Proofs from Group Theory

December 8, 2009

Let G be a group such that $a, b \in G$. Prove that $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof [We need to show that $(a * b) * (b^{-1} * a^{-1}) = e$.] By the associative property of groups, $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$. By definition of identity element, we obtain $a * a^{-1}$. Again, by property of identity, we obtain e as desired. ■

Cancellation Law: Let G be a group such that $a, b, c \in G$. If $a*c = b*c$, then $a = b$.

Proof Suppose $a * c = b * c$. Since $c \in G$, it follows that an element d exists such that $c * d = e$. Now, if we multiply both sides by d on the right, we obtain $(a * c) * d = (b * c) * d$. By associativity, we obtain $a * (c * d) = b * (c * d)$. Since $c * d = e$, we obtain $a * e = b * e$, and by definition of identity element, we obtain $a = b$ as desired. ■

Let G be a group. Then G has a unique identity element e.

Proof Suppose that there exist two identity elements, d and e. Let $a \in G$. Since d is an identity element, then $a * d = a = d * a$. Likewise, $a * e = a = e * a$. Now, this implies that $d = d * e = e$. Hence, $e = d$, proving that there can only be one identity element. ■

Let G be a group, and let $a \in G$. Then a has a unique inverse.

Proof Suppose that there exist two elements, b and c, which serve as inverses to a. Since b is an inverse to a, then $a * b = e = b * a$. Likewise, $a * c = e = c * a$. Now, since $e = b * a$ and $e = c * a$, it follows that $b * a = c * a$. By the Cancellation Law, it follows that $b = c$. Thus, there can only be one inverse of a. ■

Let G be a group. If $g \in G$ and $g^2 = g$, then $g = e$.

Proof Suppose that $g^2 = e$. By laws of exponents, this implies that $g * g = g$. Now, if we multiply both sides by g^{-1} on the left, we obtain $g^{-1} * g * g = g^{-1} * g$. By associativity, we obtain $(g^{-1} * g) * g = g^{-1} * g$. By the identity, we obtain $e * g = e$, implying that $g = e$ as desired. ■

Let G be a group. If $x \in G$ and $x^2 = e$, then G is abelian.

Proof Let $a, b \in G$. Then we may assume that $a^2 = e$ and $b^2 = e$. Now, $(a * b)^2 = (a * b) * (a * b)$. By associativity, we obtain $a * b * a * b$. The equality $a * b * a * b = e$ can be implied by our assumption. If we multiply by a on the left and b on the right on both sides of the equality, we obtain $a * a * b * a * b * b = a * e * b \iff a^2 * b * a * b^2 = ab \iff b * a = a * b$. Hence, G is abelian. ■

Prove that any cyclic group is abelian.

Proof Let G be a cyclic group with a generator c. Let $a, b \in G$. Then $a = c^j$ and $b = c^k$ for some integers j and k. Hence, $a * b = c^j * c^k$. By laws of exponents and commutativity of addition, we obtain $c^{j+k} = c^{k+j} = c^k * c^j = b * a$. This implies that $a * b = b * a$, so G is abelian. ■

Let G be a group such that $a * b * c = e$ for all $a, b, c \in G$. Prove that $b * c * a = e$ as well.

Proof Suppose that $a * b * c = e$. If we multiply by a^{-1} on the left and a on the right, then we obtain $a^{-1} * (a * b * c) * a = a^{-1} * e * a$. By associativity and definition of the identity element, we obtain $(a^{-1} * a) * b * c * a = e \Longleftrightarrow e * b * c * a = e \Longleftrightarrow b * c * a = e$. ■

Let G be a group such that $a \in G$. Define a function $f_a : G \to G$ where $f_a(x) = a * x$. Prove that f_a is bijective.

Proof

> Let $x, y \in G$. [We need to show that $f_a(x) = f_a(y)$ implies the equality $x = y$.] Suppose $f_a(x) = f_a(y)$. It follows that $a * x = a * y$. By the Cancellation Law, we can cancel the a to obtain $x = y$, thus showing that f_a is one-to-one.
>
> Now, let $z \in G$. [We need to show that $f_a(x) = z$ for some $x \in G$.} Suppose $f_a(x) = z$ for some $x \in G$. It follows that $a * x = z$. By multiplying both sides by a^{-1}, we obtain $x = z * a^{-1}$. Now, since $a \in G$, then $a^{-1} \in G$ by the existence of an inverse. Also, by closure, since $z \in G$ and $a^{-1} \in G$, then $z * a^{-1} \in G$. Hence, we have found an $x \in G$ such that $f_a(x) = z$, and this proves that f_a is onto.

Therefore, we have proven that f_a is bijective as desired. ■

Let G be a group and let H and K be subgroups of G. Prove that $H \cap K$ is also a subgroup.

Proof Since H and K are subgroups, then $e \in H$ and $e \in K$, implying that $e \in H \cap K$. Now, let $a, b \in H \cap K$. This implies that $a, b \in H$, and since H is a subgroup, then $a * b \in H$ and $a^{-1} \in H$. Likewise, $a, b \in K$, and since K is a subgroup, then $a * b \in K$ and $a^{-1} \in K$. It follows then that $a * b \in H \cap K$ and $a^{-1} \in H \cap K$. Hence, $H \cap K$ is a subgroup of G. ■

Theorem: Let G be a group and let a and b be elements of the group. If G is abelian, then $(a * b)^n = a^n * b^n$ for any integer $n \geq 2$.

Proof (by induction):

Base Step: Let $n = 2$. Then $(a * b)^2 = (a * b) * (a * b) = a * b * a * b$. Since G is abelian, we obtain $a * b * b * a = a * b^2 * a = a * a * b^2 = a^2 * b^2$. Since P_2 is true, then we may assume that P_n is true. Hence, we may form the inductive hypothesis that $(a * b)^n = a^n * b^n$ for any integer $n \geq 2$.

Induction Step: [We must prove that $(a * b)^{n+1} = a^{n+1} * b^{n+1}$.]

Now we will substitute $n + 1$ for n. By commutativity, associativity, and the laws of exponents, $(a * b)^{n+1} = (a * b)^n * (a * b) = (a * b)^n * b * a$. By our inductive hypothesis, we obtain $a^n * b^n * b * a = a^n * b^{n+1} * a = a * a^n * b^{n+1} = a^{n+1} * b^{n+1}$, thus proving the P_{n+1} assertion true. By the Principle of Mathematical Induction, it follows that P_n is true, so we have shown that $(a * b)^n = a^n * b^n$ if G is abelian. ■

Let G be a group. The set $Z(G) = \{x \in G | xg = gx \text{ for all } g \in G\}$ of all elements that commute with every other element of G is called the *center* of G. Prove that $Z(G)$ is a subgroup of G.

Proof The identity element is a trivial member of the subgroup, so $Z(G)$ is non-empty. Now we must show that $Z(G)$ is closed and has an inverse. To see that the group is closed, let $z_1, z_2 \in Z(G)$ and $g \in G$. [We must prove that $(z_1 z_2)x = x(z_1 z_2)$.] By associativity and the definition of center, $(z_1 z_2)x = z_1(z_2 x) =$

$z_1(xz_2) = (z_1x)z_2 = (xz_1)z_2 = x(z_1z_2)$, so $z_1z_2 \in Z(G)$. Now, $z_1x = xz_1$ implies that $z_1^{-1}x = xz_1^{-1}$, so $z_1^{-1} \in Z(G)$. So we have shown that $Z(G)$ has an identity element, is closed under binary operations, and has the inverse element. Hence, $Z(G)$ is a subgroup of G. ■

Let G be a group. The set $C(a) = \{x \in G | xa = ax\}$ of all elements that commute with a is called the *centralizer* of a. Prove that $C(a)$ is a subgroup of G.

Proof The subgroup is not empty, as $a \in G$. The identity element is a trivial member of the subgroup, so all we really have to show is that $C(a)$ is closed and has an inverse. To see that the group is closed, let $x, y \in G$ so that $xa = ax$ and $ya = ay$. [We must prove that $(xy)a = a(xy)$.] By associativity and the definition of centralizer, $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, so $xy \in C(a)$. Now, $xa = ax$ implies that $x^{-1}a = ax^{-1}$, so $x^{-1} \in C(a)$. So we have shown that $C(a)$ has an identity element, is closed under binary operations, and has the inverse element. Hence, $C(a)$ is a subgroup of G. ■

Let G be an abelian group, and let $H = \{a \in G | a^5 = e\}$. Prove that H is a subgroup of G.

Proof The identity element is trivially a member of H since $e^5 = e$, making H a nonempty set. To show closure, let $a, b \in H$ so that $a^5 = e$ and $b^5 = e$. Since G is abelian, we have that $(a * b)^5 = a^5 * b^5 = e * e = e$, so $a * b \in H$. The inverse element is in H since $(a^{-1})^5 = a^{-5} = (a^5)^{-1} = e^{-1} = e$. So we have shown that H has an identity element, is closed under binary operations, and has the inverse element. Hence, H is a subgroup of G. ■

Theorem: Every subgroup of a cyclic group is cyclic.

Proof Let G be a cyclic group with generator a and let H be a subgroup of G. Let m be the smallest positive integer so that $a^m \in H$. Since G is cyclic, then every element of H has the form a^k for some integer k. By the quotient-remainder theorem, $k = mq + r$ for some $q, r \in \mathbb{Z}$ such that $0 \leq r < m$. It follows that $a^k = a^{mq+r} = (a^m)^q a^r$. Now, we can manipulate the equality to obtain $a^r = (a^m)^{-q} a^k$. Since a^m and a^k are in H, then $a^r \in H$. Since $r < m$, then $r = 0$ since a^m is the smallest positive power of a in H. Therefore, $k = mq$ and every element of H is of the form $(a^m)^q$, implying that $H = \langle a^m \rangle$ and H is cyclic. ■

Let G and H be two abelian groups. Prove that $G \times H$ is abelian.

Proof Let (g_1, h_1) and (g_2, h_2) be two elements of the group $G \times H$. Then $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$. Since G and H are abelian, then we obtain $(g_2g_1, h_2h_1) = (g_2, h_2)(g_1, h_1)$. Hence, $(g_1, h_1)(g_2, h_2) = (g_2, h_2)(g_1, h_1)$, proving that $G \times H$ is abelian. ■

A group K is considered *idempotent* if $a^2 = e$ for all $a \in K$. Prove that if G and H are idempotent, then $G \times H$ is also idempotent.

Proof Let $g \in G$ and $h \in H$ such that $g^2 = e$ and $h^2 = e$. Also, let $(g, h) \in G \times H$. Then $(g, h)^2 = (g, h)(g, h) = (g^2, h^2) = (e, e)$. We have shown that $(g^2, h^2) = (e, e)$, proving that $G \times H$ is idempotent. ■

Lagrange's Theorem: If G is a finite group and H is a subgroup of G, then $|G|$ is divisible by $|H|$.

Let H and K be subgroups of a group G such that $|H| = 5$ and $|K| = 12$. Prove that $H \cap K = \{e\}$, where e is the identity element.

Proof As shown above, $H \cap K$ is a subgroup of G. By inclusion of intersection, we know that $H \cap K \subseteq H$ and $H \cap K \subseteq K$. By Lagrange's Theorem, it follows that $|H|$ and $|K|$ are both divisible by $|H \cap K|$. By substitution, we can say that 5 and 12 are both divisible by $|H \cap K|$. Since 5 and 12 are relatively prime, then $|H \cap K| = 1$, implying that $H \cap K$ only has the identity element e. ■

Theorem: Let G be a finite group. If $a \in G$, then $o(a)$ divides $|G|$.

Proof Let K be a subgroup of G such that $K = \langle a \rangle$. By a previous theorem, $|K| = o(a)$. By Lagrange's Theorem, $|K|$ divides $|G|$, implying that $o(a)$ divides $|G|$. ■

Theorem: Any group of prime order is cyclic.

Proof Let G be a group of prime order p, where p is a prime number. Let a be a non-identity element of G. This implies that the cyclic subgroup $\langle a \rangle$ has an order greater than 1. By Lagrange's Theorem, $|\langle a \rangle|$ divides $|G|$. Now, since $|G|$ is prime, then it is divisible only by 1 and p. Since $|\langle a \rangle| \neq 1$, then $|\langle a \rangle| = p$. Since $|G| = p$, then $G = \langle a \rangle$, so G is cyclic. ■

Theorem: Any group of order 5 or less is abelian.

Proof Any group of order 1 has only the identity element, so it is trivially abelian. By the above theorem, any groups of order 2, 3, or 5 are cyclic. Since it has been proven that cyclic groups are abelian, then it follows that any groups of order 2, 3, or 5 are also abelian. Now, by a previous theorem, if a group has order 4, then for any element a, $o(a) = 2$ or $o(a) = 4$. In order to show that a group of order 4 is abelian, we must consider two cases.

> Case 1: Suppose that G has an element of order 4. Then G is cyclic, implying that G is abelian in this case.
>
> Case 2: Suppose that G does not have an element of order 4. Then $o(a) = 2$ for any element a. We have already proven that a group with this property is abelian. So G is abelian in this case as well.

Hence, any group of order 5 or less is abelian. ■

Prove that an abelian group of order 21 must be cyclic.

Proof By Cauchy's Theorem, there exist elements x and y in the group G such that $o(x) = 3$ and $o(y) = 7$. We need to show that $o(xy) = 21$. By a previous theorem, $o(xy)$ divides $|G|$, implying that the order of xy must be $1, 3, 7$, or 21. Now, if $o(xy) = 1$, then $xy = e$, implying that $x = y^{-1}$, which contradicts our assumption that $x^3 = e = y^7$. Now, if $o(xy) = 3$, then $(xy)^3 = x^3y^3 = e$ and $x^3 = y^{-3}$. Since we assumed that $x^3 = e$, then we would obtain $y^{-3} = e$. It would follows that $y = y^7(y^{-3})^2 = ee = e$, which contradicts our assumption. If we let $o(xy) = 7$, then a similar contradiction would follow. Hence, the order of xy is 21 and G is cyclic. ■