CONJUGATES

Discussion: We've already introduced the definition of the conjugate of *x* by *a* as being the product $x^a = a^{-1}xa$. However, many group theorists prefer to define the conjugate slightly differently as $x^a = axa^{-1}$, and so below we'll switch to that definition so that you can be more familiar with it. Remember, though, that in the long run, it really doesn't make any difference which definition you use because if $a \in G$, then $a^{-1} \in G$ also, and both conjugates, axa^{-1} and $a^{-1}xa$, will reside in *G*. Additionally, another change in notation we will make is that we will use the symbol "$\sim$" instead of "$\equiv$" to denote an equivalence relation. Again, both symbols have been used for this purpose, and it's good to be familiar with several different notations for a particular concept. For the same reason, we will also work with left cosets instead of right cosets. And with that said, let's explore conjugates in greater depth!

Definition: Let *G* be a group and let $x, a \in G$. Then the conjugate of *x* by *a* is axa^{-1}.
$x, a \in G$

Theorem: Let *G* be a group. Then conjugacy of elements in *G* is an equivalence relation.

Proof: Let $x \sim y$ mean that *x* is conjugate to *y*. In other words, $x \sim y$ implies that there exists $a \in G$ such that $axa^{-1} = y$. Then to show that conjugacy of elements in *G* is an equivalence relation we have to show that it is reflexive, symmetric, and transitive.

1. (reflexive): Let $x \in G$ and let *e* be the identity element in *G*. Then the conjugate of *x* by *e* is $exe^{-1} = exe = xe = x$. Therefore, $x \sim x$, and $\sim$ is reflexive.

2. (symmetric): Let $x, y \in G$ such that *x* is conjugate to *y*. Then there exists $a \in G$ such that $axa^{-1} = y$. Hence, the conjugate of *y* by a^{-1} is
$a^{-1}ya = a^{-1}(axa^{-1})a = (a^{-1}a)x(a^{-1}a) = exe = x$. Therefore, if $x \sim y$, then $y \sim x$ and, thus, $\sim$ is symmetric.

3. (transitive): Suppose $x \sim y$ and $y \sim z$ for some $x, y, z \in G$. Then there exists $a, b \in G$ such that $axa^{-1} = y$ and $byb^{-1} = z$. Hence,
$z = byb^{-1} == b(axa^{-1})b^{-1} = (ba)x(a^{-1}b^{-1}) = (ba)x(ba)^{-1}$ which implies that $x \sim z$ and, thus, $\sim$ is transtive.

Therefore, it now follows that conjugacy is an equivalence relation on *G*.

□

A consequence of conjugacy defining an equivalence relation on *G* is that *G* can be partitioned into a collection of disjoint subsets whose union is *G*, and the elements in

each subset will be conjugate to one another. Also, notice that the different conjugacy classes need not be the same size. For example, the conjugacy class of the identity is just the identity since for each $a \in G$ we always have that $aea^{-1} = aa^{-1} = e$. However, it is reasonable to expect that other conjugacy classes will often consist of more than one element, and the following theorem shows that this will always be the case if *G* is nonabelian.

Theorem: *G* is abelian if and only if every conjugacy class in *G* contains just one element.

Proof: Suppose *G* is ableian and let $x, a \in G$. Then $axa^{-1} = aa^{-1}x = ex = x$. Thus, the conjugacy class of *x* contains just one element. Now suppose that $x, y \in G$ and that the conjugacy class of *x* contains just one element. Then we know this element must be *x* since $exe^{-1} = x$. Hence, it follows that the conjugate of *x* by any $y \in G$ also equals *x*. But $yxy^{-1} = x \Rightarrow (yxy^{-1})y = xy \Rightarrow yx(y^{-1}y) = xy \Rightarrow yxe = xy \Rightarrow yx = xy$. Therefore, *G* is ableian.

□

Corollary: The above theorem is logically equivalent to saying that *G* is nonabelian if and only if there exists a conjugacy class in *G* that contains more than just one element.

Definition: Let $a \in G$, a group. Then the centralizer of *a* in *G*, denoted by $C_G(a)$, is the set of all elements in *G* that commute with *a*. Notice that $C_G(a)$ is never empty since $e \in C_G(a)$

Theorem: $C_G(a)$ is a subgroup of *G*.

Proof: To show that $C_G(a)$ is a subgroup of *G*, we need to show that for every $x \in C_G(a)$ that $x^{-1} \in C_G(a)$, and we need to show that for every $x, y \in C_G(a)$ that $xy \in C_G(a)$.

We'll first establish the existence of inverses. Thus, suppose $x \in C_G(a)$. Then $xa = ax \Rightarrow a = x^{-1}ax \Rightarrow ax^{-1} = x^{-1}a \Rightarrow x^{-1} \in C_G(a)$.

Now we'll show closure under multiplication. Thus, suppose $x, y \in C_G(a)$. Then $xy(a) = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$. Thus, $xy \in C_G(a)$, and, therefore, $C_G(a)$ is a subgroup of *G*.

□

Theorem: If $C_G(a)$ is the centralizer of *a* in a group *G*, then $xax^{-1} = yay^{-1}$ for $x, y \in G$ if and only if *x* and *y* belong to the same left coset of $C_G(a)$ in *G*.

Proof: Suppose *x* and *y* belong to the same left coset of $C_G(a)$ in *G*. Then $x = yh$ for some $h \in C_G(a)$. Recall, also, that since $h \in C_G(a)$, then, by definition, *h* commutes with *a*. Hence, $xax^{-1} = (yh)a(yh)^{-1} = y(ha)(h^{-1}y^{-1}) = ya(hh^{-1})y^{-1} = yaey^{-1} = yay^{-1}$.

Now suppose that $xax^{-1} = yay^{-1}$. Then
$xax^{-1} = yay^{-1} \Rightarrow (y^{-1}x)ax^{-1} = ay^{-1} \Rightarrow (y^{-1}x)a = a(y^{-1}x) \Rightarrow y^{-1}x \in C_G(a)$ which means that there exists $h \in C_G(a)$ such that $y^{-1}x = h$. Hence, $yh = y(y^{-1}x) = (yy^{-1})x = ex = x$, $h \in C_G(a)$, which implies that *x* and *y* belong to the same left coset of $C_G(a)$ in *G*.

□

Corollary: If $C_G(a)$ is the centralizer of *a* in a finite group *G*, then the number of distinct conjugates of *a* in *G* is the same as the number of left cosets of $C_G(a)$ in *G*, and by Lagrange's Theorem, this number is $\left[G : C_G(a)\right] = \dfrac{|G|}{|C_G(a)|}$.

If we now put two and two together, then we note that (1) conjugacy is an equivalence relation on *G*, and (2) the number of elements in a conjugacy class containing *a* is $\left[G : C_G(a)\right] = \dfrac{|G|}{|C_G(a)|}$. From this it follows that

$|G| =$ the sum of the number of elements in each distinct conjugacy class of $G = \sum_a \dfrac{|G|}{|C_G(a)|}$

where for each distinct conjugacy class, *a* represents a single element from that class.

Theorem: Let *G* be a group and let $a \in G$. Then $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$ is a bijection.

Proof: We need to show that $f_a : G \to G$ is one-to-one and onto. Thus, suppose $x, y \in G$ such that $f_a(x) = f_a(y)$. Then
$axa^{-1} = aya^{-1} \Rightarrow a^{-1}(axa^{-1})a = a^{-1}(aya^{-1})a \Rightarrow (a^{-1}a)x(a^{-1}a) = (a^{-1}a)y(a^{-1}a) \Rightarrow exe = eye$
$\Rightarrow x = y$. Hence, $f_a : G \to G$ is one-to-one.

To show that $f_a : G \to G$ is onto, let $x \in G$. Then $a^{-1}xa \in G$ and
$f_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = (aa^{-1})x(aa^{-1}) = exe = x$. Therefore, $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$ is a bijection.

□

Theorem: Let G be a group, H a subgroup of G, and let $a \in G$. Then aHa^{-1} is a subgroup of G where $aHa^{-1} = \{aha^{-1} \mid h \in H\}$.

Proof: We need to show that aHa^{-1} is closed under multiplication and that every element in aHa^{-1} has an inverse.

Thus, suppose $axa^{-1}, aya^{-1} \in aHa^{-1}$ where $x, y \in H$. Then $(axa^{-1})(aya^{-1}) = ax(a^{-1}a)ya^{-1} = ax(e)ya^{-1} = a(xy)a^{-1} \in aHa^{-1}$ since $xy \in H$. Hence, aHa^{-1} is closed under multiplication.

Now let $axa^{-1} \in aHa^{-1}$ where $x \in H$. Then $ax^{-1}a^{-1} \in aHa^{-1}$ since $x^{-1} \in H$, and $(axa^{-1})(ax^{-1}a^{-1}) = ax(a^{-1}a)x^{-1}a^{-1} = ax(e)x^{-1}a^{-1} = a(xx^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Thus, inverses exist in aHa^{-1}, and, therefore, aHa^{-1} is a subgroup of G.

□

Theorem: Let G be a group, let H_1 and H_2 be subgroups of G, and define a relation $\sim$ by $H_1 \sim H_2$ if and only if there exists $a \in G$ such that $H_2 = aH_1a^{-1}$. Then $\sim$ is an equivalence relation.

Proof: As usual, we need to show that $\sim$ is reflexive, symmetric, and transitive.

1. (reflexive): If H is a subgroup of G, then since $H = eHe^{-1} = eHe$, $H \sim H$ and, hence, $\sim$ is reflexive.

2. (symmetric): If H_1 and H_2 are subgroups of G with $H_1 \sim H_2$, then there exists $a \in G$ such that $H_2 = aH_1a^{-1}$. Consequently, it follows that $H_1 = a^{-1}H_2a$ and $H_2 \sim H_1$. Thus, $\sim$ is symmetric.

3. (transitive): Suppose $H_1, H_2,$ and H_3 are subgroups of G with $H_1 \sim H_2$ and $H_2 \sim H_3$. Then there exist $a, b \in G$ such that $aH_1a^{-1} = H_2$ and $bH_2b^{-1} = H_3$. Hence, $H_3 = bH\ b^{-1} = b(aH_1a^{-1})b^{-1} = (ba)H_1(a^{-1}b^{-1}) = (ba)H_1(ba)^{-1}$ implies that $H_1 \sim H_3$. Therefore, $\sim$ is transitive, and, hence, $\sim$ is an equivalence relation.

□

Theorem: If G is a group, H_1 and H_2 are subgroups of G, and $a \in G$ such that $aH_1a^{-1} = H_2$, then $|H_1| = |H_2|$.

Proof: It suffices to show that $f_a : H_1 \to H_2$ defined by $f_a(x) = axa^{-1}$ is one-to-one and onto. However, we already know that this function is onto since we are given that

$aH_1a^{-1} = H_2$. Hence, we need only show that this function is one-to-one. But that is easy since if $x, y \in H_1$ and $f_a(x) = f_a(y)$, then
$axa^{-1} = aya^{-1} \Rightarrow a^{-1}(axa^{-1})a = a^{-1}(aya^{-1})a \Rightarrow (a^{-1}a)x(a^{-1}a) = (a^{-1}a)y(a^{-1}a) \Rightarrow exe = eye$
$\Rightarrow x = y$. Hence, $f_a : H_1 \to H_2$ is also one-to-one. Therefore, since $f_a : H_1 \to H_2$ is a bijection, it follows that $|H_1| = |H_2|$.

□

Definition: The center of a group *G*, denoted by $Z(G)$, is the set of all elements in *G* that commute with every other element in *G*.

Earlier we noted that

$|G| =$ the sum of the number of elements in each distinct conjugacy class of $G = \sum_a \frac{|G|}{|C_G(a)|}$.

Since each element in $Z(G)$, the center of *G*, creates a conjugacy class with only one element (itself) in it, we can rewrite the equation $|G| = \sum_a \frac{|G|}{|C_G(a)|}$ as follows, and we usually call this the class equation:

The Class Equation: The order of a group *G* is $|G| = |Z(G)| + \sum_b \frac{|G|}{|C_G(b)|}$ where $b \notin Z(G)$ and in our summation only a single value *b* is chosen from each distinct conjugacy class that contains more than one element.

Theorem: If $|G| = p^n$, *p* a prime, then $|Z(G)| > 1$.

Proof: Let $z = |Z(G)|$. Then $z \geq 1$ since $e \in Z(G)$. Also, if $Z(G) \neq G$, then there exists $b \in G$ such that $b \notin Z(G)$. Furthermore, the centralizer of *b* in *G*, $C_G(b)$, is a proper subgroup of *G* since, otherwise, if we had $C_G(b) = G$, then everything in *G* would commute with *b*, and *b* would be an element of $Z(G)$. Thus, it also follows that $|C_G(b)| < |G|$, and by Lagrange's Theorem, $|C_G(b)|$ divides $|G|$. Since $|G| = p^n$, it now follows that $|C_G(b)| = p^m$ where $1 \leq m < n$. In particular, we'll denote the power *m* that corresponds to the order of $C_G(b)$ by m_b. The rest now follows easily from the Class Equation. By this equation, $|G| = p^n = |Z(G)| + \sum_b \frac{|G|}{|C_G(b)|}$ where $b \notin Z(G)$ and we choose only one *b* from each of the remaining conjugacy classes. The class equation can clearly

be rewritten as $|G| - \sum_b \frac{|G|}{|C_G(b)|} = |Z(G)|$ which now implies that $p^n - \sum_b \frac{p^n}{p^{m_b}} = |Z(G)|$. Also, since for each term in our summation, $m_b < n$, it follows that *p* can be factored out of each term on the left-hand side of the equation to give us $p\left[p^{n-1} - \sum_b \frac{p^{n-1}}{p^{m_b}} \right] = |Z(G)|$. Since *p* divides the left-hand side of this equation, it must also divide the right-hand side, and, thus, $|Z(G)| > 1$. In particular, $|Z(G)|$ is at least *p*.

□

Theorem: If *G* is a group such that $|G| = p^2$ where *p* is a prime, then *G* is abelian.

Proof: By our previous theorem, it follows that $|Z(G)| > 1$. Hence, by Lagrange's Theorem, either $|Z(G)| = p$ or $|Z(G)| = p^2$. If $|Z(G)| = p^2$, then $Z(G) = G$ which implies that *G* is abelian and we are done. Thus, suppose $|Z(G)| = p$. Then $Z(G)$ is cyclic, and, thus, $Z(G) = \langle a \rangle$ for some $a \in Z(G)$ with $a \neq e$. Now consider $x \in G$ such that $x \notin Z(G)$. Then clearly $Z(G) \subseteq C_G(x)$, the set of all elements of *G* that commute with *x*. However, since $x \in C_G(x)$ and $x \notin Z(G)$, it follows that $|Z(G)| < |C_G(x)|$. But his means that $|C_G(x)| = p^2$, and, hence, $C_G(x) = G$. But this now implies that everything in *G* commutes with *x*, and, thus, $x \in Z(G)$. This, in turn, contradicts our previous assumption that there exists an $x \in G$ such that $x \notin Z(G)$. Therefore, that assumption was wrong, and $Z(G) = G$ which implies that *G* is abelian.

□

Theorem: Suppose *G* is abelian and $|G| = p^n m$ where *p* is prime and *p* & *m* are relatively prime. Then *G* has a subgroup of order *p*.

Proof: If *G* has an element *x* such that the order of the cyclic subgroup generated by *x* is p^k, (i.e. $|\langle x \rangle| = p^k$), then $x^{\frac{p^k}{p}} = x^{p^{k-1}}$ generates a subgroup of this cyclic group generated by *x* such that this subgroup has order *p*, ($\left|\left\langle x^{p^{k-1}} \right\rangle\right| = p$), where $(x^{p^{k-1}})^p = x^{p^{k-1} \cdot p} = x^{p^k} = e$, and we are done.

Similarly, if *G* has an element *x* such that $|\langle x \rangle| = p^k q$ where $q > 1$. *q* divides *m*, and *p* & *q* are relatively prime, then $x^{\frac{p^k q}{p}} = x^{p^{k-1} q}$ generates a subgroup of $\langle x \rangle$ of order *p* since $(x^{p^{k-1} q})^p = x^{p^{k-1} q \cdot p} = x^{p^k q} = e$, and again, we are done.

Thus, suppose that for every non-trivial element x_i of G we have that $|\langle x\rangle| = q_i$ where, regardless of the value of i, $q_i > 1$, q_i divides m, and p & q_i are relatively prime. Thus, let $x_1 \in G$ such that $|\langle x_1\rangle| = q_1$. Also, let $N_1 = \langle x_1\rangle$. Then N_1 is a normal subgroup of G since G is abelian, and $|G/N_1| = |G|/|N_1| = p^n \cdot \frac{m}{q_1}$. Now let $x_2 \in G$ where $|\langle x_2\rangle| = q_2$, q_2 divides m, and p & q_2 are relatively prime. Also, let $N_2 = \langle x_2\rangle$. Then by our isomorphism theorems, $\frac{N_2}{N_2 \cap N_1} \cong \frac{N_2 N_1}{N_1}$. Now let

$r_2 = \frac{q_2}{|N_2 \cap N_1|} = \frac{|N_2|}{|N_2 \cap N_1|} = \left|\frac{N_2}{N_2 \cap N_1}\right| = \left|\frac{N_2 N_1}{N_1}\right| = \frac{|N_2 N_1|}{|N_1|} = \frac{|N_2 N_1|}{q_1}$. This string of equalities tells us two things. First, since $r_2 = \frac{q_2}{|N_2 \cap N_1|}$, r_2 divides q_2, and thus, r_2 and p are relatively prime. Additionally, $r_2 q_1 = |N_2 N_1|$, and hence, $r_2 q_1$ divides $|G|$ and $r_2 q_1$ and p are relatively prime. Consequently, $r_2 q_1$ divides m, and $\left|\frac{G}{N_2 N_1}\right| = \frac{|G|}{|N_2 N_1|} = \frac{p^n m}{r_2 q_1} = p^n \cdot \frac{m}{r_2 q_1}$. Now let $N_3 = \langle x_3\rangle$ where $|N_3| = |\langle x_3\rangle| = q_3$, q_3 divides m, and p & q_3 are relatively prime. Then $\frac{N_3}{N_3 \cap N_2 N_1} \cong \frac{N_3 N_2 N_1}{N_2 N_1}$. Additionally, let

$s_3 = \frac{q_3}{|N_3 \cap N_2 N_1|} = \frac{|N_3|}{|N_3 \cap N_2 N_1|} = \left|\frac{N_3}{N_3 \cap N_2 N_1}\right| = \left|\frac{N_3 N_2 N_1}{N_2 N_1}\right| = \frac{|N_3 N_2 N_1|}{|N_2 N_1|} = \frac{|N_3 N_2 N_1|}{r_2 q_1}$. Then s_3 divides q_3 which means that p and s_3 are relatively prime. Furthermore, $s_3 r_2 q_1 = |N_3 N_2 N_1|$ tells us that $s_3 r_2 q_1$ divides $|G| = p^n m$, but since p is relatively prime to the product $s_3 r_2 q_1$, it follows that $s_3 r_2 q_1$ divides m. Hence, $\left|\frac{G}{N_3 N_2 N_1}\right| = \frac{|G|}{|N_3 N_2 N_1|} = \frac{p^n m}{s_3 r_2 q_1} = p^n \cdot \frac{m}{s_3 r_2 q_1}$. Now, on the one hand, we can continue this process of taking the elements x_i and forming quotient groups $\frac{G}{N_1 N_2 N_3 \ldots N_i}$, showing that their order is $p^n \cdot \frac{m}{q_1 r_2 s_3 \ldots z_i}$ where $q_1 r_2 s_3 \ldots z_i$ divides m and is relatively prime to p. However, we eventually we will get to the point where we have factored everything out and are left with only the trivial group of order 1. But on the other hand when we get to the last x_k, this process also yields a quotient group of order $p^n \cdot \frac{m}{q_1 r_2 s_3 \ldots z_k} \geq p^n > 1$. And this is a contradiction. Thus, there must exist a non-trivial element x of G such that the order of $|\langle x\rangle|$ is either p^k or $p^k q$, and we have shown above how each of these cases allows us to find an element of order p.

□

Theorem: If G is a group such that $|G| = p^n$ where p is a prime, then G contains a normal subgroup of order p^{n-1}.

Proof: We prove this theorem by applying mathematical induction to the power n. Thus, suppose $|G| = p^1 = p$. Then $p^{1-1} = p^0 = 1$, and $\{e\}$ is a normal subgroup of order 1.

Now suppose that our theorem is true for all n such that $1 \le n \le k$, and we'll prove that our theorem is also true for $n = k+1$. Hence, suppose that $|G| = p^{k+1}$. Then by previous proof, there exists $a \in Z(G)$ such that $a \ne e$. Furthermore, since $|G| = p^{k+1}$, it follows that $|\langle a \rangle| = p^m$ for $1 \le m \le k+1$. Hence, consider $a^{\frac{p^m}{p}}$. Clearly, $(a^{\frac{p^m}{p}})^p = a^{p^m} = e \Rightarrow |< a^{\frac{p^m}{p}} >| = p$, and $< a^{\frac{p^m}{p}} > \lhd G$. Let $b = a^{\frac{p^m}{p}} = a^{p^{m-1}}$, let $H = \langle b \rangle$, and consider G/H where $|G/H| = |G|/|H| = \frac{p^{k+1}}{p} = p^k$. By our induction hypothesis, G/H has a normal subgroup of the form N/H of order p^{k-1}. However, this means that $N \lhd G$ and $p^{k-1} = |N/H| = |N|/|H| = \frac{|N|}{p}$. Thus, $|N| = p^{k-1}p = p^k$, and the theorem is proved by mathematical induction.

□

Cauchy's Theorem: If G is a finite group and p is a prime such that p divides $n = |G|$, then G has cyclic subgroup of order p.

Proof: Let p be a prime, and we'll proceed by induction on n, the order of the group. In this case, the smallest possible value for $|G|$ such that p divides $|G|$ is p itself. But in this case, every nontrivial element of G generates a cyclic subgroup of order p. Thus, let's assume that $|G| = n > p$, where p divides n, and by way of induction we'll also assume that if G has a subgroup H of any order $m < n$ such that p divides m, then G has a cyclic subgroup of order p. We'll now extend this result to the case $m = n$.

If G is abelian, then the result has already been established by previous proof. Thus, assume that G is not abelian and let $x \in G$ such that $x \notin Z(G)$, the center of G. Note that if there were no elements in G that did not belong to the center, then G would be abelian. Also, let $C_G(x)$ be the centralizer of x, the set of all elements of G that commute with x. Then $|C_G(x)| < |G|$ since, otherwise, we would have $C_G(x) = G$ which would mean that every element in G would commute with x, and, hence, x would belong to $Z(G)$. Thus, $|C_G(x)| < |G|$, and if p divides $|C_G(x)|$, then our induction hypothesis tells us that $C_G(x)$

has a cyclic subgroup of order *p*, and we're done. Thus, assume that *p* doesn't divide $|C_G(x)|$.

If *p* divides $|G|$ but *p* does not divide $|C_G(x)|$, then clearly *p* must divide $\frac{|G|}{|C_G(x)|}$. Now consider the class equation $|G| = |Z(G)| + \sum_x \frac{|G|}{|C_G(x)|}$ where $x \notin Z(G)$ and we pick just one *x* from each conjugacy class that doesn't contain elements of the center, $Z(G)$. If we rewrite this equation as $|G| - \sum_x \frac{|G|}{|C_G(x)|} = |Z(G)|$, then *p* divides the left-hand side of this equation, and so it must divide $|Z(G)|$ as well. But since $Z(G)$ is abelian, a previous proof guarantees that $Z(G)$ has a cyclic subgroup of order *p*, and this subgroup is a subgroup of *G* as well. Therefore, *G* has a cyclic subgroup of order *p*, and the theorem is proved by mathematical induction.

□

Corollary: If *G* is a finite group such that $|G| = p^n$, then $Z(G)$ contains an element that is not the identity.

Proof: Using the class equation again, we have $|G| = |Z(G)| + \sum_x \frac{|G|}{|C_G(x)|}$ where $x \notin Z(G)$ and we pick just one *x* from each conjugacy class that doesn't contain elements of the center, $Z(G)$. Thus, as in our theorem above, $|C_G(x)| < |G|$ and since every subgroup of *G* has order a power of *p*, it follows that $\frac{|G|}{|C_G(x)|}$ is divisible by *p*. Hence, *p* divides the left-hand side of the equation $|G| - \sum_x \frac{|G|}{|C_G(x)|} = |Z(G)|$, and, thus, it also divides the right-hand side. Therefore, $|Z(G)| > 1$, and $Z(G)$ contains an element that is not the identity.

□