Lagrange's Theorem, Applications, Generalizations, Converse

Recall

Recall

Let G be a group and let S be a subgroup of G.

Recall

Let G be a group and let S be a subgroup of G. We explained why

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Lagrange's Theorem.

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Lagrange's Theorem. If G is a finite group and S is a subgroup of G,

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Lagrange's Theorem. If G is a finite group and S is a subgroup of G, then $|S|$ divides $|G|$.

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Lagrange's Theorem. If G is a finite group and S is a subgroup of G, then $|S|$ divides $|G|$.

Proof.

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Lagrange's Theorem. If G is a finite group and S is a subgroup of G, then $|S|$ divides $|G|$.

Proof. $|G|/|S| = [G : S]$

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Lagrange's Theorem. If G is a finite group and S is a subgroup of G, then $|S|$ divides $|G|$.

Proof. $|G|/|S| = [G : S] \in \mathbb{Z}$.

Recall

Let G be a group and let S be a subgroup of G. We explained why

$$|G| = [G : S] \cdot |S|.$$

If G is finite, this can be rewritten

$$[G : S] = |G|/|S|.$$

This yields

Lagrange's Theorem. If G is a finite group and S is a subgroup of G, then $|S|$ divides $|G|$.

Proof. $|G|/|S| = [G : S] \in \mathbb{Z}$. $\square$

Applications, 1

Applications, 1

If G is finite and $a \in G$,

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem.

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem. If G is finite and $a \in G$, then $|a|$ divides $|G|$.

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem. If G is finite and $a \in G$, then $|a|$ divides $|G|$. Hence G satisfies the identity

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem. If G is finite and $a \in G$, then $|a|$ divides $|G|$. Hence G satisfies the identity

$$x^{|G|} = 1.$$

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem. If G is finite and $a \in G$, then $|a|$ divides $|G|$. Hence G satisfies the identity

$$x^{|G|} = 1.$$

Proof.

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem. If G is finite and $a \in G$, then $|a|$ divides $|G|$. Hence G satisfies the identity

$$x^{|G|} = 1.$$

Proof. $|a| = |\langle a \rangle|$ and $\langle a \rangle \leq |G|$,

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem. If G is finite and $a \in G$, then $|a|$ divides $|G|$. Hence G satisfies the identity

$$x^{|G|} = 1.$$

Proof. $|a| = |\langle a \rangle|$ and $\langle a \rangle \leq |G|$, so $|a|$ divides $|G|$.

Applications, 1

If G is finite and $a \in G$, then the powers of a form a subgroup of G:

$$\langle a \rangle := \{1, a, a^2, \ldots, a^{n-1}\} \leq G$$

where $n = |a| := |\langle a \rangle|$ = the **order** of a (i.e., n is the least positive integer such that $a^n = 1$).

Theorem. If G is finite and $a \in G$, then $|a|$ divides $|G|$. Hence G satisfies the identity

$$x^{|G|} = 1.$$

Proof. $|a| = |\langle a \rangle|$ and $\langle a \rangle \leq |G|$, so $|a|$ divides $|G|$. $\square$

Applications, 2

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem. If $|G| = p$ is prime, then $G \cong C_p$.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem. If $|G| = p$ is prime, then $G \cong C_p$.

Proof.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem. If $|G| = p$ is prime, then $G \cong C_p$.

Proof. Choose any nonidentity element $a \in G$.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem. If $|G| = p$ is prime, then $G \cong C_p$.

Proof. Choose any nonidentity element $a \in G$. $|a| \neq 1$, so $|a| = p$. Thus, $\langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\}$ is a p-element subgroup of the p-element group G.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem. If $|G| = p$ is prime, then $G \cong C_p$.

Proof. Choose any nonidentity element $a \in G$. $|a| \neq 1$, so $|a| = p$. Thus, $\langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\}$ is a p-element subgroup of the p-element group G. Necessarily, $G = \langle a \rangle$

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem. If $|G| = p$ is prime, then $G \cong C_p$.

Proof. Choose any nonidentity element $a \in G$. $|a| \neq 1$, so $|a| = p$. Thus, $\langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\}$ is a p-element subgroup of the p-element group G. Necessarily, $G = \langle a \rangle \cong C_p$.

Applications, 2

Lagrange's Theorem implies that if $|G|$ has few prime divisors, then there are few possible numbers that can be $|S|$ for a subgroup $S \leq G$. This fact simplifies the classification of finite groups whose order is divisible by few primes.

The most extreme case of this is when $|G| = p$ = a prime number. In this case, $|S| = 1$ or $|S| = p$.

Theorem. If $|G| = p$ is prime, then $G \cong C_p$.

Proof. Choose any nonidentity element $a \in G$. $|a| \neq 1$, so $|a| = p$. Thus, $\langle a \rangle = \{1, a, a^2, \ldots, a^{p-1}\}$ is a p-element subgroup of the p-element group G. Necessarily, $G = \langle a \rangle \cong C_p$. $\square$

Generalizations

Generalizations

We have already seen one generalization: if $S \leq G$, then

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite.

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get $|K| = [K : H] \cdot |H|$.

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get $|K| = [K : H] \cdot |H|$. Hence

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get $|K| = [K : H] \cdot |H|$. Hence

$$[G : H] \cdot \underline{|H|} = |G| = [G : K] \cdot |K| = [G : K] \cdot [K : H] \cdot \underline{|H|}.$$

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get $|K| = [K : H] \cdot |H|$. Hence

$$[G : H] \cdot \underline{|H|} = |G| = [G : K] \cdot |K| = [G : K] \cdot [K : H] \cdot \underline{|H|}.$$

Canceling the underlined terms from the left and right yields

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get $|K| = [K : H] \cdot |H|$. Hence

$$[G : H] \cdot \underline{|H|} = |G| = [G : K] \cdot |K| = [G : K] \cdot [K : H] \cdot \underline{|H|}.$$

Canceling the underlined terms from the left and right yields

$$[G : H] = [G : K] \cdot [K : H].$$

This establishes the **multiplicativity of index**.

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get $|K| = [K : H] \cdot |H|$. Hence

$$[G : H] \cdot \underline{|H|} = |G| = [G : K] \cdot |K| = [G : K] \cdot [K : H] \cdot \underline{|H|}.$$

Canceling the underlined terms from the left and right yields

$$[G : H] = [G : K] \cdot [K : H].$$

This establishes the **multiplicativity of index**. By Induction, if $S_n \leq \cdots \leq S_2 \leq S_1 \leq G$, then

Generalizations

We have already seen one generalization: if $S \leq G$, then

$$|G| = [G : S] \cdot |S|.$$

(This generalizes Lagrange's Theorem because it asserts something for infinite groups.)

Generalizing further, assume that $H \leq K \leq G$ and $|G|$ is finite. Applying Lagrange's Theorem to K we get $|K| = [K : H] \cdot |H|$. Hence

$$[G : H] \cdot \underline{|H|} = |G| = [G : K] \cdot |K| = [G : K] \cdot [K : H] \cdot \underline{|H|}.$$

Canceling the underlined terms from the left and right yields

$$[G : H] = [G : K] \cdot [K : H].$$

This establishes the **multiplicativity of index**. By Induction, if $S_n \leq \cdots \leq S_2 \leq S_1 \leq G$, then

$$[G : S_n] = [G : S_1] \cdot [S_1 : S_2] \cdot [S_2 : S_3] \cdots [S_{n-1} : S_n].$$

The converse of Lagrange's Theorem

The converse of Lagrange's Theorem

The converse of Lagrange's Theorem is true for abelian groups, but not necessarily for all groups.

The converse of Lagrange's Theorem

The converse of Lagrange's Theorem is true for abelian groups, but not necessarily for all groups.

Theorem.

The converse of Lagrange's Theorem

The converse of Lagrange's Theorem is true for abelian groups, but not necessarily for all groups.

Theorem. If G is a finite abelian group and d divides $|G|$, then G has a subgroup of order d.

The converse of Lagrange's Theorem

The converse of Lagrange's Theorem is true for abelian groups, but not necessarily for all groups.

Theorem. If G is a finite abelian group and d divides $|G|$, then G has a subgroup of order d.

Continuation of these ideas

Continuation of these ideas

Continuation 1.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime,

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime,

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime, then either $G \colon C_{p^2}$ or $G \colon C_p \times C_p$.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime, then either $G \colon C_{p^2}$ or $G \colon C_p \times C_p$. The latter case holds exactly when all nonidentity elements of G have order p.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime, then either $G \colon C_{p^2}$ or $G \colon C_p \times C_p$. The latter case holds exactly when all nonidentity elements of G have order p.
2. If $|G| = pq$ where $p < q$ are prime,

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime, then either $G \colon C_{p^2}$ or $G \colon C_p \times C_p$. The latter case holds exactly when all nonidentity elements of G have order p.
2. If $|G| = pq$ where $p < q$ are prime,

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime, then either $G \colon C_{p^2}$ or $G \colon C_p \times C_p$. The latter case holds exactly when all nonidentity elements of G have order p.
2. If $|G| = pq$ where $p < q$ are prime, then either $G \cong C_{pq}$ or G is a nonabelian subgroup of the **affine group**, $\mathrm{Aff}(1, \mathbb{Z}_q)$, containing the **translation subgroup**.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime, then either $G \colon C_{p^2}$ or $G \colon C_p \times C_p$. The latter case holds exactly when all nonidentity elements of G have order p.
2. If $|G| = pq$ where $p < q$ are prime, then either $G \cong C_{pq}$ or G is a nonabelian subgroup of the **affine group**, $\mathrm{Aff}(1, \mathbb{Z}_q)$, containing the **translation subgroup**. The latter can only happen if $p \mid (q - 1)$.

Continuation of these ideas

Continuation 1. We can enrich subgroup lattices by assigning indices to edges of Hasse diagrams.

Continuation 2. New terminology related to subgroup lattices:

1. trivial subgroup, nontrivial subgroup.
2. proper subgroup, improper subgroup.
3. minimal subgroup, maximal subgroup.

Continuation 3. With a little more work, we can classify finite groups G where $|G| = pq$, $p \leq q$, is a product of two primes.

1. If $|G| = p^2$ where p is prime, then either $G \colon C_{p^2}$ or $G \colon C_p \times C_p$. The latter case holds exactly when all nonidentity elements of G have order p.
2. If $|G| = pq$ where $p < q$ are prime, then either $G \cong C_{pq}$ or G is a nonabelian subgroup of the **affine group**, $\mathrm{Aff}(1, \mathbb{Z}_q)$, containing the **translation subgroup**. The latter can only happen if $p \mid (q-1)$. In this case, there is only one isomorphism type of size pq.