<u>Modern Algebra I: Group Theory</u>

List of Theorems and Proofs

Theorem # 1: An equilateral triangle has exactly 6 symmetries.

Proof:

Theorem # 2: The combination (composition) of any two symmetries is another symmetry.

Proof:

Theorem # 3 (The Sudoku Property): In a (group) operation table, every element appears exactly once in each row and column.

Proof:

Theorem # 4 (The Cancellation Law): Let a, b, c be symmetries (or, as we found out later, elements of a general group). Then $ab = ac$ implies $b = c$.

Proof:

Theorem # 5 (Uniqueness of the Identity): The identity element in a group is unique.

Proof:

Theorem # 6 (Uniqueness of Inverses): Each element has exactly one inverse.

Proof:

Modern Algebra I: Group Theory

List of Theorems and Proofs

Theorem # 7: A group G is abelian if and only if $(ab)^2 = a^2b^2$.

Proof:

Theorem # 8: $(ab)^{-1} = b^{-1}a^{-1}$ (that is, the inverse of ab is $b^{-1}a^{-1}$) .

Proof:

Theorem # 9: $(n\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, +)$ for every $n \in \mathbb{Z}$.

Proof:

Modern Algebra I: Group Theory

List of Theorems and Proofs

Theorem # 10 (The Subgroup Test): A nonempty subset H of a group G is a subgroup if and only if H is closed under the operation of G and each element of H has its inverse in H.

Proof:

Theorem # 11: Let H be a subgroup of G. Then the identity of H is the identity of G.

Proof:

Theorem # 12: Let H be a subgroup of G and $h \in H$. Then the inverse of h in H is the inverse of h in G.

Proof:

Theorem # 13 (The Finite Subgroup Test): A nonempty finite subset H of a group G is a subgroup if and only if H is closed under the operation of G.

Proof:

Theorem # 14: $(G,\cdot)$ and $(H,*)$ are isomorphic groups. Then if G is abelian then H is abelian.

Proof:

Theorem # 15: Suppose $(G,\cdot)$ and $(H,*)$ are groups and $\varphi: G\rightarrow H$ is an isomorphism. Then $\varphi(e_G) = e_H$.

Proof:

Theorem # 16: Suppose $(G, \cdot)$ and $(H,*)$ are groups and $\varphi: G \to H$ is an isomorphism. Let $a \in G$, then $\varphi(a)^{-1} = \varphi(a^{-1})$.

Proof:

Theorem # 17: Suppose $(G,\cdot)$ and $(H,*)$ are groups and φ: G$\to H$ is an isomorphism. Let $a \in G$ and $n \in N$, then $\varphi(a)^n = \varphi(a^n)$.

Proof:

Theorem # 18: Suppose $(G,\cdot)$ and $(H,*)$ are groups and $\varphi: G \to H$ is an isomorphism. Let $a \in G$. Then, $|\varphi(a)| = |a|$.

Proof:

Theorem # 19: Suppose $(G,\cdot)$ and $(H,*)$ are groups and $\varphi: G \to H$ is an isomorphism.

(1) If G is cyclic, then H is cyclic.
(2) If G is abelian, then H is abelian.

Proof:

Theorem # 20: The inverse of an isomorphism is again an isomorphism. That is, if $\varphi: G \to H$ is an isomorphism then $\varphi^{-1}: H \to G$ is an isomorphism.

Proof:

Theorem # 21: The composition of two isomorphisms is an isomorphism. That is, if $f: A \to B$ and $g: B \to C$ are isomorphisms, then $g \circ f: A \to C$ is an isomorphism.

Proof:

Theorem #22 (Equality of Cosets): Let G be a group, H a subgroup of G, and $a, b \in G$. Then:

(1) $aH = bH$ if and only if $a \in bH$,
(2) $aH = bH$ if and only if $a^{-1}b \in H$.

Proof:

Theorem #23: Let G be a group and H a subgroup of G. Then the left cosets of H in G are all of equal size and partition G:

$$G = \coprod_{a \in G} aH$$

That is:

(1) Every element is contained in a coset: for any $a \in G$ there exists a $b \in G$ such that $a \in bH$.
(2) Distinct (nonequal) cosets are disjoint: if $aH \neq bH$ then $aH \cap bH = \emptyset$.
(3) The number of elements in each coset is the same: $|aH| = |bH|$ for any $a, b \in G$.

Proof:

Theorem #24: Let G be a group and H a nonempty subset of G. Then G/H is a group if and only if H is a normal subgroup of G.

[this theorem is extremely important! Unfortunately, we have omitted this proof due to time constraints. However, you should still recall (and be familiar with) how the left cosets equaling the right cosets were the condition that enabled the cosets we formed in D_4 to be a group.]

Theorem #25 (Normal Subgroup Test): Let G be a group and H a subgroup of G. Then H is normal if and only if $aHa^{-1} \subseteq H$ for any $a \in G$.

Proof:

Theorem #26: Let G and H be groups and $\phi: G \to H$ a homomorphism. Then:

(1) $\ker \phi$ is a subgroup of G,
(2) $\ker \phi$ is normal in G,
(3) $\text{im}\ \phi$ is a subgroup of G.

Proof:

Theorem #27 (Lagrange's Theorem): Let G be a group and H a subgroup of G. Then $|H|$ divides $|G|$.

Proof: (Hint: use Theorem 23)

Theorem #28: Let G and H be groups and $\phi: G \to H$ a homomorphism. Then ϕ is injective if and only if $\ker \phi = \{e_G\}$.

Proof:

Theorem #29: Let G and H be groups and $\phi: G \to H$ a homomorphism. Then $G/\ker\phi \cong \text{im}\phi$.

Explanation: while we did not give a rigorous proof of this result, we did an explanatory sketch of the proof, which you should be familiar with. (This is one of the fundamental theorems of group theory!)