left congruent modulo H* if $g_1^{-1} g_2 \in H$.

We say that g_1 and g_2 are *right congruent modulo H* if $g_1 g_2^{-1} \in H$.

Proposition 13. *Let G be a group and $H \leq G$. Then left and right congruence modulo H is an equivalence relation.*

Proof. Let $g \in G$. Then $g^{-1} g = 1 \in H$, so g is left congruent to itself modulo H. Thus left congruence is reflexive.

Let $g_1, g_2 \in G$. Suppose that $g_1^{-1} g_2 \in H$. Thus $g_2^{-1} g_1 = (g_1^{-1} g_2)^{-1} \in H$ since H is closed under inverses. Thus left congruence is symmetric.

Let $g_1, g_2, g_3 \in G$. Suppose that $g_1^{-1} g_2 \in H$ and $g_2^{-1} g_3 \in H$. Then $g_1^{-1} g_3 = g_1^{-1} g_2 g_2^{-1} g_3 \in H$ since H is closed under multipliation. Thus left congruence is transitive.

The proof for right congruence is analogous. □

Corollary 2. *Let G be a group and let $H \leq G$. Then the collection of left (right) cosets of H in G partition G.*

Proposition 14. *Let G be a group and let $H \leq G$. Let $g \in G$. Then the maps*

$$\lambda_g : H \to gH \text{ given by } \phi(h) = gh$$

and

$$\rho_g : H \to Hg \text{ given by } \phi(h) = hg$$

are bijective.

Proof. Let $gh \in gH$; then $h \mapsto gh$, so λ_g is surjective. Let $gh_1, gh_2 \in gH$; then $h_1 = h_2$ by cancellation, so λ_g is injective. The proof for ρ_g is analogous. □

Corollary 3. *Let G be a group and let $H \leq G$. Let $g \in G$. Then $|gH| = |Hg| = |H|$.*

Definition 6. Let G be a group and $H \leq G$. The collection of left cosets of H in G is called the *left coset space* of H in G. The collection of right cosets of H in G is called the *right coset space* of H in G.

Proposition 15. *Let G be a group and $H \leq G$. Then there is a correspondence between the left and right coset spaces of H in G given by*

$$gH \leftrightarrow Hg^{-1}.$$

Proof. The map $\phi : gH \mapsto Hg^{-1}$ is well-defined and injective:

$$\begin{aligned} g_1H = g_2H &\Leftrightarrow g_2^{-1}g_1H = H \\ &\Leftrightarrow g_2^{-1}g_1 \in H \\ &\Leftrightarrow Hg_2^{-1}g_1 = H \\ &\Leftrightarrow Hg_2^{-1} = Hg_1^{-1}. \end{aligned}$$

Since $\phi(g^{-1}H) = Hg$, the map is surjective. □

Corollary 4. *Let G be a group and $H \leq G$. Then the left coset space of H in G and the right coset space of H in G have the same cardinality.*

Definition 7. Let G be a group and let $H \leq G$.

The *index* of H is G is the cardinality of the left coset space of H in G, and is denoted by $[G : H]$.

Theorem 1 (Lagrange's Theorem)**.** *Let G be a finite group and $H \leq G$. Then $|G| = |H|[G : H]$.*

Proof. The cardinality of each left coset is the cardinality of H. There are $[G : H]$ of these in G. Since these cosets form a partition of G, the result follows. □

Proposition 16. *Let G be a finite group and let $g \in G$.*
Then $\text{ord}(g)$ *divides $|G|$.*

Proof. Since $\langle g \rangle \leq G$ and $\text{ord}(g) = |\langle g \rangle|$, the result follows from Lagrange's Theorem. □

Proposition 17. *Let G be a finite group such that $|G|$ is prime.*
Then G is cyclic.

Proof. Let G be a group of order p, where p is prime. Let $p \in G$. Then $\text{ord}(g)||G|$ so $\text{ord}(g) = p$ or $\text{ord}(g) = 1$. Thus if $g \neq 1$ then $G = \langle g \rangle$. $\square$

0.3. **Normal Subgroups.**

Definition 8. Let G be a group and $H \leq G$.

We say that H is a *normal* subgroup, and write $H \triangleleft G$, if $gH = Hg$ for every $g \in G$.

Proposition 18. *Let G be a group and let $H \leq G$. The following conditions are equivalent:*

(1) *$gH = Hg$ for every $g \in G$;*
(2) *$g^{-1}Hg = H$ for every $g \in G$;*
(3) *$g^{-1}Hg \subset H$ for every $g \in G$.*

Proof. That **(1)** $\Leftrightarrow$ **(2)** and **(2)** $\Rightarrow$ **(3)** are obvious.

Suppose that $g^{-1}Hg \subset H$ for every $g \in G$. Let $g \in G$; then $g^{-1} \in G$, so $gHg^{-1} \subset H$. Thus $H \subset g^{-1}Hg$. □

Proposition 19. *Let G be a group. Then $G \triangleleft G$ and $1 \triangleleft G$.*

Proposition 20. *Let G be a group and let $\mathcal{N}$ be a collection of normal subgroups of G. Then $\cap\mathcal{N}$ is a normal subgroup of G.*

Proof. Let $\mathcal{N} = \{H_\alpha \triangleleft G \mid \alpha \in A\}$, where A is some indexing set. Then for any $g \in G$,

$$g^{-1}(\cap_{\alpha\in A} H_\alpha)g = \cap_{\alpha\in A} g^{-1}H_\alpha g = \cap_{\alpha\in A} H_\alpha$$

□

Proposition 21. *Let G be an abelian group and let $H \leq G$. Then $H \triangleleft G$.*

Proof. For $H \triangleleft G$ and $g \in G$, $h \in H$ we have $gh = hg$. Thus $gH = Hg$. □

Proposition 22. *Let $\phi : G \to H$ be a homomorphism and let $K \in \ker(\phi)$. Then $K \triangleleft G$.*

Proof. We have $\phi(g^{-1}Kg) = \phi(g)^{-1}\phi(K)\phi(g) = \phi(g)^1 \cdot 1_H\phi(g) = 1_H$. Thus $g^{-1}Kg \subset K$. □

Definition 9. Let G be a group and let $X, Y \subset G$. Set

$$XY = \{xy \in G \mid x \in X \text{ and } y \in Y\} \quad \text{and} \quad X^{-1} = \{x^{-1} \in G \mid x \in X\}.$$

Proposition 23. *Let G be a group and let $H, K \leq G$. Then $HK \leq G$ if and only if $HK = KH$.*

Proof. If $M \leq G$, then $M^{-1} = M$. Thus if $HK \leq G$, then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$.

Suppose $HK = KH$. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$ so that h_1k_1 and h_2k_2 are arbitrary members of HK. Since $HK = KH$, there exists $k_3 \in K$ such that $k_1h_2 = h_2k_3$. Then $h_1k_1h_2k_2 = h_1h_2k_3k_2 \in HK$.

Let $h \in H$ and $k \in K$ so that hk is an arbitrary member of HK. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. Thus $HK \leq G$. □

Proposition 24. *Let G be a group, $H \leq G$, and $K \triangleleft G$. Then $HK = KH$, and $HK \leq G$.*

Proof. We have $hK = Kh$ for every $h \in H$, so $HK = KH$. Thus $HK \leq G$ by the previous proposition. □

1. Groups of Order Four

Proposition 25. *Let G be a finite group and let $g \in G$. Then* $\text{ord}(g)$ *divides* $|G|$.

Proof. The order of g is equal to the order of the cyclic subgroup generated by g. By LaGrange's Theorem, this order divides the order of the group G. □

Proposition 26. *Let G be a group such that $g^2 = 1$ for every $g \in G$. Then G is abelian.*

Proof. For $g \in G$, $g^2 = 1 \Rightarrow g = g^{-1}$. For $g, h \in G$, $gh \in G$ so $(gh)^2 = 1$. That is, $1 = ghgh = g^{-1}h^{-1}gh$. Thus $hg = gh$. □

Proposition 27. *Every group of order four is abelian.*

Proof. Let G be a group of order four. If G has an element of order 4, then this element generates G, so G is cyclic, and therefore is abelian in this case. Otherwise, every element of G has order 2 or 1, so $g^2 = 1$ for every $g \in G$; thus G is abelian in this case. □

Proposition 28. *Let G be a group of order four.*
Then either $G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. Suppose that G has an element g of order 4. Then $G = \langle g \rangle = \{1, g, g^2, g^3\}$. Let $\phi : G \to \mathbb{Z}_4$ be given by $g^n \mapsto \overline{n}$. So $\phi(g^{m+n}) = \overline{m+n} = \overline{m} + \overline{n} = \phi(g^m) + \phi(g^n)$, so ϕ is a homomorphism. It is easily seen that ϕ is a homomorphism. Clearly ϕ is bijective, so ϕ is an isomorphism.

Suppose that G does not have an element of order 4. Since G has exactly one element of order 1, that being the identity, and since the order of an element divides the order of the group, the other element of G have order 2.

Let $g, h \in G$ be element of order 2. Then $G = \{1, g, h, gh\}$. Let $\phi : G \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be given by $1 \mapsto (0,0)$, $g \mapsto (1,0)$, $h \mapsto (0,1)$, and $gh \mapsto (1,1)$. Direct computation shows that this is an isomorphism. □

Definition 10. Let $K_4 = \{1, g, h, gh\}$ such that $g^2 = 1$ and $h^2 = 1$. These relations completely determine the a group structure on K_4, called the *Klein Four* group.

2. Homomorphisms

Proposition 29. *Let $\phi : G \to H$ be a group homomorphism. Let $g \in G$ be an element of finite order. Then* $\text{ord}(\phi(g))$ *divides* $\text{ord}(g)$.

Proof. Note that $1_H = \phi(1_G) = \phi(g^{\text{ord}(g)}) = \phi(g)^{\text{ord}(g)}$. Thus $\text{ord}(\phi(g))|\text{ord}(g)$. □

Problem 1. Find all injective homomorphisms $K_4 \to D_5$.

Proof. Solution The image of an injective homomorphism is a subgroup of the range which is isomorphic to the domain. The order of a subgroup of D_5 divides 10, since $|D_5| = 10$. Thus D_5 has no subgroup of order 4, an there cannot be an injective homomorphism $K_4 \to D_5$. □

Problem 2. Find all surjective homomorphisms $\mathbb{Z}_5 \times \mathbb{Z}_2 \to D_5$.

Proof. Solution Since $|\mathbb{Z}_5 \times \mathbb{Z}_2| = |D_5|$, any surjective homomorphism would be bijective, and hence an isomorphism. But these groups cannot be isomorphic, since $\mathbb{Z}_5 \times \mathbb{Z}_2$ is abelian and D_5 isn't. □

Problem 3. Find all surjective homomorphisms $\mathbb{Z}_{10} \times \mathbb{Z}_2 \to \mathbb{Z}_8$.

Proof. Solution It follows from the isomorphism theorem that the order of the image of a group homomorphism divides the order of the domain. Thus we cannot have a group of order 8 as a homomorphic image of a group of order 20. □

Problem 4. Find all surjective homomorphisms $\mathbb{Z}_{10} \times \mathbb{Z}_2 \to D_5$.

Proof. Solution The homomorphic image of an abelian group is abelian, so again there are none. □

Problem 5. Find all homomorphisms K_4 to S_3.

Proof. Solution Let $\sigma = (123)$ and $\tau = (12)$. We know that

$$S_3 = \{\epsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}.$$

Let $\phi : K_4 \to S_3$ be a homomorphism. Then $\text{ord}(\phi(g))|2$, so $\phi(g) \in \{\epsilon, \tau, \tau\sigma, \tau\sigma^2\}$; similarly

$\phi(h) = \epsilon$; otherwise, $\phi(gh) = \phi(g)\phi(h)$ is an element of order 3. On the other hand, we get a homomorphism in both of these cases, as one can check. Similarly, we may send g to any of 3 reflections, and h to either the same reflection or to ϵ; the same comments apply to h. Thus we get ten homomorphisms:

- $g \mapsto \epsilon, h \mapsto \epsilon$;
- $g \mapsto \epsilon, h \mapsto \tau$;
- $g \mapsto \epsilon, h \mapsto \tau\sigma$;
- $g \mapsto \epsilon, h \mapsto \tau\sigma^2$;
- $g \mapsto \tau, h \mapsto \epsilon$;
- $g \mapsto \tau, h \mapsto \tau$;
- $g \mapsto \tau\sigma, h \mapsto \epsilon$;
- $g \mapsto \tau\sigma, h \mapsto \tau\sigma$;
- $g \mapsto \tau\sigma^2, h \mapsto \epsilon$;
- $g \mapsto \tau\sigma^2, h \mapsto \tau\sigma^2$.

Note that the kernel of each of these homomorphisms contains one of g, h, or gh, or all three. □

3. Automorphisms

Problem 6. Find an automorphism which is not an inner automorphism.

Proof. Let $G = \langle g \rangle$ be a cyclic group of order 5. Then G is abelian. The map $\phi : G \to G$ given by $g^n \mapsto g^{2n}$ is a homomorphism, since $\phi(g^m g^n) = \phi(g^{m+n}) = g^{2(m+n)} = g^{2m}g^{2n}$. It is injective since if $g^n \in \ker(\phi)$, then $g^{2n} = 1$, so $5|2n$ since $\text{ord}(g) = 5$. Since 5 is prime, we have $5|n$. Thus $g^n = 1$ in G. Since $g \mapsto g^2$, ϕ is not the identity homomorphism.

Now let $h \in G$. Then $\text{inn}_h(g^n) = hg^nh^{-1} = g^n$, since G is abelian. Thus inn_h is the identity homomorphism, and ϕ is not an inner automorphism. □

Definition 11. Let G be a group and let $\phi \in \mathrm{Aut}(G)$. The *fixed set* of ϕ is

$$\mathrm{Fix}(\phi) = \{g \in G \mid \phi(g) = g\}.$$

If $H \leq \mathrm{Aut}(G)$, the fixed set of H is

$$\begin{aligned}\mathrm{Fix}(H) &= \{g \in G \mid \phi(g) = g \text{ for all } \phi \in H\} \\ &= \cap_{\phi \in H} \mathrm{Fix}(\phi).\end{aligned}$$

Problem 7. Let G be a group and let $\phi \in \mathrm{Aut}(G)$. Show that $\mathrm{Fix}(\phi) \leq G$.

Proof. Solution Let $g, h \in \mathrm{Fix}(\phi)$. Then $\phi(gh) = \phi(g)\phi(h) = gh$, so $gh \in \mathrm{Fix}(\phi)$. Also $\phi(g^{-1}) = \phi(g)^{-1} = g^{-1}$, so $g^{-1} \in \mathrm{Fix}(\phi)$. Thus $\mathrm{Fix}(\phi) \leq G$. □

Problem 8. Let G be a group and assume $\mathrm{inn}_g \in \mathrm{Aut}(G)$. Find $\mathrm{Fix}(\mathrm{inn}_g)$.

Proof. Solution Let $x \in \mathrm{Fix}(\mathrm{inn}_g)$. Then $gxg^{-1} = x$, so $gx = xg$. Thus $x \in C_G(g)$. On the other hand, if $gx = xg$, we have $\mathrm{inn}_g(x) = x$. Thus $\mathrm{Fix}(\mathrm{inn}_g) = C_G(g)$, the set of all elements which commute with g. □

Problem 9. Let G be a group and assume $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. Find $\mathrm{Fix}(\mathrm{Inn}(G))$.

Proof. Solution We have

$$\begin{aligned}\mathrm{Fix}(\mathrm{Inn}(G)) &= \cap_{g \in G} \mathrm{Fix}(\mathrm{inn}_g) \\ &= \cap_{g \in G} C_G(g) \\ &= Z(G),\end{aligned}$$

the set of all elements of G which commute with every element of G. □

Definition 12. Let G be a group and let $g \in G$. The *stabilizer* of g in $\mathrm{Aut}(G)$ is

$$\mathrm{Stb}(g) = \{\phi \in \mathrm{Aut}(G) \mid \phi(g) = g.$$

Clearly $\phi \in \mathrm{Stb}(g) \Leftrightarrow g \in \mathrm{Fix}(\phi)$.

Problem 10. Let G be a group and let $g \in G$. Show that $\mathrm{Stb}(g) \leq \mathrm{Aut}(G)$.

Proof. Solution Let $\phi, \psi \in \mathrm{Stb}(g)$. Then $(\psi \circ \phi) = \psi(\phi(g)) = \psi(g) = g$, so $\psi \circ \phi \in \mathrm{Stb}(g)$. Also if $\phi(g) = g$, then $\phi^{-1}(\phi(g)) = \phi(g)$, so $\phi^{-1}(g) = g$ and $\phi^{-1} \in \mathrm{Stb}(g)$. Thus $\mathrm{Stb}(g) \leq \mathrm{Aut}(G)$. □

4. Lifting

Problem 11. Let G be a finite group and let $H \triangleleft G$. Let p be a prime integer. Suppose that G/H has an element of order p. Show that G has an element of order p.

Proof. Solution Let $\overline{G} = G/H$ and for $g \in G$, denote the coset gH by $\overline{g}$.

Let $\overline{g} \in \overline{G}$ be an element of order p. Then $\overline{g}^p = \overline{g^p} = \overline{1}$, which means that $g^p \in H$. Since G is finite, the element g^p has finite order, say $\mathrm{ord}(g^p) = k$. Let $h = g^k$. Then $h^p = (g^k)^p = (g^p)^k = 1$, so $\mathrm{ord}(h) | p$; thus $\mathrm{ord}(h) = 1$ or p. If $\mathrm{ord}(h) = 1$, this means that $h = 1$, in which case $\mathrm{ord}(g) = p$. Otherwise h has order p. □

Problem 12. Let G be a finite group and let $g \in G$. Suppose that $C_G(g) \triangleleft G$. Show that every element of G has a power which commutes with g.

Proof. Solution Since $C_G(g)$ is normal, $G/C_G(g)$ is a group. Let $\overline{G} = G/C_G(g)$ and for $h \in G$, let $\overline{h} = hC_G(g)$.

Let $h \in G$. Since G is finite, so is $\overline{G}$. Thus $\overline{h}$ has finite order, say $\text{ord}(\overline{h}) = n$. Thus $\overline{h^n} = \overline{h}^n = \overline{1}$, which means that $h^n \in C_G(g)$. Thus h^n commutes with g. □

Problem 13. Show that $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group in which every element has finite order.

Proof. Solution Since $\mathbb{Q}$ is abelian and $\mathbb{Z} \leq \mathbb{Q}$, we have $\mathbb{Z} \triangleleft \mathbb{Q}$. Thus $\mathbb{Q}/\mathbb{Z}$ is a group. A factor group of an abelian group is always abelian, so $\mathbb{Q}/\mathbb{Z}$ is an abelian group.

Note that two rational numbers represent the same coset if and only if their difference is an integer. Then $\mathbb{Q}/\mathbb{Z}$ is infinite, since there are an infinite number of rational numbers such that none of their differences is an integer.

For example, let m and n be positive integers. Then $\frac{1}{n} - \frac{1}{m} = \frac{m-n}{mn}$, which is not an integer unless mn divides $m - n$. Since $|m - n| \leq mn$, this is never the case. Thus the rational numbers of the form $\frac{1}{n}$ represent an infinite number of distinct cosets of $\mathbb{Q}/\mathbb{Z}$.

Now let $\frac{m}{n} + \mathbb{Z}$ be a coset. Then $n\frac{m}{n} = m \in \mathbb{Z}$, so the order of $\frac{m}{n}$ divides m, and in particular, it is finite. □

Department of Mathematics, Arkansas School of Mathematics, Sciences and the Arts

E-mail address: baileym@asmsa.org