UNIVERSITÄT DES SAARLANDES

Proseminar Geometrische Strukturen

Endliche Gruppen

Lars Lauer

Universität des Saarlandes - Jan. 26, 2021

Inhalt

- Beispiele endlicher Gruppen

Inhalt

- Beispiele endlicher Gruppen
- Sylow-Sätze

Inhalt

- Beispiele endlicher Gruppen
- Sylow-Sätze
- Einige Gruppen kleiner Ordnung

Inhalt

- Beispiele endlicher Gruppen
- Sylow-Sätze
- Einige Gruppen kleiner Ordnung
- Klassifikationsprogramm der einfachen endlichen Gruppen

Beispiel endlicher Gruppen

Beispiele endlicher Gruppen

- Zyklische Gruppe $(\mathbb{Z}_n, +_n)$
  $\{0, 1, ..., n-1\}$ mit $a +_n b = (a+b) \bmod n$

Beispiele endlicher Gruppen

- Zyklische Gruppe $(\mathbb{Z}_n, +_n)$
  $\{0, 1, ..., n-1\}$ mit $a +_n b = (a+b) \bmod n$

- Produkt zyklischer Gruppen $(\mathbb{Z}_n \times \mathbb{Z}_m, +)$
  mit $(a, b) + (c, d) = (a +_n c, b +_m d)$

Beispiele endlicher Gruppen

- Zyklische Gruppe $(\mathbb{Z}_n, +_n)$
  $\{0, 1, ..., n-1\}$ mit $a +_n b = (a + b) \bmod n$

- Produkt zyklischer Gruppen $(\mathbb{Z}_n \times \mathbb{Z}_m, +)$
  mit $(a, b) + (c, d) = (a +_n c, b +_m d)$

- Symmetrische Gruppe $(S_n, \circ)$
  bijektiven Abbildungen von $\{1, ..., n\} \rightarrow \{1, ..., n\}$

Beispiele endlicher Gruppen

- Zyklische Gruppe $(\mathbb{Z}_n, +_n)$
  $\{0, 1, ..., n-1\}$ mit $a +_n b = (a + b) \bmod n$

- Produkt zyklischer Gruppen $(\mathbb{Z}_n \times \mathbb{Z}_m, +)$
  mit $(a, b) + (c, d) = (a +_n c, b +_m d)$

- Symmetrische Gruppe $(S_n, \circ)$
  bijektiven Abbildungen von $\{1, ..., n\} \to \{1, ..., n\}$

- Alternierende Gruppe $A_n \subseteq S_n$
  Erzeugnis der 3-Zyklen $\langle (a, b, c) \rangle, (a, b, c) \in S_n$

Diedergruppe

Definition

Diedergruppe $D_n = \{id, d, d^2, ..., d^{n-1}, s, sd, sd^2, ..., sd^{n-1}\}$
mit $s^2 = id$, $sdsd = id$ und $d^n = id$

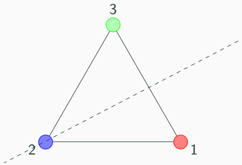
Diedergruppe D_n sind die Isometrien des gleichmäßigen n-Ecks
d ist die Drehung um $\frac{360}{n}$ Grad
s ist die Spiegelung an der Symmetrieachse

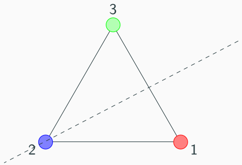
Diedergruppe D_3

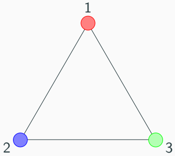
Isometrien des gleichmäßigen Dreiecks

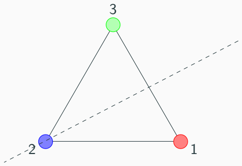
$D_3 = \{id, d, d^2, s, sd, sd^2\}$

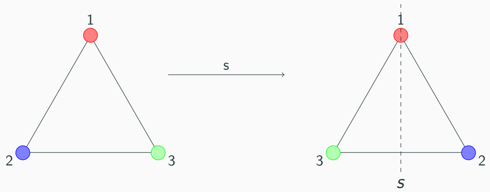
d ist die Drehung um 120 Grad
s, sd, sd^2 sind die drei Spiegelungen

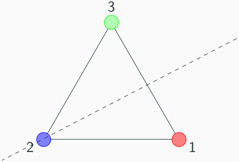

3
2
1

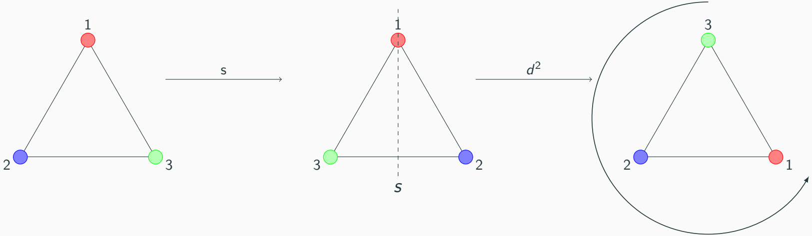

3
2
1

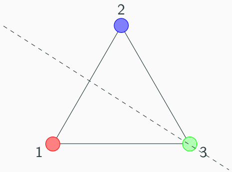

1
2
3

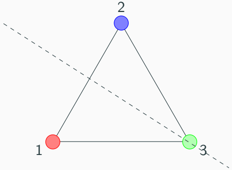

3
2
1

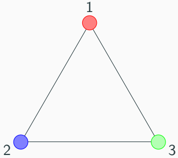

1
2
3
s
1
3
2
s

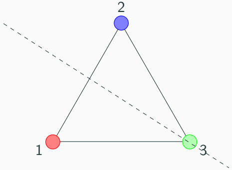

3
2
1

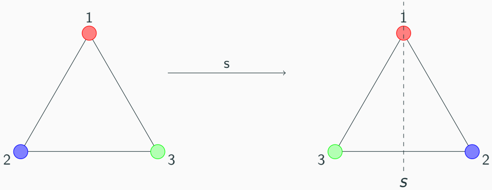

1
2
3
s
1
3
2
s
d²
3
2
1

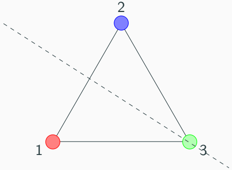

2
1
3

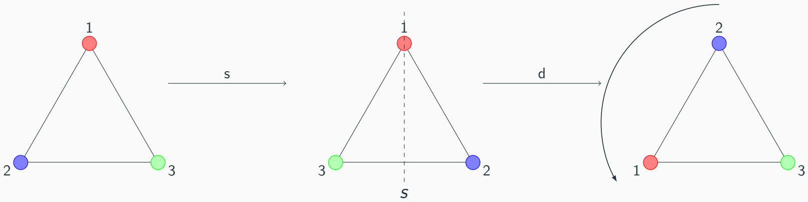

2
1
3

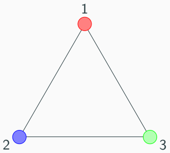

1
2
3


2
1
3

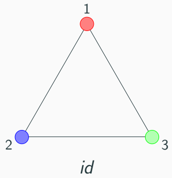

1
2
3
s
1
3
2
s

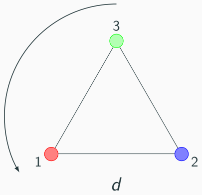

2
1
3

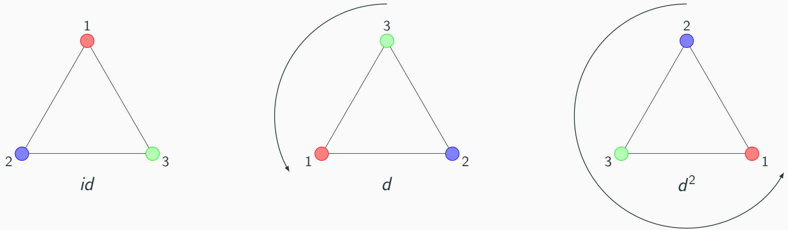

1
2
3
s
1
3
2
s
d
2
1
3

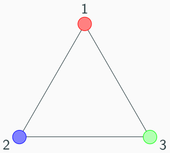


id

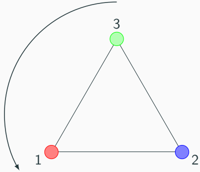

1
2
3
id


3
1
2
d

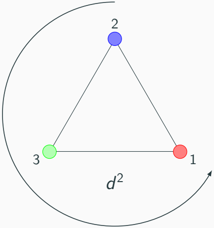

1
2
3
id
3
1
2
d
2
3
1
d²



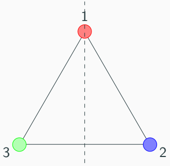
id



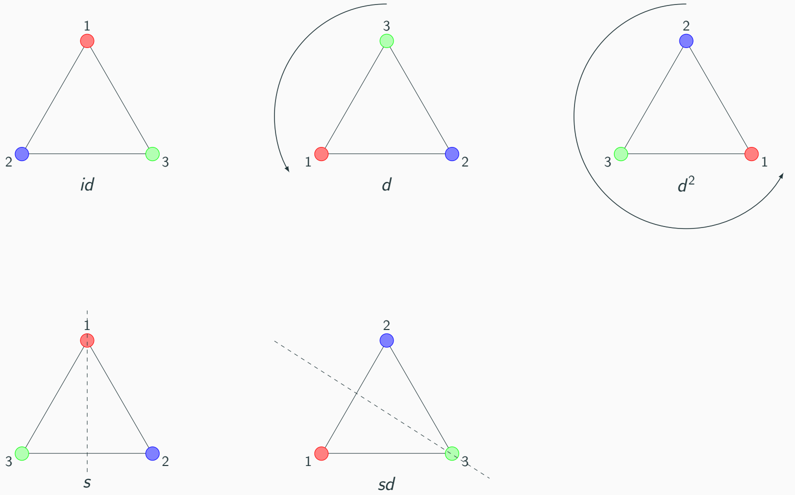
d



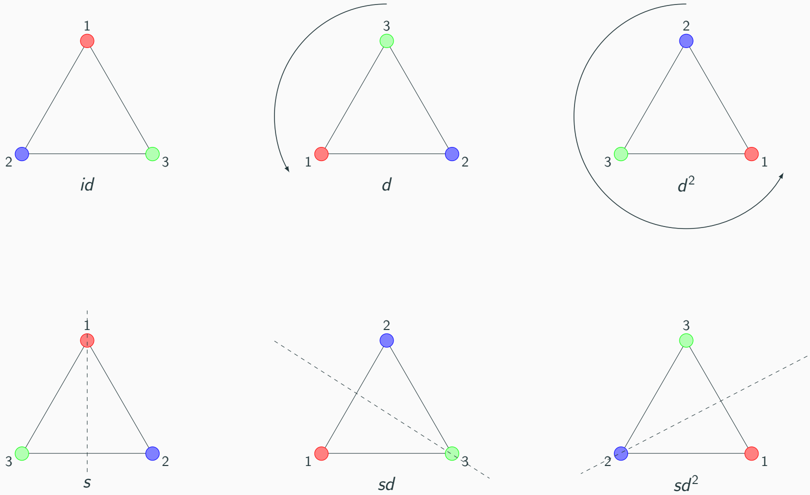
d^2



s



id
d
d²
s
sd


1
2
3
id
3
1
2
d
2
3
1
d^2
1
3
2
s
2
1
3
sd
3
2
1
sd^2

Sylow-Sätze

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Die Untergruppe H wird auch p-Sylow-Untergruppe oder Sylow-Untergruppe genannt.

Vorbereitung des Beweises

Vorbereitungslemma 1

Es sei $n = p^l m, l \geq 1$ und $p \nmid m$. Dann gilt $p \nmid \binom{n}{p^l}$.

Vorbereitung des Beweises

Vorbereitungslemma 1

Es sei $n = p^l m, l \geq 1$ und $p \nmid m$. Dann gilt $p \nmid \binom{n}{p^l}$.

Beweis:

- $\binom{n}{p^l} = \frac{n(n-1)\ldots(n-j)(n-p^l+1)}{p^l(p^l-1)\ldots(p^l-j)\ldots 1}$
  Man ordne jedem Faktor $(n-j)$ den Faktor $(p^l - j)$ im Nenner zu.

Vorbereitung des Beweises

Vorbereitungslemma 1

Es sei $n = p^l m, l \geq 1$ und $p \nmid m$. Dann gilt $p \nmid \binom{n}{p^l}$.

Beweis:

- $\binom{n}{p^l} = \frac{n(n-1)\dots(n-j)(n-p^l+1)}{p^l(p^l-1)\dots(p^l-j)\dots 1}$
  Man ordne jedem Faktor $(n-j)$ den Faktor $(p^l - j)$ im Nenner zu.
- $j = p^e k$, wobei $k \nmid p$ ist.

Vorbereitung des Beweises

Vorbereitungslemma 1

Es sei $n = p^l m, l \geq 1$ und $p \nmid m$. Dann gilt $p \nmid \binom{n}{p^l}$.

Beweis:

- $\binom{n}{p^l} = \frac{n(n-1)\dots(n-j)(n-p^l+1)}{p^l(p^l-1)\dots(p^l-j)\dots1}$
  Man ordne jedem Faktor $(n-j)$ den Faktor $(p^l - j)$ im Nenner zu.
- $j = p^e k$, wobei $k \nmid p$ ist.
- Da $e < l$, sind n und p^l teilbar durch p^e.
  Somit sind $n - j$ und $p^l - j$ teilbar durch p^e aber nicht durch p^l.

Vorbereitung des Beweises

Vorbereitungslemma 1

Es sei $n = p^l m, l \geq 1$ und $p \nmid m$. Dann gilt $p \nmid \binom{n}{p^l}$.

Beweis:

- $\binom{n}{p^l} = \frac{n(n-1)\ldots(n-j)(n-p^l+1)}{p^l(p^l-1)\ldots(p^l-j)\ldots 1}$
  Man ordne jedem Faktor $(n-j)$ den Faktor $(p^l - j)$ im Nenner zu.
- $j = p^e k$, wobei $k \nmid p$ ist.
- Da $e < l$, sind n und p^l teilbar durch p^e.
  Somit sind $n - j$ und $p^l - j$ teilbar durch p^e aber nicht durch p^l.
- Also ist der Nenner genauso oft teilbar durch p wie der Zähler.

Vorbereitung des Beweises

Vorbereitungslemma 1

Es sei $n = p^l m, l \geq 1$ und $p \nmid m$. Dann gilt $p \nmid \binom{n}{p^l}$.

Beweis:

- $\binom{n}{p^l} = \frac{n(n-1)...(n-j)(n-p^l+1)}{p^l(p^l-1)...(p^l-j)...1}$
  Man ordne jedem Faktor $(n-j)$ den Faktor $(p^l - j)$ im Nenner zu.
- $j = p^e k$, wobei $k \nmid p$ ist.
- Da $e < l$, sind n und p^l teilbar durch p^e.
  Somit sind $n - j$ und $p^l - j$ teilbar durch p^e aber nicht durch p^l.
- Also ist der Nenner genauso oft teilbar durch p wie der Zähler.
- Somit ist $p \nmid \binom{n}{p^l}$

Vorbereitung des Beweises

Vorbereitungslemma 2

Die endliche Gruppe G operiere auf der Menge aller Teilmengen von G bzgl. der Linksmultiplikation. Sei $U \subseteq G$, dann ist $|G_U|$ ein Teiler von $|U|$.

Vorbereitung des Beweises

Vorbereitungslemma 2

Die endliche Gruppe G operiere auf der Menge aller Teilmengen von G bzgl. der Linksmultiplikation. Sei $U \subseteq G$, dann ist $|G_U|$ ein Teiler von $|U|$.

Beweis:

- U besteht aus Bahnen $G_U g$ mit $g \in U$.

Vorbereitungslemma 2

Die endliche Gruppe G operiere auf der Menge aller Teilmengen von G bzgl. der Linksmultiplikation. Sei $U \subseteq G$, dann ist $|G_U|$ ein Teiler von $|U|$.

Beweis:

- U besteht aus Bahnen $G_U g$ mit $g \in U$.
- $G_U g$ sind Rechtsnebenklassen.
  Somit ist U eine Vereinigung von Rechtsnebenklassen.

Vorbereitung des Beweises

Vorbereitungslemma 2

Die endliche Gruppe G operiere auf der Menge aller Teilmengen von G bzgl. der Linksmultiplikation. Sei $U \subseteq G$, dann ist $|G_U|$ ein Teiler von $|U|$.

Beweis:

- U besteht aus Bahnen $G_U g$ mit $g \in U$.
- $G_U g$ sind Rechtsnebenklassen.
  Somit ist U eine Vereinigung von Rechtsnebenklassen.
- Es gilt $G_U g_1 = G_U g_2$ oder $G_U g_1$ und $G_U g_2$ sind disjunkt.

Vorbereitungslemma 2

Die endliche Gruppe G operiere auf der Menge aller Teilmengen von G bzgl. der Linksmultiplikation. Sei $U \subseteq G$, dann ist $|G_U|$ ein Teiler von $|U|$.

Beweis:

- U besteht aus Bahnen $G_U g$ mit $g \in U$.
- $G_U g$ sind Rechtsnebenklassen.
  Somit ist U eine Vereinigung von Rechtsnebenklassen.
- Es gilt $G_U g_1 = G_U g_2$ oder $G_U g_1$ und $G_U g_2$ sind disjunkt.
- Es folgt $|U| = |G_U g_{i_1}| + ... + |G_U g_{i_r}|$ und auch $|G_U|$ teilt $|U|$.

Beweis des 1.Sylow-Satzes

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Beweis des 1.Sylow-Satzes

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Beweis:

- G operiert auf $X = \{M \subset G | p^l = |M|\}$ mit $g(M) = gM$.
  $|G| = p^l m$ und $|X| = \binom{n}{p^l}$ und $p \nmid |X|$ (1.Lemma).

Beweis des 1.Sylow-Satzes

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Beweis:

- G operiert auf $X = \{M \subset G | p^l = |M|\}$ mit $g(M) = gM$.
  $|G| = p^l m$ und $|X| = \binom{n}{p^l}$ und $p \nmid |X|$ (1.Lemma).
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$

Beweis des 1.Sylow-Satzes

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Beweis:

- G operiert auf $X = \{M \subset G | p^l = |M|\}$ mit $g(M) = gM$.
  $|G| = p^l m$ und $|X| = \binom{n}{p^l}$ und $p \nmid |X|$ (1.Lemma).
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$
- $p \nmid |X|$ folgt es gibt B_i mit $p \nmid |B_i|$.

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Beweis:

- G operiert auf $X = \{M \subset G | p^l = |M|\}$ mit $g(M) = gM$.
  $|G| = p^l m$ und $|X| = \binom{n}{p^l}$ und $p \nmid |X|$ (1.Lemma).
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$
- $p \nmid |X|$ folgt es gibt B_i mit $p \nmid |B_i|$.
- Sei $U \in X$ und $U \in B_i$. Dann ist $|G_U|$ eine p-Potenz (2.Lemma)

Beweis des 1.Sylow-Satzes

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Beweis:

- G operiert auf $X = \{M \subset G | p^l = |M|\}$ mit $g(M) = gM$.
  $|G| = p^l m$ und $|X| = \binom{n}{p^l}$ und $p \nmid |X|$ (1.Lemma).
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$
- $p \nmid |X|$ folgt es gibt B_i mit $p \nmid |B_i|$.
- Sei $U \in X$ und $U \in B_i$. Dann ist $|G_U|$ eine p-Potenz (2.Lemma)
- $p^l m = |G| = |G_U||B_i|$(Bahnformel) und somit $|G_U| = p^l$

Beweis des 1.Sylow-Satzes

1.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$ mit $p \nmid m$ und $l \geq 1$.
Dann enthält G eine Untergruppe H der Ordnung p^l.

Beweis:

- G operiert auf $X = \{M \subset G | p^l = |M|\}$ mit $g(M) = gM$.
  $|G| = p^l m$ und $|X| = \binom{n}{p^l}$ und $p \nmid |X|$ (1.Lemma).
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$
- $p \nmid |X|$ folgt es gibt B_i mit $p \nmid |B_i|$.
- Sei $U \in X$ und $U \in B_i$. Dann ist $|G_U|$ eine p-Potenz (2.Lemma)
- $p^l m = |G| = |G_U||B_i|$(Bahnformel) und somit $|G_U| = p^l$
- Aus $G_U < G$ folgt die Behauptung.

2.Sylow-Satz

Sei G eine endliche Gruppe und J eine Untergruppe von G. Sei p eine Primzahl und p teile $|J|$. H sei eine p-Sylow-Untergruppe von G. Dann gibt es eine zu H konjugierte Untergruppe $H' = gHg^{-1}$, so dass $J \cap H'$ eine Sylow-Untergruppe von J ist.

Index einer Gruppe

Definition Index

Sei $H < G$, dann ist der Index von H in G die Anzahl der Nebenklassen von H in G. Geschrieben $[G : H]$

Index einer Gruppe

Definition Index

Sei $H < G$, dann ist der Index von H in G die Anzahl der Nebenklassen von H in G. Geschrieben $[G : H]$

Satz 3.16

Sei G endlich und $H < G$: $|G| = |H|[G : H]$.

Index einer Gruppe

Definition Index

Sei $H < G$, dann ist der Index von H in G die Anzahl der Nebenklassen von H in G. Geschrieben $[G : H]$

Satz 3.16

Sei G endlich und $H < G$: $|G| = |H|[G : H]$.

Satz 3.17

Sei G endlich und $J < H < G$: $[G : J] = [G : H][H : J]$

[Rosebrock, 2019]

Beweis des 2.Sylow-Satzes

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1 H) = (gg_1)H$

Beweis des 2.Sylow-Satzes

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1H) = (gg_1)H$
- Stabilisator von $x = 1H$ ist H

Beweis des 2.Sylow-Satzes

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1 H) = (gg_1)H$
- Stabilisator von $x = 1H$ ist H
- $gHg^{-1}gx = gHg^{-1}gH = gHH = gH = gx$ somit $G_{gx} = gHg^{-1}$

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1 H) = (gg_1)H$
- Stabilisator von $x = 1H$ ist H
- $gHg^{-1}gx = gHg^{-1}gH = gHH = gH = gx$ somit $G_{gx} = gHg^{-1}$
- Auf J operiert auf X einschränken

Beweis des 2.Sylow-Satzes

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1H) = (gg_1)H$
- Stabilisator von $x = 1H$ ist H
- $gHg^{-1}gx = gHg^{-1}gH = gHH = gH = gx$ somit $G_{gx} = gHg^{-1}$
- Auf J operiert auf X einschränken
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$

Beweis des 2.Sylow-Satzes

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1 H) = (gg_1)H$
- Stabilisator von $x = 1H$ ist H
- $gHg^{-1}gx = gHg^{-1}gH = gHH = gH = gx$ somit $G_{gx} = gHg^{-1}$
- Auf J operiert auf X einschränken
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$
- $|X| = |G|/|H| = m$ somit $p \nmid |X|$ folgt es gibt B_i mit $p \nmid |B_i|$.

Beweis des 2.Sylow-Satzes

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1 H) = (gg_1)H$
- Stabilisator von $x = 1H$ ist H
- $gHg^{-1}gx = gHg^{-1}gH = gHH = gH = gx$ somit $G_{gx} = gHg^{-1}$
- Auf J operiert auf X einschränken
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$
- $|X| = |G|/|H| = m$ somit $p \nmid |X|$ folgt es gibt B_i mit $p \nmid |B_i|$.
- Für $gx \in B_i$ gilt $G_{gx} = H' = gHg^{-1}$ und $J_{gx} = H' \cap J$

Beweis des 2.Sylow-Satzes

Beweis:

- $X = G/H = \{gH | g \in G\}$ mit $g(g_1H) = (gg_1)H$
- Stabilisator von $x = 1H$ ist H
- $gHg^{-1}gx = gHg^{-1}gH = gHH = gH = gx$ somit $G_{gx} = gHg^{-1}$
- Auf J operiert auf X einschränken
- X teilen in disjunkte Bahnen $|X| = |B_1| + |B_2| + ... + |B_k|$
- $|X| = |G|/|H| = m$ somit $p \nmid |X|$ folgt es gibt B_i mit $p \nmid |B_i|$.
- Für $gx \in B_i$ gilt $G_{gx} = H' = gHg^{-1}$ und $J_{gx} = H' \cap J$
- $[J : (H' \cap J)] = |B_i|$ und $|J| = |H' \cap J|[J : (H' \cap J)]$ folgt aus p teilt$|J|$ und $p \nmid |B_i|$, dass $H' \cap J$ p-Sylow-Untergruppe von J ist

3.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$, wobei p nicht m teilt und $l \geq 1$. Sei k die Anzahl der p-Sylow-Untergruppen von G. Dann ist p ein Teiler von $k-1$ und k ein Teiler von m.

Vorbereitung des Beweises

Vorbereitungslemma 1

1. Sei $J < G$ und $|J| = p^k$.

Dann ist J in einer p-Sylow-Untergruppe enthalten

2. Alle p-Sylow-Untergruppen sind zueinander konjugiert.

Vorbereitung des Beweises

Vorbereitungslemma 1

1. Sei $J < G$ und $|J| = p^k$.
Dann ist J in einer p-Sylow-Untergruppe enthalten
2. Alle p-Sylow-Untergruppen sind zueinander konjugiert.

Beweis:

- Aus $|J| = p^k$ folgt, dass nur J p-Sylow-UG von J ist

Vorbereitung des Beweises

Vorbereitungslemma 1

1. Sei $J < G$ und $|J| = p^k$.

Dann ist J in einer p-Sylow-Untergruppe enthalten

2. Alle p-Sylow-Untergruppen sind zueinander konjugiert.

Beweis:

- Aus $|J| = p^k$ folgt, dass nur J p-Sylow-UG von J ist
- Sei H p-Sylow-Untergruppe von G, dann gibt es $H' = gHg^{-1}$ mit $J \cap H' = J$ und somit gilt $J \subset H'$

Vorbereitung des Beweises

Vorbereitungslemma 1

1. Sei $J < G$ und $|J| = p^k$.

Dann ist J in einer p-Sylow-Untergruppe enthalten

2. Alle p-Sylow-Untergruppen sind zueinander konjugiert.

Beweis:

- Aus $|J| = p^k$ folgt, dass nur J p-Sylow-UG von J ist
- Sei H p-Sylow-Untergruppe von G, dann gibt es $H' = gHg^{-1}$ mit $J \cap H' = J$ und somit gilt $J \subset H'$
- Aus $|H| = |H'|$ folgt H' ist p-Sylow-Untergruppe (1.)

Vorbereitung des Beweises

Vorbereitungslemma 1

1. Sei $J < G$ und $|J| = p^k$.
Dann ist J in einer p-Sylow-Untergruppe enthalten
2. Alle p-Sylow-Untergruppen sind zueinander konjugiert.

Beweis:

- Aus $|J| = p^k$ folgt, dass nur J p-Sylow-UG von J ist
- Sei H p-Sylow-Untergruppe von G, dann gibt es $H' = gHg^{-1}$ mit $J \cap H' = J$ und somit gilt $J \subset H'$
- Aus $|H| = |H'|$ folgt H' ist p-Sylow-Untergruppe (1.)
- Wenn J p-Sylow-Untergruppe war, folgt $|J| = |H| = |H'|$ und somit $J = H' = gHg^{-1}$ (2.)

Vorbereitung des Beweises

Definition

$G(H) = \{g \in G | gHg^{-1} = H\}$ heißt Normalisator.

- $G(H) = G \Leftrightarrow H$ ist Normalteiler in G

Vorbereitung des Beweises

Vorbereitungslemma 2

Sei $H < G$, so gilt $G(H) < G$ und $H \triangleleft G(H)$

Vorbereitung des Beweises

Vorbereitungslemma 2

Sei $H < G$, so gilt $G(H) < G$ und $H \lhd G(H)$

Beweis:

- $g, j \in G(H)$, dann $H = gHg^{-1} = gjHj^{-1}g^{-1}$ also $gj \in G(H)$

Vorbereitung des Beweises

Vorbereitungslemma 2

Sei $H < G$, so gilt $G(H) < G$ und $H \triangleleft G(H)$

Beweis:

- $g, j \in G(H)$, dann $H = gHg^{-1} = gjHj^{-1}g^{-1}$ also $gj \in G(H)$
- $g \in G(H)$, dann $g^{-1}Hg = g^{-1}gHg^{-1}g = H$ also $g^{-1} \in G(H)$

Vorbereitung des Beweises

Vorbereitungslemma 2

Sei $H < G$, so gilt $G(H) < G$ und $H \lhd G(H)$

Beweis:

- $g, j \in G(H)$, dann $H = gHg^{-1} = gjHj^{-1}g^{-1}$ also $gj \in G(H)$
- $g \in G(H)$, dann $g^{-1}Hg = g^{-1}gHg^{-1}g = H$ also $g^{-1} \in G(H)$
- $1H1 = H$ also $1 \in G(H)$

Vorbereitung des Beweises

Vorbereitungslemma 2

Sei $H < G$, so gilt $G(H) < G$ und $H \lhd G(H)$

Beweis:

- $g, j \in G(H)$, dann $H = gHg^{-1} = gjHj^{-1}g^{-1}$ also $gj \in G(H)$
- $g \in G(H)$, dann $g^{-1}Hg = g^{-1}gHg^{-1}g = H$ also $g^{-1} \in G(H)$
- $1H1 = H$ also $1 \in G(H)$
- $h \in H$ erfüllt $hHh^{-1} = H$ und somit ist $H \subset G(H)$ und damit $H \lhd G(H)$

3.Sylow-Satz

Sei G eine Gruppe der Ordnung $p^l m$, wobei p nicht m teilt und $l \geq 1$. Sei k die Anzahl der p-Sylow-Untergruppen von G. Dann ist p ein Teiler von $k-1$ und k ein Teiler von m.

Beweis des 3.Sylow-Satzes

Beweis: k teilt m

- G operiert auf $X = \{M | p^l = |M|\}$ mit $g(M) = gMg^{-1}$

Beweis des 3.Sylow-Satzes

Beweis: k teilt m

- G operiert auf $X = \{M | p^l = |M|\}$ mit $g(M) = gMg^{-1}$
- Da H p-Sylow-UG folgt aus Lemma 2, dass $GH = \{U | U \text{ ist p-Sylow-UG von G}\}$

Beweis des 3.Sylow-Satzes

Beweis: k teilt m

- G operiert auf $X = \{M | p^l = |M|\}$ mit $g(M) = gMg^{-1}$

- Da H p-Sylow-UG folgt aus Lemma 2, dass $GH = \{U | U \text{ ist p-Sylow-UG von G}\}$

- Es gilt $|G| = |G(H)|k = |G(H)|[G : G(H)]$ und somit $[G : G(H)] = k$

Beweis des 3.Sylow-Satzes

Beweis: k teilt m

- G operiert auf $X = \{M | p^l = |M|\}$ mit $g(M) = gMg^{-1}$
- Da H p-Sylow-UG folgt aus Lemma 2, dass $GH = \{U | U \text{ ist p-Sylow-UG von G}\}$
- Es gilt $|G| = |G(H)|k = |G(H)|[G : G(H)]$ und somit $[G : G(H)] = k$
- Aus $mp^l = |G| = |H|[G : H]$ folgt $m = [G : H]$ und somit $m = [G : H] = [G : G(H)][G(H) : H] = k[G(H) : H]$

Beweis des 3.Sylow-Satzes

Beweis: p teilt $k-1$

- H operiert auf $X = \{H_i | p^l = |H_i| \wedge H_i < G\}$, $h(H_i) = hH_ih^{-1}$

Beweis des 3.Sylow-Satzes

Beweis: p teilt $k-1$

- H operiert auf $X = \{H_i | p^l = |H_i| \wedge H_i < G\}$, $h(H_i) = hH_ih^{-1}$
- X teilen in disjunkte Bahnen $B_1, ..., B_r$ mit $B_1 = \{H\}$

Beweis des 3.Sylow-Satzes

Beweis: p teilt $k-1$

- H operiert auf $X = \{H_i | p^l = |H_i| \wedge H_i < G\}$, $h(H_i) = hH_ih^{-1}$
- X teilen in disjunkte Bahnen $B_1, ..., B_r$ mit $B_1 = \{H\}$
- Sei B_j eine Bahn mit $B_j = \{H_i\}$, aus $|H| = |H(H_i)||B_j|$ folgt $hH_ih^{-1} = H_i$ für alle $h \in H$

Beweis des 3.Sylow-Satzes

Beweis: p teilt $k-1$

- H operiert auf $X = \{H_i | p^l = |H_i| \wedge H_i < G\}$, $h(H_i) = hH_ih^{-1}$
- X teilen in disjunkte Bahnen $B_1, ..., B_r$ mit $B_1 = \{H\}$
- Sei B_j eine Bahn mit $B_j = \{H_i\}$, aus $|H| = |H(H_i)||B_j|$ folgt $hH_ih^{-1} = H_i$ für alle $h \in H$
- Somit gilt $H \subset G(H_i)$ und $H_i \subset G(H_i)$ und somit H, H_i sind p-Sylow-UG von $G(H_i)$

Beweis des 3.Sylow-Satzes

Beweis: p teilt $k-1$

- H operiert auf $X = \{H_i | p^l = |H_i| \wedge H_i < G\}$, $h(H_i) = hH_ih^{-1}$
- X teilen in disjunkte Bahnen $B_1, ..., B_r$ mit $B_1 = \{H\}$
- Sei B_j eine Bahn mit $B_j = \{H_i\}$, aus $|H| = |H(H_i)||B_j|$ folgt $hH_ih^{-1} = H_i$ für alle $h \in H$
- Somit gilt $H \subset G(H_i)$ und $H_i \subset G(H_i)$ und somit H, H_i sind p-Sylow-UG von $G(H_i)$
- Da $H_i \lhd G(H_i)$(Lemma 2) gilt für $g \in G(H_i)$ $H \overset{Lemma2}{=} gH_ig^{-1} = H_i$

Beweis des 3.Sylow-Satzes

Beweis: p teilt $k-1$

- H operiert auf $X = \{H_i | p^l = |H_i| \wedge H_i < G\}$, $h(H_i) = hH_ih^{-1}$
- X teilen in disjunkte Bahnen $B_1, ..., B_r$ mit $B_1 = \{H\}$
- Sei B_j eine Bahn mit $B_j = \{H_i\}$, aus $|H| = |H(H_i)||B_j|$ folgt $hH_ih^{-1} = H_i$ für alle $h \in H$
- Somit gilt $H \subset G(H_i)$ und $H_i \subset G(H_i)$ und somit H, H_i sind p-Sylow-UG von $G(H_i)$
- Da $H_i \lhd G(H_i)$(Lemma 2) gilt für $g \in G(H_i)$ $H \overset{Lemma2}{=} gH_ig^{-1} = H_i$
- Aus $|B_j| > 1$ für $j \neq 1$ und $p^l = |H| = |H(H_i)||B_j|$ folgt $k = |X| = 1 + p^{k_1} + p^{k_2} + ... + p^{k_r}$ und somit p teilt $k-1$

Einige Gruppen kleiner Ordnung

Satz von Cauchy

Satz von Cauchy

Sei G eine endliche Gruppe und p eine Primzahl, die die Ordnung der Gruppe teilt. Dann enthält G ein Element der Ordnung p.

Satz von Cauchy

Sei G eine endliche Gruppe und p eine Primzahl, die die Ordnung der Gruppe teilt. Dann enthält G ein Element der Ordnung p.

Für endliche Gruppen gilt $\langle g \rangle = \{e, g, g^2, ..., g^n\}$.

Satz von Cauchy

Sei G eine endliche Gruppe und p eine Primzahl, die die Ordnung der Gruppe teilt. Dann enthält G ein Element der Ordnung p.

Für endliche Gruppen gilt $\langle g \rangle = \{e, g, g^2, ..., g^n\}$.

Beweis:

- Sei H Sylow-Untergruppe der Ordnung p^l und $1 \neq h \in H$

Satz von Cauchy

Sei G eine endliche Gruppe und p eine Primzahl, die die Ordnung der Gruppe teilt. Dann enthält G ein Element der Ordnung p.

Für endliche Gruppen gilt $\langle g \rangle = \{e, g, g^2, ..., g^n\}$.

Beweis:

- Sei H Sylow-Untergruppe der Ordnung p^l und $1 \neq h \in H$
- $|\langle h \rangle|$ teilt $|H| \Rightarrow |\langle h \rangle| = |h| = p^k, 0 < k \leq l$

Satz von Cauchy

Sei G eine endliche Gruppe und p eine Primzahl, die die Ordnung der Gruppe teilt. Dann enthält G ein Element der Ordnung p.

Für endliche Gruppen gilt $\langle g \rangle = \{e, g, g^2, ..., g^n\}$.

Beweis:

- Sei H Sylow-Untergruppe der Ordnung p^l und $1 \neq h \in H$
- $|\langle h \rangle|$ teilt $|H| \Rightarrow |\langle h \rangle| = |h| = p^k, 0 < k \leq l$
- $g = h^{p^{k-1}}$ hat Ordnung p, da $g^p = h^{p * p^{k-1}} = 1$ und $g \neq 1$ und Ordnung von g muss $|H|$ teilen

Anwendung von Satz von Cauchy

Korollar

Sei p eine Primzahl, dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung p.

Anwendung von Satz von Cauchy

Korollar

Sei p eine Primzahl, dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung p.

Es gibt nur eine zyklische Gruppe der Ordnung p.
(2.15 [Rosebrock, 2019])

Anwendung von Satz von Cauchy

Korollar

Sei p eine Primzahl, dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung p.

Es gibt nur eine zyklische Gruppe der Ordnung p.
(2.15 [Rosebrock, 2019])

Beweis:

- Sei G eine Gruppe mit $|G| = p$

Anwendung von Satz von Cauchy

Korollar

Sei p eine Primzahl, dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung p.

Es gibt nur eine zyklische Gruppe der Ordnung p.
(2.15 [Rosebrock, 2019])

Beweis:

- Sei G eine Gruppe mit $|G| = p$
- Aus dem Satz von Cauchy folgt, es gibt $g \in G$ mit $|g| = p$

Anwendung von Satz von Cauchy

Korollar

Sei p eine Primzahl, dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung p.

Es gibt nur eine zyklische Gruppe der Ordnung p.
(2.15 [Rosebrock, 2019])

Beweis:

- Sei G eine Gruppe mit $|G| = p$
- Aus dem Satz von Cauchy folgt, es gibt $g \in G$ mit $|g| = p$
- Somit ist $< g >= G$ und somit G zyklisch.

Anwendung von Satz von Cauchy

Korollar

Sei p eine Primzahl, dann gibt es bis auf Isomorphie nur eine Gruppe der Ordnung p.

Es gibt nur eine zyklische Gruppe der Ordnung p.
(2.15 [Rosebrock, 2019])

Beweis:

- Sei G eine Gruppe mit $|G| = p$
- Aus dem Satz von Cauchy folgt, es gibt $g \in G$ mit $|g| = p$
- Somit ist $< g >= G$ und somit G zyklisch.
- Also ist $G \cong \mathbb{Z}_p$

Einige Gruppen kleiner Ordnung

- Sei p eine Primzahl mit $p \geq 3$ und G eine Gruppe der Ordnung $2p$, so ist G isomorph zu $\mathbb{Z}_{2p}$ oder D_p

Einige Gruppen kleiner Ordnung

- Sei p eine Primzahl mit $p \geq 3$ und G eine Gruppe der Ordnung $2p$, so ist G isomorph zu $\mathbb{Z}_{2p}$ oder D_p

- Ist p eine Primzahl, so sind alle Gruppen der Ordnung p^2 abelsch

Einige Gruppen kleiner Ordnung

- Sei p eine Primzahl mit $p \geq 3$ und G eine Gruppe der Ordnung $2p$, so ist G isomorph zu $\mathbb{Z}_{2p}$ oder D_p
- Ist p eine Primzahl, so sind alle Gruppen der Ordnung p^2 abelsch
- Seien $p > q$ Primzahlen und sei G eine Gruppe der Ordnung pq und $q \nmid (p-1)$, dann ist G isomorph zu $\mathbb{Z}_{pq}$

Ordnung	**Anzahl**	**Abelsch**	**Nichtabelsch**
1	1	Triviale Gruppe $\{e\}$	
2	1	$\mathbb{Z}_2$	
3	1	$\mathbb{Z}_3 \cong A_3$	
4	2	$\mathbb{Z}_4,\ D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	1	$\mathbb{Z}_5$	
6	2	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$	$D_3 \cong S_3$
7	1	$\mathbb{Z}_7$	
8	5	$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_4, Q
9	2	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	2	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$	D_5
11	1	$\mathbb{Z}_{11}$	
12	5	$\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2$	$D_6, A_4, \mathbb{Z}_3 \rtimes \mathbb{Z}_4$
13	1	$\mathbb{Z}_{13}$	
14	2	$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$	D_7
15	1	$\mathbb{Z}_{15}$	

[Rosebrock, 2019]

Klassifikationsprogramm der einfachen endlichen Gruppen

Klassifikationsprogramm der einfachen endlichen Gruppen

Definition: einfache Gruppe

Eine Gruppe heißt einfach, falls sie als Normalteiler nur G und $\{e\}$ besitzt und falls $G \neq \{e\}$

Es gibt das Klassifikationsprogramm der einfachen endlichen Gruppen in dem alle einfachen endlichen Gruppen bestimmt sind.

Historischer Hintergrund

- Über 100 Mathematiker waren von Ende der 1920er bis Anfang der 1980er Jahre daran beteiligt

[Wikipedia, 2021]

Historischer Hintergrund

- Über 100 Mathematiker waren von Ende der 1920er bis Anfang der 1980er Jahre daran beteiligt
- Der frühere Beweis verteilt sich auf über 500 Fachartikel mit zusammen fast 15.000 gedruckten Seiten

[Wikipedia, 2021]

Historischer Hintergrund

- Über 100 Mathematiker waren von Ende der 1920er bis Anfang der 1980er Jahre daran beteiligt
- Der frühere Beweis verteilt sich auf über 500 Fachartikel mit zusammen fast 15.000 gedruckten Seiten
- Um 1980 "vorläufiger" Abschluss aber erst 2002 wurden alle Lücken geschlossen

[Wikipedia, 2021]

Historischer Hintergrund

- Über 100 Mathematiker waren von Ende der 1920er bis Anfang der 1980er Jahre daran beteiligt
- Der frühere Beweis verteilt sich auf über 500 Fachartikel mit zusammen fast 15.000 gedruckten Seiten
- Um 1980 "vorläufiger" Abschluss aber erst 2002 wurden alle Lücken geschlossen
- Diese Version hat ungefähr 1200 Seiten

[Wikipedia, 2021]

Historischer Hintergrund

- Über 100 Mathematiker waren von Ende der 1920er bis Anfang der 1980er Jahre daran beteiligt
- Der frühere Beweis verteilt sich auf über 500 Fachartikel mit zusammen fast 15.000 gedruckten Seiten
- Um 1980 "vorläufiger" Abschluss aber erst 2002 wurden alle Lücken geschlossen
- Diese Version hat ungefähr 1200 Seiten
- Ronald Solomon, Richard Lyons und Daniel Gorenstein begannen 1994 eine auf 12 Bände angelegte Darstellung des Beweises, die 2023 abgeschlossen werden soll

[Wikipedia, 2021]

Klassifikationsprogramm der einfachen endlichen Gruppen

- $\mathbb{Z}_p$, wobei p eine Primzahl ist

[Wikipedia, 2021]

Klassifikationsprogramm der einfachen endlichen Gruppen

- $\mathbb{Z}_p$, wobei p eine Primzahl ist
- A_n für $n > 4$

[Wikipedia, 2021]

Klassifikationsprogramm der einfachen endlichen Gruppen

- $\mathbb{Z}_p$, wobei p eine Primzahl ist
- A_n für $n > 4$
- 26 sporadische Gruppen

[Wikipedia, 2021]

Klassifikationsprogramm der einfachen endlichen Gruppen

- $\mathbb{Z}_p$, wobei p eine Primzahl ist
- A_n für $n > 4$
- 26 sporadische Gruppen
- 16 Familien von Lie-Typ, die sich von gewissen Lie-Algebren herleiten

[Wikipedia, 2021]

Quellen:

Rosebrock, S. (2019).
Anschauliche Gruppentheorie: Eine computerorientierte geometrische Einführung.
Springer Berlin Heidelberg.

Wikipedia (2021).
Endliche einfache Gruppe — Wikipedia, the free encyclopedia.
http://de.wikipedia.org/w/index.php?title=Endliche%20einfache%20Gruppe&oldid=207008386.
[Online; accessed 24-January-2021].