Modern Algebra I

Lecture 12

Jung-Chen Liu

liujc@math.ntnu.edu.tw

2009, Fall

Today, we will cover the section

Section II.5: The Sylow Theorems

Chapter II

The Structure of Groups

Section II.5: The Sylow Theorems

Chapter II

The Structure of Groups

Section II.5: The Sylow Theorems

Remark. In this section, we will make use of *actions of a group on a set* to prove **Cauchy's theorem** and the **Sylow Theorems**.

Chapter II

The Structure of Groups

Section II.5: The Sylow Theorems

Remark. In this section, we will make use of *actions of a group on a set* to prove **Cauchy's theorem** and the **Sylow Theorems**.

Chapter II

The Structure of Groups

Section II.5: The Sylow Theorems

Remark. In this section, we will make use of *actions of a group on a set* to prove **Cauchy's theorem** and the **Sylow Theorems**.

Chapter II

The Structure of Groups

Section II.5: The Sylow Theorems

Remark. In this section, we will make use of *actions of a group on a set* to prove **Cauchy's theorem** and the **Sylow Theorems**.

Chapter II

The Structure of Groups

Section II.5: The Sylow Theorems

Remark. In this section, we will make use of *actions of a group on a set* to prove **Cauchy's theorem** and the **Sylow Theorems**.

Remark. Since we will apply some results that we covered last week,

Chapter II

The Structure of Groups

Section II.5: The Sylow Theorems

Remark. In this section, we will make use of *actions of a group on a set* to prove **Cauchy's theorem** and the **Sylow Theorems**.

Remark. Since we will apply some results that we covered last week, let's review some of the definitions and theorems in Section II.4 first.

Section II.4: The Action of a Group on a Set

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S is a function $G \times S \to S$,

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$,

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x$, $\forall x \in S$, and

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given,

Section II.4: The Action of a Group on a Set

Definition (4.1)**.** An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S. *I usually read the element gx as the element obtained when g acts on x.*

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Theorem (4.2). Let G be a group that acts on a set S.

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Theorem (4.2). Let G be a group that acts on a set S.

(i) The relation on S defined by

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Theorem (4.2). Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x, \forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x), \forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Theorem (4.2). Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x$, $\forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x)$, $\forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Theorem (4.2). Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x$, $\forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x)$, $\forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Theorem (4.2). Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

Section II.4: The Action of a Group on a Set

Definition (4.1). An **action** of a group G on a set S is a function $G \times S \to S$, usually denoted by $(g, x) \mapsto gx$, such that

- $ex = x$, $\forall x \in S$, and
- $(g_1 g_2)x = g_1(g_2 x)$, $\forall g_1, g_2 \in G$ and $x \in S$.

When such an action is given, we say that the group G **acts on** the set S.

Theorem (4.2). Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i)

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S;

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S; the orbit of $x \in S$ is denoted $\overline{x}$,

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S; the orbit of $x \in S$ is denoted $\overline{x}$, i.e., $\overline{x} = \{gx \mid g \in G\}$.

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S; the orbit of $x \in S$ is denoted $\overline{x}$, i.e., $\overline{x} = \{gx \mid g \in G\}$. The subgroup G_x is called the subgroup fixing x,

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S; the orbit of $x \in S$ is denoted $\overline{x}$, i.e., $\overline{x} = \{gx \mid g \in G\}$. The subgroup G_x is called the subgroup fixing x, the isotropy group of x,

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S; the orbit of $x \in S$ is denoted $\overline{x}$, i.e., $\overline{x} = \{gx \mid g \in G\}$. The subgroup G_x is called the subgroup fixing x, the isotropy group of x, or the stabilizer of x.

Section II.4: The Action of a Group on a Set

Theorem (4.2)**.** Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S; the orbit of $x \in S$ is denoted $\overline{x}$, i.e., $\overline{x} = \{gx \mid g \in G\}$. The subgroup G_x is called the subgroup fixing x, the isotropy group of x, or the stabilizer of x.

Theorem (4.3)**.** If a group G acts on a set S,

Section II.4: The Action of a Group on a Set

Theorem (4.2). Let G be a group that acts on a set S.

(i) The relation on S defined by

$$x \sim x' \iff gx = x' \text{ for some } g \in G$$

is an equivalence relation.

(ii) For each $x \in S$,

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Definition. The equivalence classes of the equivalence relation of Theorem 4.2 (i) are called the orbits of G on S; the orbit of $x \in S$ is denoted $\overline{x}$, i.e., $\overline{x} = \{gx \mid g \in G\}$. The subgroup G_x is called the subgroup fixing x, the isotropy group of x, or the stabilizer of x.

Theorem (4.3). If a group G acts on a set S, then

$$|\overline{x}| = [G : G_x], \forall x \in S.$$

Lemma (5.1)

If a group G of order p^n

Lemma (5.1)

If a group G of order p^n (p prime)

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$,

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$,

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.

Hence S can be written as a disjoint union

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.
Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.
Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.

Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.

For every $i = 1, \ldots, n$,

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.
Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.
For every $i = 1, \ldots, n$, by Theorem (4.3),

Theorem (4.3). If a group G acts on a set S, then

$$|\overline{x}| = [G : G_x], \forall x \in S.$$

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.
Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.
For every $i = 1, \ldots, n$, by Theorem (4.3), we have

$$|\overline{x_i}| = [G : G_{x_i}]$$

Theorem (4.3). If a group G acts on a set S, then

$$|\overline{x}| = [G : G_x], \forall x \in S.$$

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.

Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.

For every $i = 1, \ldots, n$, by Theorem (4.3), we have

$$|\overline{x_i}| = [G : G_{x_i}] \Big| |G| = p^n$$

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.

Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.

For every $i = 1, \ldots, n$, by Theorem (4.3), we have

$$|\overline{x_i}| = [G : G_{x_i}] \Big| |G| = p^n \text{ and } |\overline{x_i}| > 1$$

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.

Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.

For every $i = 1, \ldots, n$, by Theorem (4.3), we have

$$|\overline{x_i}| = [G : G_{x_i}] \Big| |G| = p^n \text{ and } |\overline{x_i}| > 1 \implies p \Big| |\overline{x_i}|.$$

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.
Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \; \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.
For every $i = 1, \ldots, n$, by Theorem (4.3), we have

$$|\overline{x_i}| = [G : G_{x_i}] \Big| |G| = p^n \text{ and } |\overline{x_i}| > 1 \implies p \Big| |\overline{x_i}|.$$

Therefore, $|S| \equiv |S_0| \pmod{p}$.

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.
Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \ \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.
For every $i = 1, \ldots, n$, by Theorem (4.3), we have

$$|\overline{x_i}| = [G : G_{x_i}] \Big| |G| = p^n \text{ and } |\overline{x_i}| > 1 \implies p \Big| |\overline{x_i}|.$$

Therefore, $|S| \equiv |S_0| \pmod{p}$.

This Lemma will be used several times today.

Lemma (5.1)

If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. Since $\overline{x} = \{gx \mid g \in G\}$, $\overline{x} = \{x\} \iff x \in S_0$.
Hence S can be written as a disjoint union

$$S = S_0 \cup \overline{x_1} \cup \cdots \cup \overline{x_n}, \text{ with } |\overline{x_i}| > 1 \ \forall i = 1, \ldots, n.$$

Then $|S| = |S_0| + |\overline{x_1}| + \cdots + |\overline{x_n}|$.
For every $i = 1, \ldots, n$, by Theorem (4.3), we have

$$|\overline{x_i}| = [G : G_{x_i}] \Big| |G| = p^n \text{ and } |\overline{x_i}| > 1 \implies p \Big| |\overline{x_i}|.$$

Therefore, $|S| \equiv |S_0| \pmod{p}$.

This Lemma will be used several times today. Please try to memorize it now.

Theorem (5.2, Cauchy)

Theorem (5.2, Cauchy)

If G is a finite group with $p \Big| |G|$,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e \implies a_2 \cdots a_p = a_1^{-1}$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e \implies a_2 \cdots a_p = a_1^{-1} \implies a_2 \cdots a_p a_1 = e$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e \implies a_2 \cdots a_p = a_1^{-1} \implies a_2 \cdots a_p a_1 = e$
  $\implies \cdots \implies a_{k+1} \cdots a_p a_1 \cdots a_k = e.$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e \implies a_2 \cdots a_p = a_1^{-1} \implies a_2 \cdots a_p a_1 = e$ $\implies \cdots \implies a_{k+1} \cdots a_p a_1 \cdots a_k = e.$
- for $0, k, k' \in \mathbb{Z}_p$, $x \in S$,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e \implies a_2 \cdots a_p = a_1^{-1} \implies a_2 \cdots a_p a_1 = e$ $\implies \cdots \implies a_{k+1} \cdots a_p a_1 \cdots a_k = e.$
- for $0, k, k' \in \mathbb{Z}_p$, $x \in S$, $0x = x$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e \implies a_2 \cdots a_p = a_1^{-1} \implies a_2 \cdots a_p a_1 = e$ $\implies \cdots \implies a_{k+1} \cdots a_p a_1 \cdots a_k = e.$
- for $0, k, k' \in \mathbb{Z}_p$, $x \in S$, $0x = x$ and $(k + k')x = k(k'x)$.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- $a_1 a_2 \cdots a_p = e \implies a_2 \cdots a_p = a_1^{-1} \implies a_2 \cdots a_p a_1 = e$ $\implies \cdots \implies a_{k+1} \cdots a_p a_1 \cdots a_k = e.$
- for $0, k, k' \in \mathbb{Z}_p$, $x \in S$, $0x = x$ and $(k + k')x = k(k'x)$.

Therefore, this action of $\mathbb{Z}_p$ on S is well-defined.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1),

Lemma (5.1)**.** If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

Lemma (5.1)**.** If a group G of order p^n (p prime) acts on a finite set S and if $S_0 := \{x \in S \mid gx = x, \forall g \in G\}$, then

$$|S| \equiv |S_0| \pmod{p}.$$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0 \iff a_1 = \cdots = a_p$ and $a_1 \cdots a_p = e$.

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0 \iff a_1 = \cdots = a_p$ and $a_1 \cdots a_p = e$. Since $(e, \ldots, e) \in S_0$,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0 \iff a_1 = \cdots = a_p$ and $a_1 \cdots a_p = e$. Since $(e, \ldots, e) \in S_0$, $|S_0| \neq 0$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0 \iff a_1 = \cdots = a_p$ and $a_1 \cdots a_p = e$. Since $(e, \ldots, e) \in S_0$, $|S_0| \neq 0$ and so $|S_0| \geq 2$,

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0 \iff a_1 = \cdots = a_p$ and $a_1 \cdots a_p = e$. Since $(e, \ldots, e) \in S_0$, $|S_0| \neq 0$ and so $|S_0| \geq 2$, i.e., $\exists a \in G \setminus \{e\}$ such that $(a, a, \ldots, a) \in S_0$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0 \iff a_1 = \cdots = a_p$ and $a_1 \cdots a_p = e$. Since $(e, \ldots, e) \in S_0$, $|S_0| \neq 0$ and so $|S_0| \geq 2$, i.e., $\exists a \in G \setminus \{e\}$ such that $(a, a, \ldots, a) \in S_0 \implies a^p = e$

Theorem (5.2, Cauchy)

If G is a finite group with $p \big| |G|$, where p is a prime, then G contains an element of order p.

Proof. Let $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}$ and let the group $\mathbb{Z}_p$ act on S by cyclic permutation, i.e., $k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k)$.

- Since $(a_1, a_2, \ldots, a_p) \in S \iff a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, $|S| = n^{p-1}$, where $|G| = n$.
- Since $p \big| |G| = n$, $|S| \equiv 0 \pmod{p}$.
- Since $|\mathbb{Z}_p| = p$, by Lemma (5.1), $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

On the other hand, $(a_1, \ldots, a_p) \in S_0 \iff a_1 = \cdots = a_p$ and $a_1 \cdots a_p = e$. Since $(e, \ldots, e) \in S_0$, $|S_0| \neq 0$ and so $|S_0| \geq 2$, i.e., $\exists a \in G \setminus \{e\}$ such that $(a, a, \ldots, a) \in S_0 \implies a^p = e \implies |a| = p$.

p-Groups and p-Subgroups

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group,

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Remark. $\{e\}$ is a p-subgroup of G for every prime p,

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Remark. $\{e\}$ is a p-subgroup of G for every prime p, because $|e| = 1 = p^0$.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. "$\Leftarrow$" follows from Lagrange's Theorem.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. "$\Leftarrow$" follows from Lagrange's Theorem. For "$\Rightarrow$",

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. "$\Leftarrow$" follows from Lagrange's Theorem. For "$\Rightarrow$", if $|G|$ is not a power of p,

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. "$\Leftarrow$" follows from Lagrange's Theorem. For "$\Rightarrow$", if $|G|$ is not a power of p, then there exists a prime number q such that $q \big| |G|$.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. "$\Leftarrow$" follows from Lagrange's Theorem. For "$\Rightarrow$", if $|G|$ is not a power of p, then there exists a prime number q such that $q \big| |G|$. By Cauchy's Theorem, G contains an element of order q,

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. "$\Leftarrow$" follows from Lagrange's Theorem. For "$\Rightarrow$", if $|G|$ is not a power of p, then there exists a prime number q such that $q \big| |G|$. By Cauchy's Theorem, G contains an element of order q, but this contradicts the assumption.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Proof. "$\Leftarrow$" follows from Lagrange's Theorem. For "$\Rightarrow$", if $|G|$ is not a power of p, then there exists a prime number q such that $q \big| |G|$. By Cauchy's Theorem, G contains an element of order q, but this contradicts the assumption. Hence $|G|$ must be a power of p.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Because we will use the class equation of G to prove this corollary,

p-Groups and p-Subgroups

Definition.

- A group in which every element has order a power of some fixed prime p is called a p-group.
- If H is a subgroup of a group G and if H is a p-group, H is said to be a p-subgroup of G.

Corollary (5.3)**.** A finite group G is a p-group if and only if $|G|$ is a power of p.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Because we will use the class equation of G to prove this corollary, let's review the class equation first.

Class Equations (Review)

Class Equations (Review)

Definition. Let G be a group.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \; \forall x \in G\}$ is the **center** of G.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \; \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \; \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \; \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \; \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.
- $|\overline{x}| = 1 \iff x \in C(G)$.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.
- $|\overline{x}| = 1 \iff x \in C(G)$.

Definition. Let G be a finite group

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.
- $|\overline{x}| = 1 \iff x \in C(G)$.

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$,

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.
- $|\overline{x}| = 1 \iff x \in C(G)$.

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$,

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.
- $|\overline{x}| = 1 \iff x \in C(G)$.

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$.

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.
- $|\overline{x}| = 1 \iff x \in C(G)$.

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$

Class Equations (Review)

Definition. Let G be a group.

- $C(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ is the **center** of G.
- For each $x \in G$,
  - $\{gxg^{-1} \mid g \in G\}$ is the **conjugacy class** of x.
  - $C_G(x) = \{g \in G \mid gx = xg\}$.

Remark. Let G be a group and for each $x \in G$, let $\overline{x}$ be the conjugacy class of x.

- $|\overline{x}| = [G : C_G(x)]$.
- $|\overline{x}| = 1 \iff x \in C(G)$.

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Since $[G : C_G(x_i)] > 1$

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Since $[G : C_G(x_i)] > 1$ and since $[G : C_G(x_i)] \Big| |G|$

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Since $[G : C_G(x_i)] > 1$ and since $[G : C_G(x_i)] \Big| |G| = p^n$,

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Since $[G : C_G(x_i)] > 1$ and since $[G : C_G(x_i)] \Big| |G| = p^n$, $p \Big| [G : C_G(x_i)]$ for all i.

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Since $[G : C_G(x_i)] > 1$ and since $[G : C_G(x_i)] \Big| |G| = p^n$, $p \Big| [G : C_G(x_i)]$ for all i. Therefore, $p \Big| |C(G)|$

Class Equations (Application)

Definition. Let G be a finite group and let $\overline{x_1}, \ldots, \overline{x_m}$ be the distinct conjugacy classes of G such that $[G : C_G(x_i)] > 1$, i.e., $x_i \notin C(G)$. The equation $|G| = |C(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$ is called the **class equation** of the group G.

Corollary (5.4)**.** The center $C(G)$ of a nontrivial finite p-group G contains more than one element.

Proof. Consider the class equation of G

$$|G| = |C(G)| + \sum [G : C_G(x_i)].$$

Since $[G : C_G(x_i)] > 1$ and since $[G : C_G(x_i)] \Big| |G| = p^n$, $p \Big| [G : C_G(x_i)]$ for all i. Therefore, $p \Big| |C(G)|$ and this implies $|C(G)| > 1$.

p-subgroups of a Finite Group

Since the next lemma gives some information about the normalizer of p-subgroups of a finite group,

p-subgroups of a Finite Group

Since the next lemma gives some information about the normalizer of p-subgroups of a finite group, we first review the normalizer of a subgroup of a group G.

p-subgroups of a Finite Group

Remark. Let H be a subgroup of a group G.

p-subgroups of a Finite Group

Remark. Let H be a subgroup of a group G. Then $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of G

p-subgroups of a Finite Group

Remark. Let H be a subgroup of a group G. Then $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of G and is called the *normalizer of* H.

p-subgroups of a Finite Group

Remark. Let H be a subgroup of a group G. Then $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of G and is called the *normalizer of* H. Moreover, we know that

p-subgroups of a Finite Group

Remark. Let H be a subgroup of a group G. Then $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of G and is called the *normalizer of* H. Moreover, we know that

- H is a normal subgroup of the group $N_G(H)$,

p-subgroups of a Finite Group

Remark. Let H be a subgroup of a group G. Then $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is a subgroup of G and is called the *normalizer of* H. Moreover, we know that

- H is a normal subgroup of the group $N_G(H)$, and
- $H \lhd G \iff N_G(H) = G$.

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G,

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation.

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$xH \in S_0$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$xH \in S_0 \iff hxH = xH, \forall h \in H$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \end{aligned}$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x^{-1}Hx = H \text{ (because } |H| = |x^{-1}Hx| < \infty) \end{aligned}$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x^{-1}Hx = H (\text{because } |H| = |x^{-1}Hx| < \infty) \end{aligned}$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x^{-1}Hx = H (\text{because } |H| = |x^{-1}Hx| < \infty) \\ &\iff x \in N_G(H). \end{aligned}$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x^{-1}Hx = H (\text{because } |H| = |x^{-1}Hx| < \infty) \\ &\iff x \in N_G(H). \end{aligned}$$

Hence $|S_0|$ is the number of left cosets xH with $x \in N_G(H)$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x^{-1}Hx = H (\text{because } |H| = |x^{-1}Hx| < \infty) \\ &\iff x \in N_G(H). \end{aligned}$$

Hence $|S_0|$ is the number of left cosets xH with $x \in N_G(H)$ and that is $|S_0| = [N_G(H) : H]$.

p-subgroups of a Finite Group

Lemma (5.5). If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x^{-1}Hx = H (\text{because } |H| = |x^{-1}Hx| < \infty) \\ &\iff x \in N_G(H). \end{aligned}$$

Hence $|S_0|$ is the number of left cosets xH with $x \in N_G(H)$ and that is $|S_0| = [N_G(H) : H]$. Since $|H|$ is a power of p,

p-subgroups of a Finite Group

Lemma (5.5). If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Proof. Let S be the set of left cosets of H in G and let H act on S by left translation. Then $|S| = [G : H]$ and

$$\begin{aligned} xH \in S_0 &\iff hxH = xH, \forall h \in H \\ &\iff x^{-1}hx \in H, \forall h \in H \\ &\iff x^{-1}Hx = H (\text{because } |H| = |x^{-1}Hx| < \infty) \\ &\iff x \in N_G(H). \end{aligned}$$

Hence $|S_0|$ is the number of left cosets xH with $x \in N_G(H)$ and that is $|S_0| = [N_G(H) : H]$. Since $|H|$ is a power of p, by Lemma (5.1),

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \pmod{p}.$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that $p \mid [G : H]$,

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.

Proof. By Lemma (5.5),

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.

Proof. By Lemma (5.5),

$$[N_G(H) : H] \equiv [G : H] \pmod{p}$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.

Proof. By Lemma (5.5),

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.

Proof. By Lemma (5.5),

$$[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$$
$$\Longrightarrow \quad [N_G(H) : H] \geq p$$

p-subgroups of a Finite Group

Lemma (5.5)**.** If H is a p-subgroup of a finite group G, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

Corollary (5.6)**.** If H is a p-subgroup of a finite group G such that $p \mid [G : H]$, then $N_G(H) \neq H$.

Proof. By Lemma (5.5),

$$\begin{aligned} & [N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p} \\ \Longrightarrow \quad & [N_G(H) : H] \geq p \\ \Longrightarrow \quad & H \lneq N_G(H). \end{aligned}$$

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$, by Lemma (5.5),

First Sylow Theorem

Theorem (5.7). Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5),

Lemma (5.5). If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

First Sylow Theorem

Theorem (5.7). Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \Big| [N_G(H) : H]$.

Lemma (5.5). If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \Big| [N_G(H) : H]$. Then $p \Big| |N_G(H)/H|$.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \big| [N_G(H) : H]$. Then $p \big| |N_G(H)/H|$. By Cauchy's Theorem,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \Big| [N_G(H) : H]$. Then $p \Big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \Big| [N_G(H) : H]$. Then $p \Big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12),

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \big| [N_G(H) : H]$. Then $p \big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \big| [N_G(H) : H]$. Then $p \big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \Big| [N_G(H) : H]$. Then $p \Big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$,

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \Big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \Big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \Big| [N_G(H) : H]$. Then $p \Big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, $H \lhd H_1$.

First Sylow Theorem

Theorem (5.7)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \big| [N_G(H) : H]$. Then $p \big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, $H \lhd H_1$. Moreover,

First Sylow Theorem

Theorem (5.7). Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \big| [N_G(H) : H]$. Then $p \big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, $H \lhd H_1$. Moreover, $|H_1| = |H||H_1/H|$

First Sylow Theorem

Theorem (5.7). Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \big| [N_G(H) : H]$. Then $p \big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, $H \lhd H_1$. Moreover, $|H_1| = |H||H_1/H| = p^i p = p^{i+1}$.

First Sylow Theorem

Theorem (5.7). Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of order p^i with $i < n$ is normal in some subgroup of order p^{i+1}.

Proof. Since $p \big| |G|$, by Cauchy's Theorem, G contains an element a of order p. Thus G contains a subgroup $\langle a \rangle$ of order p. Let H be a subgroup of order p^i with $1 \leq i < n$. Since $p \big| p^{n-i} m = [G : H]$, by Lemma (5.5), we have $p \big| [N_G(H) : H]$. Then $p \big| |N_G(H)/H|$. By Cauchy's Theorem, $N_G(H)/H$ contains a subgroup of order p. By Corollary (I.5.12), this subgroup is of the form H_1/H, where H_1 is a subgroup of $N_G(H)$ containing H. Since $H \lhd N_G(H)$, $H \lhd H_1$. Moreover, $|H_1| = |H||H_1/H| = p^i p = p^{i+1}$. The proof is complete since $i = 1, 2, \ldots, n-1$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime)

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group}$$

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

- Sylow p-subgroups always exists,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

- Sylow p-subgroups always exists, though they may be trivial,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

- Sylow p-subgroups always exists, though they may be trivial, and every p-subgroup is contained in a Sylow p-subgroup.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

- Sylow p-subgroups always exists, though they may be trivial, and every p-subgroup is contained in a Sylow p-subgroup. *(For the case of finite groups, this statement is clear*

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

- Sylow p-subgroups always exists, though they may be trivial, and every p-subgroup is contained in a Sylow p-subgroup. *(For the case of finite groups, this statement is clear since there are only finitely many subgroups in a finite group.*

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

- Sylow p-subgroups always exists, though they may be trivial, and every p-subgroup is contained in a Sylow p-subgroup. *(For the case of finite groups, this statement is clear since there are only finitely many subgroups in a finite group. However, Zorn's Lemma is needed to show this statement for the case of infinite groups.)*

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Remark. Let p be a prime number.

- Sylow p-subgroups always exists, though they may be trivial, and every p-subgroup is contained in a Sylow p-subgroup. *(For the case of finite groups, this statement is clear since there are only finitely many subgroups in a finite group. However, Zorn's Lemma is needed to show this statement for the case of infinite groups.)*
- Theorem (5.7) shows that a finite group G has a nontrivial Sylow p-subgroup for every prime p that divides $|G|$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of G

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$. Hence, if $|H| = p^n$,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$. Hence, if $|H| = p^n$, then H has the maximal possible order among all p-subgroups,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$. Hence, if $|H| = p^n$, then H has the maximal possible order among all p-subgroups, and so H is a maximal p-subgroup of G,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$. Hence, if $|H| = p^n$, then H has the maximal possible order among all p-subgroups, and so H is a maximal p-subgroup of G, i.e., H is a Sylow p-subgroup of G.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$. Hence, if $|H| = p^n$, then H has the maximal possible order among all p-subgroups, and so H is a maximal p-subgroup of G, i.e., H is a Sylow p-subgroup of G. Conversely, if $|H| = p^i$ and $i \neq n$,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$. Hence, if $|H| = p^n$, then H has the maximal possible order among all p-subgroups, and so H is a maximal p-subgroup of G, i.e., H is a Sylow p-subgroup of G. Conversely, if $|H| = p^i$ and $i \neq n$, then by the First Sylow Theorem, H is contained in a subgroup of order p^{i+1}

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

Proof. Note that every p-subgroup K of G has order p^i for some $0 \leq i \leq n$. Hence, if $|H| = p^n$, then H has the maximal possible order among all p-subgroups, and so H is a maximal p-subgroup of G, i.e., H is a Sylow p-subgroup of G. Conversely, if $|H| = p^i$ and $i \neq n$, then by the First Sylow Theorem, H is contained in a subgroup of order p^{i+1} and so H is not a Sylow p-subgroup.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

Proof. Suppose K is a conjugate of a Sylow p-subgroup P.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

Proof. Suppose K is a conjugate of a Sylow p-subgroup P. Then $K = gPg^{-1}$ for some $g \in G$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

Proof. Suppose K is a conjugate of a Sylow p-subgroup P. Then $K = gPg^{-1}$ for some $g \in G$. Note that $|K| = |gPg^{-1}| = |P|$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

Proof. Suppose K is a conjugate of a Sylow p-subgroup P. Then $K = gPg^{-1}$ for some $g \in G$. Note that $|K| = |gPg^{-1}| = |P|$. Hence, by (i), $|K| = |P| = p^n$

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

Proof. Suppose K is a conjugate of a Sylow p-subgroup P. Then $K = gPg^{-1}$ for some $g \in G$. Note that $|K| = |gPg^{-1}| = |P|$. Hence, by (i), $|K| = |P| = p^n$ and so K is also a Sylow p-subgroup.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Proof. By (ii), gPg^{-1} is also a Sylow p-subgroup of G, for all $g \in G$.

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Proof. By (ii), gPg^{-1} is also a Sylow p-subgroup of G, for all $g \in G$. Since there is only one Sylow p-subgroup,

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Proof. By (ii), gPg^{-1} is also a Sylow p-subgroup of G, for all $g \in G$. Since there is only one Sylow p-subgroup, $gPg^{-1} = P$ for all $g \in G$

Sylow p-subgroups

Definition. A subgroup P of a group G is said to be a *Sylow p-subgroup* (p prime) if P is a maximal p-subgroup of G, i.e.,

$$P \leq H \leq G \text{ with } H \text{ a } p\text{-group} \implies P = H.$$

Corollary (5.8)**.** Let G be a group of order $p^n m$ with p prime, $n \geq 1$, and $gcd(m, p) = 1$. Let H be a p-subgroup of G.

(i) H is a Sylow p-subgroup of $G \iff |H| = p^n$.

(ii) Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup.

(iii) If there is only one Sylow p-subgroup P, then P is normal in G.

Proof. By (ii), gPg^{-1} is also a Sylow p-subgroup of G, for all $g \in G$. Since there is only one Sylow p-subgroup, $gPg^{-1} = P$ for all $g \in G$ and so P is normal in G.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G,

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular,

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group,

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$,

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$,

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0$$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H$$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$
$$\implies x^{-1}Hx \leq P$$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$
$$\implies x^{-1}Hx \leq P \implies H \leq xPx^{-1}.$$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$
$$\implies x^{-1}Hx \leq P \implies H \leq xPx^{-1}.$$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$
$$\implies x^{-1}Hx \leq P \implies H \leq xPx^{-1}.$$

If H is a Sylow p-subgroup,

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$
$$\implies x^{-1}Hx \leq P \implies H \leq xPx^{-1}.$$

If H is a Sylow p-subgroup, then $|H| = |P| = |xPx^{-1}|$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$
$$\implies x^{-1}Hx \leq P \implies H \leq xPx^{-1}.$$

If H is a Sylow p-subgroup, then $|H| = |P| = |xPx^{-1}|$ and so $H = xPx^{-1}$,

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Proof. Let S be the set of left cosets of P in G and let H act on S by left translation. Since H is a p-group, by Lemma (5.1), $|S_0| \equiv |S| = [G : P] \pmod{p}$. However, $p \nmid [G : P]$, so $|S_0| \neq 0$, i.e., $S_0 \neq \varnothing$. Then $\exists xP \in S_0$. Note that

$$xP \in S_0 \implies hxP = xP, \forall h \in H \implies x^{-1}hx \in P, \forall h \in H$$
$$\implies x^{-1}Hx \leq P \implies H \leq xPx^{-1}.$$

If H is a Sylow p-subgroup, then $|H| = |P| = |xPx^{-1}|$ and so $H = xPx^{-1}$, i.e., H and P are conjugate.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G \iff P$ is the only Sylow p-subgroup of G.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G \iff P$ is the only Sylow p-subgroup of G.

Proof. In Corollary (5.8, (iii)), we have seen that if P is the only Sylow p-subgroup of G, then P is normal in G.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G \iff P$ is the only Sylow p-subgroup of G.

Proof. In Corollary (5.8, (iii)), we have seen that if P is the only Sylow p-subgroup of G, then P is normal in G. Conversely, assume $P \lhd G$ and let Q be a Sylow p-subgroup of G.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G \iff P$ is the only Sylow p-subgroup of G.

Proof. In Corollary (5.8, (iii)), we have seen that if P is the only Sylow p-subgroup of G, then P is normal in G. Conversely, assume $P \lhd G$ and let Q be a Sylow p-subgroup of G. By the Second Sylow Theorem, $Q = gPg^{-1}$ for some $g \in G$.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G \iff P$ is the only Sylow p-subgroup of G.

Proof. In Corollary (5.8, (iii)), we have seen that if P is the only Sylow p-subgroup of G, then P is normal in G. Conversely, assume $P \lhd G$ and let Q be a Sylow p-subgroup of G. By the Second Sylow Theorem, $Q = gPg^{-1}$ for some $g \in G$. Since $P \lhd G$, $gPg^{-1} = P$

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G \iff P$ is the only Sylow p-subgroup of G.

Proof. In Corollary (5.8, (iii)), we have seen that if P is the only Sylow p-subgroup of G, then P is normal in G. Conversely, assume $P \lhd G$ and let Q be a Sylow p-subgroup of G. By the Second Sylow Theorem, $Q = gPg^{-1}$ for some $g \in G$. Since $P \lhd G$, $gPg^{-1} = P$ and so $Q = P$.

Second Sylow Theorem

Theorem (5.9, Second Sylow Theorem)**.** If H is a p-subgroup of a finite group G and if P is any Sylow p-subgroup of G, then $\exists x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.

Remark. If P is a Sylow p-subgroup of a finite group G, then $P \lhd G \iff P$ is the only Sylow p-subgroup of G.

Proof. In Corollary (5.8, (iii)), we have seen that if P is the only Sylow p-subgroup of G, then P is normal in G. Conversely, assume $P \lhd G$ and let Q be a Sylow p-subgroup of G. By the Second Sylow Theorem, $Q = gPg^{-1}$ for some $g \in G$. Since $P \lhd G$, $gPg^{-1} = P$ and so $Q = P$. Hence P is the only Sylow p-subgroup of G.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime,

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. The Second Sylow Theorem tells us that every Sylow p-subgroup is conjugate to P.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. The Second Sylow Theorem tells us that every Sylow p-subgroup is conjugate to P. Hence, by Corollary (4.4) (iii),

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. The Second Sylow Theorem tells us that every Sylow p-subgroup is conjugate to P. Hence, by Corollary (4.4) (iii),

Corollary (4.4 (iii))**.** Let G be a finite group and let K be a subgroup of G. The number of subgroups of G conjugate to K is $[G : N_G(K)]$, which divides $|G|$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. The Second Sylow Theorem tells us that every Sylow p-subgroup is conjugate to P. Hence, by Corollary (4.4) (iii), the number of Sylow p-subgroup of G is $[G : N_G(P)]$, which divides $|G|$.

Corollary (4.4 (iii))**.** Let G be a finite group and let K be a subgroup of G. The number of subgroups of G conjugate to K is $[G : N_G(K)]$, which divides $|G|$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. The Second Sylow Theorem tells us that every Sylow p-subgroup is conjugate to P. Hence, by Corollary (4.4) (iii), the number of Sylow p-subgroup of G is $[G : N_G(P)]$, which divides $|G|$.

Corollary (4.4 (iii))**.** Let G be a finite group and let K be a subgroup of G. The number of subgroups of G conjugate to K is $[G : N_G(K)]$, which divides $|G|$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0$

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P$

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G,

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.)

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem,

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$. However, because $y \in N_G(Q)$,

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$. However, because $y \in N_G(Q)$, $yQy^{-1} = Q$

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$. However, because $y \in N_G(Q)$, $yQy^{-1} = Q$ and so $Q = P$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$. However, because $y \in N_G(Q)$, $yQy^{-1} = Q$ and so $Q = P$. Therefore, $S_0 = \{P\}$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$. However, because $y \in N_G(Q)$, $yQy^{-1} = Q$ and so $Q = P$. Therefore, $S_0 = \{P\}$. Since P is a p-group,

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$. However, because $y \in N_G(Q)$, $yQy^{-1} = Q$ and so $Q = P$. Therefore, $S_0 = \{P\}$. Since P is a p-group, by Lemma (5.1), $|S| \equiv |S_0| = 1 \pmod{p}$.

Third Sylow Theorem

Theorem (5.10, Third Sylow Theorem)**.** If G is a finite group and p is a prime, then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

Proof. Let P be a Sylow p-subgroup of G. Let S be the set of Sylow p-subgroups of G and let P act on S by conjugation. Note that $Q \in S_0 \iff xQx^{-1} = Q, \forall x \in P \iff P \leq N_G(Q)$. Since P and Q are both Sylow p-subgroups of G, P and Q are Sylow p-subgroups of $N_G(Q)$. (This is because the power of p in $|G|$ and $|N_G(Q)|$ are the same.) By the Second Sylow Theorem, $\exists y \in N_G(Q)$ such that $P = yQy^{-1}$. However, because $y \in N_G(Q)$, $yQy^{-1} = Q$ and so $Q = P$. Therefore, $S_0 = \{P\}$. Since P is a p-group, by Lemma (5.1), $|S| \equiv |S_0| = 1 \pmod{p}$. Hence $|S| = kp+1$ for some $k \in \mathbb{N} \cup \{0\}$.

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G,

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$.

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers,

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$.

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G,

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N.

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

$$x \in N_G(N)$$

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

$$x \in N_G(N) \implies xNx^{-1} = N$$

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

$$x \in N_G(N) \implies xNx^{-1} = N \implies xPx^{-1} \leq N$$

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

$$x \in N_G(N) \implies xNx^{-1} = N \implies xPx^{-1} \leq N$$
$$\implies xPx^{-1} = P$$

Because P is the only Sylow p-subgroup of N

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

$$x \in N_G(N) \implies xNx^{-1} = N \implies xPx^{-1} \leq N$$
$$\implies xPx^{-1} = P \implies x \in N_G(P) = N$$

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

$$x \in N_G(N) \implies xNx^{-1} = N \implies xPx^{-1} \leq N$$
$$\implies xPx^{-1} = P \implies x \in N_G(P) = N$$

Therefore, $N_G(N) \leq N$

Theorem (5.11)

If P is a Sylow p-subgroup of a finite group G, then

$$N_G\big(N_G(P)\big) = N_G(P).$$

Proof. Let $N = N_G(P)$. By the definition of normalizers, we know that $P \leq N \leq N_G(N)$. Since $P \lhd N$ and since P is a Sylow p-subgroup of G, P is the only Sylow p-subgroup of N. Note that

$$\begin{aligned} x \in N_G(N) &\implies xNx^{-1} = N \implies xPx^{-1} \leq N \\ &\implies xPx^{-1} = P \implies x \in N_G(P) = N \end{aligned}$$

Therefore, $N_G(N) \leq N$ and thus $N_G\big(N_G(P)\big) = N_G(P)$.

Exercise for Section II.5

1, 6, 7, 8, 9, 10, 11, 13.