MANIPULATING GROUP ELEMENTS

SECOLINSKY

Statement 1. *Consider* $< G, \cdot >$ *and* $a_1, a_2 \in G$ *. Then* $\left(a_1 = a_1^{-1} \wedge a_2 = a_2^{-1}\right) \Rightarrow (a_1\, a_2)^{-1} = a_2\, a_1$.

Proof. Since a_1, a_2 are their own inverses, we have that $a_1 a_1 a_2 a_2 = a_2 a_1 a_1 a_2 = e$. Thus $(a_1 a_2)^{-1} = a_2 a_1$. □

Statement 2. $(\forall x, y, a_1 \in G)\,(\ a_1^{-1} = x a_1 y \Rightarrow a_1^{-1} = y a_1 x\ )$.

Proof. Since $a_1^{-1} = x a_1 y$, $a_1(x a_1 y) = e$. Also $y^{-1} = a_1 x a_1$. So $y^{-1} y = y y^{-1} = y a_1 x a_1 = e$. Therefore, $a_1^{-1} = y a_1 x$. □

Statement 3. *Consider* $< G, \cdot >$ *and* $a_1, a_2, a_3 \in G$. $[\ (a_1 a_2 a_3)^{-1} = a_1 a_2 a_3\ ] \Rightarrow (a_3 a_1 a_2)^{-1} = a_3 a_1 a_2$ *and* $(a_2 a_3 a_1)^{-1} = a_2 a_3 a_1$.

Proof. Assume $(a_1 a_2 a_3)^{-1} = a_1 a_2 a_3$. We then have that $a_1 a_2 a_3 a_1 a_2 a_3 = a_3 a_1 a_2 a_3 a_1 a_2 = a_2 a_3 a_1 a_2 a_3 a_1$. Therefore, $(a_3 a_1 a_2)^{-1} = a_3 a_1 a_2$ and $(a_2 a_3 a_1)^{-1} = a_2 a_3 a_1$. □

Statement 4. *Consider* $< G, \cdot >$ *and* $a_1, a_2, a_3 \in G$. $[\ a_1 a_2 = a_3,\ a_1 = a_1^{-1},\ a_2 = a_2^{-1},$ *and* $a_3 = a_3^{-1}\ ] \Rightarrow [a_2 a_3 = a_1 \wedge a_3 a_1 = a_2]$.

Proof. Snce $a_1 = a_1^{-1}$, $a_1^{-1}(a_3 a_3^{-1}) = a_1$. Also $a_1 a_2 = a_3$ implies $a_2 = a_1^{-1} a_3$. So $a_2 a_3 = a_1$. Because $a_1 a_2 = a_3$, $a_1 = a_3 a_2^{-1}$. Thus $a_3 a_1 = a_2$. □

Statement 5. *Consider* $< G, \cdot >$ *and* $a_1, a_2 \in G$. $(\forall n \in \mathbb{N})[\ (a_2 a_1 a_2^{-1})^n = a_2 a_1^n a_2^{-1}\ ]$.

Proof. Let $p(n) := [(a_2 a_1 a_2^{-1})^n = a_2 a_1^n a_2^{-1}]$, and $T = \{n \in \mathbb{N} : p(n)\}$. $1 \in T$ since $(a_2 a_1 a_2^{-1})^1 = a_2 a_1^1 a_2^{-1}$. Now assume $p(k)$. Thus $(a_2 a_1 a_2^{-1})^k = a_2 a_1^k a_2^{-1}$. Multiplying both sides by $(a_2 a_1 a_2^{-1})$, we have that $(a_2 a_1 a_2^{-1})^{k+1} = a_2 a_1^{k+1} a_2^{-1}$. Thus $p(k)$ implies $p(k+1)$ and $1 \in T$. This completes the inductive proof. □

Statement 6. *Consider* $< G, \cdot >$ *and* $a_1, a_2 \in G$ *such that* $a_1 a_2 = a_2 a_1$. *Then* $(\forall n \in \mathbb{N})[\ (a_1 a_2)^n = a_1^n a_2^n\ ]$

Proof. Let $p(n) := [\ (a_1 a_2)^n = a_1^n a_2^n\ ]$ and $T = \{n \in \mathbb{N} : p(n)\}$. $1 \in T$ since $(a_1 a_2)^1 = a_1^1 a_2^1$. Assume $p(k)$ so that $(a_1 a_2)^k = a_1^k a_2^k$. Multiplying both sides by $(a_1 a_2)$, $(a_1 a_2)^{k+1} = (a_1^k a_2^k)(a_1 a_2) = a_1^k a_2^k (a_2 a_1) = a_1^{k+1} a_2^{k+1}$. This completes the inductive proof. □

Statement 7. *Consider the group* $< G, \cdot >$ *and let* $a_1 \in G$. *If* $a_1^3 = e$, *then there is an* $a_2 \in G$ *such that* $a_1 = a_2^2$.

Proof. Since $a_1^3 = e$, $a_1 = (a_1^{-1})^2$. Thus $a_2 = a_1^{-1}$. □

Statement 8. *Consider the group* $< G, \cdot >$ *and let* $a_1 \in G$. *If* $a_1^2 = e$, *then there is an* $a_2 \in G$ *such that* $a_1 = a_2^3$.

Proof. Since $a_1^2 = e$, $a_1^2\, a_1^2 = e$. Thus $a_1 = (a_1^{-1})^3$. □

Statement 9. *Let* $a_1, a_2 \in G$. *If* $a_1^2 a_2 a_1 = a_2^{-1}$, *then there's an* $a_3 \in G$ *such that* $a_2 = a_3^3$.

Proof. $a_2^{-1} = a_1^2a_2a_1 = a_1a_1a_2a_1 = a_1(a_2)(a_1^2a_2a_1)a_1a_2a_1 = (a_1a_2a_1)(a_1a_2a_1)(a_1a_2a_1) = (a_1a_2a_1)^3$. Let $a_1a_2a_1 = a_3$. Thus $a_2^{-1} = a_3^3$ and $a_2 = (a_3^{-1})^3$. □

Statement 10. *Let $a_1 \in G$. If a_1^{-1} has a cube root, then a_1 has a cube root.*

Proof. Since a_1^{-1} has a cube root, there is an $a_2 \in G$ such that $a_1^{-1} = a_2^3$. So $a_1a_1^{-1} = a_1a_2^3 = e$ implies that $a_1 = (a_2^{-1})^3$. □

Statement 11. *Let $a_1, a_2 \in G$ such that $a_1a_2a_1 = e$.*
$(\forall n \in \mathbb{N})[\ (a_1a_2)^{2n} = a_2^n\ ]$.

Proof. Let $p(n) := (a_1a_2)^{2n} = a_2^n$ and $T = \{n \in \mathbb{N} : p(n)\}$. $1 \in T$ since $(a_1a_2)^2 = (a_1a_2a_1)a_2 = ea_2 = a_2$. Now assume $m \in T$ so that $(a_1a_2)^{2m} = a_2^m$. Multiplying both sides by a_2 yields that $(a_1a_2)^{2m}a_2 = a_2^{m+1}$. This completes the proof. □

Statement 12. *Let $a_1, a_2, a_3 \in G$. If $a_1a_2a_1 = a_3$, then there's an $a_4 \in G$ such that $a_2a_3 = a_4^2$.*

Proof. We have that $a_2a_3 = a_2a_1a_2a_1 = (a_2a_1)^2$. Thus $a_4 = a_2a_1$. □

Statement 13. *Let $a_1, a_2 \in G$.*
$(\forall n \in \mathbb{N})[\ (a_2a_1a_2^{-1})^n = a_2a_1^na_2^{-1}\ ]$.

Proof. Let $p(n) := (a_2a_1a_2^{-1})^n = a_2a_1^na_2^{-1}$ and $T = \{n \in \mathbb{N} : p(n)\}$. $1 \in T$ since $(a_2a_1a_2^{-1})^1 = a_2a_1^1a_2^{-1}$. Assume $k \in T$ so that $(a_2a_1a_2^{-1})^k = a_2a_1^ka_2^{-1}$. Multiplying both sides by $a_2a_1a_2^{-1}$, we have that $(a_2a_1a_2^{-1})^{k+1} = (a_2a_1^ka_2^{-1})(a_2a_1a_2^{-1}) = a_2a_1^{k+1}a_2^{-1}$. This completes the proof that $T = \mathbb{N}$. □