Theorem System Test

Deepak Jassal

November 13, 2025

Contents

1 Testing All Theorem Environments **2**
1.1 Basic Environments . . . 2
1.2 Environments with Proofs . . . 2
1.3 Regular Proof Environment . . . 3
1.4 Examples and Remarks . . . 3
1.5 Referenced Theorems . . . 4
1.6 More Examples . . . 4

1 Testing All Theorem Environments

1.1 Basic Environments

Definition 1.1.1: Group

A **group** is a set G with a binary operation $*$ such that:

1. **Associativity**: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$
2. **Identity**: There exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$
3. **Inverses**: For each $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

Theorem 1.1.2: Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. That is, $|H|$ divides $|G|$.

Lemma 1.1.3: Subgroup Test

A subset H of a group G is a subgroup if and only if:

1. H is non-empty
2. For all $a, b \in H$, $ab \in H$
3. For all $a \in H$, $a^{-1} \in H$

Corollary 1.1.4

Every group of prime order is cyclic.

Proposition 1.1.5

The intersection of two subgroups is also a subgroup.

Claim 1.1.6: Order of Element

In a finite group, the order of any element divides the order of the group.

Fact 1.1.7

The symmetric group S_n has order $n!$.

1.2 Environments with Proofs

Lemma 1.2.1: Cyclic Subgroups

If a is an element of a group G, then the set $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G.

Proof for Lemma.

Let $x, y \in \langle a \rangle$. Then $x = a^m$ and $y = a^n$ for some $m, n \in \mathbb{Z}$. Then $xy = a^m a^n = a^{m+n} \in \langle a \rangle$. Also, $x^{-1} = a^{-m} \in \langle a \rangle$. Therefore, $\langle a \rangle$ is a subgroup. $\square$

Corollary 1.2.2

If G is a cyclic group of order n, then G has exactly $\phi(n)$ generators, where ϕ is Euler's totient function.

Proof for Corollary.

Let $G = \langle a \rangle$ be cyclic of order n. Then a^k is a generator if and only if $\gcd(k, n) = 1$. There are exactly $\phi(n)$ such integers k with $1 \leq k \leq n$. $\square$

Proposition 1.2.3

The center of a group $Z(G) = \{g \in G : gh = hg \text{ for all } h \in G\}$ is a subgroup of G.

Proof for Proposition.

Let $x, y \in Z(G)$. For any $h \in G$, we have $(xy)h = x(yh) = x(hy) = (xh)y = (hx)y = h(xy)$, so $xy \in Z(G)$. Also, $x^{-1}h = hx^{-1}$ for all $h \in G$, so $x^{-1} \in Z(G)$. $\square$

Claim 1.2.4: Abelian Center

If G is a group, then $Z(G)$ is abelian.

Proof for Claim.

Let $x, y \in Z(G)$. Since x commutes with all elements of G, it commutes with y in particular. Therefore $xy = yx$, so $Z(G)$ is abelian. $\square$

1.3 Regular Proof Environment

Proof.

Let's prove that every subgroup of a cyclic group is cyclic. Suppose $G = \langle a \rangle$ is cyclic and H is a subgroup of G. If $H = \{e\}$, then H is cyclic. Otherwise, let m be the smallest positive integer such that $a^m \in H$. We claim $H = \langle a^m \rangle$. For any $a^n \in H$, by the division algorithm, $n = mq + r$ with $0 \leq r < m$. Then $a^r = a^{n-mq} = a^n(a^m)^{-q} \in H$, so by minimality of m, we must have $r = 0$. Thus $a^n = (a^m)^q \in \langle a^m \rangle$. $\square$

1.4 Examples and Remarks

Example.

Consider the group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under addition modulo 6. The subgroups are: $\{0\}$, $\{0, 2, 4\}$, $\{0, 3\}$, and $\mathbb{Z}_6$ itself. Notice that the orders are 1, 3, 2, and 6, which all divide 6.

Example.

The symmetric group S_3 has order 6. Its subgroups have orders 1, 2, 3, and 6, which all divide 6. However, S_3 is not abelian.

This shows that Lagrange's Theorem has a converse that is *not true* in general.

Remark.

While Lagrange's Theorem tells us about possible subgroup orders, it doesn't guarantee that subgroups of those orders actually exist. This leads to the study of Sylow theorems.

1.5 Referenced Theorems

Theorem 1.5.1: Cauchy's Theorem

If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Proof for Theorem 1.5.1.

Example text $\square$

Definition 1.5.2: Simple Group

A group G is called **simple** if it has no non-trivial proper normal subgroups.

We can reference these later: Theorem 1.5.1 and Definition 1.5.2.

1.6 More Examples

Fact 1.6.1

The alternating group A_n is simple for $n \geq 5$.

Claim 1.6.2: Index Formula

If H is a subgroup of G, then $[G : H] = |G|/|H|$.

Example.

Let $G = \mathbb{Z}_{12}$. The possible subgroup orders are divisors of 12: 1, 2, 3, 4, 6, 12. For example:

- Order 2: $\langle 6 \rangle = \{0, 6\}$
- Order 3: $\langle 4 \rangle = \{0, 4, 8\}$
- Order 4: $\langle 3 \rangle = \{0, 3, 6, 9\}$