Modern Algebra I

Lecture 14

Jung-Chen Liu

liujc@math.ntnu.edu.tw

2009, Fall

Chapter II

The Structure of Groups

Chapter II

The Structure of Groups

Section II.6: Classification of Finite Groups

Chapter II

The Structure of Groups

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15)

Chapter II

The Structure of Groups

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Chapter II

The Structure of Groups

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

Chapter II

THE STRUCTURE OF GROUPS

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

- if $|G| = p$ is a prime,

Chapter II

THE STRUCTURE OF GROUPS

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

- if $|G| = p$ is a prime, then $G \cong \mathbb{Z}_p$;

Chapter II

The Structure of Groups

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

- if $|G| = p$ is a prime, then $G \cong \mathbb{Z}_p$;
- if $|G| = p^2$ for some prime p,

Chapter II

THE STRUCTURE OF GROUPS

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

- if $|G| = p$ is a prime, then $G \cong \mathbb{Z}_p$;
- if $|G| = p^2$ for some prime p, then G is abelian;

Chapter II

THE STRUCTURE OF GROUPS

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

- if $|G| = p$ is a prime, then $G \cong \mathbb{Z}_p$;
- if $|G| = p^2$ for some prime p, then G is abelian; by the Fundamental Theorem of Finitely Generated Abelian Groups,

Chapter II

The Structure of Groups

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

- if $|G| = p$ is a prime, then $G \cong \mathbb{Z}_p$;
- if $|G| = p^2$ for some prime p, then G is abelian; by the Fundamental Theorem of Finitely Generated Abelian Groups, $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$;

Chapter II

The Structure of Groups

Section II.6: Classification of Finite Groups

In this section, we shall classify all groups of smaller orders (≤ 15) and all groups of order pq with p, q prime.

Last week, we used the following observations

- if $|G| = p$ is a prime, then $G \cong \mathbb{Z}_p$;
- if $|G| = p^2$ for some prime p, then G is abelian; by the Fundamental Theorem of Finitely Generated Abelian Groups, $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$;

and got

Order	*Distinct Groups*
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Order	*Distinct Groups*
13	
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Order	*Distinct Groups*
13	
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Order	*Distinct Groups*
13	
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	
5	
6	
7	
8	
9	
10	
11	
12	

Order	*Distinct Groups*
13	
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	
5	$\mathbb{Z}_5$
6	
7	
8	
9	
10	
11	
12	

Order	*Distinct Groups*
13	
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	
5	$\mathbb{Z}_5$
6	
7	$\mathbb{Z}_7$
8	
9	
10	
11	
12	

Order	*Distinct Groups*
13	
14	
15	

Order	*Distinct Groups*	*Order*	*Distinct Groups*
1	$\langle e \rangle$	13	
2	$\mathbb{Z}_2$	14	
3	$\mathbb{Z}_3$	15	
4			
5	$\mathbb{Z}_5$		
6			
7	$\mathbb{Z}_7$		
8			
9			
10			
11	$\mathbb{Z}_{11}$		
12			

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	
5	$\mathbb{Z}_5$
6	
7	$\mathbb{Z}_7$
8	
9	
10	
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	
7	$\mathbb{Z}_7$
8	
9	
10	
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	
11	$\mathbb{Z}_{11}$
12	
13	$\mathbb{Z}_{13}$
14	
15	

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Note that the number of Sylow q-subgroup of G is of the form $kq + 1$ with $kq + 1 \mid p$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Note that the number of Sylow q-subgroup of G is of the form $kq + 1$ with $kq + 1 \mid p$. Since $p < q$,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Note that the number of Sylow q-subgroup of G is of the form $kq + 1$ with $kq + 1 \mid p$. Since $p < q$, $kq + 1 = 1$,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Note that the number of Sylow q-subgroup of G is of the form $kq + 1$ with $kq + 1 \mid p$. Since $p < q$, $kq + 1 = 1$, i.e., Q is the unique Sylow q-subgroup of G

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Note that the number of Sylow q-subgroup of G is of the form $kq + 1$ with $kq + 1 \mid p$. Since $p < q$, $kq + 1 = 1$, i.e., Q is the unique Sylow q-subgroup of G and so Q is a normal subgroup of G.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- Similarly, since the number of Sylow p-subgroup of G is of the form $kp + 1$ with $kp + 1 \mid q$

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- Similarly, since the number of Sylow p-subgroup of G is of the form $kp + 1$ with $kp + 1 \mid q$ and since q is a prime number,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- Similarly, since the number of Sylow p-subgroup of G is of the form $kp + 1$ with $kp + 1 \mid q$ and since q is a prime number, $kp + 1 = 1$ or q.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- Similarly, since the number of Sylow p-subgroup of G is of the form $kp + 1$ with $kp + 1 \mid q$ and since q is a prime number, $kp + 1 = 1$ or q. However, we have $p \nmid q - 1$,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- Similarly, since the number of Sylow p-subgroup of G is of the form $kp + 1$ with $kp + 1 \mid q$ and since q is a prime number, $kp + 1 = 1$ or q. However, we have $p \nmid q - 1$, so $kp + 1 = 1$,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- Similarly, since the number of Sylow p-subgroup of G is of the form $kp + 1$ with $kp + 1 \mid q$ and since q is a prime number, $kp + 1 = 1$ or q. However, we have $p \nmid q - 1$, so $kp + 1 = 1$, i.e., P is the unique Sylow p-subgroup of G,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- Similarly, since the number of Sylow p-subgroup of G is of the form $kp + 1$ with $kp + 1 \mid q$ and since q is a prime number, $kp + 1 = 1$ or q. However, we have $p \nmid q - 1$, so $kp + 1 = 1$, i.e., P is the unique Sylow p-subgroup of G, thus P is a normal subgroup of G.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- Since p and q are relatively prime,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- Since p and q are relatively prime, $P \cap Q = \{e\}$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- Moreover, $|PQ| = \frac{|P||Q|}{|P \cap Q|}$

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- Moreover, $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq$

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- Moreover, $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|$

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- Moreover, $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|$ and so $PQ = G$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- $PQ = G$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- $PQ = G$.

Hence $G \cong P \times Q$

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- $PQ = G$.

Hence $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q$

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Proof. Let P be a Sylow p-subgroup of G and let Q be a Sylow q-subgroup of G.

- Q is a normal subgroup of G.
- P is a normal subgroup of G.
- $P \cap Q = \{e\}$.
- $PQ = G$.

Hence $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ is cyclic.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Since $15 = 3 \cdot 5$ and since $3 < 5$ are primes that satisfy the condition in the above lemma,

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Since $15 = 3 \cdot 5$ and since $3 < 5$ are primes that satisfy the condition in the above lemma, we know that if G is a group of order 15

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Since $15 = 3 \cdot 5$ and since $3 < 5$ are primes that satisfy the condition in the above lemma, we know that if G is a group of order 15 then $G \cong \mathbb{Z}_{15}$.

Groups of Order 15

Next, for groups of order 15, we proved the following lemma.

Lemma. Let G be a group of order pq, where $p < q$ are primes with $p \nmid q - 1$. Then $G \cong \mathbb{Z}_{pq}$.

Since $15 = 3 \cdot 5$ and since $3 < 5$ are primes that satisfy the condition in the above lemma, we know that if G is a group of order 15 then $G \cong \mathbb{Z}_{15}$. Hence we have

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	
11	$\mathbb{Z}_{11}$
12	
13	$\mathbb{Z}_{13}$
14	
15	

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	
11	$\mathbb{Z}_{11}$
12	
13	$\mathbb{Z}_{13}$
14	
15	$\mathbb{Z}_{15}$

Order $2p$ with Odd Prime p

Review: Dihedral Groups

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \leq i \leq \lfloor \frac{n-1}{2} \rfloor} (i, n + 2 - i)$

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n + 2 - i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n + 2 - i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $a^n = e$;

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $a^n = e$; $b^2 = e$;

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $a^n = e$; $b^2 = e$; if $0 < k < n$, $a^k \neq e$.

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $a^n = e$; $b^2 = e$; if $0 < k < n$, $a^k \neq e$.

(ii) $ba = a^{-1}b$, i.e., $bab^{-1} = a^{-1}$.

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n + 2 - i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $a^n = e$; $b^2 = e$; if $0 < k < n$, $a^k \neq e$.

(ii) $ba = a^{-1}b$, i.e., $bab^{-1} = a^{-1}$.

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $a^n = e$; $b^2 = e$; if $0 < k < n$, $a^k \neq e$.

(ii) $ba = a^{-1}b$, i.e., $bab^{-1} = a^{-1}$.

Any group G which is generated by elements $a, b \in G$ satisfying (i) and (ii) for some $n \ge 3$

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $a^n = e$; $b^2 = e$; if $0 < k < n$, $a^k \neq e$.

(ii) $ba = a^{-1}b$, i.e., $bab^{-1} = a^{-1}$.

Any group G which is generated by elements $a, b \in G$ satisfying (i) and (ii) for some $n \ge 3$ is isomorphic to D_n.

Review: Dihedral Groups

Definition. The dihedral group of degree n, denoted by D_n, is the subgroup of S_n generated by $a = (1, 2, 3, \ldots, n)$ and $b = \prod_{2 \le i \le \lfloor \frac{n-1}{2} \rfloor} (i, n+2-i)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}.$$

Theorem (I.6.13)**.** For each $n \ge 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

(i) $|a| = n$ and $|b| = 2$.

(ii) $ba = a^{-1}b$, i.e., $bab^{-1} = a^{-1}$.

Any group G which is generated by elements $a, b \in G$ satisfying (i) and (ii) for some $n \ge 3$ is isomorphic to D_n.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.

Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$, by Cauchy's Theorem.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- Because 2 and p are relatively prime, $P \cap Q = \{e\}$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- Because 2 and p are relatively prime, $P \cap Q = \{e\}$. Hence, we have $|PQ| = \frac{|P||Q|}{|P \cap Q|} = 2p = |G|$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- Because 2 and p are relatively prime, $P \cap Q = \{e\}$. Hence, we have $|PQ| = \frac{|P||Q|}{|P \cap Q|} = 2p = |G|$ and so $G = PQ$,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- Because 2 and p are relatively prime, $P \cap Q = \{e\}$. Hence, we have $|PQ| = \frac{|P||Q|}{|P \cap Q|} = 2p = |G|$ and so $G = PQ$, i.e., $G = \langle a, b \rangle$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- Because $p > 2$, we know that P is the unique Sylow p-subgroup of G

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- Because $p > 2$, we know that P is the unique Sylow p-subgroup of G and so P is a normal subgroup of G.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p - 1$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p - 1$. Note that

$$bab^{-1} = a^r \implies a = b^{-1}a^r b$$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

$$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r$$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r$$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r$$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

  and this implies $a^{r^2-1} = e$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

  and this implies $a^{r^2-1} = e$. Thus $p \mid r^2 - 1$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

  and this implies $a^{r^2-1} = e$. Thus $p \mid r^2 - 1 = (r+1)(r-1)$,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

  and this implies $a^{r^2-1} = e$. Thus $p \mid r^2 - 1 = (r+1)(r-1)$, and so $p \mid r+1$ or $p \mid r-1$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

  and this implies $a^{r^2-1} = e$. Thus $p \mid r^2 - 1 = (r+1)(r-1)$, and so $p \mid r+1$ or $p \mid r-1$. Since $0 \leq r \leq p-1$,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- Since P is a normal subgroup of G, $bab^{-1} \in P$ and so $bab^{-1} = a^r$ for some r with $0 \leq r \leq p-1$. Note that

  $$bab^{-1} = a^r \implies a = b^{-1}a^r b = (b^{-1}ab)^r.$$

  Moreover, since $b^2 = e$, we have

  $$a = (b^{-1}ab)^r = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

  and this implies $a^{r^2-1} = e$. Thus $p \mid r^2 - 1 = (r+1)(r-1)$, and so $p \mid r+1$ or $p \mid r-1$. Since $0 \leq r \leq p-1$, $r = p-1$ or 1.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian. Hence P and Q are both normal subgroups of G with $P \cap Q = \{e\}$ and $G = PQ$,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian. Hence P and Q are both normal subgroups of G with $P \cap Q = \{e\}$ and $G = PQ$, so $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian. Hence P and Q are both normal subgroups of G with $P \cap Q = \{e\}$ and $G = PQ$, so $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.
  - If $r = p - 1$, i.e., $bab^{-1} = a^{p-1}$

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian. Hence P and Q are both normal subgroups of G with $P \cap Q = \{e\}$ and $G = PQ$, so $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.
  - If $r = p - 1$, i.e., $bab^{-1} = a^{p-1} = a^{-1}$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian. Hence P and Q are both normal subgroups of G with $P \cap Q = \{e\}$ and $G = PQ$, so $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.
  - If $r = p - 1$, i.e., $bab^{-1} = a^{p-1} = a^{-1}$. Since $G = \langle a, b \rangle$,

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian. Hence P and Q are both normal subgroups of G with $P \cap Q = \{e\}$ and $G = PQ$, so $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.
  - If $r = p - 1$, i.e., $bab^{-1} = a^{p-1} = a^{-1}$. Since $G = \langle a, b \rangle$, $G \cong D_p$.

Order $2p$ with Odd Prime p

Let p be an odd prime and let G be a group of order $2p$.
Then $\exists a \in G$ with $|a| = p$ and $\exists b \in G$ with $|b| = 2$.
Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

- $P \cap Q = \{e\}$ and $G = PQ = \langle a, b \rangle$.
- P is a normal subgroup of G.
- $bab^{-1} = a^r$ with $r = p - 1$ or 1.
  - If $r = 1$, i.e., $bab^{-1} = a$, then $ba = ab$ and so $G = \langle a, b \rangle$ is abelian. Hence P and Q are both normal subgroups of G with $P \cap Q = \{e\}$ and $G = PQ$, so $G \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$.
  - If $r = p - 1$, i.e., $bab^{-1} = a^{p-1} = a^{-1}$. Since $G = \langle a, b \rangle$, $G \cong D_p$.

Therefore, we have

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	
11	$\mathbb{Z}_{11}$
12	
13	$\mathbb{Z}_{13}$
14	
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	
13	$\mathbb{Z}_{13}$
14	
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

The Quaternion Group Q_8

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Note that A, A^{-1}, B, B^{-1} all have order 4,

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Note that A, A^{-1}, B, B^{-1} all have order 4, so Q_8 has at least four elements of order 4.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Note that A, A^{-1}, B, B^{-1} all have order 4, so Q_8 has at least four elements of order 4. Recall that D_4 has only two elements of order 4.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Note that A, A^{-1}, B, B^{-1} all have order 4, so Q_8 has at least four elements of order 4. Recall that D_4 has only two elements of order 4. Hence D_4 and Q_8 are not isomorphic.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Moreover, if G is a group generated by two elements a, b such that $|a| = |b| = 4$, $a^2 = b^2$, and $ba = a^3b$, then G is isomorphic to the quaternion group Q_8.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Moreover, if G is a group generated by two elements a, b such that $|a| = |b| = 4$, $a^2 = b^2$, and $ba = a^3b$, then G is isomorphic to the quaternion group Q_8.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Moreover, if G is a group generated by two elements a, b such that $|a| = |b| = 4$, $a^2 = b^2$, and $ba = a^3b$, then G is isomorphic to the quaternion group Q_8.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Moreover, if G is a group generated by two elements a, b such that $|a| = |b| = 4$, $a^2 = b^2$, and $ba = a^3b$, then G is isomorphic to the quaternion group Q_8.

The Quaternion Group Q_8

Definition. The quaternion group Q_8 is the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Remark. Last week, we have shown

- $A^2 = B^2 = -I$ and $A^4 = B^4 = I$.
- $BA = A^3B$.
- $Q_8 = \{A^j B^k \mid 0 \leq j \leq 3, \text{ and } 0 \leq k \leq 1\}$ is a group of order 8 and Q_8 is not isomorphic to D_4.

Moreover, if G is a group generated by two elements a, b such that $|a| = |b| = 4$, $a^2 = b^2$, and $ba = a^3b$, then G is isomorphic to the quaternion group Q_8.

Groups of Order 8

Let G be a group of order 8.

Groups of Order 8

Let G be a group of order 8.

- If G is abelian,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic.

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic. Last week, we have shown that if G is a nonabelian group,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic. Last week, we have shown that if G is a nonabelian group, then $G \cong D_4$ or Q_8.

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic. Last week, we have shown that if G is a nonabelian group, then $G \cong D_4$ or Q_8. More precisely, we showed

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic. Last week, we have shown that if G is a nonabelian group, then $G \cong D_4$ or Q_8. More precisely, we showed

Proposition (6.3)**.** Up to isomorphism,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic. Last week, we have shown that if G is a nonabelian group, then $G \cong D_4$ or Q_8. More precisely, we showed

Proposition (6.3)**.** Up to isomorphism, there are exactly two distinct nonabelian groups of order 8,

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic. Last week, we have shown that if G is a nonabelian group, then $G \cong D_4$ or Q_8. More precisely, we showed

Proposition (6.3)**.** Up to isomorphism, there are exactly two distinct nonabelian groups of order 8, namely the dihedral group D_4

Groups of Order 8

Let G be a group of order 8.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, or $\mathbb{Z}_8$.
- On the other hand, we already know two nonabelian groups of order 8, namely D_4 and Q_8, and they are not isomorphic. Last week, we have shown that if G is a nonabelian group, then $G \cong D_4$ or Q_8. More precisely, we showed

Proposition (6.3)**.** Up to isomorphism, there are exactly two distinct nonabelian groups of order 8, namely the dihedral group D_4 and the quaternion group Q_8.

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2,$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,\ D_4$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Groups of Order 12

Let G be a group of order 12.

Groups of Order 12

Let G be a group of order 12.

- If G is abelian,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic, (because D_6 has an element of order 6 while A_4 has no elements of order 6).

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic, (because D_6 has an element of order 6 while A_4 has no elements of order 6).

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic, (because D_6 has an element of order 6 while A_4 has no elements of order 6).

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \left((1,2,3), \overline{2}\right)$ and $\left((1,2), \overline{1}\right)$, which is not isomorphic to either A_4 or D_6.

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6.

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6. We also showed that if G is a group generated by $\alpha, \beta \in G$ satisfying $|\alpha| = 6$, $\alpha^3 = \beta^2$, and $\beta\alpha = \alpha^{-1}\beta$,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6. We also showed that if G is a group generated by $\alpha, \beta \in G$ satisfying $|\alpha| = 6$, $\alpha^3 = \beta^2$, and $\beta\alpha = \alpha^{-1}\beta$,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6. We also showed that if G is a group generated by $\alpha, \beta \in G$ satisfying $|\alpha| = 6$, $\alpha^3 = \beta^2$, and $\beta\alpha = \alpha^{-1}\beta$,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6. We also showed that if G is a group generated by $\alpha, \beta \in G$ satisfying $|\alpha| = 6$, $\alpha^3 = \beta^2$, and $\beta\alpha = \alpha^{-1}\beta$,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6. We also showed that if G is a group generated by $\alpha, \beta \in G$ satisfying $|\alpha| = 6$, $\alpha^3 = \beta^2$, and $\beta\alpha = \alpha^{-1}\beta$, then $G \cong T$.

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6. We also showed that if G is a group generated by $\alpha, \beta \in G$ satisfying $|\alpha| = 6$, $\alpha^3 = \beta^2$, and $\beta\alpha = \alpha^{-1}\beta$, then $G \cong T$.
- Next, we will show in Proposition (6.4) that if G is a nonabelian group,

Groups of Order 12

Let G be a group of order 12.

- If G is abelian, then by the Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6$, or $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12}$.
- On the other hand, we already know two nonabelian groups of order 12, namely A_4 and D_6, and they are not isomorphic. Last week, we constructed a nonabelian T of order 12, the subgroup of $S_3 \times \mathbb{Z}_4$ generated by $a = \big((1,2,3), \overline{2}\big)$ and $\big((1,2), \overline{1}\big)$, which is not isomorphic to either A_4 or D_6. We also showed that if G is a group generated by $\alpha, \beta \in G$ satisfying $|\alpha| = 6$, $\alpha^3 = \beta^2$, and $\beta\alpha = \alpha^{-1}\beta$, then $G \cong T$.
- Next, we will show in Proposition (6.4) that if G is a nonabelian group, then $G \cong A_4$, D_6, or T.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. We will show that G is isomorphic to A_4, D_6, or T.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8),

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8),

Proposition (4.8)**.** Let H be a subgroup of a group G

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8),

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8),

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\mathrm{Ker}\,\phi \subseteq P$.

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\mathrm{Ker}\,\phi \subseteq P$. Since $|P| = 3$,

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\operatorname{Ker} \phi \subseteq P$. Since $|P| = 3$, $\operatorname{Ker} \phi = \{e\}$ or $\operatorname{Ker} \phi = P$.

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\mathrm{Ker}\,\phi \subseteq P$. Since $|P| = 3$, $\mathrm{Ker}\,\phi = \{e\}$ or $\mathrm{Ker}\,\phi = P$.

$\star$ If $\mathrm{Ker}\,\phi = \{e\}$,

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\mathrm{Ker}\,\phi \subseteq P$. Since $|P| = 3$, $\mathrm{Ker}\,\phi = \{e\}$ or $\mathrm{Ker}\,\phi = P$.

$\star$ If $\mathrm{Ker}\,\phi = \{e\}$, then ϕ is a monomorphism

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\mathrm{Ker}\,\phi \subseteq P$. Since $|P| = 3$, $\mathrm{Ker}\,\phi = \{e\}$ or $\mathrm{Ker}\,\phi = P$.

$\star$ If $\mathrm{Ker}\,\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$.

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\mathrm{Ker}\,\phi \subseteq P$. Since $|P| = 3$, $\mathrm{Ker}\,\phi = \{e\}$ or $\mathrm{Ker}\,\phi = P$.

$\star$ If $\mathrm{Ker}\,\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$.

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\mathrm{Ker}\,\phi \subseteq P$. Since $|P| = 3$, $\mathrm{Ker}\,\phi = \{e\}$ or $\mathrm{Ker}\,\phi = P$.

$\star$ If $\mathrm{Ker}\,\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$. By Theorem (I.6.8), A_4 is the unique subgroup of S_4 of index 2,

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\operatorname{Ker}\phi \subseteq P$. Since $|P| = 3$, $\operatorname{Ker}\phi = \{e\}$ or $\operatorname{Ker}\phi = P$.

$\star$ If $\operatorname{Ker}\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$. By Theorem (I.6.8), A_4 is the unique subgroup of S_4 of index 2, so $\phi(G) = A_4$ and so $G \cong A_4$.

Proposition (4.8)**.** Let H be a subgroup of a group G and let G act on the set S of all left cosets of H in G by left translation. Then the kernel of the induced homomorphism $G \to A(S)$ is contained in H.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\operatorname{Ker}\phi \subseteq P$. Since $|P| = 3$, $\operatorname{Ker}\phi = \{e\}$ or $\operatorname{Ker}\phi = P$.

- If $\operatorname{Ker}\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$. By Theorem (I.6.8), A_4 is the unique subgroup of S_4 of index 2, so $\phi(G) = A_4$ and so $G \cong A_4$.
- If $\operatorname{Ker}\phi = P$,

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\operatorname{Ker}\phi \subseteq P$. Since $|P| = 3$, $\operatorname{Ker}\phi = \{e\}$ or $\operatorname{Ker}\phi = P$.

- If $\operatorname{Ker}\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$. By Theorem (I.6.8), A_4 is the unique subgroup of S_4 of index 2, so $\phi(G) = A_4$ and so $G \cong A_4$.
- If $\operatorname{Ker}\phi = P$, then $P \lhd G$

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\operatorname{Ker}\phi \subseteq P$. Since $|P| = 3$, $\operatorname{Ker}\phi = \{e\}$ or $\operatorname{Ker}\phi = P$.

$\star$ If $\operatorname{Ker}\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$. By Theorem (I.6.8), A_4 is the unique subgroup of S_4 of index 2, so $\phi(G) = A_4$ and so $G \cong A_4$.

$\star$ If $\operatorname{Ker}\phi = P$, then $P \lhd G$ and so P is the unique Sylow 3-subgroup of G.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\operatorname{Ker}\phi \subseteq P$. Since $|P| = 3$, $\operatorname{Ker}\phi = \{e\}$ or $\operatorname{Ker}\phi = P$.

$\star$ If $\operatorname{Ker}\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$. By Theorem (I.6.8), A_4 is the unique subgroup of S_4 of index 2, so $\phi(G) = A_4$ and so $G \cong A_4$.

$\star$ If $\operatorname{Ker}\phi = P$, then $P \lhd G$ and so P is the unique Sylow 3-subgroup of G. Therefore, G contains only two elements of order 3.

Proposition (6.4)

There are, up to isomorphism, exactly three distinct nonabelian groups of order 12, namely A_4, D_6, and T.

Proof. Let G be a nonabelian group of order 12. Let P be a Sylow 3-subgroup of G. Then $|P| = 3$ and $[G : P] = 4$. By Proposition (4.8), there exists a homomorphism $\phi : G \to S_4$ such that $\operatorname{Ker}\phi \subseteq P$. Since $|P| = 3$, $\operatorname{Ker}\phi = \{e\}$ or $\operatorname{Ker}\phi = P$.

$\star$ If $\operatorname{Ker}\phi = \{e\}$, then ϕ is a monomorphism and so $G \cong \phi(G)$. Note that $\phi(G)$ is a subgroup of S_4 with $[S_4 : \phi(G)] = 2$. By Theorem (I.6.8), A_4 is the unique subgroup of S_4 of index 2, so $\phi(G) = A_4$ and so $G \cong A_4$.

$\star$ If $\operatorname{Ker}\phi = P$, then $P \lhd G$ and so P is the unique Sylow 3-subgroup of G. Therefore, G contains only two elements of order 3. Let c and $c^2 = c^{-1}$ be these two elements.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \big| |C_G(c)|$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \Big| |C_G(c)|$, so by Cauchy's Theorem, $\exists d \in C_G(c)$ such that $|d| = 2$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \Big| |C_G(c)|$, so by Cauchy's Theorem, $\exists d \in C_G(c)$ such that $|d| = 2$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \big| |C_G(c)|$, so by Cauchy's Theorem, $\exists d \in C_G(c)$ such that $|d| = 2$. Let $a = cd$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \big| |C_G(c)|$, so by Cauchy's Theorem, $\exists d \in C_G(c)$ such that $|d| = 2$. Let $a = cd$. Then $|a| = 6$, because

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \big| |C_G(c)|$, so by Cauchy's Theorem, $\exists d \in C_G(c)$ such that $|d| = 2$. Let $a = cd$. Then $|a| = 6$, because

- $cd = dc$, *since* $d \in C_G(c)$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \big| |C_G(c)|$, so by Cauchy's Theorem, $\exists d \in C_G(c)$ such that $|d| = 2$. Let $a = cd$. Then $|a| = 6$, because

- $cd = dc$, *since* $d \in C_G(c)$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- c and $c^2 = c^{-1}$ are the only two elements of order 3 in G.

Note that

- Corollary (4.4) (i) tells us that $[G : C_G(c)]$ is the number of conjugates of c in G,
- every conjugate of c has order 3.

Hence $[G : C_G(c)] \leq 2$, i.e., $[G : C_G(c)] = 1$ or 2, and so $|C_G(c)| = 12$ or 6. In either case, $2 \big| |C_G(c)|$, so by Cauchy's Theorem, $\exists d \in C_G(c)$ such that $|d| = 2$. Let $a = cd$. Then $|a| = 6$, because

- $cd = dc$, *since* $d \in C_G(c)$
- $|c| = 3$, $|d| = 2$, and $gcd(3, 2) = 1$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2.
Let $b \in G \setminus \langle a \rangle$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2.
Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2.
Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2.
Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2.
Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption. Hence $bab^{-1} = a^5 = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption. Hence $bab^{-1} = a^5 = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption. Hence $bab^{-1} = a^5 = a^{-1}$. On the other hand, because $b \in G \setminus \langle a \rangle$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption. Hence $bab^{-1} = a^5 = a^{-1}$. On the other hand, because $b \in G \setminus \langle a \rangle$ and $|G/\langle a \rangle| = 2$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption. Hence $bab^{-1} = a^5 = a^{-1}$. On the other hand, because $b \in G \setminus \langle a \rangle$ and $|G/\langle a \rangle| = 2$, $b \neq e$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption. Hence $bab^{-1} = a^5 = a^{-1}$. On the other hand, because $b \in G \setminus \langle a \rangle$ and $|G/\langle a \rangle| = 2$, $b \neq e$ and $b^2 \in \langle a \rangle$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Since $[G : \langle a \rangle] = 2$, $\langle a \rangle \lhd G$ and $G/\langle a \rangle$ is a group of order 2. Let $b \in G \setminus \langle a \rangle$. Then $G = \langle a \rangle \cup b\langle a \rangle = \langle a, b \rangle$. Since $\langle a \rangle \lhd G$, $bab^{-1} \in \langle a \rangle$. Moreover, since $|bab^{-1}| = |a| = 6$, $bab^{-1} = a$ or a^5. If $bab^{-1} = a$, then $ba = ab$ and this implies that $G = \langle a, b \rangle$ is abelian, which contradicts our assumption. Hence $bab^{-1} = a^5 = a^{-1}$. On the other hand, because $b \in G \setminus \langle a \rangle$ and $|G/\langle a \rangle| = 2$, $b \neq e$ and $b^2 \in \langle a \rangle$. Hence $b^2 = e, a, a^2, a^3, a^4$, or a^5.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1}$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1}$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ and $ba^4b^{-1} = (bab^{-1})^4$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ and $ba^4b^{-1} = (bab^{-1})^4 = a^{-4}$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ and $ba^4b^{-1} = (bab^{-1})^4 = a^{-4} = a^2$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ and $ba^4b^{-1} = (bab^{-1})^4 = a^{-4} = a^2$, so $a^4 = a^2$

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ and $ba^4b^{-1} = (bab^{-1})^4 = a^{-4} = a^2$, so $a^4 = a^2$ and this implies $a^2 = e$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ and $ba^4b^{-1} = (bab^{-1})^4 = a^{-4} = a^2$, so $a^4 = a^2$ and this implies $a^2 = e$, but this contradicts $|a| = 6$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = a$, then $ba = b^3 = ab$ and so G is abelian, which contradicts our assumption.
- If $b^2 = a^5 = a^{-1}$, then $a = b^{-2}$ and so $ba = b^{-1} = ab$, which leads to a contradiction again.
- If $b^2 = a^2$, note that $ba^2b^{-1} = bb^2b^{-1} = b^2 = a^2$ and $ba^2b^{-1} = (bab^{-1})^2 = (a^{-1})^2 = a^{-2}$, so $a^2 = a^{-2}$ and this implies $a^4 = e$, but this contradicts $|a| = 6$.
- If $b^2 = a^4$, note that $ba^4b^{-1} = bb^2b^{-1} = b^2 = a^4$ and $ba^4b^{-1} = (bab^{-1})^4 = a^{-4} = a^2$, so $a^4 = a^2$ and this implies $a^2 = e$, but this contradicts $|a| = 6$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$, then we have $G = \langle a, b \rangle$, $|a| = 6$, $a^3 = b^2$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$, then we have $G = \langle a, b \rangle$, $|a| = 6$, $a^3 = b^2$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$, then we have $G = \langle a, b \rangle$, $|a| = 6$, $a^3 = b^2$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$, then we have $G = \langle a, b \rangle$, $|a| = 6$, $a^3 = b^2$, and $bab^{-1} = a^{-1}$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$, then we have $G = \langle a, b \rangle$, $|a| = 6$, $a^3 = b^2$, and $bab^{-1} = a^{-1}$. Therefore, $G \cong T$.

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$, then we have $G = \langle a, b \rangle$, $|a| = 6$, $a^3 = b^2$, and $bab^{-1} = a^{-1}$. Therefore, $G \cong T$.

Hence, $G \cong A_4$, D_6, or T,

Proof of Proposition (6.4)

- G is a nonabelian group of order 12. $G = \langle a, b \rangle$.
- $a \in G$ with $|a| = 6$, i.e., $|\langle a \rangle| = 6$. $b \in G$ with $bab^{-1} = a^{-1}$.

Hence $b^2 = e$, a, a^2, a^3, a^4, or a^5.

- If $b^2 = e$, then we have $G = \langle a, b \rangle$, $a^6 = b^2 = e$, $a^k \neq e$ for $0 < k < 6$, and $bab^{-1} = a^{-1}$. By Theorem (I.6.13), $G \cong D_6$.
- If $b^2 = a^3$, then we have $G = \langle a, b \rangle$, $|a| = 6$, $a^3 = b^2$, and $bab^{-1} = a^{-1}$. Therefore, $G \cong T$.

Hence, $G \cong A_4$, D_6, or T, and this completes the proof.

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,\ D_4$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,\ D_4$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_2 \oplus \mathbb{Z}_6,$

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,\ D_4$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_2 \oplus \mathbb{Z}_6,\ \mathbb{Z}_{12},$

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,\ D_4$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_2 \oplus \mathbb{Z}_6,\ \mathbb{Z}_{12},\ A_4,$

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,\ D_4$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_2 \oplus \mathbb{Z}_6,\ \mathbb{Z}_{12},\ A_4,\ D_6,$
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Order	*Distinct Groups*
1	$\langle e \rangle$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2 \oplus \mathbb{Z}_2,\ \mathbb{Z}_4$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ D_3 = S_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2 \oplus \mathbb{Z}_4,\ \mathbb{Z}_8,\ Q_8,\ D_4$
9	$\mathbb{Z}_3 \oplus \mathbb{Z}_3,\ \mathbb{Z}_9$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_2 \oplus \mathbb{Z}_6,\ \mathbb{Z}_{12},\ A_4,\ D_6,\ T$

Order	*Distinct Groups*
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$

Remark

We have finished classifying all groups of order ≤ 15*.*

Remark

We have finished classifying all groups of order ≤ 15*.*

Next, we will classify all groups of order pq *with* p, q *prime.*

Remark

We have finished classifying all groups of order ≤ 15*.*
Next, we will classify all groups of order pq *with* p, q *prime.*

- If $p = q$,

Remark

We have finished classifying all groups of order ≤ 15*.*
Next, we will classify all groups of order pq *with* p, q *prime.*

- If $p = q$, since every group of order p^2 is abelian,

Remark

We have finished classifying all groups of order ≤ 15*.*
Next, we will classify all groups of order pq *with* p, q *prime.*

- If $p = q$, since every group of order p^2 is abelian, there are only two distinct groups (up to isomorphism) of order p^2:

Remark

We have finished classifying all groups of order ≤ 15*.*
Next, we will classify all groups of order pq *with* p, q *prime.*

- If $p = q$, since every group of order p^2 is abelian, there are only two distinct groups (up to isomorphism) of order p^2: $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Remark

We have finished classifying all groups of order ≤ 15*.*
Next, we will classify all groups of order pq *with* p, q *prime.*

- If $p = q$, since every group of order p^2 is abelian, there are only two distinct groups (up to isomorphism) of order p^2: $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.
- If $p \neq q$,

Remark

We have finished classifying all groups of order ≤ 15*.*
Next, we will classify all groups of order pq *with* p, q *prime.*

- If $p = q$, since every group of order p^2 is abelian, there are only two distinct groups (up to isomorphism) of order p^2: $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.
- If $p \neq q$, we may assume $p > q$.

Remark

We have finished classifying all groups of order ≤ 15*.*
Next, we will classify all groups of order pq *with* p, q *prime.*

- If $p = q$, since every group of order p^2 is abelian, there are only two distinct groups (up to isomorphism) of order p^2: $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.
- If $p \neq q$, we may assume $p > q$. The following proposition will classify all groups of order pq.

Proposition (6.1)

Let $p > q$ be prime numbers.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$,

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$,

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof. For the second case $q \mid p - 1$,

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof. For the second case $q \mid p - 1$, we only need to show that if G is a nonabelian group of order pq,

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof. For the second case $q \mid p - 1$, we only need to show that if G is a nonabelian group of order pq, then G is isomorphic to the group K that is described above.

Proposition (6.1)

Let $p > q$ be prime numbers.

- If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$. *(We have shown this earlier.)*
- If $q \mid p - 1$, then there are (up to isomorphism) exactly two distinct groups of order pq:
  - the cyclic group $\mathbb{Z}_{pq}$,
  - a nonabelian group K generated by elements c and d such that $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof. For the second case $q \mid p - 1$, we only need to show that if G is a nonabelian group of order pq, then G is isomorphic to the group K that is described above. The existence of such a group K are proved in Exercise 1 and 2.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. *We want to show that G is isomorphic to the group K that is described in Proposition (6.1).*

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$,

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$,

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian,

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$.

Hence, we can see inductively that $b^qab^{-q} = a^{r^q}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$.

Hence, we can see inductively that $b^qab^{-q} = a^{r^q}$. Thus we have $a = a^{r^q}$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$.

Hence, we can see inductively that $b^qab^{-q} = a^{r^q}$. Thus we have $a = a^{r^q}$ and so $r^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$.

Hence, we can see inductively that $b^qab^{-q} = a^{r^q}$. Thus we have $a = a^{r^q}$ and so $r^q \equiv 1 \pmod{p}$. *In order to connect G with the group K, we need the following remark.*

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let G be a nonabelian group of order pq. By Cauchy's Theorem, there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

Let $P = \langle a \rangle$ and $Q = \langle b \rangle$. Since

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{pq}{1} = pq = |G|,$$

we have $G = PQ = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Moreover, since $p > q$, G has only one Sylow p-subgroup and so $P \lhd G$. Hence $bab^{-1} \in P$, i.e., $bab^{-1} = a^r$ for some r. Since G is nonabelian, $r \not\equiv 1 \pmod{p}$. Moreover,

$b^2ab^{-2} = b(bab^{-1})b^{-1} = ba^rb^{-1} = (bab^{-1})^r = (a^r)^r = a^{r^2}$ and

$b^3ab^{-3} = b(b^2ab^{-2})b^{-1} = ba^{r^2}b^{-1} = (bab^{-1})^{r^2} = (a^r)^{r^2} = a^{r^3}$.

Hence, we can see inductively that $b^qab^{-q} = a^{r^q}$. Thus we have $a = a^{r^q}$ and so $r^q \equiv 1 \pmod{p}$. *In order to connect G with the group K, we need the following remark.*

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number,

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$,

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q,

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system $\Leftrightarrow$ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system $\Leftrightarrow$ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system $\Leftrightarrow$ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.

Remark. Let $p > q$ be prime numbers with $q \mid p-1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p-1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system $\maltese$ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.
- Moreover, since $|H| = q$ is a prime number,

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system $\maltese$ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.
- Moreover, since $|H| = q$ is a prime number, $\forall \overline{a} \in H \setminus \{\overline{1}\}$, $\langle \overline{a} \rangle = H$.

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system ✠ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.
- Moreover, since $|H| = q$ is a prime number, $\forall \overline{a} \in H \setminus \{\overline{1}\}$, $\langle \overline{a} \rangle = H$. Hence, if $r, s \in \mathbb{Z}$ are both solutions of the above system ✠,

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system ✠ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.
- Moreover, since $|H| = q$ is a prime number, $\forall \overline{a} \in H \setminus \{\overline{1}\}$, $\langle \overline{a} \rangle = H$. Hence, if $r, s \in \mathbb{Z}$ are both solutions of the above system ✠, i.e., $\overline{r}, \overline{s} \in H \setminus \{\overline{1}\}$,

Remark. Let $p > q$ be prime numbers with $q \mid p - 1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p - 1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system ✠ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.
- Moreover, since $|H| = q$ is a prime number, $\forall \overline{a} \in H \setminus \{\overline{1}\}$, $\langle \overline{a} \rangle = H$. Hence, if $r, s \in \mathbb{Z}$ are both solutions of the above system ✠, i.e., $\overline{r}, \overline{s} \in H \setminus \{\overline{1}\}$, then $\overline{s} = \overline{r}^t$ for some $1 \leq t \leq q - 1$,

Remark. Let $p > q$ be prime numbers with $q \mid p-1$.

- Note that $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ is a group under multiplication. Since $q \mid p-1 = |\mathbb{Z}_p^\times|$ and since q is a prime number, $\mathbb{Z}_p^\times$ has a subgroup H of order q. Note that $\forall \overline{a} \in H$, $\overline{a}^q = \overline{1}$ in $\mathbb{Z}_p^\times$.
- Consider the polynomial $X^q - 1 \in \mathbb{Z}_p[X]$. Since $\mathbb{Z}_p$ is a field and since $X^q - 1$ has degree q, $X^q - 1$ has at most q zeros in $\mathbb{Z}_p$. Hence, the elements in H are precisely the zeros of $X^q - 1$ in $\mathbb{Z}_p$. In other words, an integer k is a solution of the system ✠ $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$ if and only if $\overline{k} \in H \setminus \{1\}$.
- Moreover, since $|H| = q$ is a prime number, $\forall \overline{a} \in H \setminus \{\overline{1}\}$, $\langle \overline{a} \rangle = H$. Hence, if $r, s \in \mathbb{Z}$ are both solutions of the above system ✠, i.e., $\overline{r}, \overline{s} \in H \setminus \{\overline{1}\}$, then $\overline{s} = \overline{r}^t$ for some $1 \leq t \leq q-1$, i.e., $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

We want to show that if G is a nonabelian group of order pq, then G is isomorphic to K.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p - 1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system

$$\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}.$$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$.

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$. Hence the group homomorphism $G \to K$ induced by $a \mapsto c$ and $b_1 \mapsto d$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$. Hence the group homomorphism $G \to K$ induced by $a \mapsto c$ and $b_1 \mapsto d$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$. Hence the group homomorphism $G \to K$ induced by $a \mapsto c$ and $b_1 \mapsto d$

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$. Hence the group homomorphism $G \to K$ induced by $a \mapsto c$ and $b_1 \mapsto d$ is an isomorphism

Proof of Proposition (6.1)

Let $p > q$ be prime numbers such that $q \mid p-1$ and let $K = \langle c, d \rangle$ be a nonabelian group with $|c| = p$, $|d| = q$, $dc = c^s d$, where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$.

Let G be a nonabelian group of order pq. We have shown that there exist elements $a, b \in G$ such that $|a| = p$, $|b| = q$, and $G = \{a^i b^j \mid 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have also seen that $bab^{-1} = a^r$ for some r with $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. Note that both r and s are solutions to the system $\begin{cases} X \not\equiv 1 \pmod{p} \\ X^q \equiv 1 \pmod{p} \end{cases}$. Hence $s \equiv r^t \pmod{p}$ for some $1 \leq t \leq q-1$. Take $b_1 = b^t \in G$. Then $\langle b_1 \rangle = \langle b \rangle$ and so $G = \langle a, b_1 \rangle$. Note that $b_1 a b_1^{-1} = b^t a b^{-t} = a^{r^t} = a^s$. Hence the group homomorphism $G \to K$ induced by $a \mapsto c$ and $b_1 \mapsto d$ is an isomorphism and this completes the proof.

Exercise for Section II.6

1, 2, 3, 4, 6, 7

Chapter III: Rings

For the remaining classes for this semester, we will cover some basic ring theory that you have learned in your undergraduate algebra classes.

Chapter III: Rings

For the remaining classes for this semester, we will cover some basic ring theory that you have learned in your undergraduate algebra classes.

Chapter III: Rings

For the remaining classes for this semester, we will cover some basic ring theory that you have learned in your undergraduate algebra classes.

Chapter III: Rings

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "*$+$*"*

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",*

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc)$, $\forall a, b, c \in R$

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1)**.** A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$",* such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and $\exists 1_R \in R$ such that $\forall a \in R$, $1_R a = a 1_R = a$,

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and $\exists 1_R \in R$ such that $\forall a \in R$, $1_R a = a 1_R = a$, then R is said to be a **ring with identity**.

Chapter III: Rings

Section III.1: Rings and Homomorphisms

Definition (1.1). A **ring** is a nonempty set R together with two binary operations, *usually denoted as addition "$+$" and multiplication "$\cdot$"*, such that

(i) $(R, +)$ is an abelian group,

(ii) $(ab)c = a(bc), \forall a, b, c \in R$ (associative multiplication),

(iii) $a(b + c) = ab + ac$ (left distributive law) and
$(a + b)c = ac + bc$ (right distributive law).

- If $(R, +, \cdot)$ is a ring and $ab = ba, \forall a, b \in R$, then R is called a **commutative ring**.
- If $(R, +, \cdot)$ is a ring and $\exists 1_R \in R$ such that $\forall a \in R$, $1_R a = a 1_R = a$, then R is said to be a **ring with identity**.

Theorem (1.2)

Let R be a ring. Then

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Proof. Note that

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Proof. Note that $0a = (0 + 0)a$

because $0 = 0 + 0$

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Proof. Note that $0a = (0+0)a = 0a + 0a$

right distribution law

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Proof. Note that $0a = (0+0)a = 0a + 0a \implies 0a = 0$

because $(R, +)$ is a group

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Proof. Note that $0a = (0+0)a = 0a + 0a \implies 0a = 0$ and $a0 = a(0+0)$

because $0 = 0 + 0$

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R,$

Proof. Note that $0a = (0+0)a = 0a + 0a \implies 0a = 0$ and

$$a0 = a(0+0) = a0 + a0$$

left distribution law

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,

Proof. Note that $0a = (0+0)a = 0a + 0a \implies 0a = 0$ and

$a0 = a(0+0) = a0 + a0 \implies a0 = 0.$

because $(R, +)$ is a group

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that $(-a)b + ab = (-a + a)b$

right distribution law

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

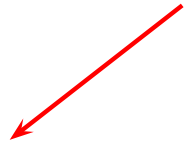
Proof. Note that $(-a)b + ab = (-a + a)b = 0b$

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that $(-a)b + ab = (-a + a)b = 0b = 0$,



the first statement

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that $(-a)b + ab = (-a + a)b = 0b = 0$, so $(-a)b = -(ab)$.

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that $(-a)b + ab = (-a + a)b = 0b = 0$, so $(-a)b = -(ab)$. Similarly, $a(-b) + ab = a(-b + b)$

left distribution law

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that $(-a)b + ab = (-a + a)b = 0b = 0$, so $(-a)b = -(ab)$. Similarly, $a(-b) + ab = a(-b + b) = a0$

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that $(-a)b + ab = (-a + a)b = 0b = 0$, so $(-a)b = -(ab)$. Similarly, $a(-b) + ab = a(-b + b) = a0 = 0$,

the first statement

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,

Proof. Note that $(-a)b + ab = (-a + a)b = 0b = 0$, so $(-a)b = -(ab)$. Similarly, $a(-b) + ab = a(-b + b) = a0 = 0$, so $a(-b) = -(ab)$.

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,

Proof. Use the second statement twice.

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,

Proof. Use the second statement twice. More precisely,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,

Proof. Use the second statement twice. More precisely, $(-a)(-b) = -(a(-b))$

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,

Proof. Use the second statement twice. More precisely,
$(-a)(-b) = -(a(-b)) = -(-(ab))$

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,

Proof. Use the second statement twice. More precisely, $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,
- $(na)b = a(nb) = n(ab), \forall n \in \mathbb{Z}$ and $\forall a, b \in R$,

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,
- $(na)b = a(nb) = n(ab), \forall n \in \mathbb{Z}$ and $\forall a, b \in R$,
- $(\sum_{i=1}^{n} a_i)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j, \forall a_i, b_j \in R$.

Theorem (1.2)

Let R be a ring. Then

- $0a = a0 = 0, \forall a \in R$,
- $(-a)b = a(-b) = -(ab), \forall a, b \in R$,
- $(-a)(-b) = ab, \forall a, b \in R$,
- $(na)b = a(nb) = n(ab), \forall n \in \mathbb{Z}$ and $\forall a, b \in R$,
- $\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j, \forall a_i, b_j \in R$.

Proof. The proofs for the last two statements are straight forward using the left and right distribution laws.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor
  if $\exists b \in R \setminus \{0\}$ such that $ab = 0$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor**

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R,

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$,

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$, $ab = ac$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$, $ab = ac$ or $ba = ca$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$, $ab = ac$ or $ba = ca \implies b = c$.

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$, $ab = ac$ or $ba = ca \implies b = c$.

This is because $ab = ac \implies ab - ac = 0 \implies a(b - c) = 0 \implies b - c = 0 \implies b = c$

Zero Divisors

Definition (1.3)**.** Let R be a ring and let $a \in R \setminus \{0\}$.

- a is called a left zero divisor (resp. right zero divisor) if $\exists b \in R \setminus \{0\}$ such that $ab = 0$ (resp. $ba = 0$).
- a is called a **zero divisor** if a is both a left zero divisor and a right zero divisor.

Remark. A ring R has no zero divisors if and only if the right and left cancelation laws hold in R, i.e., $\forall a, b, c \in R$, $a \neq 0$, $ab = ac$ or $ba = ca \implies b = c$.

This is because $ab = ac \implies ab - ac = 0 \implies a(b - c) = 0 \implies b - c = 0 \implies b = c$

and $ba = ca \implies ba - ca = 0 \implies (b - c)a = 0 \implies b - c = 0 \implies b = c$.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible
  if $\exists b \in R$ such that $ba = 1_R$

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$).

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible**

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit**

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible,

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

(ii) The set of units in a ring R with identity,

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

(ii) The set of units in a ring R with identity, denoted by $U(R)$,

Invertible

Definition (1.4)**.** Let R be a ring with identity 1_R and let $a \in R$.

- a is said to be left invertible (resp. right invertible) if $\exists b \in R$ such that $ba = 1_R$ (resp. $ab = 1_R$). The element b is called a left (resp. right) inverse of a.
- a is said to be **invertible** or to be a **unit** if it is both left and right invertible.

Remark.

(i) If $a \in R$ is invertible, then its left inverse and right inverse must coincide.

(ii) The set of units in a ring R with identity, denoted by $U(R)$, is a group under multiplication.

Definition (5.1)

Let R be a ring.

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.
- R is called a **field**

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.
- R is called a **field** if it is a commutative division ring.

Definition (5.1)

Let R be a ring.

- R is called an **integral domain** if
  - R is commutative,
  - R has an identity $1_R \neq 0$,
  - R has no zero divisors.
- R is called a **division ring** if
  - R has an identity $1_R \neq 0$,
  - every nonzero element of R is a unit.
- R is called a **field** if it is a commutative division ring.

Remark. A field is a commutative ring with an identity $1_R \neq 0$ such that every nonzero element is a unit.