Groups, Group Actions, and the Class Equation

Dylan C. Beck

Basics and Preliminaries

Given a nonempty set G equipped with a map $\cdot : G \times G \to G$ that sends $(g, h) \mapsto g \cdot h$, we say that the pair $(G, \cdot)$ is a **group** whenever the following properties hold for G.

(i.) The map $\cdot$ is associative, i.e., we have that $g \cdot (h \cdot k) = (g \cdot h) \cdot k$ for any g, h, and k in G.

(ii.) There exists an element e_G of G such that $e_G \cdot g = g = g \cdot e_G$ for all elements g of G.

(iii.) Given an element g in G, there exists an element g^{-1} in G such that $g \cdot g^{-1} = e_G = g^{-1} \cdot g$.

One can show that the element e_G is unique and that for each element g of G, the element g^{-1} is unique, hence we refer to the element e_G of property (ii.) as the **identity** element of G, and we refer to the element g^{-1} of property (iii.) as the **inverse** of g.

Usually, we will omit the operation $\cdot$ of G and simply use concatenation, e.g., $g \cdot h \overset{\text{def}}{=} gh$. Given a nonempty set $H \subseteq G$, we say that H is a **subgroup** of G whenever H is a group with respect to the operation of G. Often, it is convenient to use the following proposition and its corollary.

Proposition 1. Given a group G and a nonempty set $H \subseteq G$ such that gh^{-1} is in H for all elements g, h in H, we have that $(H, \cdot)$ is a subgroup of G.

Corollary 1. Given a group G and a nonempty set $H \subseteq G$ such that H is closed under the operation of G and closed under taking inverses, we have that H is a subgroup of G.

We refer to the cardinality $|G|$ of a group as its **order**. Under suitable conditions, the set

$$\frac{G}{H} = \{gH \mid g \in G\}$$

of left cosets of H in G is a group (called the **quotient group**) with respect to the operation $\cdot$ of G. Explicitly, G/H is a group if and only if ghg^{-1} is in H for all g in G and h in H. Equivalently, G/H is a group if and only if the map $G \times H \to G$ that sends $(g, h) \mapsto ghg^{-1}$ restricts to a binary operation on H if and only if H is closed under conjugation by elements of G. Given that this holds, we say that H is a **normal** subgroup of G, and we write $H \trianglelefteq G$. One can show that the integer $[G : H] \overset{\text{def}}{=} |G/H|$ is well-defined in this case. Quite generally, the integer $[G : H]$ gives the number of distinct left (or right) cosets of H in G. We refer to $[G : H]$ as the **index** of H in G.

Theorem 1. (Lagrange's Theorem) Given a group G and any subgroup H of G, we have that $|G| = [G : H]|H|$. Put another way, the order of any subgroup H of G must divide the order of G.

Proof. We establish first that $aH \sim bH$ if and only if $ab^{-1} \in H$ is an equivalence relation on the left cosets of H in G. By assumption that H is a subgroup of G, we have that $e_G = aa^{-1}$ is in H so that $aH \sim aH$. Given that $aH \sim bH$, we have that ab^{-1} is in H, from which it follows that $ba^{-1} = (ab^{-1})^{-1}$ is in H so that $bH \sim aH$. Last, if we have that $aH \sim bH$ and $bH \sim cH$, then ab^{-1} and bc^{-1} are both in H so that $ac^{-1} = (ab^{-1})(bc^{-1})$ is in H, i.e., we have that $aH \sim cH$.

We claim now that each left coset of H in G has cardinality $|H|$. Consider the map $f_g : H \to gH$ defined by $f_g(h) = gh$. Certainly, this map is surjective. Given that $f_g(h) = f_g(h')$, we have that $gh = gh'$, from which it follows that $h = h'$ by the cancellative property of G. We conclude that f_g is a bijection for each element g in G, hence we have that $|H| = |gH|$ for all elements g in G.

Consequently, we may partition G as $G = \cup_{i=1}^n g_i H$, where the elements $g_1, \dots, g_n$ each belong to a distinct left coset of H in G. Considering that $n = [G : H]$ by definition and $|g_i H| = |H|$ for each integer $1 \leq i \leq n$ by the paragraph above, we conclude that $G = [G : H]|H|$. $\square$

Q1, August 2013. Consider a group G with subgroups H and K. Consider the set

$$HK = \{hk \,|\, h \in H, k \in K\}.$$

(a.) Prove that HK is a subgroup of G if and only if $HK = KH$. Conclude that if either H or K is a normal subgroup of G, then HK is a subgroup of G.

(b.) Prove that if H and K are finite, then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Given groups $(G, \cdot)$ and $(H, \star)$, a map $\varphi : G \to H$ is a **group homomorphism** whenever

$$\varphi(g \cdot h) = \varphi(g) \star \varphi(h)$$

for all elements g, h in G. Put another way, the map φ respects the operations of both G and H. We refer to the set $\ker \varphi = \{g \in G \,|\, \varphi(g) = e_H\}$ as the **kernel** of φ.

Proposition 2. Given a group homomorphism $\varphi : G \to H$, we have that

(i.) $\varphi(e_G) = e_H$ and

(ii.) $\varphi(g^{-1}) = [\varphi(g)]^{-1}$ for all elements g in G.

Proposition 3. Given a group homomorphism $\varphi : G \to H$, we have that φ is injective (or one-to-one) if and only the kernel of φ is trivial, i.e., $\ker \varphi = \{e_G\}$.

Proof. We will assume first that φ is injective. Given an element g in $\ker \varphi$, by Proposition 2, we have that $\varphi(g) = e_H = \varphi(e_G)$ so that $g = e_G$ by the injectivity of φ.

Conversely, we will assume that $\ker \varphi$ is trivial. Given any elements g and h in G such that $\varphi(g) = \varphi(g')$, by Proposition 2, we have that $e_H = \varphi(g)[\varphi(h)]^{-1} = \varphi(g)\varphi(h^{-1}) = \varphi(gh^{-1})$. By hypothesis that $\ker \varphi$ is trivial, it follows that $gh^{-1} = e_G$ so that $g = h$, as desired. $\square$

Q1, January 2015. Given a finite group G of odd order such that $gh = hg$ for all $g, h \in G$, prove that for each element $x \in G$, there exists a unique element $y \in G$ such that $y^2 = x$.

One of the most important facts about any algebraic structure is the following.

Theorem 2. (First Isomorphism Theorem) Given any groups $(G, \cdot)$ and $(H, \star)$ and a group homomorphism $\varphi : G \to H$, there exists a group isomorphism $\psi : G/\ker\varphi \to \varphi(G)$.

Proof. We must first demonstrate that $\varphi(G)$ is a subgroup of H and that $\ker\varphi$ is a normal subgroup of G. We leave this to the reader. Once this is accomplished, we may view $G/\ker\varphi$ as a group with respect to the operation $\cdot$ of G, hence it suffices to find a group isomorphism $\psi : G/\ker\varphi \to \varphi(G)$. Consider the map $\psi : G/\ker\varphi \to \varphi(G)$ defined by $\psi(g \cdot \ker\varphi) = \varphi(g)$. We must establish that ψ is well-defined, i.e., we must show that if $g \cdot \ker\varphi = h \cdot \ker\varphi$, then $\psi(g \cdot \ker\varphi) = \psi(h \cdot \ker\varphi)$. By definition, we have that $g \cdot \ker\varphi = h \cdot \ker\varphi$ if and only if $h^{-1}g \cdot \ker\varphi = e_G \cdot \ker\varphi$ if and only if $h^{-1}g$ is in $\ker\varphi$ if and only if $\varphi(h^{-1}g) = e_H$ if and only if $\varphi(h^{-1}) \star \varphi(g) = e_H$ if and only if $[\varphi(h)]^{-1} \star \varphi(g) = e_H$ if and only if $\varphi(g) = \varphi(h)$ if and only if $\psi(g \cdot \ker\varphi) = \psi(h \cdot \ker\varphi)$. We conclude that ψ is well-defined. By hypothesis that φ is a group homomorphism, it follows that ψ is a group homomorphism, and ψ is clearly surjective, hence it suffices to show that ψ is injective. Observe that $g \cdot \ker\varphi$ is in $\ker\psi$ if and only if $\varphi(g) = \psi(g \cdot \ker\varphi) = e_H$ if and only if g is in $\ker\varphi$ if and only if $g \cdot \ker\varphi = e_G \cdot \ker\varphi$ implies that $\ker\psi$ is trivial so that ψ is injective, as desired. $\square$

Theorem 3. (Second Isomorphism Theorem) Given a group G with a subgroup H and a normal subgroup N, we have that $HN/N \cong H/(H \cap N)$.

Proof. We must first demonstrate that HN is a subgroup of G such that $N \trianglelefteq HN$ and that $H \cap N$ is a subgroup of H. We leave these details to the reader. Once this is accomplished, it suffices by the First Isomorphism Theorem to find a surjective group homomorphism $\varphi : H \to HN/N$ such that $\ker\varphi = H \cap N$. We leave it to the reader to verify that the map $\varphi(h) = hN$ does the job. $\square$

Theorem 4. (Third Isomorphism Theorem) Given a group G with normal subgroups N and H such that $N \subseteq H$, we have that $(G/N)/(H/N) \cong G/H$.

Proof. We must first demonstrate that N is a normal subgroup of H and that H/N is a subgroup of G/N. We leave these details to the reader. Once this is accomplished, it suffices by the First Isomorphism Theorem to find a surjective group homomorphism $\varphi : G/N \to G/H$ such that $\ker\varphi = H/N$. We leave it to the reader to verify that the map $\varphi(gN) = gH$ does the job. Considering that this map is defined on a quotient group, we must also establish that this map is well-defined. $\square$

Theorem 5. (Fourth Isomorphism Theorem) Given a group G with a normal subgroup N, there exists a one-to-one correspondence $\{\text{subgroups of } G \text{ that contain } N\} \leftrightarrow \{\text{subgroups of } G/N\}$ that sends $H \mapsto H/N$ for a subgroup H of G that contains N with the following properties.

1.) Given any subgroups H and K of G such that $N \subseteq H$ and $N \subseteq K$, we have that $H \subseteq K$ if and only if $H/N \subseteq K/N$. Put another way, this bijection is inclusion-preserving.

2.) Given any subgroups H and K of G such that $N \subseteq H \subseteq K$, we have that

$$[K : H] = [K/N : H/N].$$

3.) Given any subgroups H and K of G such that $N \subseteq H$ and $N \subseteq K$, we have that

$$(H \cap K)/N = (H/N) \cap (K/N).$$

4.) Given any subgroup H of G such that $N \subseteq H$, we have that $H \trianglelefteq G$ if and only if $H/N \trianglelefteq G/N$.

We say that a group is **abelian** whenever $gh = hg$ for all elements g and h of G. Unfortunately, there exist groups that are not abelian, hence we define the **center** of G

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}$$

to be the set of all elements that commute with everything in G. Of course, any element g of G commutes with any power g^k of g, hence the subgroup $\langle g \rangle = \{g^k \mid k \text{ is an integer}\}$ is an abelian subgroup of any group G. We refer to the subgroup $\langle g \rangle$ as the **cyclic subgroup generated by** g. Conversely, if there exists an element g of G such that $G = \langle g \rangle$, we say that G is **cyclic**.

Proposition 4. Given a cyclic group G with infinite order, we have that $G \cong (\mathbb{Z}, +)$. Given a cyclic group G with order n, we have that $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$. Put another way, the unique (up to isomorphism) infinite cyclic group is $\mathbb{Z}$, and the unique cyclic group of order n is $\mathbb{Z}/n\mathbb{Z}$.

Proof. Use the First Isomorphism Theorem. We leave the details to the reader. □

Once we have established an isomorphism between two algebraic structures, we may use known properties about one of the objects to derive information about the other object.

Corollary 2. Given a cyclic group G with infinite order, prove that there exist no proper non-trivial cyclic subgroups of G, i.e., the only proper cyclic subgroup of G is $\{e_G\}$. Given a cyclic group G with order n, prove that for each integer $d \mid n$, there exists a cyclic subgroup of G of order d.

Proposition 5. Given a group G such that $G/Z(G)$ is cyclic, we have that G is abelian.

Proof. We will assume that $G/Z(G)$ is cyclic with generator $gZ(G)$. Given any two elements h and k of G, we have that $hZ(G) = [gZ(G)]^m = g^m Z(G)$ and $kZ(G) = [gZ(G)]^n = g^n Z(G)$ so that $g^{-m}h$ is in $Z(G)$ and $g^{-n}k$ is in $Z(G)$. Consequently, there exist some elements z_1 and z_2 of $Z(G)$ such that $g^{-m}h = z_1$ and $g^{-n}k = z_2$. By definition of $Z(G)$, we conclude as desired that

$$hk = (g^m z_1)(g^n z_2) = g^m g^n z_1 z_2 = g^n g^m z_2 z_1 = (g^n z_2)(g^m z_1) = kh.$$ □

Q1, January 2014. Given a finite group G, recall that the centralizer of $x \in G$ is the set

$$Z_G(x) = \{g \in G \mid gx = xg\}.$$

(a.) Prove that $Z_G(x)$ is a subgroup of G such that $[G : Z_G(x)]$ is the number of elements of G conjugate to x.

(b.) Given that the order of G is odd, prove that x and x^{-1} are not conjugate unless $x = e_G$.

Group Actions

Consider a group $(G, \cdot)$ and a nonempty set X. We say that a map $* : G \times X \to X$ that sends $(g, x) \mapsto g * x$ is a **group action** whenever the map $*$ obeys the properties

(i.) $g * (h * x) = (g \cdot h) * x$ for all g, h in G and x in X and

(ii.) $e_G * x = x$ for all x in X.

One could also say that G acts on X by $*$. We define the **kernel** of a group action by

$$K_* \stackrel{\text{def}}{=} \{g \in G \mid g * x = x \text{ for all } x \in X\}.$$

On the other hand, we define the **stabilizer** of an element x in X by

$$\operatorname{Stab}_G(x) = \{g \in G \mid g * x = x\},$$

from which it follows that $K_* = \cap_{x \in X} \operatorname{Stab}_G(x)$. We say that a group action is **faithful** whenever its kernel K_* is trivial, i.e., whenever we have that $K_* = \{e_G\}$. We will also consider the set

$$\operatorname{Fix}_G(X) = \{x \in X \mid g * x = x \text{ for all } g \in G\}.$$

Proposition 6. Given a group G acting on a nonempty set X by $*$, prove that $K_* \trianglelefteq G$.

Proof. Use the one-step subgroup test of Proposition 1; then, prove that for any element x in X, g in G, and k in K_*, we have that $gkg^{-1} * x = x$. We leave the details to the reader. $\square$

Theorem 6. (The Orbit-Stabilizer Theorem) Given a group G acting on a nonempty set X, the relation $x \sim y$ if and only if $y = g*x$ for some element g of G is an equivalence relation. We denote by $\mathcal{O}(x) = \{g*x \mid g \in G\}$. Further, the number of elements in the equivalence class of any element x in X is the index of the stabilizer of x in G, i.e., we have that $|\mathcal{O}(x)| = \#\{g*x \mid g \in G\} = [G : \operatorname{Stab}_G(x)]$.

Proof. We must first demonstrate that $\sim$ is (1.) reflexive, (2.) symmetric, and (3.) transitive. We leave these details to the reader. Once this is established, we may denote by $\mathcal{O}(x) = \{g * x \mid g \in G\}$ the equivalence class of x under $\sim$. We refer to this as the **orbit** of x. Consider the map

$$\begin{aligned} \mathcal{O}(x) &\to G/\operatorname{Stab}_G(x) \\ y = g * x &\mapsto g \operatorname{Stab}_G(x) \end{aligned}$$

from the equivalence class of x modulo $\sim$ to the left cosets of $\operatorname{Stab}_G(x)$ in G. We claim that this map is a bijection, hence we have that $\#\{g * x \mid g \in G\} = |\mathcal{O}(x)| = [G : \operatorname{Stab}_G(x)]$.

Certainly, the map is surjective. On the other hand, we have that $g \operatorname{Stab}_G(x) = h \operatorname{Stab}_G(x)$ if and only if $h^{-1}g \operatorname{Stab}_G(x) = e_G \operatorname{Stab}_G(x)$ if and only if $h^{-1}g$ is in $\operatorname{Stab}_G(x)$ if and only if $h^{-1}g*x = x$ if and only if $h*(h^{-1}g*x) = h*x$ if and only if $hh^{-1}*(g*x) = h*x$ if and only if $e_G*(g*x) = h*x$ if and only if $g * x = h * x$, from which it follows that the map is injective, as desired. $\square$

We say that a group action is **transitive** whenever there is only one orbit, i.e., for any two elements x and y of X, there exists an element g of G such that $y = g * x$.

Corollary 3. If G is a finite group acting on a nonempty set X, then $|G| = |\mathcal{O}(x)| \cdot |\operatorname{Stab}_G(x)|$.

The Class Equation

Given a group G, the conjugation map $G \times G \to G$ that sends $(g, h) \mapsto ghg^{-1}$ defines a group action of G on itself. One can easily verify that

(i.) $e_G * g = e_G g e_G^{-1} = g$ for all g in G and

(ii.) $k * (h * g) = k * (hgh^{-1}) = khgh^{-1}k^{-1} = khg(kh)^{-1} = kh * g$ for all elements g, h, k in G.

We say that two elements g and h of G are **conjugate** in G if and only if there exists an element k of G such that $h = kgk^{-1} = k * g$. Consequently, two elements of G are conjugate in G precisely when they are in the same orbit of G acting on itself by conjugation. Observe that

$$\operatorname{Stab}_G(g) = \{h \in G \mid h * g = g\} = \{h \in G \mid hgh^{-1} = g\} = \{h \in G \mid hg = gh\}$$

is the set of elements of G that commute with g. We refer to this set as the **centralizer** of g in G, and we denote it by $Z_G(g)$. Consequently, we may identify the stabilizer of g under the action of conjugation with the centralizer of g in G. By the Orbit-Stabilizer Theorem, it follows that

$$|\mathcal{O}(x)| = [G : \operatorname{Stab}_G(x)] = [G : Z_G(g)].$$

Considering that $\mathcal{O}(g) = \{h * g \mid h \in G\} = \{hgh^{-1} \mid h \in G\}$, it follows that $\mathcal{O}(g)$ is the conjugacy class of g in G, and the above displayed equation says that the number of elements conjugate to g in G is precisely the index of the centralizer of g in G. We conclude the following.

Theorem 7. (The Class Equation) Given a finite group G with center $Z(G)$ and representatives $g_1, \dots, g_n$ of the distinct conjugacy classes of G not contained in the center $Z(G)$, we have that

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : Z_G(g_i)].$$

Proof. Considering that G acts on itself by conjugation, it follows by the Orbit-Stabilizer Theorem that the equivalence relation $x \sim y$ if and only if $y = gxg^{-1}$ for some element g of G partitions G:

$$G = \bigcup_{g \in G} \mathcal{O}(g) = \mathcal{O}(z_1) \cup \cdots \cup \mathcal{O}(z_k) \cup \mathcal{O}(g_1) \cup \cdots \cup \mathcal{O}(g_n),$$

where the z_i are elements of the center $Z(G)$ and the g_j are representatives of the distinct conjugacy classes of G not contained in the center. Consequently, we have that

$$|G| = \sum_{i=1}^{k} |\mathcal{O}(z_i)| + \sum_{j=1}^{n} |\mathcal{O}(g_j)| = \sum_{i=1}^{k} 1 + \sum_{j=1}^{n} [G : \operatorname{Stab}_G(g_j)] = |Z(G)| + \sum_{i=1}^{n} [G : Z_G(g_i)]. \qquad \square$$

Of course, the Class Equation follows from a more general fact about group actions.

Theorem 8. (The Class Equation of a Group Action) Consider a group G that acts on a finite set X via $*$. Consider the set $\operatorname{Fix}_G(X) = \{x \in X \mid g * x = x \text{ for all } g \in G\}$, and let $x_1, \dots, x_n$ be representatives for the distinct cosets $G/\operatorname{Stab}_G(x_i)$ not contained in $\operatorname{Fix}_G(X)$. We have that

$$|X| = |\operatorname{Fix}_G(X)| + \sum_{i=1}^{n} [G : \operatorname{Stab}_G(x_i)].$$

Once we have the Class Equation (and the more general version) at our disposal, we can tackle many more of the group theory questions from previous qualifying exams in algebra.

Q4, August 2019. Consider a group G. We say that $x, y \in G$ are *conjugate* whenever $y = gxg^{-1}$ for some element $g \in G$. Conjugacy forms an equivalence relation with equivalence classes

$$[x] = \{gxg^{-1} \mid g \in G\}.$$

(a.) Prove that $[x]$ is a singleton if and only if $x \in Z(G)$, the center of G.

(b.) Prove that $\#[x] = [G : Z_G(x)]$, where $Z_G(x) = \{g \in G \mid gx = xg\}$ is the centralizer of x.

(c.) Given a finite group G of odd order and a subgroup $N \trianglelefteq G$ of order 3, prove that $N \leq Z(G)$.

Q1, January 2017. Consider a finite group G of order p^n with p prime.

(a.) Prove that $Z(G)$ is non-trivial.

(b.) Prove that if $N \leq G$ is a normal subgroup of order p, then $N \leq Z(G)$.

Q1, August 2015. Given a group G, denote the center of G by $Z(G)$, and note that the center of G is a normal subgroup of G. Construct subgroups $Z_i(G)$ inductively as follows.

1.) Begin with $Z_0(G) = \{e_G\}$.

2.) For each integer $i \geq 0$, let $Z_{i+1}(G)$ be the subgroup of G that is the pre-image of the center of the group $G/Z_i(G)$ so that $Z_{i+1}(G)/Z_i(G)$ is the center of $G/Z_i(G)$.

We note that G is nilpotent if $Z_n(G) = G$ for some integer $n \geq 1$.

(a.) Prove that $Z_i(G)$ is a normal subgroup of G for each i.

(b.) Prove that if $|G| = p^r$ with p prime, then G is nilpotent.

Q2, January 2014. Consider a group G with a subgroup H such that $[G : H] = n$. Prove that there exists a normal subgroup K of G such that $K \subseteq H$ and $[G : K] \leq n!$.

Give them a shot; if you need a hint or to check your solutions, see the proofs provided below.

Proofs and Solutions

Q1, August 2013. Consider a group G with subgroups H and K. Consider the set

$$HK = \{hk \mid h \in H, k \in K\}.$$

(a.) Prove that HK is a subgroup of G if and only if $HK = KH$. Conclude that if either H or K is a normal subgroup of G, then HK is a subgroup of G.

(b.) Prove that if H and K are finite, then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Proof. (a.) We will assume first that $HK = KH$. We have therefore that for each $h_1k_1 \in HK$, there exists a $k_2h_2 \in KH$ such that $h_1k_1 = k_2h_2$, and vice-versa. Given any elements $h_1k_1, h_2k_2 \in HK$, we claim that $h_1k_1k_2^{-1}h_2^{-1} = (h_1k_1)(h_2k_2)^{-1} \in HK$. We have that $h_1k_1k_2^{-1} \in HK$ so that by hypothesis $h_1k_1k_2^{-1} = k_3h_3$ for some $k_3h_3 \in KH$. We have therefore that $h_1k_1k_2^{-1}h_2^{-1} = k_3h_3h_2^{-1}$. Likewise, we have that $k_3h_3h_2^{-1} \in KH$ so that by hypothesis $k_3h_3h_2^{-1} = h_4k_4$. We conclude that $HK \leq G$.

We will assume now that $HK \leq G$. Given any element $hk \in HK$, we have that $h^{-1}k^{-1}$ is in HK. Considering that $hkh^{-1}k^{-1}$ is in HK by hypothesis that $HK \leq G$, we find that $hkh^{-1}k^{-1} = h_1k_1$ so that $h_1^{-1}hk = k_1kh$. We claim that the map $\ell_{h_1^{-1}} : H \to H$ defined by $\ell_{h_1^{-1}}(h) = h_1^{-1}h$ is surjective, from which it follows that $HK \subseteq KH$. Of course, this is the case because $h = h_1^{-1}(h_1h) = \ell_{h_1^{-1}}(h_1h)$. Conversely, given any element $kh \in KH$, we have that $h = he_G \in HK$ and $k = e_Gk \in HK$ so that $kh = (e_Gk)(he_G) \in HK$ by assumption that $HK \leq G$. We conclude that $HK = KH$.

We note that if $H \trianglelefteq G$, then $gHg^{-1} \subseteq H$ (or equivalently $gHg^{-1} = H$) for every g in G by definition. Particularly, we have that $kHk^{-1} = H$ for every k in K so that $kH = Hk$ for every k in K, i.e., $HK = KH$. Likewise, a similar result follows if $K \trianglelefteq G$. By the exposition we have given above, we conclude that if either H or K is normal in G, then HK is a subgroup of G. $\square$

Proof. (b.) Considering that H is finite, we may write $H = \{h_1, \dots, h_n\}$. Observe that an element of HK is of the form h_ik for some $k \in K$, hence $HK = \cup_{i=1}^n h_iK$ is the union of left cosets of K in HK. We claim that there are $\frac{|H|}{|H \cap K|}$ distinct left cosets of K in HK. Observe that $h_iK = h_jK$ if and only if $h_j^{-1}h_iK = K$ if and only if $h_j^{-1}h_i \in K$ if and only if $h_j^{-1}h_i \in H \cap K$ if and only if $h_i(H \cap K) = h_j(H \cap K)$, hence the distinct left cosets of K in HK are in bijection with the distinct left cosets of $H \cap K$ in H. By Lagrange's Theorem, we have that $[HK : K] = [H : H \cap K] = \frac{|H|}{|H \cap K|}$. Considering that each left coset of K in HK has $|K|$ elements, we conclude that $|HK| = \frac{|H||K|}{|H \cap K|}$. $\square$

Q1, January 2015. Given a finite abelian group G of odd order, prove that for each element $x \in G$, there exists a unique element $y \in G$ such that $y^2 = x$.

Proof. Consider the map $\varphi : G \to G$ defined by $\varphi(g) = g^2$. By hypothesis that G is abelian, we have $\varphi(gh) = (gh)^2 = ghgh = gghh = g^2h^2 = \varphi(g)\varphi(h)$ so that φ is a group homomorphism with

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_G\} = \{g \in G \mid g^2 = e_G\}.$$

We note that the order of each element of G divides the order of G, hence there are no elements of order 2 in G. We conclude that $\ker \varphi = \{e_G\}$. Of course, any injective map from a finite set into itself must also be surjective, hence we have that $\varphi(G) = G$, i.e., for each element $x \in G$, there exists an element $y \in G$ such that $y^2 = x$. Consider an element $z \in G$ such that $z^2 = x$. We have that $\varphi(y) = \varphi(z)$, from which it follows that $y = z$ by the injectivity of φ, so y is unique. $\square$

Q1, January 2014. Given a finite group G, recall that the centralizer of $x \in G$ is the set

$$Z_G(x) = \{g \in G \mid gx = xg\}.$$

(a.) Prove that $Z_G(x)$ is a subgroup of G such that $[G : Z_G(x)]$ is the number of elements of G conjugate to x.

(b.) Given that the order of G is odd, prove that x and x^{-1} are not conjugate unless $x = e_G$.

Proof. (a.) Certainly, we have that e_G is in $Z_G(x)$ so that $Z_G(x)$ is nonempty. Consider the elements g and h in $Z_G(x)$. We claim that $gh^{-1} \in Z_G(x)$. We have that $xgh^{-1} = gxh^{-1}$ since $gx = xg$ and $x = h^{-1}xh$ since $hx = xh$, from which it follows that $xgh^{-1} = gxh^{-1} = g(h^{-1}xh)h^{-1} = gh^{-1}x$. We conclude therefore that $Z_G(x)$ is a subgroup of G. We note that $[G : Z_G(x)]$ is the number of left (or right) cosets of $Z_G(x)$ in G. Given that $G = \{g_1, \dots, g_n\}$, the left cosets of $Z_G(x)$ in G are

$$g_1 Z_G(x), \dots, g_n Z_G(x).$$

We note that two left cosets $g_j Z_G(x)$ and $g_k Z_G(x)$ are equal if and only if $g_k^{-1} g_j \in Z_G(x)$ if and only if $g_k^{-1} g_j x = x g_k^{-1} g_j$ if and only if $g_j x g_j^{-1} = g_k x g_k^{-1}$ are in the same conjugacy class. We conclude as desired that $[G : Z_G(x)]$ is the number of elements of G conjugate to x. □

Proof. (b.) We will assume that $|G|$ is odd. By Lagrange's Theorem, we have that $[G : Z_G(x)]$ divides $|G|$ for each element $x \in G$, from which it follows that $[G : Z_G(x)]$ is odd for each $x \in G$.

On the contrary, let us assume that x is a non-identity element such that x and x^{-1} are conjugate. We claim that $x \neq x^{-1}$. On the contrary, if $x = x^{-1}$, then we have that $x^2 = e_G$, from which it follows that $|G|$ is even — a contradiction. We conclude therefore that $x \neq x^{-1}$. Considering that $[G : Z_G(x)]$ is odd, there exists a non-identity element y conjugate to x so that $y \neq x$, $y \neq x^{-1}$, and $y \neq y^{-1}$. We have that $gxg^{-1} = y$ for some $g \in G$ so that $g^{-1}x^{-1}g = y^{-1}$, hence y^{-1} is conjugate to x^{-1}. Conjugation is an equivalence relation, so we have that y^{-1} is conjugate to x. We have therefore that y and y^{-1} are conjugate, from which it follows that $[G : Z_G(x)]$ is even — a contradiction. We conclude therefore that no non-identity element x is conjugate to its inverse x^{-1}. □

Q4, August 2019. Consider a group G. We say that $x, y \in G$ are *conjugate* whenever $y = gxg^{-1}$ for some element $g \in G$. Conjugacy forms an equivalence relation with equivalence classes

$$[x] = \{gxg^{-1} \mid g \in G\}.$$

(a.) Prove that $[x]$ is a singleton if and only if $x \in Z(G)$, the center of G.

(b.) Prove that $\#[x] = [G : Z_G(x)]$, where $Z_G(x) = \{g \in G \mid gx = xg\}$ is the centralizer of x.

(c.) Given a finite group G of odd order and a subgroup $N \trianglelefteq G$ of order 3, prove that $N \leq Z(G)$.

Proof. (a.) Observe that $[x] = \{gxg^{-1} \mid g \in G\}$ is a singleton if and only if $gxg^{-1} = hxh^{-1}$ for all $g, h \in G$ if and only if $h^{-1}gx = xh^{-1}g$ for all $h, g \in G$. We have already seen that the map $\ell_{h^{-1}} : G \to G$ defined by $\ell_{h^{-1}}(g) = h^{-1}g$ is surjective, hence we conclude that $[x]$ is a singleton if and only if x commutes with every element of G if and only if $x \in Z(G)$ by definition. □

Proof. (b.) We have already established this (cf. Proposition 3 or (1a.) from January 2014). $\square$

Proof. (c.) Considering that N is a subgroup of G of order 3, it follows that $N = \{e_G, n, n^2\}$ for some element n of N of order 3. By hypothesis that N is normal in G, we have that $gNg^{-1} \subseteq N$ for all elements g in G, hence G acts on N by conjugation. Using the Class Equation for Group Actions with $X = N$ under the action of conjugation, we have that

$$3 = |N| = |\mathrm{Fix}_G(N)| + \sum_{i=1}^{k} [G : Z_G(g_i)]$$

for some representatives $g_1, \dots, g_k$ of the distinct conjugacy classes of G not contained in $\mathrm{Fix}_G(N)$. On the contrary, we will assume that $N \not\leq Z(G)$ hence either n or n^2 is not in $Z(G)$.

(i.) Given that n is not in $Z(G)$, it follows that n is not in $\mathrm{Fix}_G(N)$. Consequently, we have that $|\mathcal{O}(n)| = [G : Z_G(g_i)] \geq 2$. On the other hand, we must have that $[G : Z_G(g_i)] \leq 2$ by the Class Equation, hence we have that $[G : Z_G(g_i)] = 2$. By Lagrange's Theorem, we have that $[G : Z_G(g_i)]$ divides the order of G, and the order of G is odd by assumption — a contradiction.

(ii.) Given that n^2 is not in $Z(G)$, it follows that n is not in $Z(G)$. Contrapositively, if n is in $Z(G)$, then $gng^{-1} = n$ for all g in G, hence we have that $gn^2g^{-1} = gnng^{-1} = ngng^{-1} = n^2gg^{-1} = n^2$ for all g in G so that n^2 is in $Z(G)$. We are therefore done by the paragraph above.

We conclude therefore that both n and n^2 are in $Z(G)$ so that $N \leq Z(G)$. $\square$

Q1, January 2017. Consider a finite group G of order p^n with p prime.

(a.) Prove that $Z(G)$ is non-trivial.

(b.) Prove that if $N \leq G$ is a normal subgroup of order p, then $N \leq Z(G)$.

Proof. (a.) Consider the Class Equation

$$p^n = |G| = |Z(G)| + \sum_{i=1}^{r} [G : Z_G(g_i)],$$

where $g_1, \dots, g_r$ are the representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G and $Z_G(g_i)$ is the centralizer of g_i in G. By definition of $Z_G(g_i)$, we have that $Z_G(g_i) \neq G$ for each integer $1 \leq i \leq r$. By Lagrange's Theorem, we have that $[G : Z_G(g_i)]$ divides $|G| = p^n$, hence we have that $[G : Z_G(g_i)] = p^m$ for some integer $1 \leq m \leq n$. By rearranging the Class Equation, we have that $|Z(G)| = p^n - \sum_{i=1}^{r} [G : Z_G(g_i)]$. Considering that both quantities on the right are divisible by p, we conclude that $|Z(G)|$ is divisible by p, hence $Z(G)$ is non-trivial. $\square$

Proof. (b.) Considering that N is a normal subgroup of order p, we note that G acts on N by conjugation. Consider the Class Equation for Group Action with $X = N$. We have that

$$p = |N| = |\mathrm{Fix}_G(N)| + \sum_{i=1}^{s} [G : Z_G(g_i)],$$

where $g_1, \dots, g_s$ are the representatives of the distinct conjugacy classes of G not contained in the center $\text{Fix}_G(N)$ and $Z_G(g_i)$ is the centralizer of g_i in G. We claim that each term in the sum has size one so that for each $n \in N$, we have that $g_i^{-1} n g_i = n$, from which it follows that $N \leq Z(G)$. By definition of $Z_G(g_i)$, we have that $Z_G(g_i) \neq G$ for each integer $1 \leq i \leq s$. By Lagrange's Theorem, we have that $[G : Z_G(g_i)]$ divides $|G| = p^n$, hence we have that $[G : Z_G(g_i)] = p^m$ for some integer $1 \leq m \leq n$. Considering that $|N| = p$, if this were possible, we would have a contradiction. We conclude that each term in the class equation has size one so that $N \leq Z(G)$. □

Q1, August 2015. Given a group G, denote the center of G by $Z(G)$, and note that the center of G is a normal subgroup of G. Construct subgroups $Z_i(G)$ inductively as follows.

1.) Begin with $Z_0(G) = \{e_G\}$.

2.) For each integer $i \geq 0$, let $Z_{i+1}(G)$ be the subgroup of G that is the pre-image of the center of the group $G/Z_i(G)$ so that $Z_{i+1}(G)/Z_i(G)$ is the center of $G/Z_i(G)$.

We note that G is nilpotent if $Z_n(G) = G$ for some integer $n \geq 1$.

(a.) Prove that $Z_i(G)$ is a normal subgroup of G for each i.

(b.) Prove that if $|G| = p^r$ with p prime, then G is nilpotent.

Proof. (a.) Consider the action of G on $G/Z_i(G)$ by conjugation with kernel K. We have that

$$\begin{aligned} K &= \{g \in G \mid g \cdot hZ_i(G) = hZ_i(G) \text{ for every coset } hZ_i(G)\} \\ &= \{g \in G \mid g(hZ_i(G))g^{-1} = hZ_i(G) \text{ for every coset } hZ_i(G)\} \\ &= \{g \in G \mid g(hZ_i(G)) = (hZ_i(G))g \text{ for every coset } hZ_i(G)\} \\ &= \text{ pre-image of the center of the group } G/Z_i(G) = Z_{i+1}(G). \end{aligned}$$

Considering that the kernel of a group action is always a normal subgroup, we conclude that $Z_i(G)$ is a normal subgroup of G for each $i \geq 1$. Certainly, $Z_0(G) = \{e_G\}$ is also a normal subgroup. □

Proof. (b.) Given that $|G| = p^r$ with p prime, the order of each subgroup $Z_i(G)$ of G is p^{k_i} for some positive integer $0 \leq k_i \leq r$ so that the order of $G/Z_i(G)$ is p^{r-k_i}. Considering that $Z_i(G) \subseteq Z_{i+1}(G)$, we have that $p^{k_i} \leq p^{k_{i+1}}$. Given that $p^{k_i} = p^{k_{i+1}}$ for any integer $i \geq 0$, we have that $Z_i(G) = Z_{i+1}(G)$ so that $Z_{i+1}(G)/Z_i(G)$ is trivial. By the Class Equation, a nontrivial group of prime power order cannot have a trivial center. Considering that $G/Z_i(G)$ has order p^{r-k_i}, we must have that $r - k_i = 0$ so that $Z_i(G) = G$. Consequently, we may assume that p^{k_i} is a strictly increasing sequence, hence the sequence p^{r-k_i} is a strictly decreasing, from which it follows that $p^{r-k_n} = 0$ for some integer $n \gg 0$. Either way, we conclude that $Z_n(G) = G$ for some integer $n \geq 0$, so G is nilpotent. □