PROSEMINAR LINEARE ALGEBRA

von Daniel Cagara

Zunächst benötigen wir einige Elemente der Gruppentheorie.

Definition 1. *Eine Gruppe ist ein Tupel, bestehend aus einer nicht leeren Menge G und einer Verknüpfung $\circ$, für das folgende Bedingungen gelten:*

i. Die Verknüpfung der Gruppe ist assoziativ, d.h. für beliebige Elemente a, $b, c \in G$ gilt

$$(a \circ b) \circ c = a \circ (b \circ c)$$

ii. Es existiert ein neutrales Element, d.h. es gibt ein Element $e \in G$ sodass gilt

$$a \circ e = e \circ a = a\,,\ \forall a \in G$$

iii. Zu jedem Element $a \in G$ existiert ein inverses Element $b \in G$, d.h. es gilt

$$a \circ b = b \circ a = e$$

Dabei wird das inverse Element b auch als a^{-1} bezeichnet.

Definition 2. *Eine Gruppe $(G, \circ)$ nennt man kommutativ, oder auch abelsch, wenn für alle Elemente $a, b \in G$ gilt dass*

$$a \circ b = b \circ a$$

Definition 3. *Zwei Gruppen G_1 und G_2 nennt man isomorph, wenn eine bijektive Abbildung*

$$\phi\colon G_1 \to G_2$$

existiert, sodass für beliebige zwei Elemente $a, b \in G$ die Bedingung

$$\phi(a\,b) = \phi(a)\phi(b)$$

stets erfüllt ist.

Beispiel 4. Betrachte die zwei Gruppen

$$G_1 = (\mathbb{Z}, +)\ \ G_2 = (2\mathbb{Z}, +)$$

Ferner betrachte die Abbilung

$$\phi\colon \mathbb{Z} \to 2\mathbb{Z},\ \phi(x) = 2x$$

Offensichtlich ist die Bedingung aus Definition 3 erfüllt, da

$$\phi(a+b) = 2(a+b) = 2a + 2b = \phi(a) + \phi(b)$$

Die Bijektivität folgt aus der Gleichmächtigkeit der Mengen $\mathbb{Z}$ und $2\mathbb{Z}$, und somit sind die Gruppen G_1 und G_2 isomorph.

Definition 5. *Gegeben sei eine nichtleere Menge K, sowie zwei Verknüpfungen $+$ und $\cdot$.*

K heisst mit diesen beiden Verknüpfungen ein Ring, wenn folgende Bedingungen erfüllt sind:

i. K bildet bezühlich der Verknüpfung $+$ eine abelsche Gruppe, d.h.

- *Die Verknüpfung $+$ ist kommutativ, und es gilt für beliebige Elemente $a, b, c \in K$* dass

$$(a+b)+c = a+(b+c)$$

- *Es existiert ein neutrales Element $e \in K$ sodass für ein $a \in K$ gilt*

$$a + e = e + a = a$$

- *Es existiert für jedes $a \in K$ ein inverses Element $b \in K$, sodass gilt*

$$a + b = b + a = e$$

- *Die Vorraussetzung für Kommutativität ist erfüllt, d.h für zwei beliebige Elemente $a, b \in K$ gilt*

$$a + b = b + a$$

ii. Es gelten sowohl linke als auch rechte Distributivgesetze, d.h. für beliebige $a, b, c \in K$ gelten folgende Bedingungen

$$a \cdot b + a \cdot c = a \cdot (b+c)$$
$$a \cdot c + b \cdot c = (a+b) \cdot c$$

Anmerkung 6. Im weiteren Verlauf schreiben wir statt $a \cdot b$ nur $a\,b$.

Definition 7. *Ein Ring heisst assoziativ, wenn für beliebige $a, b, c \in K$ gilt, dass*

$$(a\,b)\,c = a\,(b\,c)$$

Definition 8. *Ein Ring heisst kommutativ, wenn für beliebige $a, b \in K$ gilt, dass*

$$a\,b = b\,a$$

Definition 9. *Sei K ein Ring, und $b \in K$. Man nennt b das Einselement von K wenn für beliebige $a, b \in K$ folgendes erfüllt ist*

$$b\,a = a = a\,b$$

Ein Ring enthält entweder genau ein oder kein Einselement. Man bezeichnet das Einselement auch mit 1*.*

Definition 10. *Sei $(K, +, \cdot)$ ein Ring. Das Tupel $(K, +)$ wird als additive Gruppe des Ringes K bezeichnet, und wird oft mit K^+ notiert.*

Warnung 11. Sei $(K, +, \cdot)$ ein Ring. Das Tupel $(K, \cdot)$ ist im Allgemeinen keine Gruppe. Das neutrale Element bezüglich der Addition, die 0, hat zum Beispiel kein inverses Element. Durchaus kann aber eine Teilmenge von K bezüglich der Verknüpfung $\cdot$ eine Gruppe bilden.

Definition 12. *Sei $(K, +, \cdot)$ ein assoziativer und kommutativer Ring, mit Einselement 1.*

Definiere K_{inv} als die Teilmenge von K, für dessen Elemente das inverse Element existiert.

Das Tupel $(K_{\text{inv}}, \cdot)$ bildet eine Gruppe. Diese Gruppe wird als „multiplikative Gruppe des Ringes K“ bezeichnet. Für diese Gruppe schreiben wir K^*.

Definition 13. *Seien K_1 und K_2 Ringe. Sie heissen isomorph, wenn eine bijektive Abbildung*

$$\phi\colon K \to K$$

existiert, für die für beliebige Elemente $a, b \in K$ folgende Bedingungen gelten

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(a\,b) &= \phi(a)\,\phi(b) \end{aligned}$$

Beispiel 14. Betrachte die Ringe $K_1 := (\mathbb{C}, +, \cdot), K_2 := (\mathbb{C}, +, \cdot)$

Betrachte nun die bijektive Abbldung

$$\phi\colon \mathbb{C} \to \mathbb{C},\ \phi(x) = \bar{x}$$

welche ein Element x auf sein Komplexkonjugiertes abbildet. Die Abbildung ist bijektiv, und die Voraussetzungen aus Definition 12 können leicht nachgerechnet werden:

$$\phi(a+b) = \overline{(a+b)} = \bar{a} + \bar{b} = \phi(a) + \phi(b)$$

sowie

$$\phi(a\,b) = \overline{(a\,b)} = \bar{a}\,\bar{b} = \phi(a)\,\phi(b)$$

Somit sind die Ringe K_1 und K_2 isomorph.

Die Struktur des Restklassenringes

Definition 15. ***Restklassenring***

Wähle ein festes $m \in \mathbb{Z}$ und Definiere die Menge

$$\mathbb{Z}_m = \{0, 1, 2, ..., m-1\}$$

Ferner definiere für die Funktion

$$\mathrm{Rest}_m(x) := x - m\,q = r \in \mathbb{Z}$$

unter der Nebenbedingung dass $0 \leqslant r \leqslant m-1$. Wenn wir nun ein beliebiges x einsetzen, bekommen wir Werte aus der Menge $\mathbb{Z}_m$.

Weiter definieren wir eine Addition und eine Multiplikation auf dieser Menge durch

$$\text{Addition: } a \dot{+} b = \mathrm{Rest}_m(a+b)$$
$$\text{Multiplikation: } a \bullet b = \mathrm{Rest}_m(a \cdot b)$$

*Mit diesen beiden Verknüpfungen bildet $\mathbb{Z}_m$ einen assoziativen, kommutativen Ring mit Einselement 1. Wir nennen diesen Ring auch „**Restklassenring modulo m**“.*

Definition 16. *Seien $K_1 .... K_s$ Ringe. Definiere die Menge*

$$K_1 \oplus .... \oplus K_s = \{(r_1, ..., r_s) \mid r_i \in K_i : 1 \leqslant i \leqslant s\}$$

Sie bildet mit den beiden Verknüpfungen $+$ und $\cdot$

$$(r_1, ..., r_s) + (r'_1, ..., r'_2) = (r_1 + r'_1, ..., r_s + r'_s)$$
$$(r_1, ..., r_s) \cdot (r'_1, ..., r'_2) = (r_1 \cdot r'_1, ..., r_s \cdot r'_s)$$

einen Ring. Dieser Ring wird auch kartesische Summe der Ringe K_1, ..., K_s *genannt, wobei* $(0, ..., 0)$ *das neutrale Element, und* $(1, ..., 1)$ *das Einselement ist.*

Definition 17. *Gegeben sei ein Restklassenring* $\mathbb{Z}_m$*, mit der Nebenbedingung* $m = m_1 m_2 ... m_s$ *wobei die* $m_i \in \mathbb{N}_0, 1 \leqslant i \leqslant s$ *paarweise teilerfremd sind. Es gilt*

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus .... \oplus \mathbb{Z}_{m_s}$$

Beweis:

Man wählt sich ein beliebiges Element x aus $\mathbb{Z}_m$ aus. Laut Definition des Restklassenrings muss x im Wertebereich von $[0, m-1]$ liegen. Um obere Äquivalenz zu beweisen, wählen wir eine Abbildung

$$\phi: \mathbb{Z}_m \to \mathbb{Z}_{m_1} \oplus .... \oplus \mathbb{Z}_{m_s} \text{ mit } \phi: x \longmapsto (\text{Rest}_{m_1}(x), ..., \text{Rest}_{m_s}(x)).$$

Ist diese Abildung ein Isomorphismus?

i. Im ersten Schritt zeigen wir, dass diese Abbildung ein injektiv ist, also dass folgende Inklusion gilt:

$$\text{Rest}_{m_i}(x) = \text{Rest}_{m_i}(y) \Rightarrow x = y \text{ mit } x, y \in \mathbb{Z}_m \; 1 \leqslant i \leqslant s$$

Wir gehen davon aus, dass es solche $x, y \in \mathbb{Z}_m$ gibt, sodass gilt

$$\text{Rest}_{m_i}(x) = \text{Rest}_{m_i}(y) \;\; \forall r \leqslant i \leqslant s$$

Wir wissen $x - y$ ist durch m_i teilbar, für alle $1 \leqslant i \leqslant s$. Jetzt sind die m_i teilerfremd, also ist $x - y$ auch durch ihr Produkt $m_1 m_2 .... m_s = m$ teilbar. Da $0 \leqslant x, y \leqslant m - 1$ und aus dem vorherigen Satz lässt sich nun ableiten, dass gelten muss $x = y$.

ii. Da ϕ injektiv ist, und die beiden Mengen der Abbildung gleichmächtig sind, folgt trivialer Weise die Surjektivität dieser Abbildung.

iii. Jetzt gilt es nachzurechnen, ob die Voraussetzungen aus der Definition eines Isomorphismus gelten.

1.

$$\begin{aligned} \phi(x+y) &= \phi(x) + \phi(y) \\ \Rightarrow \text{Rest}_{m_i}(x+y) &= \text{Rest}_{m_i}(\text{Rest}_{m_i}(x) + \text{Rest}_{m_i}(y)) \\ \text{weil: } (x+y) - (\text{Rest}_{m_i}(x) + \text{Rest}_{m_i}(y)) &\text{ durch } m_i \text{ teilbar} \end{aligned}$$

2.

$$\phi(x\,y) = \phi(x)\;\phi(y) \text{ analog.}$$

q.e.d

Definition 18. *Das multiplikative Inverse im Restklassenring.*

Das Multiplikative Inverse im Restklassenring wird mit dem erweiterten Euklidischen Algorithmus bestimmt. Am Folgenden Beispiel möcte ich das Multiplikative Inverse zu a=25 im Restklassenring $\mathbb{Z}_{264}$ bestimmen.

$264 = 10 \cdot 25 + 14$	$14 = 264 - 10 \cdot 25$
$25 = 1 \cdot 14 + 11$	$11 = 11 \cdot 25 - 264$
$14 = 1 \cdot 11 + 3$	$3 = 2 \cdot 264 - 21 \cdot 25$
$11 = 3 \cdot 3 + 2$	$2 = 74 \cdot 25 - 7 \cdot 264$
$3 = 1 \cdot 2 + 1$	$1 = 9 \cdot 264 - 95 \cdot 25$

Das klappt nur dann, wenn a und *m teilerfremd sind, also ggT(a,m)=1*

Das multiplikative Inverse u 25 ist in diesem Fall -95.

Definition 19. *Seien $m_1, m_2, ..., m_s$ paarweise teilerfremde ganze Zahlen.*

Für jedes Tupel x_1, ..., x_s existiert eine ganze Zahl x, sodass folgende Aussagen kongruent sind:

$$\begin{aligned} x &\equiv x_1 \bmod m_1 \\ &\;\;| \\ x &\equiv x_s \bmod m_s \end{aligned}$$

Doch wie findet man eine solche Zahl x. Hierzu bedient man sich folgender Formel:

$$x_0 := \sum_{i=1}^{s} c_i \cdot \frac{m}{m_i} \cdot x_i$$

Dabei ist c_i das Inverse zu $\frac{m}{m_i}$ im Restklassenring $\mathbb{Z}_{m_i}$, d.h. es gibt folgende Kongruenz:

$$c_i \cdot (\frac{m}{m_i}) \equiv 1 \bmod m_i$$

Wir werden jetzt beweisen, dass alle x, mit diesem x_0 kongruent sind modulo m.

Beweis:

Es ist offensichtlich, dass gilt $\frac{m}{m_i}$ *teilbar durch* m_j *ist, und somit ergibt sich*

$$c_i \cdot \frac{m}{m_i} \cdot x_i \equiv 0 \bmod m_j \quad \text{, wenn } i \neq j$$
$$c_i \cdot \frac{m}{m_i} \cdot x_i \equiv x_j \bmod m_j \quad \text{, wenn } i = j$$

Da nun ein Summand übrigbleibt, ist klar dass folgendes gilt:

$$\sum_{i=1}^{s} c_i \cdot \frac{m}{m_i} \cdot x_i \equiv x_j \bmod m_j$$

und zwar für jedes $j = 1 \ldots s$.

Wenn nun x *eine andere Zahl ist, sodass für jedes* $1 \leqslant j \leqslant s$ *erfüllt ist dass* $x_0 \equiv x_j \bmod m_j$*, dann gilt* $x - x_0 \equiv 0$ *für alle* j *weil die* m_i *laut Definition teilerfremd sind.*

Beispiel 20. In diesem Beispiel suchen wir eine Zahl x, welche die folgenden Eigenschaften erfüllt:

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 4$$
$$x \equiv 2 \bmod 5$$

Hier möchte ich konkret vorrechnen wie man diese Kongruenzen löst:

Definition 21. *Eine Gruppe* G *heisst zyklische Gruppe, wenn für jedes Element aus* G *gilt*

$$\forall x \in G, \exists n \in \mathbb{Z} : x = g^n$$

für ein festes g*. Mit anderen Worten heisst das, dass jedes element aus* G *eine Potenz von* g *ist. Dieses* g *nennt man „ein Erzeugendes der Gruppe* G*“. Man schreibt auch* $G = <g>$*, und sagt dass* G *mit* g *„erzeugt ist“.*

Beispiel 22. An dieser Stelle möchte ich einige Beispiele für zyklische Gruppen nennen.

i. $\mathbb{Z}_6^+ = \{0, 1, 2, 3, 4, 5\} = <1> = <5>$ ist eine zyklische Gruppe

ii. $\mathbb{Z}_9^\star = \{1,2,4,5,7,8\} = <2> = <5>$ ist eine zyklische Gruppe

iii. $\mathbb{Z}_8^* = \{1,3,5,7\}$ ist nicht zyklisch! (Es lässt sich kein Element finden, welches durch Potenzieren alle Elemente der Gruppe erzeugt)

Analysieren wir das Beispiel der zyklischen Gruppe $\mathbb{Z}_9^\star$ etwas ausführlicher. Es handelt sich um die multiplikative Gruppe, welche nur die Elemente des Restklassenrings beinhaltet, die ein inverses haben. Die inversen Elemente sind eben $\{1,5,7,2,4,8\}$. Weiterhin können wir die Menge auch schreiben als:

$$\mathbb{Z}_9^* = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\}$$

Hiermit lässt sich ein Isomorphismus definieren von

$$\mathbb{Z}_6^+ \to \mathbb{Z}_9^* \text{ mit der Abbildung } i \to 2^i$$

Definition 23. *Wir betrachten die Gruppe G, mit dem Einselement e und einem beliebigen $g \in G$. Die Ordnung von g, ord(g) entspricht der kleinsten Zahl $n \in \mathbb{N}$, sodass gilt*

$$g^n = e \Rightarrow \text{ord}(g) = n$$

Gibt es ein solches n nicht, so ist die Ordnung $\text{ord}(g) = \infty$.

Lemma 24. *Ist G eine endliche Gruppe, und $g \in G$, dann ist die Ordnung von g endlich, also* $\text{ord}(g) < \infty$.

Beispiel 25. Betrachte die Gruppe $\mathbb{Z}^+ := (\mathbb{Z}, +)$, und ein beliebiges Element $x \in \mathbb{Z}^+ \neq 0$. Es gilt stets $\text{ord}(x) < \infty$.

Beispiel 26. Betrachte die additive Gruppe des Restklassenrings $\mathbb{Z}_6$. Die Ordnungen der Elemente sind

i. ord(0)=1

ii. ord(1)=6 weil $3 \cdot 2 = 0$ aber $1 \cdot 2 \neq 0$ und $2 \cdot 2 \neq 0$

iii. ord(2)=3

iv. ord(3)=2

v. ord(4)=3

vi. ord(5)=6

Beispiel 27. Betrachte die multiplikative Gruppe des Restklassenrings $\mathbb{Z}_8$={1,3,5,7}. Die Ordnungen der Elemente sind:

i. ord(1)=1 weil $1^1 = 1$

ii. ord(3)=2 weil $3^2 = 1$

iii. ord(5)=2

iv. ord(7)=2

Satz 28. *Gegeben sei eine Gruppe G, und ein Element $g \in G$. Sei die Ordnung $n = \mathrm{org}(g) < \infty$.*

Sei nun ein $m \in G$. Wenn m durch n teilbar ist, so gilt

$$g^m = e$$

Beweis. Wenn m durch n teilbar ist, dann ist offensichtlich dass gilt

$$g^m = (g^n)^{m/n} = e$$

Wir nehmen an dass gilt

$$g^m = e$$

und wollen zeigen, dass hieraus folgt: m ist durch n teilbar.

Wir zerlegen m wie folgt:

$$m = q\,n + r\,, \mathrm{mit}\, 0 \leqslant r < n$$

Somit können wir schreiben:

$$e = g^m = g^{qn+r} = (g^n)^q \cdot g^r = g^r$$

□

Definition 29. *Sei G eine Gruppe, und H eine nicht leere Teilmenge von G, also $H \subseteq G$.*

Die Menge H nennt man Untergruppe, wenn die folgenden Bedingungen erfüllt sind.

i. *Für beliebige zwei Elemente $h_1, h_2 \in H$, gilt dass das Produkt ebenfalls in dieser Menge ist, sprich $h_1 h_2 \in H$*

ii. Für jedes Element $h \in H$ ist auch sein Inverses in dieser Menge, also $h^{-1} \in H$.

Beispiel 30. An dieser Stelle betrachten wir Beispiele für Untergruppen:

Betrachte die additive Gruppe des Restklassenrings $\mathbb{Z}_6^+$. Die Untergruppen dieses Rings sind:

$$\{0\}, \{0,3\}, \{0,2,4\} \text{ und } \mathbb{Z}_6^+$$

Definition 31. *Alle Untergruppen einer zyklischen Gruppe, sind ebenfalls Zyklisch.*

Beweis.

Sei G eine zyklische Gruppe, und U eine Untergruppe von G.

Weiter sei $b = a^k$ das jenige Element von U, mit dem kleinsten Exponenten k.

Wegen der Abgeschlossenheit enthält natürlich U auch alle Potenzen von b, aber keine anderen Potenzen von a. Wäre nämlich $a^x \in U$ liese sich x darstellen als $x = q\,k + r$ mit $0 \leqslant r < k$. Dann wäre aber auch $a^x\, b^{-q} = a^r$ aus U! Laut Definition ist k aber minimaler Exponent der Elemente aus U, also muss $r = 0$ sein, also $x = q\,k$ und daher a^x eine Potenz von b.

□

Definition 32. *(Die Ordnung einer Gruppe)*

Sei G eine Gruppe, die Ordnung oder auch Kardinalität bzw. Mächtigkeit entspricht einfach der Anzahl der Elemente, die sich in dieser Gruppe befinden.

Definition 33. *(Der Satz von Lagrange)*

Gegeben seien eine Gruppe G, und eine Untergruppe $H \subseteq G$. Laut dem Satz von LaGrange gilt dass die Ordnung von H ein Teiler ist von der Ordnung von G, d.h.

$$\text{ord}(H) \,|\, \text{ord}(G)$$

Beweis. Da der Fall G = H trivial ist, konzentrieren wir uns in diesem Beweis auf den Fall wenn $G \neq H$. Sei $H = \{h_1, ..., h_n\}$

Wir betrachten ein Element x welches in G ist aber nicht in H, d.h. $x \in G \backslash H$, und betrachten die Menge $x\,H = \{h_1\,x, ..., h_n\,x\}$. Diese Elemente sind alle Verschieden von den Elementen in H.

In der Tat: Aus $h_i x = h_j x$ folgt, dass $h_i = h_j$, somit wäre $x = h_j^{-1} h_i$ was definitiv Element der Menge H ist. Dies ist nicht Möglich, da wir dies durch die Definition von x ausgeschlossen haben.

Also haben wir

$$\varphi: H \to H\,x\,, h \longmapsto h\,x \text{ bijektiv}$$

$$\text{sowie } |H| = |H\,x| := h$$

Wenn die Vereinigung von H und $H\ x$ gleich G ist dann ist der Satz schon bewiesen. Aber was passiert wenn $H \cup H\ x$ kleiner ist als G dann müssen wir weitere Überlegungen anstellen.

Wähle $y \in G \backslash (H \cup H\ x)$ und betrachte wiederrum die Menge $y\ H = \{h_1 y, ..., h_2 y\}$.

Analog wie oben sind diese Elemente alle nicht gleich den Elementen von $(H \cup H\ y)$. Diese Zerlegungen können wir immer weiter fortsetzen sodass wie eine Zerlegung der folgenden Art erhalten:

$$G = H \cup H_x \cup H_y ... \cup H_z.$$

Jede der Mengen entält genau n Elemente, und daraus Folgt, dass die ord(G) teilbar ist durch n

□

Folgerung 34. *Sei G Gruppe, und $g \in G$. Ebenfalls gilt ord(g) ist ein Teiler von ord(G).*

Weil:

$< g > \leqslant G$

$| < g > | = \mathrm{Ord}(g)$

Die Struktur der Multiplikativen Gruppe des Ringes $\mathbb{Z}_m$

Die Multiplikative Gruppe des Ringes $\mathbb{Z}_m$ kann wie folgt zerlegt werden.

Satz 35. *Sei m eine natürliche Zahl mit der Primzahlzerlegung*

$$p_1^{e_1} \cdot \ldots \cdot p_s^{e_s} = m$$

Es gilt

$$\mathbb{Z}_m^* \simeq \mathbb{Z}_{{p_1}^{e_1}}^* \times \ldots \times \mathbb{Z}_{p_s^{e_s}}^*$$

denn nach dem Chinesischen Restklassensatz gilt

$$\mathbb{Z}_m \simeq \mathbb{Z}_{{p_1}^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{e_s}}$$

und somit gilt für die multiplikative Gruppe

$$\mathbb{Z}_m^* \simeq (\mathbb{Z}_{{p_1}^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{e_s}})^* = \mathbb{Z}_{{p_1}^{e_1}}^* \times \ldots \times \mathbb{Z}_{p_s^{e_s}}^*$$

Wenn nämlich $(a_1, ..., a_n) \in (\mathbb{Z}_{{p_1}^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{e_s}})^*$ *dann*

existiert ein $(b_1, ..., b_n) \in (\mathbb{Z}_{{p_1}^{e_1}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{e_s}})^*$ *sodass* $(a_1, ..., a_n) \cdot (b_1, ..., b_n) = (1, 1, ..., 1)$

Somit muss gelten $a_1 b_1 = 1$,...,$a_n b_n = 1$. *Die* a_i sind invertierbar und somit aus $\mathbb{Z}_{p_i^{e_i}}$

Definition 36. *An dieser Stele wird eine wichtige Funktion einbringen.*

$\varphi(m)$ *bezeichnet die Eulersche Funktion von m, d.h. die Anzahl der Zahlen von 0...m-1, welche zu m teilerfremd sind.*

Definition 37. *Die Ordnung der multiplikativen Gruppe des Restklassenringes* $\mathbb{Z}_m$ ist gleich $\varphi(m)$. *Wir schreiben auch*

$$\varphi(m) = |\mathbb{Z}_m^\star|$$

Sei m eine Primzahlzerlegung

$$m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$$

dann gilt

$$\varphi(m) = \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_s^{k_s})$$

$$\varphi(p^k) = p^k - p^{k-1}$$

Beweis. Die multiplikative Gruppe $\mathbb{Z}_m^*$ enthält alle zu m teilerfremde Elemente aus der Menge

$$\{1, ..., m-1\}$$

Nach der Definition der multiplikativen Gruppe ist $a \in \mathbb{Z}_m^*$ wenn folgendes erfüllt ist

$$\exists b \text{ mit } a\,b \equiv 1 \bmod m$$

Es ist sofort klar, dass a teilerfremd zu m ist. Somit ist klar dass die Mächtigkeit dieser Gruppe durch die eulersche Funktion von m dargestellt werden kann.

Die Formel mit der Primzahlzerlegung folgt trivialer Weise aus der Definition über die Zerlegung der multiplikativen Gruppe des Restklassenringes (siehe oben).

□

Folgerung 38. *Eine direkte Folgerung wäre der Satz von Euler:*

$$a^{\varphi(m)} \equiv 1 \bmod m$$

Beweis. *Es gilt a ist teilerfremd zu m, somit in der Multiplikativen Gruppe, somit ist auch die Ordnung von a ein Teiler der Ordnung der Multiplikativen Gruppe und daher ist auch die Ordnung von a ein Teiler von der eulerschen Funktion von m.* □

Folgerung 39. *Der kleine Satz von Fermat*

Gegeben sei eine Primzahl p, und eine Zahl $a \in \mathbb{N}$ welche nicht durch p teilbar ist, dann gilt

$$a^{p-1} \equiv 1 \bmod p$$

Satz 40. *$\mathbb{Z}_p^*$ ist die zyklische Gruppe der Ordnung p-1, wenn p Primzahl ist. Die multiplikative Gruppe eines endlichen Körpers ist immer zyklisch.*

Beweis. *Sei K Körper ein endlicher Körper.*

Seien x_1, ..., x_n alle Elemente seiner zyklischen Gruppe K^*. Sei $\operatorname{org}(x_1) =: d$ maximal. Wir wissen $\operatorname{ord}(x_i) \big| d$, *deswegen sind alle x_i sind Nullstellen des Polynoms $x^d - 1 = 0$ in K.*

Weil jedes Polynom des Grades n nicht mehr als n Nullstellen hat, gilt: $n \leqslant d$.

Ausserdem wissen wir: $d \,|\, |K^*|$ also $d|n$. Daraus folgt d=n, also gilt

$\{x_1, x_1^2, ..., x_1^n\} = K^*$ □

Satz 41. *$\mathbb{Z}_{p^n}^*$ ist zyklisch wenn $p \geqslant 3$ Prim und $n \geqslant 1$.*

Beweis.

Laut obigem Satz existiert eine natürliche Zahl g sodass folgende Formeln gelten:

$g^{p-1} \equiv 1 \bmod p$ (1)

$g^l \not\equiv 1 \bmod p\,, 1 \leqslant l < p-1$

Jetzt zeigen wir dass es möglich ist das g so zu wählen, dass noch zusätzlich gilt:

$g^{p-1} \not\equiv 1 \bmod p^2$ (2)

Angenommen dass gilt $g^{p-1} \equiv 1 \bmod p^2$ dann gilt:

$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + p^2(\ldots) \equiv 1 + (p-1)g^{p-2}p \,(\bmod p^2) \not\equiv 1 \bmod p^2$

Ersetze g durch $g+p$, und wir können annehmen das gilt $g^{p-1} = 1 + p\,u$ für ein u das nicht durch p teilbar ist. Wir beweisen dass g die Gruppe $\mathbb{Z}_{p^n}^*$ erzeugt.

Erst beweisen wir dass für alle $k \geqslant 0$ eine natürliche Zahl u_k existiert, sodass u_k teilerfremd p ist und folgende Formel gilt:

$g^{(p-1)p^k} = 1 + p^{k+1}u_k.$ (3)

Nehmen wir an das ist für ein $k > 0$ bereits bewiesen. Wir beweisen sie für $k+1$.

Induktionsannahme:

$k = 0$ gilt nach (1) und (2).

Induktionsschritt:

$g^{(p-1)p^{k+1}} = (1 + p^{k+1}u_k)^p = 1 + p^{k+2}u_k + \sum C_p^i (p^{k+1}u_k)^i.$

Es reicht zu zeigen dass jeder Summand in der Summe durch p^{k+3} teilbar ist.

Für $2 \leqslant i < p$ ist der Binomialkoeffizient C_p^i durch p teilbar. Dann ist der Summand $C_p^i(p^{k+1}u_k)$ durch $p^{1+i(k+1)}$ teilbar. Da $1 + i(k+1) \geqslant 1 + 2(k+1) \geqslant k+3$, ist der Summand durch p^{k+3} teilbar. Der Summand in der Summe mit $i = p$ ist durch $p^{(k+1)p}$ teilbar. Da $(k+1) \geqslant 3(k+1) \geqslant k+3$ ist auch dieser Summand durch p^{k+3} teilbar.

Jetzt berechnen wir die Ordnung d des Elementes g in $\mathbb{Z}_{p^n}^*$.

Die Ordnung d teilt die Ordnung der Gruppe $\mathbb{Z}_{p^n}^*$, also teilt die Zahl $\varphi(p^n) = p^{n-1}(p-1)$. Da $g^d \equiv 1 \bmod p^n$ ist, haben wir $g^d \equiv 1 \bmod p$ und somit $(p-1)\big|d$.

Darum hat d die Form $d = (p-1)p^k$ fuer $k \geqslant 0$. Wir wissen aus (3) dass k nicht kleiner ist als $n-1$ und somit gilt $d = \varphi(p^n)$.

Definition 42. *Es gilt*

$$\mathbb{Z}_{2^n}^* = \begin{cases} 1 \text{ wenn } n = 1 \\ \mathbb{Z}_2 \text{ wenn } n = 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}} \text{ wenn } n \geqslant 3 \end{cases}$$

Ohne Beweis.

Definition 43. *Wenn G eine abelsche Gruppe ist, und A,B zwei Untergruppen sind, sodass gilt $A \cap B = \{e\}$ dann kann man zu jedem $g \in$ AB ein eindeutiges $a \in A$ finden sowie ein eindeutiges $b \in B$ mit g=ab.*

Ferner gilt auch $AB \simeq A \times B$

Beispiel 44. Betrachte die Gruppe

$\mathbb{Z}_{16}^*$={1,3,5,7,9,11,13,15}=:G

Betrachte die beiden Untergruppen

$< -1 > = \{1, 15\}$

$< 5 > = \{1, 5, 9, 13\}$

Ihr Produkt ist die ganze Gruppe G, ausserdem gilt nach dem Lemma 42

$\mathbb{Z}_{16}^* = < -1 >< 5 > \simeq < -1 > \times < 5 > \simeq \mathbb{Z}_2^+ \times \mathbb{Z}_4^+$

Überprüfung mit Satz 41:

$\mathbb{Z}_{16}^\star = \mathbb{Z}_{2^4}^* = < -1 >_{\text{ORD}=2} \times < 5 >_{\text{ORD}=4 \text{ da } 5^4=25^2=9^2=1}$

□