Jeder endliche Schiefkörper ist ein Körper

Tomy Krischker (543843)

5. April 2013

Inhaltsverzeichnis

0.1 Einleitung

Wir wollen uns den Beweis für den Satz erarbeiten, dass jeder endliche Schiefkörper ein Körper ist. Im ersten Kapitel führen wir einige Schreibweisen ein und definieren grundlegende algebraische Strukturen. Wer weiß, was ein Schiefkörper ist, die Primkörper $\mathbb{F}_p$ kennt und mit Gruppen rechnen kann, der kann dieses Kapitel getrost überspringen. Als zweites wollen wir uns ein paar algebraische Strukturen definieren. Im dritten Abschnitt geht es um Polynome im Zusammenhang mit komplexen Einheitswurzeln. Im letzten Kapitel führen wir dann einen Widerspruchsbeweis, in dem wir die Annahme, wir hätten einen echten endlichen Schiefkörper, mit den Aussagen aus dem zweiten und dritten Kapitel zum Widerspruch führen.

Zunächst noch ein paar Bezeichnungen und Abkürzungen, die wir verwenden werden. Die meisten davon sollten klar sein, aber um Missverständnisse zu vermeiden, führen wir sie einmal auf.

Bezeichnung 0.1.1

- $\mathbb{N} = \mathbb{Z}_+$, *also* $0 \notin \mathbb{N}$
- *Sei* $n \in \mathbb{N}$. *So sei* $[n] := \{x \in \mathbb{N} | x \leq n\} = \{1, \ldots, n\}$
- *Sei* $n \in \mathbb{N}$. *So sei* $[n]_{-1} := \{x - 1 \in \mathbb{N} | x \leq n\} = \{0, \ldots, n-1\}$
- *bel. fix.: beliebig fixiert. Wählen wir ein Element a aus einer Menge A beliebig und zeigen eine Aussage über a, so gilt die Aussage für alle Elemente aus A. Im Prinzip sparen wir uns dadurch ein* $\forall a \in A$ *vor jeder neuen Zeile. Fixieren wir dieses Element, so meinen wir in den folgenden Zeilen immer das selbe Element a und können daher in Abhängigkeit von a weitere Objekte definieren, wie zB f(a).*
- *zz: zu zeigen*
- *gzz: genügt zu zeigen*
- *bzz: bleibt zu zeigen*
- *Vor: Voraussetzung; Beh: Behauptung; Bew: Beweis; Def: Definition*
- *oBdA: Ohne Beschränkung der Allgemeinheit. Wir nehmen einen von mehreren Fällen an und beschränken uns im Beweis nur auf diesen, da alle anderen Fälle symmetrisch oder trivial sind (zB:* $ab = 0$ *oBdA sei* $a = 0, b \neq 0$*).*

0.2 Gundlagen

Beschäftigen wir uns zunächst mit Gruppen:

Definition 0.2.1 (Gruppe) *Ein Paar aus einer Menge und einer darauf definierten Operation* $(\mathbb{G}, *)$ *heißt* ***Gruppe*** $: \Leftrightarrow$

- $\forall a, b \in \mathbb{G} : a * b \in \mathbb{G}$ ***(Abgeschlossenheit)***
- $\exists e_* \in \mathbb{G} \forall a \in \mathbb{G} : \ e_* * a = a * e_* = a$ *(e_* heißt* ***neutrales Element*** *von* $(\mathbb{G}, *)$*)*

- $\forall a \in \mathbb{G} \exists a^{-1} \in \mathbb{G} : \ a * a^{-1} = a^{-1} * a = e_*$ *(a^{-1} heißt zu a* ***inverses Element*** *in $(\mathbb{G}, *)$)*
- $\forall a, b, c \in \mathbb{G} : \ (a * b) * c = a * (b * c) = a * b * c$ ***(Assoziativgesetz)***

Bezeichnung 0.2.2 *Wenn die Bedeutungen klar sind, schreiben wir:*

- $\mathbb{G}$ *statt* $(\mathbb{G}, *)$
- *für allgemeine Operationen* e *statt* e_*
- *für die Multiplikation* 1 *statt* e_*
- ab *statt* $a * b$
- *für die Addition* $0 := e_+$, $a^{-1} := -a$
- $\mathbb{G}^* := \mathbb{G} \setminus \{ e \}$ *(somit gilt* $|\mathbb{G}^*| = |\mathbb{G}| - 1$*)*

Definition 0.2.3 (abelsch) *Eine Gruppe* $(\mathbb{G}, *)$ *und ihre Operation* $*$ *heißen* ***kommutativ*** *oder* ***abelsch*** $: \Leftrightarrow \ \forall a, b \in \mathbb{G} : \ ab = ba$ *(Kommutativgesetz)*

Beispiel 0.2.4
- $(\mathbb{Z}, +)$ *ist eine abelsche Gruppe.*
- $(\mathbb{Z}, *)$ *ist keine Gruppe, da zB* 2 *kein Inverses besitzt.*
- $(\mathbb{Z} \setminus \{ 2 \}, +$ *ist keine Gruppe, da zB* $1 + 1 \notin \mathbb{Z} \setminus \{ 2 \}$.
- $(\{ € \}, \clubsuit_{muh})$*, wobei* $€ \clubsuit_{muh} € := €$ *ist eine abelsche Gruppe.*
- $\emptyset$ *ist keine Gruppe, da in ihr kein neutrales Element existiert.*
- *Für* $\Sigma := \left\{ a, a^{-1}, b, b^{-1} \right\}$ *ist* $(\Sigma^\star, *)$ *die Menge aller Worte über* Σ *mit der Konkatenation als Operation, dem leeren Wort* ε *als neutralem Element und* $aa^{-1} = \epsilon$ *eine nicht abelsche Gruppe, da zB* $ab \neq ba$.

Lemma 0.2.5 *Seien* $(G, *)$ *Gruppe,* $a, b \in G$*. So gilt:*

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

(2) $ab^{-1}a^{-1}b = 1 \quad \Leftrightarrow \quad ab = ba$

Beweis. (1) $abb^{-1}a^{-1} = aa^{-1} = 1$ ✓
(2)

($\Leftarrow$) Betrachte $1 = aa^{-1}b^{-1}b = a(ba)^{-1}b = a(ab)^{-1}b = ab^{-1}a^{-1}b$

($\Rightarrow$) Betrachte $ba = b1a = bab^{-1}a^{-1}ba = abb^{-1}a^{-1}ab = ab$

□

Mit Hilfe der Gruppen können wir nun Körper definieren.

Definition 0.2.6 (Schiefkörper) *Ein Tripel aus einer Menge und zwei darauf definierten Operationen* $(\mathbb{K}, +, *)$ *heißt* ***Schiefkörper*** $: \Leftrightarrow$

- $(\mathbb{K}, +)$ *ist abelsche Gruppe*
- $(\mathbb{K}^*, *)$ *ist Gruppe*
- $\forall a, b, c \in \mathbb{K}: \ (a + b)c = ac + bc$ *(Rechtsdistributivgesetz)*
- $\forall a, b, c \in \mathbb{K}: \ c(a + b) = ca + cb$ *(Linksdistributivgesetz)*

Auch wenn nur K^* und nicht K selbst mit der Multiplikation eine Gruppe bildet, ist die Multiplikation mit 0 trotzdem definiert. Aus den Distributivgesetzen folgt: $a0 = a(0 + 0) = a0 + a0 \ \Leftrightarrow \ a0 - a0 = a0 + a0 - a0 = 0 = a0$ und analog $0 = 0a$.

Definition 0.2.7 (Körper) *Ein Schiefkörper* $\mathbb{K}$ *heißt* ***Körper*** $: \Leftrightarrow$

- $*$ *ist kommutativ*

Beispiel 0.2.8

- $(\mathbb{Z}, +, *)$ *ist kein Schiefkörper, da* $(\mathbb{Z}, *)$ *keine Gruppe.*
- $(\mathbb{Q}_+, +, *)$ *ist kein Schiefkörper, da* $(\mathbb{Q}_+, +)$ *keine Gruppe.*
- $(\mathbb{Q}, +, *)$ *ist ein Körper.*
- $(\{\in\}, \clubsuit_{muh}, \clubsuit_{muh})$ *ist ein Körper.*
- *Für* $n \in \mathbb{N}$ *ist* $(M(n, n, \mathbb{R}), +, *)$ *die Menge der reellen* $n \times n$*-Matrizen kein Schiefkörper, da es Elemente ohne multiplikative Inverse gibt.*
- $(GL(n, \mathbb{R}), +, *)$ *die Menge der reellen invertierbaren* $n \times n$*-Matrizen ist ein echter Schiefkörper, dh. Schiefkörper aber kein Körper.*

Definition 0.2.9 (Untergruppe) *Seien* $(G, *)$, $(G', *)$ *(abelsche) Gruppen mit* $G' \subseteq G$*. So heißt* G' ***(abelsche) Untergruppe*** *von* G *und* G ***(abelsche) Obergruppe*** *von* G' *und wir schreiben* $G' \leqslant G$*. Im Fall* $G \neq G'$ *heißt* G' ***echte*** *(abelsche) Untergruppe.*
Analoge Definitionen für (Schief-)körper.

Lemma 0.2.10 *Sei* $(G, *)$ *(abelsche) Gruppe,* $\emptyset \neq G' \subseteq G$*. So ist* $(G', *) \leqslant (G, *) \ \Leftrightarrow \ \forall a, b \in G' : (ab^{-1}) \in G'$

Beweis.

($\Rightarrow$) Seien $a, b \in G'$ bel. fix.. Da G' Gruppe, gilt $b^{-1} \in G'$ und damit $(ab^{-1}) \in G'$ ✓

($\Leftarrow$) gzz: G' Gruppe:

(Assoziativität, ggf. Kommutativität) wird von der Obermenge G vererbt

(Neutrales Element) Wähle $b = a$, so ist $aa^{-1} = e \in \mathbb{G}'$

(Inverse Elemente) Wähle $a = e, b$ beliebig, so ist $eb^{-1} = b^{-1} \in \mathbb{G}'$

(Abgeschlossenheit) Seien $a, b \in G'$ bel. fix., so ist $b^{-1} \in G'$ und damit $a(b^{-1})^{-1} = ab \in G'$ ✓ □

Lemma 0.2.11 *Seien $(G, *)$, $(G', *)$ (abelsche) Gruppen. So gilt: $G \cup G' \leqslant G$*

Beweis. Seien $a, b \in G \cup G'$ bel. fix.. Mit Lemma 0.2.10 gzz: $(ab^{-1}) \in G \cup G'$
Da G und G' Gruppen, gilt $ab^{-1} \in G$ und $ab^{-1} \in G'$ und damit $ab^{-1} \in G \cup G'$ □

Bemerkung 0.2.12 *Seien $\mathbb{K}$, $\mathbb{K}'$ (Schief-)körper, so gilt $\mathbb{K} \leqslant \mathbb{K}' \Leftrightarrow (\mathbb{K}, +) \leqslant (\mathbb{K}', +) \wedge (\mathbb{K}, *) \leqslant (\mathbb{K}', *)$, da alle weiteren Eigenschaften vererbt werden. Daraus folgt auch $\mathbb{K} \cup \mathbb{K}' \leqslant \mathbb{K}$.*

Zuletzt benötigen wir noch die Faktorisierung von Gruppen.

Definition 0.2.13 (Nebenklasse) *Seien $x \in \mathbb{G}$ und $H \subseteq G$ Teilmenge, so heißt $x*H := \{ x * a \in \mathbb{G} \mid a \in H \}$ die Menge aller Elemente, die man durch Multiplikation von x mit einem Element aus H erhalten kann, die **linke Nebenklasse** von x bzgl. H in $\mathbb{G}$. Analog heißt $H * x := \{ a * x \in \mathbb{G} \mid a \in H \}$ **rechte Nebenklasse**.*

Beispiel 0.2.14

- $2 + \{ 1, 4, 16 \} = \{ 3, 6, 18 \}$
- $0 * \mathbb{N} = \{ 0 \}$
- $2\mathbb{N} = \{ 2, 4, \dots \}$
- *Falls $\mathbb{G}$ kommutativ, gilt $\forall x \in \mathbb{G}, \forall H \subseteq \mathbb{G} : x * H = H * x$.*

Lemma 0.2.15 *Sei $\mathbb{G}$ Gruppe. So gilt $\forall x \in \mathbb{G} : x * \mathbb{G} = \mathbb{G}$*

Beweis.

$\subseteq$ Folgt aus der Abgeschlossenheit von $\mathbb{G}$. ✓

$\supseteq$ Seien $x, y \in \mathbb{G}$ bel fix. Da $\mathbb{G}$ Gruppe, ist $x^{-1}y \in \mathbb{G}$ und damit $xx^{-1}y = y \in x * \mathbb{G}$. ✓ □

Definition 0.2.16 (Faktorgruppe) *Sei $\mathbb{G}$ Gruppe, $H \leqslant G$, so sei $\mathbb{G}$ **faktorisiert nach** H $\mathbb{G}/H := \{ x * H \in \mathbb{G} \mid x \in \mathbb{G} \}$ die Menge aller linken Nebenklassen bzgl. H in G.*

Satz 0.2.17 *(1) $\mathbb{G}/H$ ist Gruppen*

(2) Im endlichen Fall gilt: $|\mathbb{G}/H| = \frac{|\mathbb{G}|}{|H|}$

Beweis. Auf den Beweis dieses algebraischen Satzes wollen wir verzichten und ihn an dieser Stelle nur glauben.
(2) beruht darauf, dass alle Nebenklassen gleich viele Elemente haben. □

Definition 0.2.18 ($\mathbb{F}_n$) *Sei $n \in \mathbb{N}$. So sei $\mathbb{F}_n := [n]_{-1}$ mit $(\mathbb{F}_n, +, *) :\cong (\mathbb{Z}/n * \mathbb{Z}, +, *)$ mit dem kanonischen Isomorphismus.*

Was dies bedeutet, schauen wir uns am nächsten Beispiel an:

Beispiel 0.2.19

- $\mathbb{Z}/2*\mathbb{Z} = \mathbb{Z}/\{ \dots, -4, -2, 0, 2, 4, \dots \} = \{ \{ \dots, -2, 0, 2, \dots \}, \{ \dots, -3, -1, 1, 3, \dots \} \} = \{ 2 * \mathbb{Z}, dir * \mathbb{Z} + 1 \}$, *also die Menge der Menge aller geraden und der Menge aller ungeraden Zahlen. Benennen wir die Elemente um zu $0 := 2 * \mathbb{Z}$, $1 := 2 * \mathbb{Z} + 1$ erhalten wir mit $\{ 0, 1 \}$ die Gruppe $\mathbb{F}_2 \cong \mathbb{Z}/2 * \mathbb{Z}$. $(\mathbb{F}_2, +, *)$ ist sogar ein Körper.*

- $\mathbb{F}_p$ *ist für jede Primzahl* p *ein Körper.*
- $\mathbb{F}_4$ *ist kein Körper, da* 2 *kein multiplikatives Inverses hat und die Multiplikation in* F_4^* *nicht abgeschlossen ist:* $1*1=1, 1*2=2, 1*3=3, 2*2=0, 2*3=2, 3*3=1$.
- $(\mathbb{Z}/6*\mathbb{Z})/\{6\mathbb{Z}, 6\mathbb{Z}+3\} = \{6\mathbb{Z}, 6\mathbb{Z}+1, 6\mathbb{Z}+2, 6\mathbb{Z}+3, 6\mathbb{Z}+4, 6\mathbb{Z}+5\}/\{6\mathbb{Z}, 6\mathbb{Z}+3\} = \{\{6\mathbb{Z}, 6\mathbb{Z}+3\}, \{6\mathbb{Z}+$ $\mathbb{F}_3$

Bemerkung 0.2.20 *Das Tripel* $(\mathbb{K}, +, *)$ *heißt* ***Ring****, wenn es die Schiefkörperaxiome erfüllt, es aber nicht notwendigerweise alle multiplikativen Inversen in* $\mathbb{K}$ *enthalten sind. Ein Beispiel für einen Ring ist* $\mathbb{Z}$.

Definition 0.2.21 (Polynomring) *Sei* $\mathbb{K}$ *Ring. So heißt das Tripel* $(\mathbb{K}[X], +, *1)$ *mit* $\mathbb{K}[X] := \left\{ \sum_{k=0}^{n} (a_k X^k) \,\middle|\, n \in \mathbb{N}, a_k \in \mathbb{K} \right.$ *der Menge aller Polynome mit Koeffizienten aus* $\mathbb{K}$ ***Polynomring*** *über* $\mathbb{K}$.

Bemerkung 0.2.22 *Wie bei dem Ring der ganzen Zahlen* $\mathbb{Z}$ *gelten im Polynomring der ganzen Zahlen* $\mathbb{Z}[X]$ *Teilbarkeitsregeln. Für* $a, b \in \mathbb{Z}[X]$ *gilt:* $a \mid b \;\Leftrightarrow\; \exists c \in \mathbb{Z}[X] : a * c = b$, *also* a *teilt* b *gdw.* b *ein Vielfaches von* a *ist.*

Beispiel 0.2.23
- $X^2 + X + \frac{1}{2} \in \mathbb{Q}[X]$
- $X^2 + X + \frac{1}{2} \notin \mathbb{Z}[X]$
- $\sum_{k=0}^{\infty} X^k \notin \mathbb{Z}[X]$
- $X - 1 \mid X^2 - 2X + 1$
- $X^2 - 2X + 1 \mid 2X^2 - 4X + 2$
- $X^2 - 2X + 1 \nmid X^2 - 3X + 1$

0.3 Algebrateil

Sei $\mathbb{K}$ ein beliebig fixer endlicher Schiefkörper.

Definition 0.3.1 (Stabilisator) *Für ein* $s \in \mathbb{K}$ *heißt die Menge* $C_s(K) := \{x \in \mathbb{K} | xs = sx\}$ *aller Elemente aus* $\mathbb{K}$, *die mit* s *bzgl. der Multiplikation kommutieren,* ***Stabilisator*** *von* s *über* $\mathbb{K}$.

Bezeichnung 0.3.2 *Wenn klar ist, über welcher Struktur wir den Stabilisator betrachten, schreiben wir* C_s *statt* $C_s(\mathbb{K})$.

Lemma 0.3.3 C_s *ist Unterschiefkörper von* $\mathbb{K}$.

Beweis. Mit Lemma 0.2.11 gzz. $(C_s, +)$ und $(C_s, *)$ sind Gruppen.

$(0 \in C_s)$ Betrachte $0s = 0 = s0$. Somit ist per Def. $0 \in C_s$. ✓

$(1 \in C_s)$ Betrachte $1s = s = s1$. Somit ist per Def. $1 \in C_s$. ✓

$(C_s \subseteq \mathbb{K})$ Ergibt sich aus der Definition von C_s. ✓

($(C_s, +)$ Gruppe) Seien $a, b \in C_s$. Betrachte

$$\begin{aligned}(a-b)s &= as - bs \quad \text{(Distributivgesetz)} && (1)\\ &= sa - bs \quad (\text{da } a, b \in C_s) && (2)\\ &= s(a-b) \quad \text{(Distributivgesetz)} && (3)\end{aligned}$$

Somit ist per Def. $(a-b) \in C_s$. Mit Lemma 0.2.10 folgt: $(C_s, +)$ ist Gruppe. ✓

($(C_s, *)$ Gruppe) Seien $a, b \in C_s$. Betrachte

$$\begin{aligned}(ab^{-1})s(ab^{-1})^{-1}s^{-1} &= (ab^{-1})s(ba^{-1})s^{-1} && (4)\\ &= a1sa^{-1}s^{-1} \quad (\text{da } sb = bs) && (5)\\ &= s1s^{-1} \quad (\text{da } as = sa) && (6)\\ &= 1 && (7)\end{aligned}$$

Mit Lemma 0.2.5 folgt $(ab^{-1})s = s(ab^{-1})$ und mit Lemma 0.2.10: $(C_s, *)$ ist Gruppe. ✓

□

Definition 0.3.4 (Zentralisator) *Die Menge* $Z(\mathbb{K}) := \bigcap_{s \in \mathbb{K}} C_s$ *aller Elemente aus* $\mathbb{K}$*, die mit allen Elementen aus* $\mathbb{K}$ *bzgl. der Multiplikation kommutieren, heißt* ***Zentralisator*** *über* $\mathbb{K}$*.*

Bezeichnung 0.3.5 *Wenn klar ist, über welcher Struktur wir den Zentralisator betrachten, schreiben wir* Z *statt* $Z(\mathbb{K})$*.*

Beispiel 0.3.6

- *Ist* $\mathbb{K}$ *kommutativ, so gilt* $\mathbb{K} = C_s(\mathbb{K}) = Z(\mathbb{K})$ *für alle* $s \in \mathbb{K}$
- *Wir können* C_s *und* Z *auch analog auf Gruppen definieren. So erhalten wir* $C_s(\Sigma^\star) = \left\{\varepsilon, s, s^{-1}\right\}$ *und* $Z(\Sigma^\star) = \{\varepsilon\}$

Lemma 0.3.7 *Z ist ein Körper.*

Beweis.

(Schiefkörper) Folgt aus der Def. mit Lemma. ✓

(Kommutativität) Da alle Elemente aus Z mit allen Elementen aus $\mathbb{K}$ kommutieren und $Z \subseteq \mathbb{K}$, folgt Kommutativität von Z. ✓ □

Setzen wir $q := |Z|$.

Satz 0.3.8 *Sei* $\mathcal{K}$ *Körper mit* $|\mathcal{K}| \in \mathbb{N}$*. So* $\exists p, n \in \mathbb{N} : \mathcal{K} \cong \bigoplus_{i \in [n]} \mathbb{F}_p$

Beweis. Für diesen Beweis benötigen wir weiterführende Sätze aus der Algebra. Daher wollen wir diese Aussage an dieser Stelle nur glauben. □

Korollar 0.3.9 $q =: p^n$ *ist eine Primzahlpotenz.*

Die n oben unterscheiden sich gegebenenfalls. n wird erst im nächsten Lemma fixiert.

Lemma 0.3.10 *Wir fixieren nun n und n_s für $s \in \mathbb{K}$ auf: $q^n := |\mathbb{K}|$, $q^{n_s} := |C_s|$. Somit gilt: $n_s, n \in \mathbb{N}$*

Beweis. Da $Z \subseteq \mathbb{K}$ und $\mathbb{K}$ Schiefkörper, gilt insbesondere: $\forall x \in Z \forall y \in \mathbb{K} : x * y \in \mathbb{K}$. Somit können wir $\mathbb{K}$ als n-dimensionalen Z-Vektorraum auffassen. Damit gilt: $|\mathbb{K}| = |Z|^n = q^n$.
Analog für alle n_s. □

Definition 0.3.11 $A_s := \{x^{-1}sx | x \in \mathbb{K}\}$

Beispiel 0.3.12

- $s = 1^{-1}s1 \in A_s$
- *In $\Sigma^\star$ ist* $A_a = \left\{a, bab^{-1}, b^{-1}ab, bbab^{-1}b^{-1}, b^{-1}b^{-1}abb, a^{-1}bab^{-1}a, a^{-1}b^{-1}aba, \dots\right\}$
- $\forall s \in Z : A_s = \{ s \}$. *Da s mit allen Elementen aus $\mathbb{K}$ kommutiert, gilt* $\forall x \in \mathbb{K} : x^{-1}sx = s$.

Lemma 0.3.13 $(A_s, *) \cong (\mathbb{K}^*, *)/(C_s^*, *)$

Beweis. $(\mathbb{K}^*, *)/(C_s^*, *) = \{ x * C_s^* \mid x \in \mathbb{K} \}$ per Def. . Sei $f(x * C_s^*) := x^{-1}sx$

Wohldefiniertheit Sei $x * C_s^* = y * C_s^* \in (\mathbb{K}^*, *)/(C_s^*, *) \Rightarrow \exists z \in C_s^* : x = yz$
Betrachte $f(x * C_s^*) = x^{-1}sx = (yz)^{-1}s(yz) = z^{-1}y^{-1}syz = f(yz * C_s^*) = f(y * C_s^*)$ □

Korollar 0.3.14
$|A_s| = \frac{\mathbb{K}^*}{C_s^*} = \frac{q^n-1}{q^{n_s}-1} \in \mathbb{N}$
Die A_s zerlegen $\mathbb{K}^*$ vollständig in Äquivalenzklassen.

Beweis. Folgt direkt mit Lemma 0.2.17. □

Korollar 0.3.15 $A_s = \{ s \} \Leftrightarrow s \in Z$

Korollar 0.3.16 $Z = \bigcup_{|A_s|=1} A_s$

Bezeichnung 0.3.17 *Seien $A_1, ..., A_t$ alle A_s mit $|A_s| \geq 2$*

Wir finden also solche A_t genau dann, wenn $\mathbb{K}$ nicht kommutativ.

Lemma 0.3.18 $q^n - 1 = q - 1 + \sum_{k \in [t]} \frac{q^n-1}{q^{n_k}-1}$

Beweis.

$$\mathbb{K}^* = \bigcup_{|A_s|=1} A_s \cup \bigcup_{|A_s|\geq 2} A_s = Z^* \cup \bigcup_{k\in[t]} A_k \quad \text{und damit:}$$

$$|\mathbb{K}^*| = |Z^*| + \sum_{k\in[t]} |A_k| \quad \text{setzen wir 0.3.10 und 0.3.14 ein}$$

$$q^n - 1 = q - 1 + \sum_{k\in[t]} \frac{q^n - 1}{q^{n_k} - 1}$$

□

Lemma 0.3.19 $\forall k \in [t], q > 1 : (q^{n_k} - 1) | (q^n - 1) \Rightarrow n_k \mid n$

Beweis. Seien $k \in [t]$ beliebig fixiert und $(q^{n_k} - 1) | (q^n - 1)$. Seien weiterhin $a, r \in \mathbb{Z}_+^0, r \leq n_k$, sodass $n = an_k + r \Rightarrow q^{n_k} - 1 | q^{an_k+r} \Leftrightarrow$

$$\begin{aligned}
q^{an_k+r} - 1 &\equiv 0 \mod q^{n_k} - 1 \quad | -(q_k^n - 1) \\
(q^{an_k+r} - 1) - (q^{n_k} - 1) &\equiv -(q_k^n - 1) \equiv 0 \mod q^{n_k} - 1 \\
q^{n_k} * q^{(a-1)n_k+r} - q^{n_k} &\equiv 0 \mod q^{n_k} - 1 \\
q^{n_k}(q^{(a-1)n_k+r} - 1) &\equiv 0 \mod q^{n_k} - 1 \quad | : q^{n_k} \\
q^{(a-1)n_k+r} - 1 &\equiv 0 \mod \frac{q^{n_k} - 1}{ggT\{q^{n_k} - 1, q^{n_k}\}} \\
q^{(a-1)n_k+r} - 1 &\equiv 0 \mod q^{n_k} - 1
\end{aligned}$$

Induktiv folgt:

$$\begin{aligned}
q^{(a-a)n_k+r} - 1 &\equiv 0 \mod q^{n_k} - 1 \\
q^r - 1 &\equiv 0 \mod q^{n_k} - 1
\end{aligned}$$

Da $r < n_k$ und somit $0 \leq q^r - 1 < q^{n_k} - 1$, folgt mit $q^{n_k} - 1 | q^r - 1$:
$q^r - 1 = 0 \Rightarrow q^r = 1$ Mit $q > 1$ laut Vor. folgt: $r = 0$ und somit $n = an_k + 0$, also $n_k | n$. □

Wir erhalten also

$$\forall k \in [t] : n_k \mid n \tag{8}$$

Behalten wir diese Aussage im Hinterkopf. Wir werden sie erst wieder für unseren Beweis am Ende brauchen.

0.4 Komplexe Zahlen

Beschäftigen wir uns als nächstes mit den komplexen Zahlen um später auf ein Polynom zu kommen, welches uns bei unserem Beweis weiterhelfen wird. Eine komplexe Zahl kann in kartesischen Koordination ($z = a + ib$ mit dem Realteil $Re(z) = a$ und Imaginärteil $Im(z) = b$) oder in Polarkoordinaten ($z = |z|e^{\varphi i} = |z|(\cos\varphi + i\sin\varphi)$ mit dem Radius oder Betrag $|z| = \|z\|_2 = \sqrt{a^2 + b^2}$ und dem Winkel im Bogenmaß $\varphi = \tan\frac{b}{a}$) geschrieben werden. Das Potenzieren im Komplexen mit einer reellen Zahl x funktioniert also wie folgt:

$$\begin{aligned}
z^x &= (a + ib)^x = (|z|e^{\varphi i})^x \\
&= |z|^x e^{x\varphi i}
\end{aligned}$$

Der Betrag wird also mit x potenziert und der Winkel mit x multipliziert.

Bemerkung 0.4.1 *Wenn man sich die Taylorreihen* [1] *der Winkel- und Exponentialfunktionen ansieht, kann man nachrechnen, dass* $e^{\varphi i} = \cos\varphi + i\sin\varphi$. *Insbesondere gilt also* $e^{k2\pi i} = \cos k2\pi + i\sin k2\pi = 1 + 0i = 1$ *für* $k \in \mathbb{Z}$.

Im Folgenden sind wir an den Wurzeln der 1 interessiert. Da $1 = 1e^{k2\pi i}$, kommen wir auf $1^{\frac{1}{n}} = 1^{\frac{1}{n}}(e^{k2\pi i})^{\frac{1}{n}} = e^{\frac{k}{n}2\pi i}$. Im Prinzip bewegen wir uns also mit $\frac{2\pi}{n}$ weiten Schritten auf dem Einheitskreis. Dies wollen wir nun noch einmal formal zeigen.

Definition 0.4.2 (Einheitswurzel) *Nullstellen* λ_k *des Polynoms* $x^n - 1$ *heißen* ***Einheitswurzeln*** *n-ten Grades.*

Bezeichnung 0.4.3 *Die Menge* $\Lambda_n := \{\, \lambda \in \mathbb{C} \mid \lambda^n = 1 \,\}$ *sei die Menge der Einheitswurzeln n-ten Grades. Die Menge* $\Lambda_\infty := \bigcup_{n\in\mathbb{N}} \Lambda_n$ *sei die Menge aller Einheitswurzeln.*

Lemma 0.4.4 $\Lambda_n := \left\{ e^{\frac{k}{n}2\pi i} \,\middle|\, k \in [n]_{-1} \right\}$

Beweis. Fixieren wir unser k beliebig. So gilt:

$$\begin{aligned}(e^{\frac{k}{n}2\pi i})^n - 1 &= e^{k2\pi i} - 1\\ &= (e^{2\pi i})^k - 1\\ &= 1^k - 1 = 0\end{aligned}$$

Damit sind alle $e^{\frac{k}{n}2\pi i}$ Einheitswurzeln. Da e^{xi} periodisch mit Periodenlänge 2π ist und somit unsere $e^{\frac{k}{n}2\pi i}$ paarweise verschieden sind, haben wir n paarweise verschiedene Einheitswurzeln. Da ein Polynom n-ten Grades höchstens n verschiedene Nullstellen hat, haben wir schon alle Einheitswurzeln gefunden. □

Bezeichnung 0.4.5 *Sei* $\lambda_{k/n} := e^{\frac{k}{n}2\pi i}$ *die k-te Einheitswurzel n-ten Grades.*

Definition 0.4.6 (Ordnung) *Die kleinste natürliche Potenz, in der eine Einheitswurzel* 1 *wird,* $Ord(\lambda) := \min\{m \in \mathbb{N} \mid \lambda^m = 1\}$ *heißt* ***Ordnung*** *von* λ.

Rechtfertigung 0.4.7 *Da wir eine nicht leere Teilmenge von* $\mathbb{N}$ *betrachten, wird das Minimum immer angenommen. Somit ist Ord wohldefiniert.*

Satz 0.4.8 $Ord(\lambda_{k/n}) = \frac{n}{ggT\{k,n\}}$

Beweis.
- Da $ggT\,\{k, n\} \mid n$, ist $\frac{n}{ggT\{k,n\}} \in \mathbb{N}$.

[1] Man kann Winkel- und Exponentialfunktion auch definieren als

$$e^x = \sum_{j\in\mathbb{N}} \frac{x^j}{j!}$$

$$cos(x) = \sum_{j\in\mathbb{N}} (-1)^n \frac{x^{2n}}{(2n)!} \qquad sin(x) = \sum_{j\in\mathbb{N}} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

- Da $ggT\{k,n\} \mid k$, finden wir ein $m \in \mathbb{N}$ mit $ggT\{k,n\} = \frac{k}{m}$. Betrachte

$$\begin{aligned}\lambda_{k/n}^{\frac{n}{ggT\{k,n\}}} &= (e^{\frac{k}{n}2\pi i})^{\frac{n}{ggT\{k,n\}}} \\ &= e^{\frac{kn}{n*ggT\{k,n\}}2\pi i} \\ &= e^{\frac{knm}{nk}2\pi i} \\ &= e^{m2\pi i} = 1\end{aligned}$$

- Für alle natürlichen $l < \frac{n}{ggT\{k,n\}}$ mit $\lambda_{k/n}^l = 1$ gilt:

$$\begin{aligned}\lambda_{k/n}^l &= (e^{\frac{k}{n}2\pi i})^l \\ &= e^{\frac{kl}{n}2\pi i} = 1 \quad \Rightarrow \\ \frac{kl}{n} &\in \mathbb{N} \Rightarrow \\ kl &\equiv 0 \mod n \quad | : ggT\{k,n\} \\ \frac{kl}{ggT\{k,n\}} &\equiv 0 \mod \frac{n}{ggT\{k,n\}}\end{aligned}$$

□

Korollar 0.4.9 $Ord(\lambda_{k/n}) \mid n$

Beweis. $\frac{n}{\frac{n}{ggT\{k,n\}}} = ggT\{k,n\} \in \mathbb{N}$ □

Sehen wir uns ein paar Beispiele an:

Beispiel 0.4.10

- *Für $k = 1$ ist $\lambda_{1/n} = e^{\frac{1}{n}2\pi i}$ und damit $Ord(\lambda_{1/n}) = \frac{n}{ggT\{1,n\}} = n$*
- *Eine Einheitswurzel λ kann aus verschiedenen n_i und k_i entstehen - nämlich genau dann, wenn $\frac{k_1}{n_1} = \frac{k_2}{n_2}$ und somit $\lambda = e^{\frac{k_1}{n_1}2\pi i} = e^{\frac{k_2}{n_2}2\pi i}$ ist. In dem Fall kann man $\frac{k_1}{n_1}$ und $\frac{k_2}{n_2}$ durch Kürzen und Erweitern ineinander umformen, also $\exists c \in \mathbb{Q}^* : k_1 = ck_2 \wedge n_1 = cn_2$.*
- *Da wir $Ord(\lambda_{k/n})$ nur in Abhängigkeit vom Wert von $\lambda_{k/n}$ und nicht von den k und n definiert haben, ist die Definition resräsentantenunabhängig. Dies spiegelt auch unser Satz 0.4.8 wider, denn für $\lambda_{k_1/n_1} = \lambda_{k_2/n_2}$, mit $k_1 = ck_2, n_1 = cn_2$ gilt: $Ord(\lambda_{k_1/n_1}) = \frac{n_1}{ggT\{k_1,n_1\}} = \frac{cn_2}{ggT\{ck_2,cn_2\}} = \frac{cn_2}{c*ggT\{k_2,n_2\}} = Ord(\lambda_{k_2/n_2})$*

Dies führt uns zu folgendem Lemma:

Lemma 0.4.11 $Ord(\lambda) = d \Leftrightarrow \exists p \in \mathbb{N} : ggT\{p,d\} = 1 \wedge \lambda = \lambda_{p/d}$

Beweis. $\Leftarrow$: Es gilt: $Ord(\lambda) = Ord(\lambda_{p/d}) = \frac{d}{ggT\{p,d\}} = d$ ✓

$\Rightarrow$: Per Def. gilt $\lambda^d = 1 = e^{p2\pi i}$ für ein $p \in \mathbb{N}$ Damit erhalten wir $\lambda = e^{\frac{p}{d}2\pi i} = \lambda_{p/d}$ und wegen $Ord(\lambda_{p/d}) = d = \frac{d}{ggT\{p,d\}}$ folgt $ggT\{p,d\} = 1$ ✓

□

Wir wissen nun also, dass die Menge der Einheitswurzeln d-ter Ordnung endlich und sogar relativ leicht zu ermitteln ist.

Bezeichnung 0.4.12 *Die Menge aller Einheitswurzeln d-ter Ordnung bezeichnen wir mit* $\Lambda\Omega_d := \{ \lambda \in \Lambda_\infty \mid Ord(\lambda) = d \} = \left\{ \lambda_{p/d} \,\middle|\, ggT\{p, d\} = 1 \right\}$ *nach Lemma 0.4.11*

Wir definieren uns nun ein Polynom, durch welche wir später gewisse Teilbarkeitseigenschaften erhalten, die uns zu dem Beweis des Satzes führen:

Bezeichnung 0.4.13 $\Phi_d(x) := \prod_{\lambda \in \Lambda\Omega_d} (x - \lambda)$

Beispiel 0.4.14

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x^2 + x + 1$
- $\Phi_3(x) = x^2 + 1$
- $\Phi_4(x) = x + 1$
- $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
- $\Phi_6(x) = x^2 - x + 1$

Lemma 0.4.15 $x^n - 1 = \prod_{d|n} \Phi_d(x)$

Beweis. Wir wissen schon, dass $x^n - 1 = \prod_{k \in [n]_{-1}} (x - \lambda_{k/n})$, da die $\lambda_{k/n}$ genau die Nullstellen von $x^n - 1$ sind. Betrachte:

$$\begin{aligned}
\prod_{d|n} \Phi_d(x) &= \prod_{d|n} \prod_{ggT\{p,d\}=1} (x - \lambda_{p/d}) \quad \text{(Dieses Produkt durchläuft genau allen Zahlen von 1 bis n)} \\
&= \prod_{p \in [n]} (x - \lambda_{p/n}) \quad (\text{da } \lambda_{n/n} = \lambda_{0/n}) \\
&= \prod_{k \in [n]_{-1}} (x - \lambda_{k/n}) \\
&= x^n - 1
\end{aligned}$$

□

Um gewisse Teilbarkeitseigenschaften von Φ_d ermitteln zu können, benötigen wir folgendes Lemma:

Lemma 0.4.16 $\Phi_d(x) \in \mathbb{Z}[x]$

Beweis. Der Beweis hierfür ist eine ziemlich lange und unübersichtliche, aber wenig aufregende oder erkenntnisbringende vollständige Induktion. Daher lassen wir sie an dieser Stelle als Übungsaufgabe. □

Fixieren wir unser n wieder wie in 0.3.10 und unser n_k beliebig aus 8 unter der Annahme, dass ein solches existiert (also $Z \neq \mathbb{K}$).

Lemma 0.4.17 *(1)* $\Phi_n(x) \mid (x^n - 1)$

(2) $\Phi_n(x) \mid \frac{x^n-1}{x^{n_k}-1}$

Beweis. Betrachte:

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \Phi_d(x) \\ &= \prod_{d|n_k} \Phi_d(x) \prod_{d=n} \Phi_n(x) \prod_{d|n, d\nmid n_k, d\neq n} \Phi_d(x) \\ &= (x^{n_k} - 1)\Phi_n(x) \prod_{d|n, d\nmid n_k, d\neq n} \Phi_d(x) \quad | : (x_k^n - 1) \\ \frac{x^n - 1}{x^{n_k} - 1} &= \Phi_n(x) \prod_{d|n, d\nmid n_k, d\neq n} \Phi_d(x) \end{aligned}$$

Somit sind die beiden Terme Vielfache von $\Phi_n(x)$. □

Setzen wir nun ein beliebig fixes $q \in \mathbb{Z}$ für x ein, so erhalten wir:

$$\Phi_n(q) \mid (q^n - 1)$$
$$\Phi_n(q) \mid \frac{q^n - 1}{q^{n_k} - 1}$$

Da $\Phi_n(x)$ nur ganze Zahlen als Koeffizienten hat und $q \in \mathbb{Z}$, ist auch $\Phi_n(q) \in \mathbb{Z}$ eine ganze Zahl.

Lemma 0.4.18 $\Phi_n(q) \mid (q - 1)$

Beweis. Aus 0.3.18 wissen wir: $q^n - 1 = q - 1 + \sum_{k\in[t]} \frac{q^n-1}{q^{n_k}-1}$. Da $\Phi_n(q)$ die Summe und bis auf $q - 1$ alle Summanden teilt, muss es auch $q - 1$ teilen. □

0.5 Der Beweis

Gehen wir nun zu unserem Satz über:

Satz 0.5.1 $\mathbb{K}$ *ist kommutativ.*

Beweis. Annahme: $\mathbb{K}$ ist nicht kommutativ $\Rightarrow$ $\mathbb{K} \neq Z(K)$. Mit Def 0.3.10 folgt $n > 1$

Wir wissen: $\Phi_n(x) = \prod_{\lambda\in\Lambda\Omega_n} (x - \lambda)$. Sei $\hat{\lambda} =: a + ib \in \Lambda\Omega_n$ beliebig fix. Da $1^1 = 1$ und somit $1 \in \Lambda\Omega_1$, ist $1 \notin \Lambda\Omega_n$ und damit $\hat{\lambda} \neq 1$. Da $\hat{\lambda}$ Einheitswurzel ist und somit $|\hat{\lambda}| = \sqrt{a^2 + b^2} = 1$, ist $Re(\hat{\lambda}) = a < 1$. Betrachte

$$|\hat{\lambda}|^2 = a^2 + b^2 = 1$$

und weiterhin

$$\begin{aligned}
|q - \hat{\lambda}|^2 &= |(q-a) - ib|^2 = (q-a)^2 + b^2 \\
&= q^2 - 2aq + (a^2 + b^2) \\
&= q^2 - 2aq + 1 \quad |a < 1 \\
&> q^2 - 2(1)q + 1 \\
&= (q-1)^2 \quad | \sqrt{} \\
|q - \hat{\lambda}| &> (q-1) \;\Rightarrow
\end{aligned}$$

$$|\Phi_n(q)| = |\prod_{ord(\lambda)=n} (q-\lambda)| \qquad = \prod_{ord(\lambda)=n} |q-\lambda)| > (q-1)$$

und damit $\Phi_n(q) \nmid (q-1)$. $\lightning$zu 0.4.18.

Damit folgt die Negation der Annahme: $\mathbb{K}$ ist ein Körper. □

qed.