Script generated by TTT

Title: Mayr: 2012 ds (15.11.2012)

Date: Thu Nov 15 10:15:40 CET 2012

Duration: 91:50 min

Pages: 30

Satz 82

Sei G eine endliche Gruppe; dann hat auch jedes Element in G endliche Ordnung.

Beweis:

Betrachte die Abbildung

$$\mathbb{N}_0 \ni i \mapsto a^i \qquad a \in G \text{ beliebig } \neq 1$$

Also gibt es (pigeon hole principle) minimale k und j, $0 \leq j \leq k-1$, so dass

$$a^j = a^k.$$

Daraus folgt:

$$a^{k-j} = a^0 = 1.$$

Da k minimal gewählt wurde, folgt $j = 0$ und $\mathrm{ord}(a) = k$. □

Beispiel 83

Betrachte $(\mathbb{Z}_{12}, +_{12}, 0)$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}(a)$	-	12	6	4	3	12	2	12	3	4	6	12

5.4 Untergruppen

Definition 84

Eine Unteralgebra $(T, \circ, 1)$ einer Gruppe $G = (S, \circ, 1)$ heißt Untergruppe von G, falls $(T, \circ, 1)$ eine Gruppe ist.

Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

5.4 Untergruppen

Definition 84

Eine Unteralgebra $(T, \circ, 1)$ einer Gruppe $G = (S, \circ, 1)$ heißt Untergruppe von G, falls $(T, \circ, 1)$ eine Gruppe ist.

Bemerkung: Nicht jede Unteralgebra einer Gruppe ist eine Untergruppe!

Beispiel 85

$(\mathbb{N}_0, +, 0)$ ist Unteralgebra von $(\mathbb{Z}, +, 0)$, aber keine Gruppe, da es im allgemeinen keine inversen Elemente gibt.

Satz 86

Eine Unteralgebra (bzgl. $\circ$) einer Gruppe ist eine Untergruppe, falls sie unter der Inversenbildung $^{-1}$ abgeschlossen ist.

Beweis:

Folgt sofort aus der Definition. □

Satz 87

Jede Unteralgebra (bzgl. $\circ$) einer endlichen Gruppe ist eine Untergruppe.

Beweis:

Sei $(T, \circ, 1)$ eine Unteralgebra einer endlichen Gruppe $(S, \circ, 1)$. Sei $b \in T$, $b \neq 1$. Dann gilt:

$$\mathrm{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei $m := \mathrm{ord}(b)$. Dann gilt:

$$1 = b^m = b^{m-1} \circ b = b \circ b^{m-1}$$

d. h. $b^{m-1} \in T$ ist das Inverse zu b. □

Satz 87

Jede Unteralgebra (bzgl. $\circ$) einer endlichen Gruppe ist eine Untergruppe.

Beweis:

Sei $(T, \circ, 1)$ eine Unteralgebra einer endlichen Gruppe $(S, \circ, 1)$. Sei $b \in T$, $b \neq 1$. Dann gilt:

$$\mathrm{ord}(b) \in \mathbb{N} \setminus \{1\}$$

Sei $m := \mathrm{ord}(b)$. Dann gilt:

$$1 = b^m = b^{m-1} \circ b = b \circ b^{m-1}$$

d. h. $b^{m-1} \in T$ ist das Inverse zu b. □

Satz 88

- *Sei $G = (S, \circ, 1)$, $b \in G$ und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b erzeugte Untergruppe von G. S_b ist die kleinste Untergruppe, die b enthält.

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien $G_1 = (S_1, \circ, 1)$ und $G_2 = (S_2, \circ, 1)$ Untergruppen von $G = (S, \circ, 1)$. Dann ist auch*

$$G_1 \cap G_2 = (S_1 \cap S_2, \circ, 1)$$

eine Untergruppe von G.

Satz 88

- *Sei $G = (S, \circ, 1)$, $b \in G$ und sei*

$$S_b := \{b^m;\ m \in \mathbb{Z}\} \subseteq S$$

die von b erzeugte Untergruppe von G. S_b ist die kleinste Untergruppe, die b enthält.

- *Das Bild einer Gruppe (Halbgruppe, Monoid) unter einem Homomorphismus ist wieder eine Gruppe (Halbgruppe, Monoid).*
- *Seien $G_1 = (S_1, \circ, 1)$ und $G_2 = (S_2, \circ, 1)$ Untergruppen von $G = (S, \circ, 1)$. Dann ist auch*

$$G_1 \cap G_2 = (S_1 \cap S_2, \circ, 1)$$

eine Untergruppe von G.

Beispiel 90

Betrachte $(\mathbb{Z}_{12}^*,\ \cdot_{12}\ , 1) = (\{1, 5, 7, 11\},\ \cdot_{12}\ , 1)$. Dann gilt: Die Untergruppe $(\{1, 5\},\ \cdot_{12}\ , 1)$ ist Normalteiler (folgt aus Definition).

Satz 91

Sei H Untergruppe von G, $b \in G$. Dann ist die Kardinalität von $H \circ b$ gleich der Kardinalität von H (ebenso für $b \circ H$).

Beweis:
Folgt aus der Kürzungsregel: Betrachte die Abbildung

$$H \ni h \mapsto h \circ b \in H \circ b.$$

Diese Abbildung ist surjektiv und injektiv (Kürzungsregel!):

$$h_1 \circ b = h_2 \circ b \Rightarrow h_1 = h_2$$

□

5.5 Nebenklassen und Normalteiler

Definition 89

Sei $H = (T, \circ, 1)$ eine Untergruppe von $G = (S, \circ, 1)$ und sei $b \in G$. Dann heißt

$$T \circ b := \{c \circ b;\ c \in T\} =: H \circ b$$

eine rechte Nebenklasse von H in G und

$$b \circ T := \{b \circ c;\ c \in T\} =: b \circ H$$

eine linke Nebenklasse von H in G (engl.: coset).

Die Anzahl verschiedener Nebenklassen von H in G heißt der Index von H in G:

$$\mathrm{ind}(H) = \mathrm{ind}_G(H).$$

H heißt Normalteiler von G, falls

$$H \circ b = b \circ H \quad \forall b \in G$$

d. h. H ist Normalteiler genau dann, wenn $\forall b \in G: H = b \circ H \circ b^{-1}$ („konjugiert").

Satz 92

Sei H Untergruppe von G. Dann bildet die Menge der rechten (linken) Nebenklassen von H eine Partition (Zerlegung einer Menge in disjunkte Teilmengen) von G.

Beweis:
Klar ist, dass

$$G \subseteq \bigcup_{b \in G} H \circ b$$

.

Eigenschaften von Nebenklassen:

H sei Untergruppe von G, $b, c \in G$.

- Zwei Nebenklassen $H \circ b$ und $H \circ c$ sind entweder identisch oder disjunkt.
- Für alle $b \in G$ gilt $|H \circ b| = |H|$.

Satz 93 (Lagrange)

Sei G eine endliche Gruppe und H eine Untergruppe in G. Dann

1. *haben alle Nebenklassen von H in G gleich viele Elemente;*
2. *ist $|G| = \mathrm{ind}_G(H) \cdot |H|$;*
3. *teilt $|H|$ die Kardinalität $|G|$ von G ganzzahlig.*

Beweis:

Mehr zu Joseph-Louis Lagrange!

□

5.6 Satz von Fermat

Satz 94

Sei $b \in \mathbb{N}_0$ und $p \in \mathbb{N}$ eine Primzahl. Dann gilt:

$$b^p \equiv b \bmod p, \quad (\text{falls } b \not\equiv 0 \bmod p \ : \ b^{p-1} \equiv 1 \bmod p)$$

(gemeint ist: die Gleichung $b^p = b$ gilt modulo p)

Beweis:

$\mathbb{Z}_p^* := \{n \in \{1, \ldots, p-1\}; \mathrm{ggT}(n,p) = 1\}$

1. Fall: $b = 0$: $0^p = 0 \bmod p$
2. Fall: $1 \le b < p$: Betrachte $S_b = (\{b^0, b^1, \ldots, b^{\mathrm{ord}(b)-1}\}, \cdot)$;
   S_b ist Untergruppe von $\mathbb{Z}_p^*$.
   Lagrange: $(\mathrm{ord}(b) =)\ |S_b| \ |(|\mathbb{Z}_p^*| (= p-1)$
   $$\Rightarrow (\exists q \in \mathbb{N})[q \cdot \mathrm{ord}(b)] = p-1$$
   Da $b^{\mathrm{ord}(b)} = 1$ (Einselement) ist, gilt:
   $$b^p = b^{p-1} \cdot b = b^{\mathrm{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$
3. Fall: $b \ge p$: Dann gilt:
   $$(\exists q, r \in \mathbb{N}_0, 0 \le r < p)[b = q \cdot p + r].$$
   Damit:
   $$b^p = (q \cdot p + r)^p \overset{(*)}{\equiv} r^p \bmod p \overset{(**)}{\equiv} r \bmod p = b \bmod p$$
   (*) Binomialentwicklung, die ersten p Summanden fallen weg, da jeweils $= 0 \bmod p$.
   (**) Fall 1 bzw. 2

□

Beweis:
$\mathbb{Z}_p^* := \{n \in \{1, \ldots, p-1\}; \text{ggT}(n,p) = 1\}$

1. Fall: $b = 0$: $0^p = 0 \bmod p$
2. Fall: $1 \leq b < p$: Betrachte $S_b = (\{b^0, b^1, \ldots, b^{\text{ord}(b)-1}\}, \cdot)$.
   S_b ist Untergruppe von $\mathbb{Z}_p^*$.
   Lagrange: $(\text{ord}(b) =)\ |S_b|\ ||\mathbb{Z}_p^*| (= p-1)$

$$\Rightarrow (\exists q \in \mathbb{N})[q \cdot \text{ord}(b)] = p - 1$$

   Da $b^{\text{ord}(b)} = 1$ (Einselement) ist, gilt:

$$b^p = b^{p-1} \cdot b = b^{q \cdot \text{ord}(b)} \cdot b = 1^q \cdot b = b \bmod p$$

3. Fall: $b \geq p$: Dann gilt:

$$(\exists q, r \in \mathbb{N}_0, 0 \leq r < p)[b = q \cdot p + r].$$

   Damit:

$$b^p = (q \cdot p + r)^p \overset{(*)}{=} r^p \bmod p \overset{(**)}{=} r \bmod p = b \bmod p$$

   $(*)$ Binomialentwicklung, die ersten p Summanden fallen weg, da jeweils $= 0 \bmod p$;
   $(**)$ Fall 1 bzw. 2

□

Die umgekehrte Richtung

Satz 95
Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

$$b^{n-1} \equiv 1 \bmod n \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \Longrightarrow n \text{ ist prim.}$$

Beweis:
[durch Widerspruch] Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \overset{\text{n.V.}}{\equiv} 0 \bmod n\ ,$$

also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n\ .$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Die umgekehrte Richtung

Satz 95
Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

$$b^{n-1} \equiv 1 \bmod n \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \Longrightarrow n \text{ ist prim.}$$

Beweis:
[durch Widerspruch] Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \overset{\text{n.V.}}{\equiv} 0 \bmod n\ ,$$

also

$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n\ .$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Die umgekehrte Richtung

Satz 95
Sei $n \in \mathbb{N}$, $n \geq 2$. Dann gilt:

$$b^{n-1} \equiv 1 \bmod n \text{ für alle } b \in \mathbb{Z}_n \setminus \{0\} \Longrightarrow n \text{ ist prim.}$$

Beweis:
[durch Widerspruch] Annahme: $r|n$ für ein $r \in \mathbb{N}$, $r > 1$. Dann

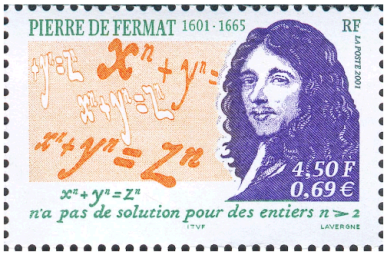
$$r^{n-1} - 1 \equiv (r \bmod n)^{n-1} - 1 \overset{\text{n.V.}}{\equiv} 0 \bmod n\ ,$$

also

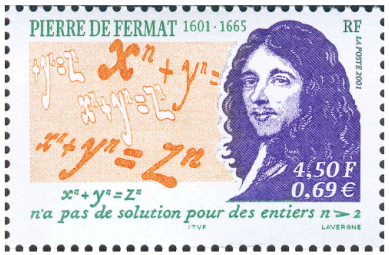
$$r^{n-1} - 1 = q \cdot n = q \cdot q' \cdot r \text{ da } r|n\ .$$

Daraus folgt aber, dass $r|1$, n also keinen nichttrivialen Teiler besitzen kann. □

Pierre de Fermat (1601–1665)



Pierre de Fermat (1601–1665)



Definition 96 (Eulersche phi-Funktion)

Sei $n \in \mathbb{N}$, $n > 1$. Dann bezeichnet

$$\varphi(n) := |\mathbb{Z}_n^*|$$

die Anzahl der zu n teilerfremden Reste.

Satz 97

Sei $n \in \mathbb{N}$, $n > 1$. Dann gilt in der Gruppe $(\mathbb{Z}_n^*, \times_n, 1)$:

$$b^{\varphi(n)} = 1 \text{ für alle } b \in \mathbb{Z}_n^* .$$

Beweis:
Folgt sofort aus dem Satz von Lagrange (Satz 93)! □

Leonhard Euler (1707–1783)

Leonhard Euler (1707–1783)

5.7 Zyklische Gruppen

Definition 98
Eine Gruppe $G = (S, \circ, 1)$ heißt zyklisch, wenn es ein $b \in G$ gibt, so dass

$$G = S_b$$

wobei $S_b = (\{b^i | i \in \mathbb{Z}\}, \circ, 1)$.

Satz 99
Sei G eine zyklische Gruppe. Falls G unendlich ist, ist G zu $(\mathbb{Z}, +, 0)$ isomorph; falls G endlich ist, dann ist G isomorph zu $(\mathbb{Z}_m, +_m, 0)$ für ein $m \in \mathbb{N}$.

Beweis:

1. Fall: Sei G unendlich. Wir wissen: $G = \{b^i | i \in \mathbb{Z}\}$ für ein geeignetes $b \in G$, nach Voraussetzung.
Betrachte die Abbildung

$$h : \mathbb{Z} \ni i \mapsto b^i \in G$$

Behauptung: h ist bijektiv.
Nach Voraussetzung ist h surjektiv.
Die Injektivität beweisen wir mittels Widerspruch.

Annahme: $(\exists i, j, i \neq j)[b^i = b^j]$
Daraus folgt:

$$b^{i-j} = 1$$

Daher ist G endlich, es gilt nämlich:

$$G \subseteq \{b^k; 0 \leq k < |i - j|\}$$

Dies ist ein Widerspruch zur Annahme, G sei unendlich!

Beweis (Forts.):

2. Fall: G endlich:
Wiederum ist die Abbildung h nach Voraussetzung surjektiv. Nach dem Schubfachprinzip

$$(\exists i, j, i \neq j)[b^i = b^j] .$$

Nach der Kürzungsregel können wir $j = 0$ wählen. Falls $i > 0$ und i minimal gewählt wird, folgt sofort

G isomorph $(\mathbb{Z}_i, +_i, 0)$.

□

Beweis:

1. Fall: Sei G unendlich. Wir wissen: $G = \{b^i | i \in \mathbb{Z}\}$ für ein geeignetes $b \in G$, nach Voraussetzung.
Betrachte die Abbildung

$$h : \mathbb{Z} \ni i \mapsto b^i \in G$$

Behauptung: h ist bijektiv.
Nach Voraussetzung ist h surjektiv.
Die Injektivität beweisen wir mittels Widerspruch.

Annahme: $(\exists i, j, i \neq j)[b^i = b^j]$
Daraus folgt:

$$b^{i-j} = 1$$

Daher ist G endlich, es gilt nämlich:

$$G \subseteq \{b^k; 0 \leq k < |i - j|\}$$

Dies ist ein Widerspruch zur Annahme, G sei unendlich!

Beweis (Forts.):

2. Fall: G endlich:
Wiederum ist die Abbildung h nach Voraussetzung surjektiv. Nach dem Schubfachprinzip

$$(\exists i, j, i \neq j)[b^i = b^j] .$$

Nach der Kürzungsregel können wir $j = 0$ wählen. Falls $i > 0$ und i minimal gewählt wird, folgt sofort

G isomorph $(\mathbb{Z}_i, +_i, 0)$.

□

Loading Image...

Satz 100
Jede Untergruppe einer zyklischen Gruppe ist wieder zyklisch.

Beweis:
Sei G zyklisch, $H \subseteq G$ Untergruppe von G.

1. Fall: $|G| = \infty$, also $G \cong (\mathbb{Z}, +, 0)$ ($\cong$ isomorph).
Sei H' die durch den Isomorphismus gegebene Untergruppe von $(\mathbb{Z}, +, 0)$, die H entspricht.
Zu zeigen ist: H' ist zyklisch.
Sei $i := \min\{k \in H'; k > 0\}$.
Die Behauptung ist:

$$H' = S_i.$$

Es gilt sicher:

$$S_i \subseteq H'.$$

Falls ein $k \in H' \setminus S_i$ existiert, folgt $k \bmod i \in H'$. Dies stellt einen Widerspruch zur Wahl von i dar. Also ist $H' = S_i$, damit ist gezeigt, dass H' und daher auch H zyklisch ist.

2. Fall: $|G| < \infty$: Der Beweis läuft analog.

□