# Groups of size $p^2$

# Groups of size $p$

# Groups of size $p$

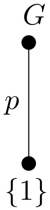
Let $G$ be a finite group whose order is a prime number $p$.

# Groups of size $p$

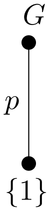
Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is

# Groups of size $p$

Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is

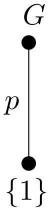


Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is



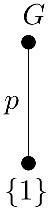

**Theorem.**

Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group.

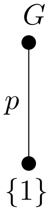
Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

# Groups of size $p$

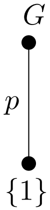
Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.

Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is

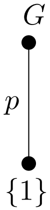



**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.

# Groups of size $p$

Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is

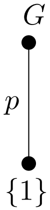



**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.
2. $G$ has no proper nontrivial subgroups.

# Groups of size $p$

Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is

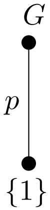



**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.
2. $G$ has no proper nontrivial subgroups.

# Groups of size $p$

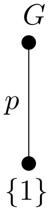
Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.
2. $G$ has no proper nontrivial subgroups.
3. $\mathrm{Sub}(G)$ is a 2-element chain.

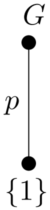
Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.
2. $G$ has no proper nontrivial subgroups.
3. $\mathrm{Sub}(G)$ is a 2-element chain.

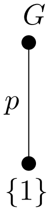
Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.
2. $G$ has no proper nontrivial subgroups.
3. $\text{Sub}(G)$ is a 2-element chain.
4. $G \cong C_p$.

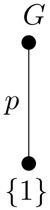
Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.
2. $G$ has no proper nontrivial subgroups.
3. $\text{Sub}(G)$ is a 2-element chain.
4. $G \cong C_p$.

Let $G$ be a finite group whose order is a prime number $p$. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a nontrivial group. The following are equivalent:

1. $|G| = p$.
2. $G$ has no proper nontrivial subgroups.
3. $\text{Sub}(G)$ is a 2-element chain.
4. $G \cong C_p$.

# Groups of size $p^2$ with one maximal subgroup

# Groups of size $p^2$ with one maximal subgroup

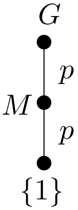
Let $G$ be a finite group whose order $p^2$ with one maximal subgroup.

# Groups of size $p^2$ with one maximal subgroup

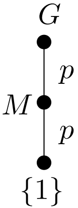
Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is



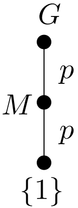
Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Theorem.**

# Groups of size $p^2$ with one maximal subgroup

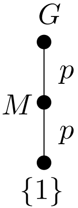
Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a group of order $p^2$.

## Groups of size $p^2$ with one maximal subgroup

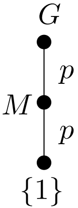
Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

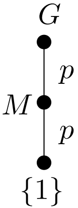



**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has one maximal subgroup.

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

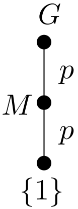



**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has one maximal subgroup.

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

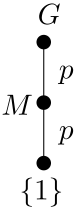



**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has one maximal subgroup.
2. $\text{Sub}(G)$ is a 3-element chain.

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

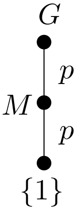



**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a 3-element chain.

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

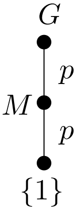



**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a 3-element chain.
3. $G \cong C_{p^2}$.

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

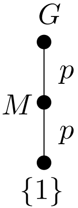



**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a 3-element chain.
3. $G \cong C_{p^2}$.

# Groups of size $p^2$ with one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a 3-element chain.
3. $G \cong C_{p^2}$.

# Groups of size $p^2$ with more than one maximal subgroup

# Groups of size $p^2$ with more than one maximal subgroup

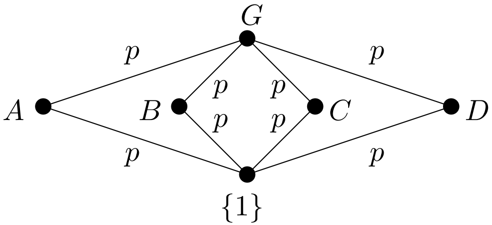
Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup.

# Groups of size $p^2$ with more than one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is

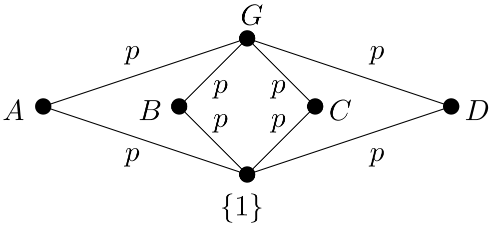
# Groups of size $p^2$ with more than one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is



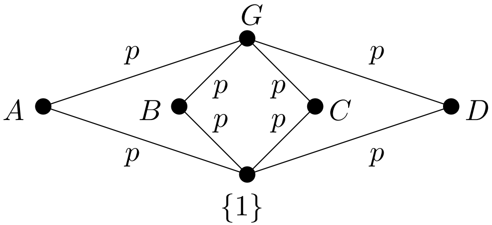
# Groups of size $p^2$ with more than one maximal subgroup

Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Observations.**

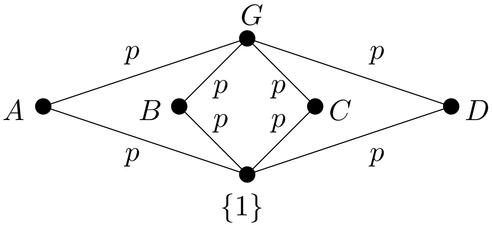
Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Observations.**

1. In this case, $G$ is not cyclic, so it satisfies $(\forall x)(x^p = 1)$.

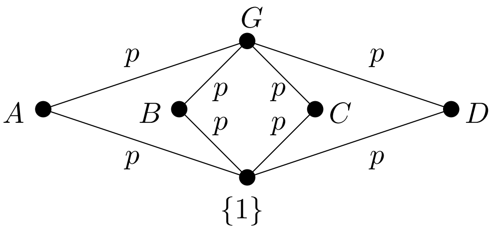
Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Observations.**

1. In this case, $G$ is not cyclic, so it satisfies $(\forall x)(x^p = 1)$.
2. If $\langle a \rangle \neq \langle b \rangle$, then $\langle a \rangle \cap \langle b \rangle = \{1\}$.

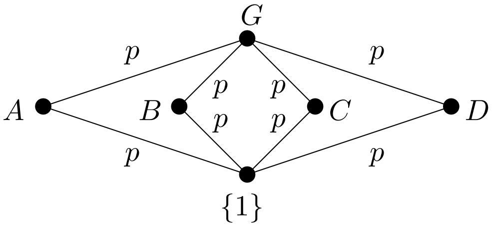
Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Observations.**

1. In this case, $G$ is not cyclic, so it satisfies $(\forall x)(x^p = 1)$.
2. If $\langle a \rangle \neq \langle b \rangle$, then $\langle a \rangle \cap \langle b \rangle = \{1\}$.
3. If $\langle a \rangle \neq \langle b \rangle$ are maximal, then $G = \langle a \rangle \cdot \langle b \rangle = \{a^i b^j \mid 0 \leq i, j < p\}$.

Let $G$ be a finite group whose order $p^2$ with more than one maximal subgroup. The subgroup lattice of $G$, labeled with indices, is




**Observations.**

1. In this case, $G$ is not cyclic, so it satisfies $(\forall x)(x^p = 1)$.
2. If $\langle a\rangle \neq \langle b\rangle$, then $\langle a\rangle \cap \langle b\rangle = \{1\}$.
3. If $\langle a\rangle \neq \langle b\rangle$ are maximal, then $G = \langle a\rangle \cdot \langle b\rangle = \{a^i b^j \mid 0 \leq i, j < p\}$.
4. If $\langle a\rangle \neq \langle b\rangle$ are maximal, then for all $g \in G$, $g^{-1}ag \notin \langle b\rangle$.

# Groups of size $p^2$ with more than one maximal subgroup

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.**

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.*

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$,

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily. If they belong to one of the (cyclic) maximal subgroups of $G$, then they commute with each other.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily. If they belong to one of the (cyclic) maximal subgroups of $G$, then they commute with each other. Else, $\langle c \rangle \neq \langle d \rangle$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily. If they belong to one of the (cyclic) maximal subgroups of $G$, then they commute with each other. Else, $\langle c \rangle \neq \langle d \rangle$. Now $(c^{-1}d^{-1}c)d = c^{-1}(d^{-1}cd) \in \langle d \rangle \cap \langle c \rangle = \{1\}$,

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily. If they belong to one of the (cyclic) maximal subgroups of $G$, then they commute with each other. Else, $\langle c \rangle \neq \langle d \rangle$. Now $(c^{-1}d^{-1}c)d = c^{-1}(d^{-1}cd) \in \langle d \rangle \cap \langle c \rangle = \{1\}$, so $c^{-1}d^{-1}cd = 1$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily. If they belong to one of the (cyclic) maximal subgroups of $G$, then they commute with each other. Else, $\langle c \rangle \neq \langle d \rangle$. Now $(c^{-1}d^{-1}c)d = c^{-1}(d^{-1}cd) \in \langle d \rangle \cap \langle c \rangle = \{1\}$, so $c^{-1}d^{-1}cd = 1$. We may rewrite this as $cd = dc$.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily. If they belong to one of the (cyclic) maximal subgroups of $G$, then they commute with each other. Else, $\langle c \rangle \neq \langle d \rangle$. Now $(c^{-1}d^{-1}c)d = c^{-1}(d^{-1}cd) \in \langle d \rangle \cap \langle c \rangle = \{1\}$, so $c^{-1}d^{-1}cd = 1$. We may rewrite this as $cd = dc$. Thus, in all cases, $c, d \in G$ commute with each other.

# Groups of size $p^2$ with more than one maximal subgroup

**Lemma.** If $|G| = p^2$, then $G$ is abelian.

*Proof.* If $G$ is cyclic, then it is abelian, so we are done in the case.

Else, $G$ has more than one maximal subgroup, and each is of the form $\langle a \rangle$ for some $a \in G$. Choose one of them arbitrarily, $A = \langle a \rangle$. If $A$ is not a normal subgroup of $G$, then there is some $g \in G$ such that $A \neq g^{-1}Ag$. Necessarily, $g^{-1}Ag = \langle b \rangle$ for some $b \in G$. But now $\langle a \rangle = A \neq g^{-1}Ag = \langle b \rangle$ and $g^{-1}ag \in g^{-1}Ag = \langle b \rangle$, contrary to an earlier observation. This contradiction shows that $A = \langle a \rangle$ is normal in $G$. The element $a$ was chosen arbitrarily in $G - \{1\}$, so every maximal subgroup of $G$ is normal.

Now choose $c, d \in G$ arbitrarily. If they belong to one of the (cyclic) maximal subgroups of $G$, then they commute with each other. Else, $\langle c \rangle \neq \langle d \rangle$. Now $(c^{-1}d^{-1}c)d = c^{-1}(d^{-1}cd) \in \langle d \rangle \cap \langle c \rangle = \{1\}$, so $c^{-1}d^{-1}cd = 1$. We may rewrite this as $cd = dc$. Thus, in all cases, $c, d \in G$ commute with each other. $\square$

# Groups of size $p^2$ with more than one maximal subgroup

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.**

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\text{Sub}(G)$ is a isomorphic to $M_{p+1}$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\text{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)]

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\text{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)]

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. Sub$(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$,

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. Sub$(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$, Sub$(G)$ is a isomorphic to $M_n$ for some $n$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. Sub$(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$, Sub$(G)$ is a isomorphic to $M_n$ for some $n$. Counting elements leads to $1 + n(p-1) = p^2$,

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\mathrm{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h \colon C_p \times C_p \to G \colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$, $\mathrm{Sub}(G)$ is a isomorphic to $M_n$ for some $n$. Counting elements leads to $1 + n(p-1) = p^2$, or $n(p-1) = p^2 - 1$,

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. $\text{Sub}(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$, $\text{Sub}(G)$ is a isomorphic to $M_n$ for some $n$. Counting elements leads to $1 + n(p-1) = p^2$, or $n(p-1) = p^2 - 1$, or $n = p + 1$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. Sub$(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$, Sub$(G)$ is a isomorphic to $M_n$ for some $n$. Counting elements leads to $1 + n(p-1) = p^2$, or $n(p-1) = p^2 - 1$, or $n = p + 1$.
[(2)⇒(1)]

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. Sub$(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$, Sub$(G)$ is a isomorphic to $M_n$ for some $n$. Counting elements leads to $1 + n(p-1) = p^2$, or $n(p-1) = p^2 - 1$, or $n = p + 1$.
[(2)⇒(1)] By (2), the number of maximal subgroups of $G$ is $p + 1$, which is greater than $1$.

# Groups of size $p^2$ with more than one maximal subgroup

**Theorem.** Let $G$ be a group of order $p^2$. The following are equivalent:

1. $G$ has more than one maximal subgroup.
2. Sub$(G)$ is a isomorphic to $M_{p+1}$.
3. $G \cong C_p \times C_p$.

*Proof.*
[(1)⇒(3)] By the Lemma, we know that $|G| = p^2$ implies that $G$ is abelian. In the case where $G$ has more than one maximal subgroup, we know that every $x \in G$ satisfies $x^p = 1$. Choose $a, b \in G$ that generate maximal subgroups $\langle a \rangle$ and $\langle b \rangle$. Verify that $h\colon C_p \times C_p \to G\colon (r^i, r^j) \mapsto a^i b^j$ is an isomorphism.
[(3)⇒(2)] Since every nontrivial proper subgroup of $G$ is maximal and of the form $\langle a \rangle$ for some $a$, Sub$(G)$ is a isomorphic to $M_n$ for some $n$. Counting elements leads to $1 + n(p-1) = p^2$, or $n(p-1) = p^2 - 1$, or $n = p + 1$.
[(2)⇒(1)] By (2), the number of maximal subgroups of $G$ is $p + 1$, which is greater than 1. □

# Final result

# Final result

If $p$ is prime, then any group of order $p^2$ is isomorphic to $C_{p^2}$ or to $C_p \times C_p$.

# Final result

If $p$ is prime, then any group of order $p^2$ is isomorphic to $C_{p^2}$ or to $C_p \times C_p$. These are not isomorphic to each other, since $C_{p^2}$ has an element of order $p^2$ and $C_p \times C_p$ does not.

# Final result

If $p$ is prime, then any group of order $p^2$ is isomorphic to $C_{p^2}$ or to $C_p \times C_p$. These are not isomorphic to each other, since $C_{p^2}$ has an element of order $p^2$ and $C_p \times C_p$ does not. Another way to say this is that $C_p \times C_p$ satisfies the law $(\forall x)(x^p = 1)$ while $C_{p^2}$ does not.