VO Algebra im Überblick

(Modul: "Überblicke über Teilgebiete der Mathematik" (UEB))

Markus Fulmek

Wintersemester 2014/15

Der vorliegende Skriptums–Entwurf basiert auf den Vorlesungen "Algebra im Überblick" von Professor Dietrich Burde [**2**] und Professor Leo Summerer [**15**].
Ich setze hier Grundkenntnisse aus den Gebieten Lineare Algebra, Zahlentheorie und Algebra voraus, wie sie in den Vorlesungen "Einführung in die lineare Algebra und Geometrie", "Zahlentheorie", "Algebraische Strukturen" und "Algebra" vermittelt werden. Um das Verständnis des hier behandelten Stoffes zu erleichtern, wiederhole ich im Anhang A dieses Skriptums *ausgewählte* Themen aus den genannten Gebieten; ohne jeden Anspruch auf Vollständigkeit.
Am Ende dieses Skriptums–Entwurfs findet sich ein Literaturverzeichnis, ein Index der verwendeten Begriffen sowie ein Verzeichnis der verwendeten Notationen und Abkürzungen
In der vorliegenden Version (2015–01–26) habe ich viele Tippfehler und einige sinnstörende Fehler ausgemerzt: Es gibt aber sicher weitere Fehler und Ungereimtheiten, die ich noch nicht bemerkt habe: Für diesbezügliche Hinweise bin ich sehr dankbar.

Universität Wien, Wintersemester 2014 Markus Fulmek

Inhaltsverzeichnis

KAPITEL 1

Gruppenwirkung und Symmetrie

1.1. Gruppenwirkungen

DEFINITION 1.1.1 (Wirkung einer Gruppe). *Sei $G = (G, \cdot)$ eine Gruppe, deren neutrales Element wir mit $\mathbb{n}$ bezeichnen, und sei S eine Menge. Eine Abbildung*

$$G \times S \to S,$$

die wir wie folgt notieren

$$(g, s) \mapsto g \cdot s \in S,$$

nennt man eine Wirkung *(oder* Aktion *oder* Operation*) von G auf S, falls gilt:*

- *für alle $g, h \in G$ und alle $s \in S$ ist $g \cdot (h \cdot s) = (g \cdot h)\, s$,*
- *für das neutrale Element $\mathbb{n} \in G$ und alle $s \in S$ ist $\mathbb{n} \cdot s = s$.*

*Eine Menge S, auf der eine Gruppe G operiert (oder agiert oder wirkt), heißt auch G–*Menge*.*

BEISPIEL 1.1.2. *Die Gruppe $\mathrm{GL}_n(\mathbb{K})$ der invertierbaren $n \times n$–Matrizen über einem Körper $\mathbb{K}$ operiert auf dem Vektorraum $\mathbb{K}^n$ durch Matrixmultiplikation*

$$(A, x) \mapsto A \cdot x.$$

BEISPIEL 1.1.3. *Jede Gruppe G operiert auf jeder Menge S durch die triviale Operation: $g \cdot s = s$ für alle $g \in G$ und alle $s \in S$.*

BEISPIEL 1.1.4. *Die symmetrische Gruppe $\mathfrak{S}_n$ operiert durch Permutationen auf der Ziffernmenge $S = \{1, 2, \ldots, n\}$.*

BEISPIEL 1.1.5. *Jede Gruppe G operiert auf sich selbst durch Konjugation: Für $S = G$ ist die Wirkung $(g, s) \mapsto g \cdot s \cdot g^{-1}$.*

BEISPIEL 1.1.6. *Die Gruppe $\mathrm{SL}_2(\mathbb{C})$ der komplexen 2×2 Matrizen $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit Determinante $\det(A) = 1$ operiert auf der* Riemannschen Zahlenkugel $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ *durch* Möbiustransformation

$$(A, z) \mapsto A \cdot z = \frac{a \cdot z + b}{c \cdot z + d}.$$

Dabei gilt $A \cdot \infty = a/c$ ($=: \infty$ für $c = 0$) und $A \cdot (-d/c) = \infty$. Die Einheitsmatrix E operiert durch $E \cdot z = \frac{1 \cdot z + 0}{0 \cdot z + 1} = z$. Für zwei Matrizen $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ rechnet

man nach:

$$\begin{aligned} A \cdot (B \cdot z) = A \cdot \left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) &= \frac{a\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + b}{c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + d} \\ &= \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + d\delta)} \\ &= \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} \cdot z \\ &= (A \cdot B) \cdot z. \end{aligned}$$

DEFINITION 1.1.7 (Symmetrische Gruppe). *Es bezeichne $\mathfrak{S}_S$ die Menge aller Bijektionen $S \to S$. $\mathfrak{S}_S$ bildet eine Gruppe mit der Komposition von Funktionen, die* Symmetrische Gruppe. *Wenn S eine endliche Menge mit $|S| = n \in \mathbb{N}$ ist, dann können wir S mit $[n] = \{1, 2 \ldots, n\}$ identifizieren und bezeichnen die symmetrische Gruppe in diesem Fall mit $\mathfrak{S}_n$ (wie üblich; statt $\mathfrak{S}_{[n]}$).*

PROPOSITION 1.1.8. *Sei G eine Gruppe, die auf einer Menge S operiert. Für jedes $g \in G$ bezeichne $L(g)$ die Wirkung $s \mapsto g \cdot s$ des Gruppenelements g auf S: Offenbar ist $L(g) : S \to S$ eine Bijektion von S, mit inverser Abbildung $L\left(g^{-1}\right)$. Die Abbildung*

$$L : G \to \mathfrak{S}_S;\ g \mapsto L(g)$$

ist ein Gruppenhomomorphismus.
Ist umgekehrt ein Gruppenhomomorphismus

$$\theta : G \to \mathfrak{S}_S$$

gegeben, so operiert die Gruppe G auf S durch $(g, s) \mapsto \theta(g)\, s$.

BEWEIS. Nach Definition einer Gruppenwirkung ist

- $L(\mathbb{m}) = \mathrm{id}$,
- $L(g) \cdot (L(h) \cdot s) = L(g \cdot h) \cdot s$ für alle $g, h \in G$ und $s \in S$.

Das ist gleichbedeutend damit, daß L ein Gruppenhomomorphismus ist. □

DEFINITION 1.1.9. *Eine Wirkung von G auf S heißt* treu, *falls der Homomorphismus $L : G \to \mathfrak{S}_S$ injektiv ist:*

$$g \cdot s = s \text{ für alle } s \in S \implies g = \mathbb{m}.$$

Zum Beispiel operiert für eine beliebige Menge S jede Untergruppe von $\mathfrak{S}_S$ treu auf S.

DEFINITION 1.1.10 (Bahn oder Orbit). *Sei G eine Gruppe, die auf einer Menge S operiert; sei $X \subseteq S$ und $s \in S$.*
Die Menge

$$G \cdot s := \{g \cdot s :\ g \in G\} \subseteq S$$

heißt die Bahn *oder der* Orbit *von s (unter der Wirkung von G). Wenn man betonen möchte, daß die Gruppe G wirkt, sagt man auch G–Bahn oder G–Orbit.*
Die Familie aller Orbits

$$\{G \cdot s :\ s \in S\}$$

bezeichnen wir mit S/G.

Für $g \in G$ bezeichnen wir mit $g \cdot X$ die Menge

$$g \cdot X := \{g \cdot x \colon \ x \in X\}\,.$$

Dann heißt die Menge

$$\mathrm{stb}_G(X) := \{g \in G \colon \ g \cdot X = X\} \subseteq G$$

der Stabilisator *der Menge X. Wenn X einpunktig ist (also $X = \{x\}$), dann schreiben wir statt $\mathrm{stb}_G(\{x\})$ kürzer $\mathrm{stb}_G(x)$. Der zu $\mathrm{stb}_G(x)$ "duale" Begriff ist die Menge der Elemente in S, die von einem festen Element $g \in G$ fixiert werden: Wir nennen diese Elemente die* Fixpunkte *von g und bezeichnen ihre Menge mit*

$$\mathrm{fxp}_S(g) := \{x \in S \colon \ g \cdot x = x\}\,.$$

Die Teilmenge $X \subseteq S$ heißt invariant *unter der Wirkung von G (oder kurz G–invariant), wenn $G \cdot x \subseteq X$ für alle $x \in X$: In diesem Fall wirkt G auch auf der Teilmenge X, man nennt dies die* induzierte Wirkung *von G auf $X \subseteq S$.*

Das Element $s \in S$ heißt ein Fixpunkt *unter der Wirkung von G, wenn $g \cdot s = s$ für alle $g \in G$: Das ist äquivalent mit $\mathrm{stb}_G(s) = G$ bzw. mit $G \cdot s = \{s\}$. Die Menge dieser Fixpunkte bezeichnen wir mit $\mathrm{fxp}_S(G)$.*

Die Wirkung von G heißt transitiv, *falls es ein $s \in S$ gibt mit $S = G \cdot s$.*

Der Orbit $G \cdot s \subseteq S$ ist die kleinste G–invariante Teilmenge von S, die s enthält.

Wenn G auf S operiert, dann ist die Relation $\sim$ auf S

$$s \sim t :\Longleftrightarrow \ \exists g \in G \colon \ t = g \cdot s \iff t \in G \cdot s \iff G \cdot t = G \cdot s$$

eine *Äquivalenzrelation*, wie man ganz leicht sieht:

- $s \sim s$, denn $s = \mathbb{m} \cdot s$: *Reflexivität*,
- $s \sim t$ heißt, es gibt ein g mit $t = g \cdot s$: Dann ist aber $s = \mathbb{m} \cdot s = \left(g^{-1} \cdot g\right) \cdot s = g^{-1} \cdot (g \cdot s) = g^{-1} \cdot t$, also $t \sim s$: *Symmetrie*,
- $r \sim s$ und $s \sim t$ bedeutet, es gibt $g, h \in G$ mit $s = g \cdot r$ und $t = h \cdot s$, also $t = h \cdot (g \cdot r) = (h \cdot g) \cdot r$, also $r \sim t$: *Transitivität*.

Die Äquivalenzklassen dieser Relation $\sim$ sind genau die G–Orbits: Diese bilden eine *Partition* von S. Wir halten diese einfache Beobachtung fest:

BEOBACHTUNG 1.1.11. *Sei S eine endliche Menge, auf der eine Gruppe G wirkt. Dann gilt*

$$|S| = \sum_{O \in S/G} |O|\,. \tag{1.1}$$

(Die Summe läuft über alle Orbits.)

Damit können wir zeigen:

SATZ 1.1.12 (Cauchy). *Sei G eine endliche Gruppe, und sei $p \in \mathbb{P}$ ein Teiler der Gruppenordnung $|G|$. Dann enthält G ein Element der Ordnung p.*

BEWEIS. Sei $S = \left\{g = \left(g_0, g_1, \ldots, g_{p-1}\right) \in G^p \colon\ g_0 \cdot g_1 \cdots g_{p-1} = \mathbb{m}\right\}$. Es gilt $|S| = |G|^{p-1}$, denn wir können die ersten $p-1$ Komponenten

$$\left(g_0, g_1, \ldots, g_{p-2}\right)$$

für jedes p–Tupel in S frei wählen; die letzte Komponente ist dann notwendigerweise gleich

$$\left(g_0 \cdot g_1 \cdots g_{p-2}\right)^{-1}.$$

Auf S wirkt die zyklische Gruppe $\mathbb{Z}/p\mathbb{Z}$ durch zyklische Vertauschung: Sei $i \in \mathbb{Z}/p\mathbb{Z}$, dann ist

$$i \cdot \left(g_0, \cdots, g_{p-1}\right) := \left(g_{0+i \pmod p}, \ldots, g_{p-1+i \pmod p}\right).$$

Jeder Orbit dieser Gruppenwirkung ist entweder einpunktig oder enthält genau p Elemente: Denn angenommen, es würde für ein i mit $p \nmid i$ gelten: $i \cdot g = g$, also

$$g_j = g_{j+i \pmod p} \text{ für alle } j = 0, 1, \ldots, p-1.$$

Dann wären ja die Komponenten

$$g_0 = g_{i \pmod p} = g_{2i \pmod p} = \cdots$$

alle gleich: Aber $i \cdot \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$ für $i \neq \mathbf{0}$, also sind alle Komponenten gleich und der Orbit ist einpunktig. Aus (1.1) folgt also:

$$|S| = |G|^{p-1} = 1 \cdot \#\left(\text{einpunktige Orbits}\right) + p \cdot \#\left(p\text{–elementige Orbits}\right).$$

Da $p \mid |G|$, folgt $p \mid \#\left(\text{einpunktige Orbits}\right)$. Klarerweise ist der Orbit von $(\mathbb{m}, \ldots, \mathbb{m}) \in S$ einpunktig, also ist $\#\left(\text{einpunktige Orbits}\right) > 0$: Daraus folgt die Behauptung. □

BEISPIEL 1.1.13. *Die symmetrische Gruppe $G = \mathfrak{S}_n$ operiert auf $S = [n]$ durch Permutation der Elemente von $[n]$. Diese Gruppenwirkung ist transitiv, es gibt also für $n > 1$ keinen Fixpunkt der Gruppenwirkung. Sehr wohl können aber einzelne Permutationen $\pi \in \mathfrak{S}_n$ Fixpunkte haben, also Elemente $i \in [n]$ mit $\pi(i) = i$: Der Stabilisator $\mathrm{stb}_{\mathfrak{S}_n}(i)$ eines Elements i ist die Menge aller Permutationen mit Fixpunkt i.*

BEISPIEL 1.1.14. *Jede Gruppe G operiert auf sich selbst (also mit $S = G$) durch* Konjugation*:*

$$(g, s) \mapsto g \cdot s \cdot g^{-1}.$$

Der Orbit von s unter dieser Gruppenwirkung ist die Konjugationsklasse *von s:*

$$\left\{g \cdot s \cdot g^{-1} \colon\ g \in G\right\}.$$

BEISPIEL 1.1.15. *Sei G eine Gruppe und $H \sqsubseteq G$ eine* Untergruppe *(nicht notwendigerweise ein* Normalteiler*) von G. Dann operiert G auf der Familie $G/H = \{g \cdot H \colon\ g \in G\}$ der* Linksnebenklassen *von H durch*

$$(g', g \cdot H) \mapsto (g' \cdot g) \cdot H.$$

Diese Gruppenwirkung hat nur einen einzigen Orbit.

BEISPIEL 1.1.16. *Sei $G = D_\infty$ die Untergruppe von $\mathfrak{S}_\mathbb{R}$, die von der Translation $T : x \mapsto x+1$ und der Spiegelung $S : x \mapsto -x$ erzeugt wird: Sie heißt die* unendliche Diedergruppe. *D_∞ operiert auf $X = \mathbb{R}$. Die Bahnen der Elemente $x = 1, \frac{1}{2}, \frac{1}{3}$ unter dieser Gruppenwirkung sind*

$$\begin{aligned} G \cdot 1 &= \mathbb{Z}, \\ G \cdot \frac{1}{2} &= \frac{1}{2} + \mathbb{Z}, \\ G \cdot \frac{1}{3} &= \left(\frac{1}{3} + \mathbb{Z}\right) \cup \left(\frac{2}{3} + \mathbb{Z}\right). \end{aligned}$$

LEMMA 1.1.17. *Sei G eine Gruppe, die auf einer Menge S operiert; sei $X \subseteq S$. Dann ist der Stabilisator $\mathrm{stb}_G(X)$ von X eine Untergruppe von G, die aber i.a. kein Normalteiler ist, denn es gilt für $g \in G$:*

$$g \cdot \mathrm{stb}_G(X) \cdot g^{-1} = \mathrm{stb}_G(g \cdot X).$$

Für ein Element $x \in S$ ist die Abbildung

$$\tilde{f}\colon\ G/\mathrm{stb}_G(x) \to G \cdot x;\ g \cdot \mathrm{stb}_G(x) \mapsto g \cdot x$$

eine wohldefinierte *Bijektion. Insbesondere gilt also für eine* endliche *Gruppe G:*

$$|G| = |\mathrm{stb}_G(x)| \cdot |G \cdot x|. \tag{1.2}$$

(In Worten: Die Mächtigkeit eines Orbits ist stets ein Teiler der Gruppenordnung.)

BEWEIS. Daß $\mathrm{stb}_G(X)$ eine Untergruppe von G ist, ist klar (siehe "Untergruppenkriterium" (A.6): $a \cdot X = X = b \cdot X \implies b^{-1} \cdot a \cdot X = X$).

Es sei $h \in \mathrm{stb}_G(X)$, also $h \cdot X = X$. Dann ist (nach Definition einer Gruppenwirkung bzw. des Stabilisators)

$$\left(g \cdot h \cdot g^{-1}\right) \cdot g \cdot X = g \cdot h \cdot X = g \cdot X,$$

also $g \cdot h \cdot g^{-1} \in \mathrm{stb}_G(g \cdot X)$. Also ist $g \cdot \mathrm{stb}_G(X) \cdot g^{-1} \subseteq \mathrm{stb}_G(g \cdot X)$. Es sei umgekehrt $h \in \mathrm{stb}_G(g \cdot X)$, also $h \cdot (g \cdot X) = g \cdot X$. Dann ist

$$\left(g^{-1} \cdot h \cdot g\right) \cdot X = g^{-1} \cdot (h \cdot (g \cdot X)) = g^{-1} g \cdot X = X,$$

also $g^{-1} \cdot h \cdot g \in \mathrm{stb}_G(X)$. Also ist $\mathrm{stb}_G(g \cdot X) \subseteq g \cdot \mathrm{stb}_G(X) \cdot g^{-1}$.

Seien $g_1, g_2 \in G$. Es gilt:

$$\begin{aligned} g_1 \cdot x = g_2 \cdot x &\iff g_2^{-1} \cdot g_1 \cdot x = x \iff g_2^{-1} \cdot g_1 \in \mathrm{stb}_G(x) \\ &\iff g_2^{-1} \cdot g_1 \cdot \mathrm{stb}_G(x) = \mathrm{stb}_G(x) \iff g_1 \cdot \mathrm{stb}_G(x) = g_2 \cdot \mathrm{stb}_G(x). \end{aligned}$$

Also ist die Abbildung $\tilde{f}$ wohldefiniert und injektiv; klarerweise ist sie auch surjektiv. □

Daraus ergibt sich sofort eine andre Formulierung von Beobachtung 1.1.11:

KOROLLAR 1.1.18 (Bahnengleichung). *Sei S eine endliche Menge, auf der eine Gruppe G wirkt. Sei $\mathcal{R}$ ein* Repräsentantensystem *der Familie S/G der G–Orbits. Dann gilt*

$$|S| = \sum_{x \in \mathcal{R}} |G/\operatorname{stb}_G(x)| = \sum_{x \in \mathcal{R}} (G : \operatorname{stb}_G(x)). \tag{1.3}$$

BEMERKUNG 1.1.19. *Wenn eine Gruppe G auf einer Menge S wirkt und $X \subseteq S$ eine Teilmenge von S ist, dann wirkt der Stabilisator von X auf X, mit der von G "geerbten" Wirkung auf S: Man nennt das auch die* induzierte Wirkung.

Ebenso erhält man aus Lemma 1.1.17:

KOROLLAR 1.1.20. *Sei G eine Gruppe, die auf einer Menge S operiert. Seien $s_1, s_2 \in S$ zwei Elemente, die demselben G–Orbit angehören, dann sind die Stabilisatoren $\operatorname{stb}_G(s_1)$ und $\operatorname{stb}_G(s_2)$ konjugierte Untergruppen in G (und daher insbesondere gleichmächtig).*

BEWEIS. Wenn s_1, s_2 demselben G–Orbit angehören, dann gibt es ein $g \in G$ mit $s_1 = g \cdot s_2$. Die Behauptung folgt also sofort aus Lemma 1.1.17:

$$g \cdot \operatorname{stb}_G(s_1) \cdot g^{-1} = \operatorname{stb}_G(g \cdot s_2).$$

□

BEISPIEL 1.1.21. *Für die Operation der unendlichen Diedergruppe D_∞ auf $\mathbb{R}$ sind die Stabilisatoren von $x = 1, \frac{1}{2}, \frac{1}{3}$ gegeben durch*

$$\begin{aligned}
\operatorname{stb}_{D_\infty}(1) &= \left\{\mathrm{id}, T^2 \cdot S\right\}, \\
\operatorname{stb}_{D_\infty}\left(\frac{1}{2}\right) &= \{\mathrm{id}, T \cdot S\}, \\
\operatorname{stb}_{D_\infty}\left(\frac{1}{3}\right) &= \{\mathrm{id}\}.
\end{aligned}$$

Denn die Gruppenelemente sind von der Form $T^n S$ oder T^n für $n \in \mathbb{Z}$, wegen $S^2 = \mathrm{id}$ und $S \cdot T^n = T^{-n} \cdot S$. Zum Beispiel hat die Gleichung $g \cdot x = x$ für $x = \frac{1}{3}$ nur die Lösung $g = \mathrm{id}$: Für $g = T^n$ folgt aus $T^n\left(\frac{1}{3}\right) = \frac{1}{3}$ natürlich $n = 0$, und für $g = T^n \cdot S$ ergibt

$$\frac{1}{3} = (T^n \cdot S)\left(\frac{1}{3}\right) = T^n\left(-\frac{1}{3}\right) = n - \frac{1}{3}$$

einen Widerspruch wegen $n \in \mathbb{Z}$.

LEMMA 1.1.22 (Burnside). *Sei G eine* endliche *Gruppe, die auf der* endlichen *Menge S wirkt. Dann gilt:*

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} \left|\operatorname{fxp}_S(g)\right| \tag{1.4}$$

BEWEIS. Der Beweis besteht aus einer typischen Anwendung des *Prinzips der doppelten Abzählung*, das in der abzählenden Kombinatorik häufig verwendet wird (siehe [**5**]): Sei

$$T = \{(g, s) \in G \times S : \ g \cdot s = s\}.$$

Dann können wir die Elemente von T auf zwei Arten abzählen:

$$\begin{aligned}|T| &= \sum_{g\in G} |\{s \in S\colon\ g\cdot s = s\}| \\ &= \sum_{s\in S} |\{g \in G\colon\ g\cdot s = s\}|\,.\end{aligned}$$

Mit den Bezeichnungen aus Definition 1.1.10 haben wir also die Gleichung

$$\sum_{g\in G} \left|\mathrm{fxp}_S(g)\right| = \sum_{s\in S} \left|\mathrm{stb}_G(s)\right|. \tag{1.5}$$

Nun formen wir um:

$$\begin{aligned}\sum_{s\in S} |\mathrm{stb}_G(s)| &= \sum_{o\in S/G}\sum_{s\in o} |\mathrm{stb}_G(s)| \quad \leftarrow \text{Orbits } o \text{ sind Partition von } S \\ &= \sum_{o\in S/G} |o|\cdot|\mathrm{stb}_G(s)| \quad \leftarrow \text{Korollar 1.1.20} \\ &= \sum_{o\in S/G} |G| = |S/G|\cdot|G|\,. \quad \leftarrow \text{siehe (1.2) in Lemma 1.1.17}\end{aligned}$$

Daraus folgt die Behauptung. □

BEMERKUNG 1.1.23. *Das Lemma von Burnside ist die Grundlage für die* Polyasche Abzähltheorie *(siehe* **[4]***).*

1.1.1. Wirkung einer Gruppe auf sich selbst durch Konjugation.

DEFINITION 1.1.24. *Falls G durch Konjugation auf sich selbst operiert, so nennen wir den Stabilisator von $x \in G$ auch den* Zentralisator *von x in G und bezeichnen ihn mit*

$$\mathrm{cnt}_G(x) := \mathrm{stb}_G(x) = \{g \in G\colon\ g\cdot x = x\cdot g\}\,.$$

Das Zentrum $Z(G)$ *von G ist der Durchschnitt über alle Zentralisatoren:*

$$Z(G) := \bigcap_{x\in G} \mathrm{cnt}_G(x) = \{g \in G\colon\ g\cdot x = x\cdot g \text{ für alle } x \in G\} \sqsubseteq G.$$

Es gilt immer $\mathtt{n}_G \in Z(G)$; wenn $Z(G) = \{\mathtt{n}_G\}$ gilt, nennt man das ein triviales Zentrum*. Für eine Untergruppe $H \sqsubseteq G$ von G heißt der der Stabilisator von H auch der* Normalisator *von H in G und bezeichnen ihn mit*

$$N_G(H) := \mathrm{stb}_G(H) = \left\{g \in G\colon\ g\cdot H\cdot g^{-1} = H\right\}.$$

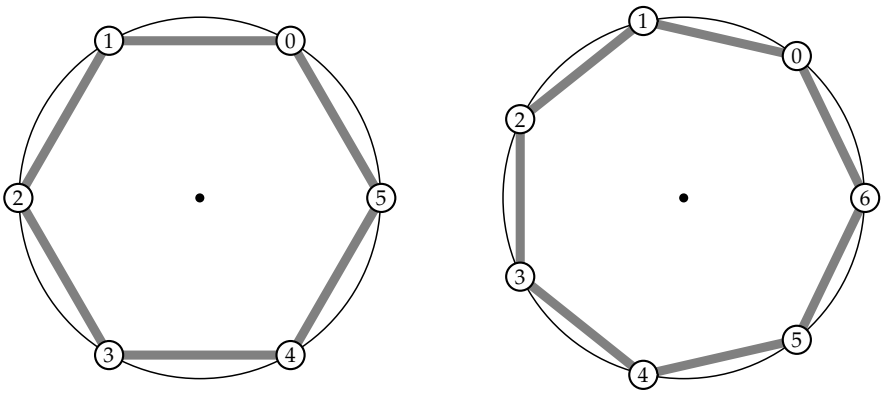
Aus dieser Definition folgt nun in Verbindung mit Lemma 1.1.17 sofort:

KOROLLAR 1.1.25. *Sei G eine* endliche *Gruppe. Die Anzahl der Konjugierten $g\cdot H\cdot g^{-1}$ einer Untergruppe H von G ist gleich $(G : N_G(H)) = |G| \,/\, |N_G(H)|$.*

BEWEIS. Die Gruppe G wirkt durch Konjugation auf der Familie der Nebenklassen G/H von H: Der *Index der Untergruppe* $N_G(H) \sqsubseteq G$ ist definitionsgemäß (siehe Definition A.3.11) die *Anzahl* der Nebenklassen von $N_G(H)$. □

Ebenso erhält man die sogenannte *Klassengleichung* (als Spezialfall der Bahnengleichung (1.3)), die viele Folgerungen für die abstrakte Gruppentheorie hat:

ABBILDUNG 1. Reguläre Polygone: Hier zur Illustration das regelmäßige Sechseck und Siebeneck.



SATZ 1.1.26 (Klassengleichung). *Sei G eine endliche Gruppe. Betrachte die Wirkung von G durch Konjugation auf sich selbst, und sei $\mathcal{R}$ ein* Repräsentantensystem *der Konjugationsklassen von G. Dann gilt*

$$|G| = \sum_{r \in \mathcal{R}} (G : \mathrm{cnt}_G(r)).$$

1.1.2. Die (endliche) Diedergruppe. Geometrisch kann man sich C_n (siehe Definition A.3.9) als die Gruppe der *Drehungen* eines regulären Polygons mit n Ecken vorstellen, siehe Abbildung 1: Drehungen sind spezielle Symmetrien eines regulären Polygons, weitere Symmetrien sind *Spiegelungen*.

DEFINITION 1.1.27. *Für $n \in \mathbb{N}$, $n \geq 3$, ist die (endliche)* Diedergruppe D_n *die Symmetriegruppe eines regulären n-Ecks: Zusätzlich zu den n Drehungen kommen nun noch* Spiegelungen *dazu. Dies kann man so fassen: Seien die Ecken des Polygons gegen den Uhrzeigersinn mit $0, 1, \ldots, n-1$ numeriert, und bezeichne*

- *r die Drehung um $2\pi/n$,*
- *s die Spiegelung an der Symmetrieachse durch die mit 0 numerierte Ecke.*

In bezug auf die numerierten Ecken wirken diese Symmetrieabbildungen so:

$$r(i) = i + 1 \pmod{n},$$
$$s(i) = n - i \pmod{n}.$$

Klarerweise gilt $r^n = \mathbb{m}_{D_n} = \mathrm{id}$ und $s^2 = \mathbb{m}_{D_n} = \mathrm{id}$, außerdem sieht man schnell, daß $s \cdot r = r^{n-1} \cdot s = r^{-1} \cdot s$ gilt: Die Diedergruppe hat also die Elemente

$$D_n = \left\{ \mathrm{id}, r, r^2, \ldots, r^{n-1}, s, r \cdot s, r^2 \cdot s, \ldots, r^{n-1} \cdot s \right\}.$$

Geometrisch ist klar, daß diese Elemente alle verschieden sind, also gilt $|D_n| = 2n$.
Es ist $D_n = \langle r \rangle \rtimes_\theta \langle s \rangle = C_n \rtimes_\theta C_2$ ein semidirektes Produkt (siehe Definition A.3.27) der zyklischen Gruppen C_n und C_2, mit dem Gruppenhomomorphismus $\theta(s)\left(r^i\right) := r^{-i}$.
Für $n \leq 2$ definiert man die Diedergruppen so:

$$D_1 := C_1,\ D_2 := C_2 \times C_2.$$

KOROLLAR 1.1.28. *Sei G eine Gruppe der Ordnung $2p$ für eine Primzahl $p > 2$. Dann ist G zyklisch oder eine* Diedergruppe.

BEWEIS. Nach Satz 1.1.12 gibt es ein Element s der Ordnung 2 und ein Element r der Ordnung p in G. Dann ist $C_p = \langle r \rangle$ ein Normalteiler in G wegen $\left(G : C_p\right) = 2$ (siehe Proposition A.3.15). Natürlich ist $s \notin C_p$, also ist

$$G = C_p \cup C_p \cdot s.$$

Da C_p ein Normalteiler ist, ist $s \cdot r \cdot s^{-1} = r^i$ für ein $i \in \mathbb{Z}$. Aus $s^2 = e$ folgt

$$r = s^2 \cdot r \cdot s^{-2} = s \cdot \left(s \cdot r \cdot s^{-1}\right) \cdot s^{-1} = r^{i^2}.$$

Das bedeutet aber $i^2 \equiv 1 \mod p$, oder $i^2 = 1$ im Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: Diese quadratische Gleichung hat *genau* (siehe Satz A.3.81) zwei Lösungen in $\mathbb{F}_p$, nämlich $i \equiv 1 \mod p$ oder $i \equiv -1 \mod p$.

Im ersten Fall ist die Gruppe G kommutativ, und $r \cdot s$ ist ein Element der Ordnung $2 \cdot p$, also $G = \langle r \cdot s \rangle \simeq C_{2p}$.

Im zweiten Fall gilt $s \cdot r = r^{-1} \cdot s$, also $G \simeq D_p$. □

BEISPIEL 1.1.29. *Jede Gruppe der Ordnung 6 ist entweder isomorph zu C_6 oder zu $\mathfrak{S}_3 \simeq D_3$: Die Gruppe D_3 wird erzeugt von den beiden Permutationen (der mit $1, 2, 3$ numerierten Ecken eines Dreiecks)*

$$s = (23)\,,\ r = (123)\,,$$

und diese beiden Permutationen erzeugen auch die $\mathfrak{S}_3$.

1.2. Die Sylow–Sätze

DEFINITION 1.2.1. *Sei $n \in \mathbb{N}_0$. Eine Gruppe G der Ordnung p^n heißt p-Gruppe.*

PROPOSITION 1.2.2. *Sei G eine nicht–triviale p–Gruppe (also $|G| = p^n$ für $n \in \mathbb{N}$), die auf einer endlichen Menge S operiert. Dann gilt:*

$$|S| \equiv \left|\mathrm{fxp}_S(G)\right| \pmod{p}.$$

BEWEIS. Sei $\mathcal{R}'$ ein *Repräsentantensystem* der Familie der G–Orbits mit *mehr als einem Element*, dann folgt aus der Bahngleichune (Korollar 1.1.18)

$$|S| = \left|\mathrm{fxp}_S(G)\right| + \sum_{x \in \mathcal{R}'} \left(G : \mathrm{stb}_G(x)\right).$$

Wenn $x \notin \mathrm{fxp}_S(G)$ ist, dann ist der Stabilisator von x eine *echte* Untergruppe von G, also

$$\mathrm{stb}_G(x) \neq G$$

und daher $\left|\mathrm{stb}_G(x)\right| = p^k$ für $0 \leq k < n$ nach dem Satz von Lagrange (A.3.12). Für alle $x \in \mathcal{R}'$ gilt also $p \mid \left(G : \mathrm{stb}_G(x)\right)$, also $\left(G : \mathrm{stb}_G(x)\right) \equiv 0 \pmod{p}$. □

KOROLLAR 1.2.3. *Jede nicht–triviale p–Gruppe G hat ein nicht–triviales Zentrum.*

BEWEIS. Dazu betrachten wir die Wirkung von G auf sich selbst (also $S = G$) durch Konjugation: Das Zentrum von G ist dann ja nichts anderes als

$$Z(G) = \mathrm{fxp}_S(G),$$

also gilt $p \mid |Z(G)|$: Da $\mathbb{1}_G \in Z(G)$, ist $|Z(G)| \neq 0$, also $|Z(G)| > 1$. □

KOROLLAR 1.2.4. *Jede Gruppe der Ordnung p^2 ist abelsch (und damit isomorph zu $C_p \times C_p$ oder C_{p^2}).*

BEWEIS. Wir müssen zeigen: $Z = Z(G) = G$. Nach Korollar 1.2.3 ist $|Z| \in \{p, p^2\}$, also genügt es zu zeigen: $|Z| = p^2$.
Angenommen, $|Z| = p$: Definitionsgemäß ist Z ein *Normalteiler* in G, also ist G/Z eine Gruppe der Ordnung p und somit zyklisch nach Proposition A.3.17. Es gibt also ein $x \in G$ mit $G/Z = \langle x \cdot Z \rangle$. Für zwei beliebige Elemente $g, h \in G$ gilt also $g = x^r \cdot z_1$ und $h = x^s \cdot z_2$ für $z_1, z_2 \in Z$. Dann folgt aber:

$$\begin{aligned} g \cdot h &= x^r \cdot z_1 \cdot x^s \cdot z_2 \\ &= x^{r+s} \cdot z_1 \cdot z_2 = x^{r+s} \cdot z_2 \cdot z_1 \ \leftarrow \text{da } z_1 \text{ im Zentrum von } G \\ &= x^s \cdot z_2 \cdot x^r \cdot z_1 = h \cdot g. \ \leftarrow \text{da } z_2 \text{ im Zentrum von } G \end{aligned}$$

Also ist G kommutativ. □

DEFINITION 1.2.5 (p–Sylow–Untergruppe). *Sei G eine endliche Gruppe der Ordnung $p^r \cdot m$ mit $p \in \mathbb{P}$ und $\mathrm{ggT}(p, m) = 1$. Eine Untergruppe $H \sqsubseteq G$ der Ordnung $|H| = p^r$ heißt p–*Sylow–Untergruppe.

SATZ 1.2.6 (1. Sylowsatz). *Sei G eine endliche Gruppe der Ordnung $p^r \cdot m$ mit $p \in \mathbb{P}$ und $\mathrm{ggT}(p, m) = 1$. Dann enthält G eine p–Sylow–Untergruppe.*

BEWEIS. Sei $S := \{X \subseteq G : \ |X| = p^r\}$. Dann wirkt G auf S durch Linksmultiplikation:

$$(g, X) \mapsto g \cdot X.$$

Es ist

$$|S| = \binom{p^r \cdot m}{p^r} = \frac{p^r \cdot m \cdot (p^r \cdot m - 1) \cdots (p^r \cdot m - p^r + 1)}{p^r \cdot (p^r - 1) \cdots 2 \cdot 1},$$

und $p \nmid |S|$, denn nach Kürzen der durch p teilbaren Faktoren in Zähler und Nenner

$$\frac{p^r \cdot m}{p^r} \cdot \frac{p^r \cdot m - p}{p^r - p} \cdot \frac{p^r \cdot m - 2 \cdot p}{p^r - 2 \cdot p} \cdots$$

durch die größtmögliche p–Potenz teilt p keinen Faktor des (gekürzten) Zählers mehr. Es muß also einen Orbit $G \cdot X$ geben mit $p \nmid |G \cdot X|$ (siehe Beobachtung 1.1.11): Wegen

$$|G| = |G \cdot X| \cdot |\mathrm{stb}_G(X)|$$

(siehe (1.2) in Lemma 1.1.17) muß also gelten

$$p^r \mid |\mathrm{stb}_G(X)|.$$

Die Gruppe $\mathrm{stb}_G(X)$ wirkt auf X durch Linksmultiplikation (induzierte Gruppenwirkung, vergleiche Bemerkung 1.1.19), und die Orbits dieser Wirkung sind genau jene *Rechtsnebenklassen* von $\mathrm{stb}_G(X)$, die in X enthalten sind:

$$\mathrm{stb}_G(X) \cdot g \subseteq X.$$

Alle diese Nebenklassen haben aber dieselbe Mächtigkeit, nämlich $|\mathrm{stb}_G(X)|$: Also gilt

$$|\mathrm{stb}_G(X)| \mid p^r.$$

Insgesamt folgt $p^r = |\mathrm{stb}_G(X)|$, und wir haben mit $\mathrm{stb}_G(X)$ die gesuchte p–Sylow–Untergruppe gefunden. □

SATZ 1.2.7 (2. Sylowsatz). *Sei G eine endliche Gruppe der Ordnung $p^r \cdot m$ mit $p \in \mathbb{P}$ und $\mathrm{ggT}(p, m) = 1$. Seien $P, Q \sqsubseteq G$ zwei p–Sylow–Untergruppen von G. Dann gibt es ein $g \in G$, sodaß*

$$P = g \cdot Q \cdot g^{-1}.$$

(Also: Je zwei p–Sylow–Untergruppen sind konjugiert.)
Außerdem ist jede *p–Untergruppe in einer p–Sylow–Untergruppe enthalen.*

BEWEIS. Die Wirkung von G auf den Linksnebenklassen G/Q von Q (durch Linksmultiplikation) kann man auf P einschränken: Das ergibt also eine Wirkung von P auf G/Q. Es gilt natürlich

$$p \nmid |G/Q| = |G| \,/\, |Q|\,,$$

und somit folgt aus der Bahnengleichung (1.3), daß es *einpunktige* Orbits geben muß (denn alle größeren Orbits haben Mächtigkeit p^m mit $0 < m \leq r$ gemäß (1.2)), also *Fixpunkte* der Wirkung von P auf G/Q. Das heißt aber, es gibt eine Linksnebenklasse $g \cdot Q$, sodaß

$$x \cdot g \cdot Q = g \cdot Q \text{ für alle } x \in P.$$

Daraus folgt

$$x \cdot g \in g \cdot Q \implies x \in g \cdot Q \cdot g^{-1}$$

für alle $x \in P$, also $P \subseteq g \cdot Q \cdot g^{-1}$, und da diese Mengen dieselbe Mächtigkeit (nämlich p^r) haben, gilt

$$P = g \cdot Q \cdot g^{-1}.$$

Sei H eine beliebige p–Untergruppe von G, und sei Q eine p–Sylow–Untergruppe: Genau wie zuvor argumentieren wir, daß H auf G/Q operiert und (mindestens) einen Fixpunkt $y \cdot Q$ hat, also

$$h \cdot y \cdot Q = y \cdot Q \text{ für alle } h \in H.$$

Genau wie zuvor folgt wieder

$$H \subseteq y \cdot Q \cdot y^{-1},$$

also ist H in einer p–Sylow–Untergruppe enthalten. □

SATZ 1.2.8 (3. Sylowsatz). *Sei G eine endliche Gruppe der Ordnung $p^r \cdot m$ mit $p \in \mathbb{P}$ und $\mathrm{ggT}(p, m) = 1$. Die Menge aller p–Sylow–Untergruppen von G sei mit $\mathrm{Syl}_p(G)$ bezeichnet. Dann gilt:*

(i) $\left|\mathrm{Syl}_p(G)\right| \mid m$,

(ii) $\left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod{p}$.

BEWEIS. Sei P eine p–Sylow–Untergruppe von G. G operiert auf $\mathrm{Syl}_p(G)$ durch Konjugation, und diese Wirkung hat nach dem 2. Sylowsatz nur einen Orbit:

$$\mathrm{Syl}_p(G) = G \cdot P \implies \left|\mathrm{Syl}_p(G)\right| = |G/N_G(P)|.$$

Natürlich ist $P \sqsubseteq N_G(P)$ eine Untergruppe des Normalisators von P; also ist

$$m = |G/P| = |G/N_G(P)| \cdot |N_G(P)/P|,$$

und daraus folgt (i).
Die Wirkung von G auf $\mathrm{Syl}_p(G)$ durch Konjugation kann man auf P einschränken und erhält so eine Wirkung von P auf $\mathrm{Syl}_p(G)$. Klarerweise ist $P \in \mathrm{Syl}_p(G)$ ein Fixpunkt dieser Wirkung (also $\mathrm{fxp}_{\mathrm{Syl}_p(G)}(P)$); sei Q ein *weiterer* Fixpunkt dieser Wirkung, d.h.

$$Q = g \cdot Q \cdot g^{-1} \text{ für alle } g \in P.$$

Dann ist also $P \sqsubseteq N_G(Q)$; und natürlich gilt auch $Q \sqsubseteq N_G(Q)$: P und Q sind also p–Sylow–Untergruppen von $N_G(Q)$ und daher (nach dem 2. Sylowsatz) konjugiert in $N_G(Q)$. Es gibt also ein $h \in N_G(Q)$ mit

$$Q = h \cdot Q \cdot h^{-1} = P.$$

Das heißt aber, P ist der *einzige* Fixpunkt dieser P–Wirkung, also folgt die Behauptung aus der Bahnengleichung (1.3) (denn alle größeren Orbits haben Mächtigkeit p^m mit $0 < m \leq r$ gemäß (1.2)). □

1.2.1. Anwendungen des Sylowsätze.

KOROLLAR 1.2.9. *Es gibt (bis auf Isomorphie) nur eine Gruppe der Ordnung 143, nämlich die zyklische* C_{143}.

BEWEIS. Es ist $143 = 11 \cdot 13$ das Produkt der Primzahlen 11 und 13. Nach dem 3. Sylowsatz gilt

- $\left|\mathrm{Syl}_{13}(G)\right| \in \{1, 11\}$ und $|\mathrm{Syl}_{11}(G)| \in \{1, 13\}$,
- $\left|\mathrm{Syl}_{13}(G)\right| \equiv 1 \pmod{13}$ und $|\mathrm{Syl}_{11}(G)| \equiv 1 \pmod{11}$;

und daraus folgt: Es gibt *genau eine* 11–Sylow–Untergruppe P und *genau eine* 13–Sylow–Untergruppe Q. Beide sind Normalteiler, denn sie stimmen mit allen ihren Konjugierten überein:

$$P \lhd G \text{ und } Q \lhd G.$$

Dann ist aber $P \cdot Q \sqsubseteq G$ eine (normale) Untergruppe von G (siehe Proposition A.3.16), die P und Q enthält. Es ist $P \cap Q = \{\mathbb{n}_G\}$, denn P und Q sind beide zyklisch, und jedes Element ungleich $\mathbb{n}_G$

- in P hat Ordnung 11,
- in Q hat Ordnung 13.

Also ist $|P \cdot Q| = 11 \cdot 13 = |G|$ (siehe Proposition A.3.7) und damit $P \cdot Q = G$. Nach Proposition A.3.25 ist $P \cdot Q \simeq P \times Q = C_{11} \times C_{13} \simeq C_{143}$. □

KOROLLAR 1.2.10. *Seien* $p > q \in \mathbb{P}$ *zwei Primzahlen. Jede Gruppe der Ordnung* $p \cdot q$ *ist* nicht *einfach.*

BEWEIS. Die Anzahl der p–Sylow–Untergruppen ist nach dem 3. Sylowsatz

- einerseits $\equiv 1 \pmod{p}$, also $\in \{1, p+1, 2p+1, \cdots\}$,
- andrerseits ein Teiler von q:

Also ist sie genau 1, da $p > q$: Diese einzige p–Sylow–Gruppe ist *normal*, da sie mit allen ihren Konjugierten übereinstimmt, und somit hat G einen *nicht–trivialen* Normalteiler. □

KOROLLAR 1.2.11. *In jeder Gruppe G der Ordnung 20 gibt es genau 4 Elemente der Ordnung 5.*

BEWEIS. Die Anzahl der 5–Sylow–Untergruppen von G ist nach dem 3. Sylowsatz ein Teiler von 4 und kongruent 1 modulo 5: Also gibt es *genau eine* 5–Sylow–Untergruppe, deren 4 Elemente $\neq \mathbb{n}_G$ alle die Ordnung 5 haben. □

1.3. Isometriegruppen des Euklidischen Raumes

DEFINITION 1.3.1. *Ein* Euklidischer Vektorraum *ist ein Paar (E, σ), wobei E ein endlich–dimensionaler $\mathbb{R}$–Vektorraum E ist und σ eine* positiv definite symmetrische Bilinearform

$$\sigma : E \times E \to \mathbb{R},$$

d.h.:

- $\sigma(x + \lambda \cdot y, r + \mu \cdot s) = \sigma(x, r) + \lambda \cdot \sigma(y, r) + \mu \cdot \sigma(x, s) + \lambda \cdot \mu \cdot \sigma(y, s)$ *für alle $x, y, r, s \in E$ und alle $\lambda, \mu \in \mathbb{R}$ (Bilinearität),*
- $\sigma(x, y) = \sigma(y, x)$ *für alle $x, y \in E$ (Symmetrie),*
- $\sigma(x, x) > 0$ *für alle $x \neq \mathbf{0}$ in E (Positive Definitheit).*

Für $x \in E$ setzen wir $\|x\| = \sqrt{\sigma(x, x)}$ und $d(x, y) = \|x - y\|$: $d \colon E \times E \to \mathbb{R}^+$ ist eine Metrik *auf E.*

Wir können den Vektorraum E nach Wahl einer Orthonormalbasis *(in bezug auf σ) mit dem Koordinatenraum $\mathbb{R}^n$ identifizieren: Dann ist $\sigma(x, y) = \langle x, y \rangle$ das übliche Skalarprodukt, und $d(x, y) = \|x - y\|$ die übliche Euklidische Metrik.*

DEFINITION 1.3.2. *Eine Abbildung $f : E \to E$ heißt* Isometrie *(oder* Bewegung*), falls für alle $x, y \in E$*

$$d(f(x), f(y)) = d(x, y)$$

gilt.

BEOBACHTUNG 1.3.3. *Eine Isometrie erhält also den Abstand zwischen zwei Punkten und ist somit offensichtlich* injektiv.

Ebenso klar ist, daß die Zusammensetzung *$\phi \circ \theta$ zweier Isometrien ϕ, θ wieder eine Isometrie ist.*

BEISPIEL 1.3.4. *Eine* Translation *von E ist eine Abbildung $T : E \to E$ der Form*

$$T(x) = x + b$$

für einen Vektor $b \in E$: Das ist offensichtlich eine Isometrie.

DEFINITION 1.3.5. *Eine lineare Abbildung $f : \mathbb{R}^n \to \mathbb{R}^n$ heißt* orthogonal, *falls*

$$\langle f(x), f(y) \rangle = \langle x, y \rangle$$

für alle $x, y \in \mathbb{R}^n$ gilt
Wegen $\langle x, y \rangle = x^t \cdot y$ erfüllt die Matrix B, die f repräsentiert, die Gleichung

$$(B \cdot x)^t \cdot (B \cdot x) = x^t \cdot B^t \cdot B \cdot y = x^t \cdot y$$

für alle $x, y \in \mathbb{R}^n$. Somit gilt $B^t \cdot B = E_n$, und B gehört zur orthogonalen Gruppe $O_n(\mathbb{R})$.

BEISPIEL 1.3.6. *Eine orthogonale lineare Abbildung $f : E \to E$ ist auch eine Isometrie, denn*

$$\begin{aligned} d(f(x), f(y))^2 &= \|f(x) - f(y)\|^2 \\ &= \langle f(x-y), f(x-y) \rangle \\ &= \langle x-y, x-y \rangle \\ &= d(x,y)^2. \end{aligned}$$

Umgekehrt haben wir:

LEMMA 1.3.7. *Es sei $f : E \to E$ eine Isometrie mit $f(\mathbf{0}) = \mathbf{0}$. Dann ist f eine orthogonale lineare Abbildung.*

BEWEIS. Mit der Polarisierungsformel (siehe Proposition A.4.2) folgt

$$\begin{aligned} 2 \cdot \langle x, y \rangle &= \|x\|^2 + \|y\|^2 - \|x-y\|^2 \\ &= d(x, \mathbf{0})^2 + d(y, \mathbf{0})^2 - d(x,y)^2 \\ &= d(f(x), f(\mathbf{0}))^2 + d(f(y), f(\mathbf{0}))^2 - d(f(x), f(y))^2 \\ &= \|f(x)\|^2 + \|f(y)\|^2 - \|f(x) - f(y)\|^2 \\ &= 2 \cdot \langle f(x), f(y) \rangle \end{aligned}$$

für alle $x, y \in E$. Also erhält f das innere Produkt.
Wir müssen noch zeigen, daß f eine lineare Abbildung ist. Sei $\mathcal{B} = (e_1, \ldots, e_n)$ die Standardbasis (eine Orthonormalbasis) des $\mathbb{R}^n$. Da f das innere Produkt erhält, ist $\mathcal{B}' = (f(e_1), \ldots, f(e_n))$ ebenfalls eine Orthonormalbasis.
Für jedes $x \in E$ haben wir die Entwicklung in der Standardbasis $\mathcal{B}$:

$$x = \sum_{k=1}^{n} \langle x, e_k \rangle \cdot e_k.$$

Und für jedes $f(x)$ haben wir die Entwicklung in der Basis $\mathcal{B}'$:

$$\begin{aligned} f(x) &= \sum_{k=1}^{n} \langle f(x), f(e_k) \rangle \cdot f(e_k) \\ &= \sum_{k=1}^{n} \langle x, e_k \rangle \cdot f(e_k), \quad \leftarrow \text{da } f \text{ das innere Produkt erhält!} \end{aligned}$$

also ist f linear. □

Wir erkennen nun, daß Isometrien einfach *affine Abbildungen* sind:

KOROLLAR 1.3.8. *Sei $f : E \to E$ eine Isometrie des Euklidischen Vektorraums E. Wir identifizieren E mit dem "Standardraum" $\mathbb{R}^n$: Dann gibt es eine orthogonale Matrix $A \in O_n(\mathbb{R})$ und einen Vektor $v \in \mathbb{R}^n$, sodaß*

$$f(x) = A \cdot x + v$$

für alle $x \in E = \mathbb{R}^n$ gilt.

BEWEIS. Sei $v = f(\mathbf{0})$; sei $T : E \to T,\ x \mapsto x + v$: T ist auch eine Isometrie (Translation). Dann ist

$$g := T^{-1} \circ f,\ x \mapsto f(x) - v$$

eine Isometrie mit $g(\mathbf{0}) = \mathbf{0}$: Also ist g nach Lemma 1.3.7 eine *orthogonale lineare* Abbildung, und $f(x) = g(x) + v$ (also $f = T \circ g$). □

Seien f, g zwei Isometrien auf $\mathbb{R}^n$, gegeben durch $f(x) = A \cdot x + v$ und $g(x) = B \cdot x + w$ mit $A, B \in O_n(\mathbb{R})$ und $v, w \in \mathbb{R}^n$. Dann gilt ganz offensichtlich

$$f^{-1}(x) = A^{-1} \cdot x - A^{-1} \cdot v,$$

d.h., jede Isometrie ist invertierbar, und ihre Umkehrabbildung ist wieder eine Isometrie.

DEFINITION 1.3.9 (Isometriengruppe). *Die Isometrien eines Euklidischen Vektorraums E bilden also eine Gruppe (mit der Komposition von Funktionen, ihr neutrales Element ist die identische Abbildung* id*), die wir mit* Iso(E) *bezeichnen.*

Die Zusammensetzung der Isometrien f und g (wie oben beschrieben) können wir auch einfach mit Matrizenmultiplikation ausdrücken:

$$(f \circ g)(x) = A \cdot (B \cdot x + w) + v = A \cdot B \cdot x + (A \cdot w + v).$$

Damit lassen sich Isometrien von $E \simeq \mathbb{R}^n$ durch $(n+1) \times (n+1)$–Matrizen beschreiben:

$$\text{Iso}(E) \simeq \left\{ \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} :\ A \in O_n(\mathbb{R}), v \in \mathbb{R}^n \right\}, \tag{1.6}$$

in folgendem Sinn: Jedes $x \in E$ identifizieren wir mit einem Punkt $\begin{pmatrix} x \\ 1 \end{pmatrix}$ der Hyperebene

$$\left\{ (x_1, \ldots, x_n, x_{n+1}) \in \mathbb{R}^{n+1} :\ x_{n+1} = 1 \right\} \subset \mathbb{R}^{n+1}.$$

Die Gruppenwirkung von Iso(E) auf dem Raum $E = \mathbb{R}^n$ erscheint dann als

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} A \cdot x + v \\ 1 \end{pmatrix}$$

Die Multiplikation in der zu Iso(E) isomorphen Matrixgruppe ist gegeben durch

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A \cdot B & A \cdot w + v \\ 0 & 1 \end{pmatrix}. \tag{1.7}$$

Das Inverse ist dann

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1} \cdot v \\ 0 & 1 \end{pmatrix}.$$

Die Translationen

$$T(n) = \left\{ \begin{pmatrix} E_n & v \\ 0 & 1 \end{pmatrix} : \ v \in \mathbb{R}^n \right\}$$

bilden einen Normalteiler in $\mathrm{Iso}(E)$, denn

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} E_n & w \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} E_n & A \cdot w \\ 0 & 1 \end{pmatrix}. \tag{1.8}$$

Die Gruppe $T(n)$ ist natürlich isomorph zur additiven Gruppe $E \simeq \mathbb{R}^n$; es gilt in diesem Sinne $O_n(\mathbb{R}) \subseteq \mathrm{Aut}(T(n))$: Sei $\theta : O_n(\mathbb{R}) \to \mathrm{Aut}(T(n))$ die Inklusion; das ist natürlich ein Gruppenhomomorphismus, dann erscheint $\mathrm{Iso}(E)$ als das *semidirekte Produkt* (siehe Definition A.3.27) von $O_n(\mathbb{R})$ und $T(n)$:

$$\mathrm{Iso}(E) = T(n) \rtimes_\theta O_n(\mathbb{R}).$$

(Betrachte dazu einfach die Multiplikation in $\mathrm{Iso}(E)$ gemäß (1.7).) Allgemeiner gilt:

LEMMA 1.3.10. *Sei $G \sqsubseteq \mathrm{Iso}(\mathbb{R}^n)$ eine* beliebige *Untergruppe der Isometrien von $\mathbb{R}^n$. Sei T_G die Menge aller* Translationen *in G, also*

$$T_G = \left\{ g \in G : \ g \sim \left(\begin{smallmatrix} E_n & t \\ 0 & 1 \end{smallmatrix} \right) \right\}.$$

Sei O_G die Menge aller orthogonalen $n \times n$–Matrizen, die in der Matrixdarstellung von Elementen aus G auftreten, also

$$O_G = \left\{ A \in O_n(\mathbb{R}) : \ \exists g \in G \text{ sodaß } g \sim \left(\begin{smallmatrix} A & v \\ 0 & 1 \end{smallmatrix} \right) \right\} \subset O_n \sqsubseteq \mathrm{Iso}(\mathbb{R}^n).$$

Dann ist die Abbildung ψ

$$G \to \mathrm{Iso}(\mathbb{R}^n) : \ g \sim \left(\begin{smallmatrix} A & v \\ 0 & 1 \end{smallmatrix} \right) \mapsto A$$

ein Homomorphismus mit Kern T_G und Bild O_G, also ist $T_G \lhd G$ und $O_G \sqsubseteq O_n(\mathbb{R})$, und es gilt

$$G/T_G \simeq O_G.$$

Außerdem ist $O_G \sqsubseteq \mathrm{Aut}(T_G)$: G ist also isomorph zum semidirekten Produkt (siehe Definition A.3.27) $T_G \rtimes_\theta O_G$, wobei θ die natürliche Einbettung der Untergruppe O_G in $\mathrm{Aut}(T_G)$ bezeichnet. Nach dem Splitting Lemma *(A.3.32) ist ein isomorphes Bild von O_G als Untergruppe in G enthalten, das wir der Einfachheit halber auch wieder mit O_G bezeichnen, also $O_G \sqsubseteq G$. Für ein $t \in T_G$ erscheint die Linksnebenklasse*

$$t \cdot O_G \simeq \left\{ \left(\begin{smallmatrix} E & t \\ 0 & 1 \end{smallmatrix} \right) \cdot \left(\begin{smallmatrix} B & v \\ 0 & 1 \end{smallmatrix} \right) = \left(\begin{smallmatrix} B & t+v \\ 0 & 1 \end{smallmatrix} \right) \right\}$$

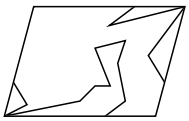
als die "um t verschobenen Untergruppe O_G".

BEWEIS. Daß die Abbildung ψ ein Homomorphismus ist, folgt sofort aus (1.7); ebenso die Aussagen über Kern und Bild.
Sei $g \in G$ beliebig mit Matrixdarstellung $g \sim \left(\begin{smallmatrix} A & v \\ 0 & 1 \end{smallmatrix} \right)$, und sei $t \in T_G$ beliebig mit Matrixdarstellung $t \sim \left(\begin{smallmatrix} E_n & w \\ 0 & 1 \end{smallmatrix} \right)$. Dann ist gemäß (1.8)

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} E_n & w \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} E_n & A \cdot w \\ 0 & 1 \end{pmatrix} \in T_G,$$

das heißt aber: Für alle $A \in S$ ist die Multiplikation mit A (also die durch A bestimmte lineare Abbildung $\mathbb{R}^n \to \mathbb{R}^n$) ein *Automorphismus* $T_G \to T_G$, und die Isomorphie zum semidirekten Produkt folgt sofort aus (1.7). □

ABBILDUNG 2. Einfache parallelogrammförmige Kachel, die ein schlichtes graphisches Motiv zeigt.



DEFINITION 1.3.11. *Sei* $G \sqsubseteq \mathrm{Iso}(\mathbb{R}^n)$ *eine Untergruppe der Isometrien von* $\mathbb{R}^n$*: Dann nennen wir die gemäß Lemma 1.3.10 enthaltenen Untergruppen* $T_G \lhd G$ *bzw.* $O_G \sqsubseteq G$ *den* Translationsteil *bzw. den* Orthogonalteil *von* G*.*

DEFINITION 1.3.12. *Eine Menge* $S \subseteq \mathbb{R}^n$ *heißt* diskret*, falls sie keinen Häufungspunkt hat: Das heißt, es gibt ein* $c > 0$*, sodaß für alle* $x \neq y \in S$ $d(x, y) \geq c$*.*

Eine Untergruppe $\Gamma \subseteq \mathrm{Iso}(E)$ *heißt* diskret*, falls alle Bahnen* $\Gamma \cdot x \subseteq \mathbb{R}^n$ *diskrete Mengen im* $\mathbb{R}^n$ *sind.*

BEISPIEL 1.3.13. *Die Untergruppe* $\Gamma \subseteq \mathrm{Iso}(\mathbb{R}^2)$*, die den Einheitskreis in sich abbildet, ist* nicht *diskret. (Sei besteht aus Drehungen um einen beliebigen Winkel und Spiegelungen an einem beliebigen Durchmesser und ist isomorph zur* $O_2(\mathbb{R})$*.)*

Im Sinne von Definition 1.3.11 ist hier $T_\Gamma = \{\mathbb{n}_\Gamma\}$*.*

BEISPIEL 1.3.14. *Die Untergruppe* $\Gamma \subseteq \mathrm{Iso}(\mathbb{R}^2)$*, die von den zwei Translationen* $t_1(x) = x + (1, 0)$ *und* $t_1(x) = x + (0, 1)$ *erzeugt wird, ist diskret: Es ist dies die Gruppe* $\Gamma = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$*; jede Bahn entspricht einem "verschobenen" Gitter* $\mathbb{Z}^2$*:*

$$\Gamma \cdot x = x + \mathbb{Z}^2.$$

Im Sinne von Definition 1.3.11 ist hier $O_\Gamma = \{\mathbb{n}_\Gamma\}$*.*

1.4. Symmetriegruppen von Ornamenten im $\mathbb{R}^2$

Wir betrachten die Ebene $\mathbb{R}^2$: Klarerweise können wir sie mit identischen parallelogrammförmigen *Kacheln* (siehe zum Beispiel Abbildung 2) lückenlos bedecken und erhalten so eine *Parkettierung* der Ebene. Wenn die Kacheln ein (für alle Kacheln identisches) *einfärbiges Motiv*[1] zeigen, entsteht durch die Parkettierung ein *doppelt–periodisches* Muster[2], das über die ganze Ebene ausgebreitet ist (siehe zum Beispiel Abbildung 3): Solch ein Muster nennen wir ein *Ornament*.

Ornamente spielen in der Kunstgeschichte eine große Rolle, insbesondere in der arabischen Welt; siehe z.B. Abbildung 4: Wir behandeln Ornamente hier aber "rein mathematisch".

[1] Das wir rein mathematisch (also ohne jede Rücksicht auf die künstlerische Qualität) einfach als Menge der gefärbten Punkte der Kachel auffassen.

[2] Wieder rein mathematisch gesehen, ist das Muster einfach die Vereinigung über alle Motive der einzelnen Kacheln.

ABBILDUNG 3. Einfaches Ornament, das durch Parkettierung der Ebene mit der Kachel aus Abbildung 2 entsteht.
Das Bild zeigt einen Ausschnitt der parkettierten Ebene; die Kacheln sind zur besseren Sichtbarkeit des entstehenden doppelt–periodischen Musters alternierend gefärbt (Färbungen des Musters spielen aber für unsere Überlegungen keine Rolle, es geht nur um die Linien). Die schwarzen Pfeile zeigen die zwei Translationen t_1, t_2, die die Symmetriegruppe des Ornaments erzeugen.

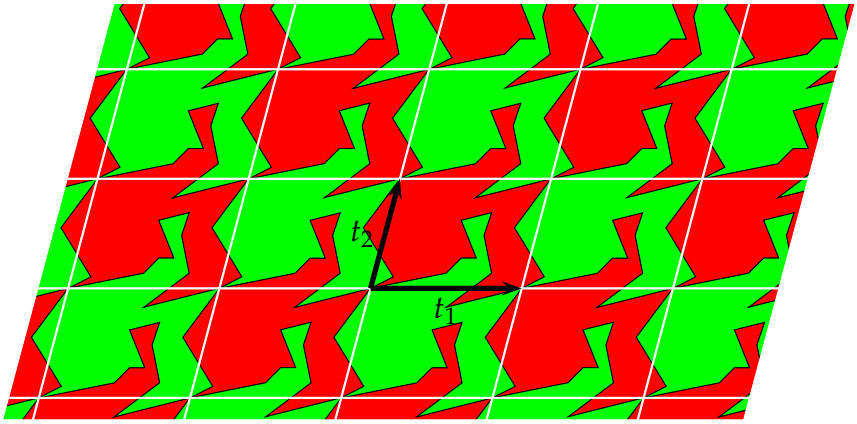
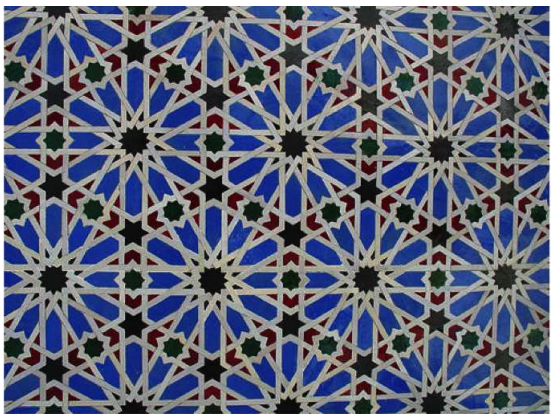


ABBILDUNG 4. Arabische Ornamentik (zu den Ornamenten in der Alhambra von Granada siehe auch **[6]**; das Bild hier wurde aus dem Skriptum von Professor Burde **[2]** übernommen).



DEFINITION 1.4.1. *Sei M eine nicht–leere Teilmenge eines Euklidischen Vektorraumes E. Eine Isometrie $s : E \to E$ heißt eine* Symmetrie *von M, falls $s(M) = M$ gilt.*

Die Menge aller Symmetrien von M bildet offensichtlich eine Untergruppe von Iso (E), *die mit* Sym (M) *bezeichnet wird.*

Wir werden im folgenden die Symmetriegruppen von Ornamenten in der Ebene behandeln:

DEFINITION 1.4.2. *Eine Untergruppe* $\Gamma \subseteq \mathrm{Iso}\left(\mathbb{R}^2\right)$ *heißt* Ornamentgruppe, *falls sie* diskret *ist und ihr Translationsteil* T_Γ *von* zwei Translationen *mit linear unabhängigen Richtungen* t_1, t_2 *erzeugt wird:*

$$T_\Gamma = \langle t_1, t_2 \rangle \simeq \mathbb{Z}^2.$$

Eine Translation $t \in T_\Gamma$ *ist also eine Linearkombination* $t = \lambda \cdot t_1 + \mu \cdot t_2$ *mit Koeffizienten* $\lambda, \mu \in \mathbb{Z}$*: Wir nennen* $t \in T_\Gamma$ unteilbar, *wenn* t kein *echtes Vielfaches eines* $t' \in T_\Gamma$ *ist, also*

$$\forall t' \in T_\Gamma, m > 1 \in \mathbb{Z}\colon\ t \neq m \cdot t' \iff \mathrm{ggT}\,(\lambda, \mu) = 1.$$

Unter einem Ornament *versteht man dann eine Menge* $M \subset \mathbb{R}^2$*, deren Symmetriegruppe* $\mathrm{Sym}\,(M)$ *eine Ornamentgruppe ist.*

(Die mathematische Fassung des Begriffs "Ornament" abstrahiert also völlig von der künstlerischen Qualität des Musters; es geht nur um dessen Symmetrien.)

BEISPIEL 1.4.3. *Als Beispiel betrachten wir das Ornament in Abbildung 3 und bestimmen seine Ornamentgruppe: Die einzigen Isometrien der Ebene, die das Ornament in sich überführen, sind Translationen in die gezeigten Richtungen. In bezug auf die Basis* $\{t_1, t_2\}$ *von* $\mathbb{R}^2$*, die aus den Richtungsvektoren der beiden Translationen besteht, sehen die erzeugenden Elemente von* $\mathrm{Sym}\,(M)$ *in Matrixdarstellung so aus:*

$$A = \left(\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \text{ und } B = \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 1 \\ \hline 0 & 0 & 1 \end{array}\right).$$

Außerdem gilt $A \cdot B = B \cdot A$*: Also besteht die Gruppe* $\mathrm{Sym}\,(M)$ *aus den Matrizen*

$$A^n \cdot B^m = \left(\begin{array}{cc|c} 1 & 0 & n \\ 0 & 1 & m \\ \hline 0 & 0 & 1 \end{array}\right)$$

wobei $n, m \in \mathbb{Z}$*, und es gilt* $\mathrm{Sym}\,(M) \simeq \mathbb{Z}^2$ *(vergleiche mit Beispiel 1.3.14).*

Es gibt aber auch kompliziertere Ornamente, die mehr Symmetrien aufweisen als nur die Translationen: Abbildung 5 zeigt ein Ornament, das überdies noch die Symmetrien eines Sechsecks hat.

1.4.1. Klassifikation der Ornamentgruppen. Man kann die Ornamentgruppen der Ebene vollständig klassifizieren: Bis auf Isomorphie gibt es genau 17, und für jede dieser Gruppen kann man ein entsprechendes Ornament aus der Kunstgeschichte finden. Den ersten Beweis dieser Klassifikation hat Fedorov [**3**] gegeben.
Geometrisch kann man sich eine Ornamentgruppe so vorstellen, daß eine fixe Gruppe von orthogonalen Abbildungen mit Translationen an die Punkte eines zweidimensionalen Gitters verschoben wird, siehe Abbildung 6: Aber das müssen wir natürlich präziser fassen.

ABBILDUNG 5. Komplexes Ornament mit mehreren Symmetrien.
Links ist eine einzelne Kachel gezeigt: Sie ist rautenförmig mit Innenwinkeln $60° = \pi/3$ und $120° = 2\pi/3$. Ihre Fläche zerfällt in 12 rechtwinklige Dreiecke, deren Katheten im Längenverhältnis $2 : 1$ zueinander stehen: Die 6 hellgrauen Dreiecke ergeben sich durch Spiegelungen aus den 6 dunkelgrauen Dreiecken, sodaß man ein Teilmotiv M für alle hellgrauen und dessen Spiegelung $\overline{M}$ für alle dunkelgrauen Dreiecke der Kachel vorgeben kann.
Rechts ist ein Ausschnitt der Parkettierung dere Ebene mit diesen Kacheln gezeigt: Man erkennt, daß die Ebene äquivalent auch mit *hexagonalen* Kacheln (angedeutet durch die strichlierten Linien) parkettiert werden kann, die sichtlich unter 6 Drehungen und 6 Spiegelungen invariant ist: Ihre Symmetriegruppe ist also die D_6.

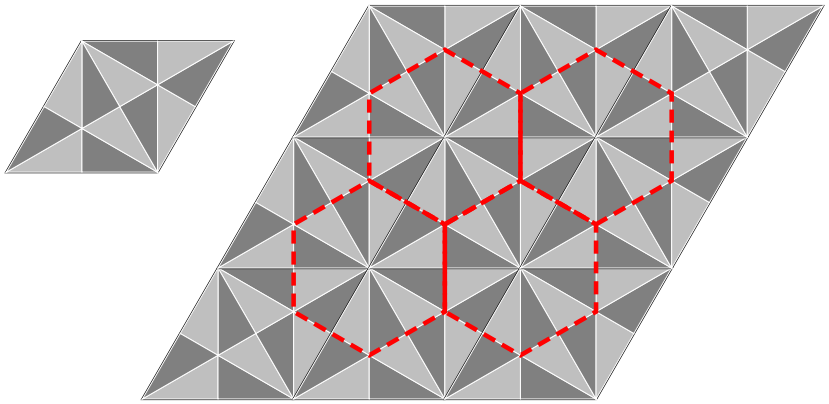
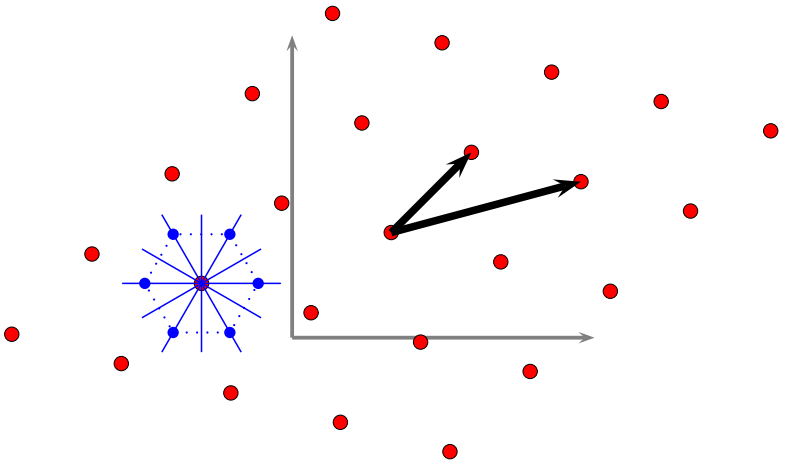


ABBILDUNG 6. "Geometrie" einer Ornamentgruppe: Die Translationen erzeugen ein zweidimensionales Gitter, in den Punkten dieses Gitters wirken isomorphe Kopien einer endlichen Gruppe von orthogonalen Abbildungen.



1.4.1.1. *Isometrien der Ebene: Lineare Algebra.* Gemäß (1.6) ist jede Isometrie g der Ebene darstellbar als

$$g \sim \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} : \ A \in O_2(\mathbb{R}), v \in \mathbb{R}^2,$$

wobei A eine orthogonale Matrix ist, also $A \cdot A^t = E_2$.
Daher gibt es *entweder* einen Winkel ϕ, sodaß

$$A = \begin{pmatrix} \sin\phi & -\cos\phi \\ \cos\phi & \sin\phi \end{pmatrix} \text{ mit } \det A = 1$$

und

$$A^n = \begin{pmatrix} \sin n\phi & -\cos n\phi \\ \cos n\phi & \sin n\phi \end{pmatrix}.$$

A entspricht geometrisch einer Drehung um den Koordinatenursprung mit Drehwinkel ϕ: Wir notieren das mit $A = D_\phi$.
Oder es gibt einen Winkel ϕ, sodaß

$$A = \begin{pmatrix} \sin\phi & \cos\phi \\ \cos\phi & -\sin\phi \end{pmatrix} \text{ mit } \det A = -1$$

gilt. Dann gilt für die Spiegelung S_0

$$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

an der x–Achse

$$A = D_\phi \cdot S_0$$

und

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

A entspricht geometrisch einer Spiegelung um die Achse, die mit der x–Achse den Winkel $\phi/2$ einschließt (siehe Abbildung 7): Wir notieren das mit $A = S_{\phi/2}$.
Für Drehungen und Spiegelungen gilt also:

$$D_\phi \cdot S_\psi = D_\phi \cdot D_{2\psi} \cdot S_0 = S_{\psi+\phi/2}, \tag{1.9}$$

$$S_\gamma \cdot S_\delta = D_{2\cdot(\gamma-\delta)}. \ \leftarrow \phi=2\cdot(\gamma-\delta), \psi=\delta \tag{1.10}$$

1.4.1.2. *Isometrien der Ebene: Elementare Geometrie.* Wir können die Isometrien der Ebene aber auch einfach geometrisch verstehen. Dazu halten wir zunächst fest:

LEMMA 1.4.4. *Seien $a, b, c \in \mathbb{R}^2$ drei* nicht kollineare *Punkte der Ebene, die also ein nicht–entartetes Dreieck Δ bilden. Sei f eine Isometrie der Ebene. Dann bilden die Punkte $f(a), f(b), f(c) \in \mathbb{R}^2$ ein Dreieck $\Delta' = f(\Delta)$, das zu Δ* kongruent *ist.*

Sei umgekehrt ein Dreieck Δ' mit Eckpunkten $a', b', c' \in \mathbb{R}^2$ gegeben, das zu Δ kongruent ist. Dann gibt es genau eine *Isometrie g der Ebene, sodaß $\Delta' = g(\Delta)$ (also $g(a) = a'$, $g(b) = b'$ und $g(c) = c'$).*

ABBILDUNG 7. Illustration: Spiegelung an x–Achse (also $x \mapsto x$, $y \mapsto s(y)$ in der Graphik), gefolgt von Drehung um Winkel φ (also $x \mapsto f(x)$, $s(y) \mapsto f(y)$ in der Graphik), ergibt Spiegelung an Achse (a in der Graphik) mit Richtungsvektor $(\cos \varphi/2, \sin \varphi/2)$.

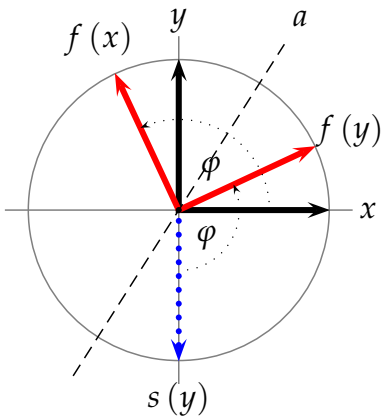
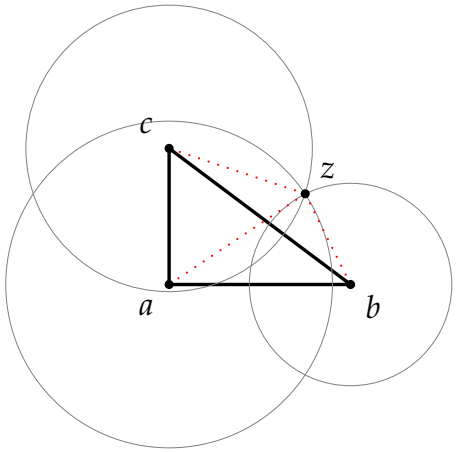


ABBILDUNG 8. Ein Punkt z der Ebene ist durch die Abstände zu den Eckpunkten a, b, c eines festen Dreiecks eindeutig bestimmt, denn drei Kreise um a, b, c können höchstens einen Punkt gemeinsam haben.



BEWEIS. Die erste Aussage ist klar: Da f eine Isometrie ist, ist $\|a-b\| = \|f(a) - f(b)\|$, $\|b-c\| = \|f(b) - f(c)\|$ und $\|c-a\| = \|f(c) - f(a)\|$; und das bedeutet ja, daß die Dreiecke Δ und $f(\Delta)$ kongruent sind.

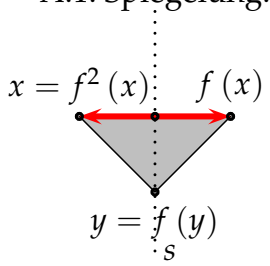
Für die zweite Aussage muß man sich vergegenwärtigen, daß ein beliebiger Punkt $z \in \mathbb{R}^2$ durch die drei Abstände

$$\|a-z\|,\ \|b-z\|,\ \|c-z\|$$

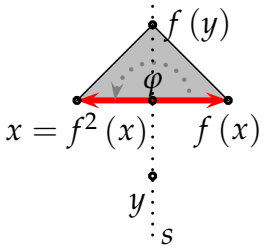
eindeutig festgelegt ist, denn drei Kreise in allgemeiner Lage können *höchstens* einen Punkt gemeinsam haben, siehe Abbildung 8. □

ABBILDUNG 9. Die möglichen Bahnen von x unter $\langle f \rangle$, wenn $x, f(x)$ und $f^2(x)$ kollinear sind.

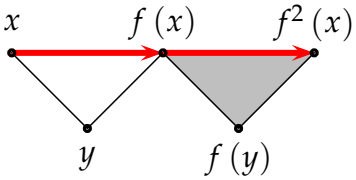
A.1: Spiegelung.



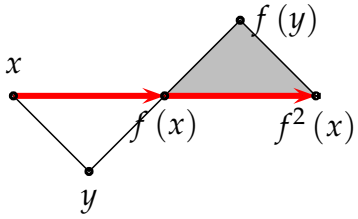
A.2: Drehung um $\varphi = \pi$.



B.1: Translation.



B.2: Gleitspiegelung.



PROPOSITION 1.4.5. *Eine Isometrie der Ebene $f \neq \mathrm{id} \in \mathrm{Iso}(\mathbb{R}^2)$ ist eine der folgenden Abbildungen:*

- *eine* Translation *mit Richtungsvektor $t \neq \mathbf{0}$,*
- *eine* Spiegelung *an einer Geraden s,*
- *eine* Drehung *um einen Winkel $\phi \in (0, 2\pi)$ mit Drehzentrum m,*
- *eine* Gleitspiegelung *(also eine Translation gefolgt von einer Spiegelung an einer Geraden mit demselben Richtungsvektor).*

BEWEIS. Sei $x \in \mathbb{R}^2$. Wir untersuchen die Möglichkeiten, wie die Bahn von x unter $\langle f \rangle \sqsubseteq \mathrm{Iso}(\mathbb{R}^2)$ aussehen kann, und betrachten dazu die Punkte

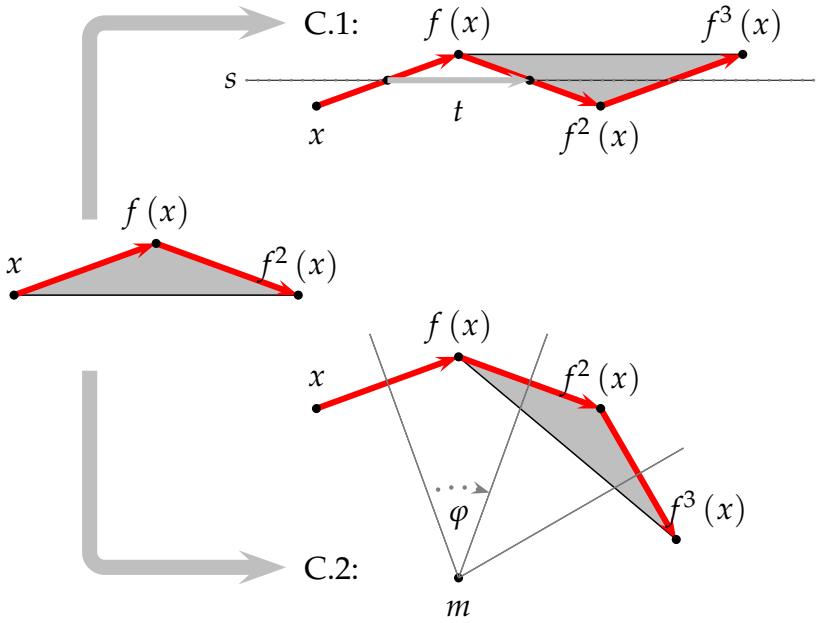
$$x, f(x), f^2(x) \in \mathbb{R}^2.$$

Diese Punkte können *kollinear* sein (also auf einer gemeinsamen Geraden g liegen): Sei für diesen Fall y ein Punkt auf der Streckensymmetrale s von $\overline{x f(x)}$, der nicht auf g liegt. Es gibt dann zwei Fälle:

Fall A: $f^2(x) = x$. Das Dreieck $(x, f(x), y)$ wird unter f auf ein kongruentes Dreieck abgebildet (vergleiche Lemma 1.4.4), also ist entweder $f(y) = y$ und f ist die Spiegelung an s (siehe Abbildung 9, Bild A.1), oder $f(y)$ ist der an g gespiegelte Punkt und f ist eine Drehung um $\pi = 180°$ mit Zentrum $\frac{1}{2}(x + f(x))$ (siehe Abbildung 9, Bild A.2).

Fall B: $f^2(x) \neq x$. Analog zu Fall A gibt es wieder zwei Möglichkeiten, nämlich eine Translation um den Vektor $v = (f(x) - x)$ oder eine *Gleitspiegelung*, genauer gesagt, die Translation um v, gefolgt von der Spiegelung an g (siehe Abbildung 9, Bilder B.1 und B.2):

ABBILDUNG 10. Die möglichen Bahnen von x unter $\langle f \rangle$, wenn $x, f(x)$ und $f^2(x)$ *nicht* kollinear sind: Dann müssen die Dreiecke $\Delta = \Delta\left(x, f(x), f^2(x)\right)$ und $f(\Delta) = \Delta\left(f(x), f^2(x), f^3(x)\right)$ *kongruent* sein.



Nun betrachten wir den Fall, daß $\left(x, f(x), f^2(x)\right)$ *nicht* kollinear sind, also ein (nicht–entartetes) Dreieck bilden. Es gibt nur zwei Möglichkeiten für das Bild dieses Dreiecks unter f; diese entsprechen einer Gleitspiegelung (siehe Abbildung 10, Bild C.1) und einer Drehung, deren Zentrum der Schnittpunkt der Streckensymmetralen von $\overline{x\, f(x)}$ und von $\overline{f(x)\, f^2(x)}$ ist (siehe Abbildung 10, Bild C.2). □

DEFINITION 1.4.6 (Punktgruppe). *Sei* $\Gamma \sqsubseteq \mathrm{Iso}\left(\mathbb{R}^2\right)$ *eine Ornamentgruppe, dann wird ihr Orthogonalteil* O_Γ *als* Punktgruppe *der Ornamentgruppe* Γ *bezeichnet.*

PROPOSITION 1.4.7. *Sei* $\Gamma \sqsubseteq \mathrm{Iso}\left(\mathbb{R}^2\right)$ *eine Ornamentgruppe, dann erscheint ihre Punktgruppe* O_Γ *als eine* endliche Untergruppe *von* $\mathrm{Iso}\left(\mathbb{R}^2\right)$*, die einen Punkt der Ebene fixiert; und* O_Γ *kann nur* entweder *eine zyklische Gruppe* C_1, C_2, C_3, C_4, C_6 oder *eine Diedergruppe* D_1, D_2, D_3, D_4, D_6 *sein.*

BEWEIS. Daß O_Γ als Untergruppe in G "auftaucht", folgt an sich "abstrakt" sofort daraus, daß gemäß Lemma 1.3.10 G isomorph zum semidirekten Produkt

$$G \simeq T_G \rtimes_\theta O_G$$

ist, sodaß gemäß Lemma A.3.32 (eine isomorphe Kopie von) O_G eine Untergruppe von G ist. Wir wollen uns das aber zusätzlich ganz konkret klarmachen: Wenn die Punktgruppe O_G *keine* echte Drehung (um einen Winkel $\phi \in (0, 2\pi)$) enthält, dann kann offenbar nur entweder $O_G = \{\mathbb{n}_G\} \simeq C_1$ gelten oder (für die Spiegelung $S = S_\phi \in \mathrm{Iso}\left(\mathbb{R}^2\right)$) $O_G = \{\mathbb{n}_G, S\} \simeq D_1$.

Wenn hingegen eine *echte Drehung* in O_G enthalten ist, dann muß ihre Ordnung *endlich* sein, weil eine Ornamentgruppe nur *diskrete* Orbits erzeugt. Sei also A eine Drehung *maximaler* Ordnung m in O_G: Dann gibt es also ein Element $g = (A, v) \in G$ (mit Drehzentrum[3] $z = (A - E_2)^{-1} \cdot v$), und die von g erzeugte Untergruppe $\langle g \rangle \sqsubseteq G$ ist isomorph zur C_m und fixiert klarerweise ihr Drehzentrum z, ebenso klar ist, daß $\langle A \rangle$ *alle* Drehungen von O_G enthält[4]. Wenn O_G zusätzlich auch eine *Spiegelung* S enthält, dann ist auch $S' = A \cdot S$ in O_G (siehe (1.9)); und in G gibt es dementsprechend zwei Spiegelungen S, S' mit nicht–parallelen Achsen, die sich also in einem Punkt z schneiden: Diese beiden Spiegelungen erzeugen aber die Diedergruppe $\langle S, S' \rangle \simeq D_m$ (denn $S' \cdot S = A$).
Tatsächlich kann eine Drehung in einer Punktgruppe aber nur die Ordnung $1, 2, 3, 4$ oder 6 haben: Das nennt man auch die *kristallographische Restriktion*. Denn aus $\det(A) = 1$ folgt nach dem Satz von Cayley–Hamilton (Satz A.4.4 im Anhang)

$$A^2 - \operatorname{trace}(A) \cdot A + E_2 = 0,$$

also

$$A + A^{-1} = \operatorname{trace}(A) \cdot E_2.$$

Nun gilt ja für jede Translation $v \in T_G$

$$A \cdot v \in T_G \text{ und } A^{-1} \cdot v \in T_G,$$

somit ist also auch $\operatorname{trace}(A) \cdot v \in T_G$ für alle $v \in T_G$: Wir können inbesondere eine *unteilbare* Translation v wählen und erhalten damit

$$\operatorname{trace}(A) \in \mathbb{Z}.$$

Da aber $A = D_\phi$ für einen Winkel ϕ, ist

$$\operatorname{trace}(A) = 2\cos\phi,$$

also $|\operatorname{trace}(A)| \leq 2$ und somit $\operatorname{trace}(A) \in \{-2, -1, 0, 1, 2\}$: Für den Drehwinkel ϕ gibt es also nur die Möglichkeiten $\phi = \pi, \frac{2\pi}{3}, \frac{\pi}{2}, \frac{\pi}{3}, 0$, und A hat dementsprechend Ordnung $2, 3, 4, 6$ oder 1. □

Ein geometrischer Beweis für die Klassifikation der Ornamentgruppen des $\mathbb{R}^2$ ist in [**9**] enthalten: Abbildung 11 zeigt eine schematische Darstellung der 17 Ornamentgruppen.

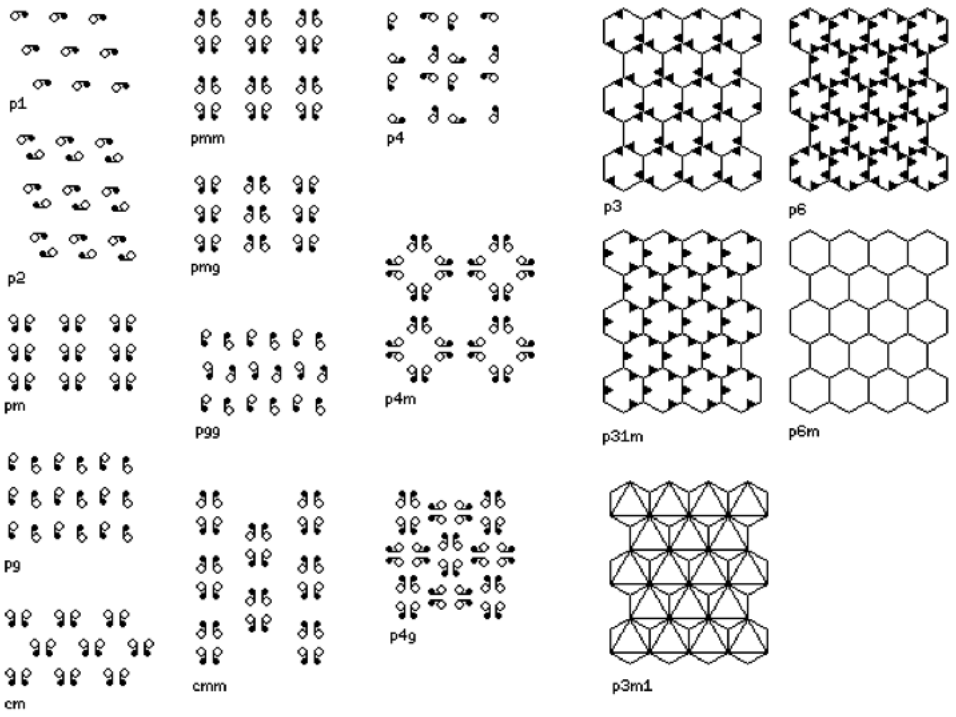
1.4.1.3. *Ornamentgruppen im $\mathbb{R}^n$: Kristallographischen Gruppen.* Ornamentgruppen kann man allgemeiner für $\mathbb{R}^n$ definieren: Man spricht dann von *kristallographischen Gruppen*; ihre Klassifikation kann mit algebraischen Methoden erreicht werden (die wir hier nur skizzenhaft andeuten): Nach einem Satz von Bieberbach gibt es in jeder Dimension n nur *endlich* viele solche Gruppen.
Wir wissen, daß es für jede kristallographische Gruppe Γ eine kurze exakte Sequenz von Gruppen

$$\{\mathbb{n}\} \to \mathbb{Z}^n \simeq T_\Gamma \xrightarrow{\phi} \Gamma \xrightarrow{\psi} O_\Gamma \to \{\mathbb{n}\} \tag{1.11}$$

[3] $A - E_2$ ist invertierbar, weil die Gleichung $A \cdot x = x$ nur die Nullösung hat, wenn A eine echte Drehung ist.

[4] Denn sonst enthielte O_G eine Drehung mit Ordnung k und $k \nmid m$: Dann wäre aber die Ordnung m nicht maximal.

ABBILDUNG 11. Schematische Darstellung der 17 Ornamentgruppen



gibt, die *zerfällt*: Es gibt eine *Transversale*, also einen injektiven Homomorphismus $\iota : O_\Gamma \to \Gamma$ sodaß $\psi \circ \iota = \mathrm{id}$. Außerdem gilt[5]:

$$O_\Gamma \sqsubseteq \mathrm{Aut}\left(\mathbb{Z}^n\right) = \mathrm{GL}_n\left(\mathbb{Z}\right) = \left\{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\right\}.$$

O_Γ bestimmt aber keine eindeutige Untergruppe in $\mathrm{Aut}\left(\mathbb{Z}^n\right)$: Denn der injektive Homomorphismus $\phi : \mathbb{Z}^n \to \Gamma$ ist keineswegs eindeutig (Abbildung 12 illustriert dies für $n = 2$); ein Element $x \in O_\Gamma$ wirkt auf $\mathbb{Z}^n$ vermöge

$$\phi^{-1} \circ \tau\left(x\right) \circ \phi.$$

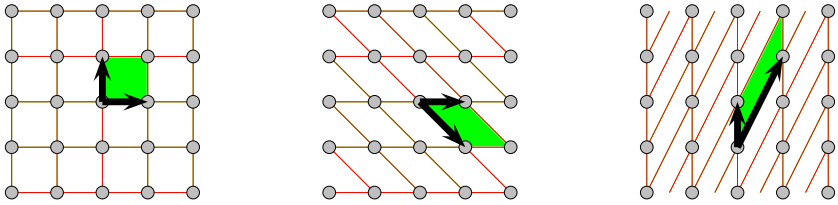
O_Γ bestimmt also eine *Konjugationsklasse* (von endlichen konjugierten Untergruppen) in $\mathrm{GL}_n\left(\mathbb{Z}\right)$.

PROPOSITION 1.4.8 (C. Jordan, 1880). *Die Gruppe* $\mathrm{GL}_n\left(\mathbb{Z}\right)$ *hat nur endlich viele Konjugationsklassen endlicher Untergruppen.*

Diese Konjugationsklassen heißen *arithmetische Ornamentklassen*: Wenn man alle arithmetischen Ornamentklassen bestimmt hat, dann muß man für jede von ihnen eine Erweiterung der exakten Sequenz (1.11) finden (es gibt dafür auch immer nur endlich viele Möglichkeiten) und erhält so alle Ornamentgruppen.

[5]Eine invertierbare Matrix A mit ganzzahligen Eintragungen hat eine ganzzahlige Determinante $d \in \mathbb{Z}$, also ist $\det\left(A^{-1}\right) = 1/d$: Wenn A^{-1} auch ganzzahlig ist, muß $\det\left(A\right) = \pm 1$ gelten.

ABBILDUNG 12. Ein und dassselbe Gitter kann auf verschiedene Weise als isomorphes Bild von $\mathbb{Z}^2$ erzeugt werden.



1.4.1.4. *Konjugationsklassen endlicher Untergruppen von* $\mathrm{GL}_2(\mathbb{Z})$. Als Beispiel für den Satz von Jordan 1.4.8 bestimmen wir die Konjugationsklassen endlicher Untergruppen von $\mathrm{GL}_2(\mathbb{Z})$. Wir betrachten dazu die folgenden vier Elemente in $\mathrm{GL}_2(\mathbb{Z})$:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad W = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}. \tag{1.12}$$

Es gilt $V^2 = -E$, und die Ordungen von U, V und W sind 3, 4 und 6, wie man leicht nachrechnet.

PROPOSITION 1.4.9. *Es gibt für die Ebene* $\mathbb{R}^2$ *genau* 13 *arithmetische Ornamentklassen, also* 13 *endliche, nicht–konjugierte Untergruppen von* $\mathrm{GL}_2(\mathbb{Z})$*, und zwar sind dies die 5 zyklischen Gruppen*

$$\langle E \rangle \simeq C_1,\ \langle -E \rangle \simeq C_2,\ \langle U \rangle \simeq C_3,\ \langle V \rangle \simeq C_4,\ \langle W \rangle \simeq C_6$$

sowie die 8 Diedergruppen

$$\begin{aligned} \left\langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle &\simeq D_1, & \left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle &\simeq D_1. \\ \left\langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right), -E \right\rangle &\simeq D_2, & \left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), -E \right\rangle &\simeq D_2. \\ \left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), U \right\rangle &\simeq D_3, & \left\langle \left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right), U \right\rangle &\simeq D_3. \\ \left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), V \right\rangle &\simeq D_4, & \left\langle \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), W \right\rangle &\simeq D_6. \end{aligned}$$

BEWEIS. Wir folgen dem elementaren Beweis aus **[10]** und gliedern die Argumentation in mehrere Unterpunkte.

Sei A ein Element von $\mathrm{GL}_2(\mathbb{Z})$ von *endlicher* Ordnung $m \geq 1$:

- Aus $A^m = E_2$ folgt, daß die *Eigenwerte* von A m–te Einheitswurzeln sind:
$$A \cdot v = \lambda \cdot v \implies v = A^m \cdot v = \lambda^m \cdot v \implies \lambda^m = 1.$$
- A ist diagonalisierbar: Denn angenommen nicht, dann hat A jedenfalls zwei gleiche Eigenwerte. Sei v ein Eigenvektor von A für λ, den wir zu einer Basis $\{v, w\}$ ergänzen: In bezug auf diese Basis hat A die Matrixdarstellung $\left(\begin{smallmatrix} \lambda & a \\ 0 & b \end{smallmatrix}\right)$ mit $a, b \in \mathbb{C}$ und $a \neq 0$. Da das charakteristische Polynom von A nach Annahme gleich $(x - \lambda)^2$ ist, ist $\lambda = b$. Es gilt (wie man leicht sieht)
$$\begin{pmatrix} \lambda & a \\ 0 & \lambda \end{pmatrix}^n = \begin{pmatrix} \lambda^n & n \cdot a \cdot \lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix} \neq E_2 \text{ für alle } n \in \mathbb{N},$$
also hat A unendliche Ordnung, ein Widerspruch.

Es gibt also doch eine Transformation $T \in \mathrm{GL}_2(\mathbb{C})$ mit

$$T \cdot A \cdot T^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}.$$

- Wenn A die Ordnung 2 hat (also $A^2 = E_2$), dann folgt

$$\left(T \cdot A \cdot T^{-1}\right) \cdot \left(T \cdot A \cdot T^{-1}\right) = \left(\begin{smallmatrix} \lambda^2 & 0 \\ 0 & \mu^2 \end{smallmatrix}\right) = E_2,$$

also $\lambda^2 = \mu^2 = 1 \implies \lambda, \mu = \pm 1$. Somit ist A also *konjugiert* zu einer der folgenden vier Matrizen:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -E = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.13}$$

Dabei hat E Ordnung 1, und die anderen Matrizen Ordnung 2. Die *einzige* Matrix aus $\mathrm{SL}_2(\mathbb{Z})$ der Ordnung 2 ist $-E$ (denn aus $A = T \cdot (-E) \cdot T^{-1}$ folgt natürlich schon $A = -E$).

- Wenn A Ordnung $m \geq 3$ hat, dann gilt $A \in \mathrm{SL}_2(\mathbb{Z})$: Denn 1 und -1 sind die einzigen *reellen* Einheitswurzeln, und A kann nicht nur Eigenwerte ± 1 haben (sonst wäre $A^2 = E$), als muß (mindestens) einer der Eigenwerte λ, μ von A *nicht* reell sein; o.B.d.A. sei dies λ. Aber das charakteristische Polynom hat ja *ganzzahlige* (also reelle) Koeffizienten, daher muß die zweite Nullstelle die konjugiert komplexe Zahl $\mu = \overline{\lambda}$ sein, und $\det(A) = \lambda \cdot \overline{\lambda} = |\lambda| = 1$. Anders formuliert: Wenn $A \notin \mathrm{SL}_2(\mathbb{Z})$, dann ist die Ordnung von A gleich 2.
- Für alle $A \in \mathrm{GL}_2(\mathbb{Z})$ gilt $\mathrm{ord}(A) \in \{1, 2, 3, 4, 6\}$ (vergleiche dazu die kristallographische Restriktion im Beweis von Proposition 1.4.7): Denn für $m \geq 3$ ist $A \in \mathrm{SL}_2(\mathbb{Z})$, und

$$\mathrm{trace}(A) = \lambda + \overline{\lambda} = e^{\frac{2\pi i}{m}} + e^{-\frac{2\pi i}{m}} = 2\cos\left(\frac{2\pi}{m}\right)$$

muß natürlich *ganzzahlig* sein, mit $|\mathrm{trace}(A)| \leq 2$: Aus $2\cos\frac{2\pi}{m} \in = \{-2, -1, 0, 1, 2\}$ folgt $m = 2, 3, 4, 6, 1$; und diese Fälle treten auch alle auf (die Matrizen aus (1.13) haben Ordnung $m = 1$ und $m = 2$, und die Matrizen U, V, W aus (1.12) haben Ordnungen $3, 4, 6$).

Sei G im folgenden eine endliche Untergruppe von $\mathrm{GL}_2(\mathbb{Z})$. $G' := G \cap \mathrm{SL}_2(\mathbb{Z})$ ist dann eine *normale* Untergruppe in G (Index $(G : G') \leq 2$: Denn wenn es zwei verschiedene Elemente X, Y in $G \setminus \mathrm{SL}_2(\mathbb{Z})$ gibt, dann ist $\det(X \cdot Y) = 1$ und somit $X \cdot Y \in G' \iff X \cdot G' = Y \cdot G'$: Es gibt also genau 2 Nebenklassen von G') und eine Untergruppe in $\mathrm{SL}_2(\mathbb{Z})$: Wir untersuchen also einmal die *endlichen* Untergruppen von $\mathrm{SL}_2(\mathbb{Z})$ genauer.

Wir beginnen mit der einfachen Beobachtung, daß für jede Primzahl $p \in \mathbb{P}$ die Abbildung $\pi_p \colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_p)$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \pmod p & b \pmod p \\ c \pmod p & d \pmod p \end{pmatrix}$$

ein *Homomorphismus* ist.

- Die Abbildung $\pi_3\colon\ \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_3)$, eingeschränkt auf die *endliche* Untergruppe $G \sqsubseteq \mathrm{SL}_2(\mathbb{Z})$
$$\pi_3\colon\ G \to \mathrm{SL}_2(\mathbb{F}_3),$$
ist ein *Monomorphismus* (also *injektiv*). Nehmen wir (indirekt) an, es sei $A \neq E$ in $\ker\pi$; d.h., $A \equiv E \pmod 3$. Da G endlich ist, ist insbesondere $\mathrm{ord}(A) < \infty$. Da $-E = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ die *einzige* Matrix der Ordnung 2 in $\mathrm{SL}_2(\mathbb{Z})$ ist und $-E \not\equiv E \pmod 3$, muß $\mathrm{ord}(A) \geq 3$ gelten, daher sind die Eigenwerte nicht reell und somit konjugiert komplexe Einheitswurzeln $\lambda \neq \overline{\lambda}$. Aus $A \equiv E \pmod 3$ folgt klarerweise $\mathrm{trace}(A) \equiv 2 \pmod 3$, und weil $|\mathrm{trace}(A)| = \left|\lambda + \overline{\lambda}\right| < |\lambda| + \left|\overline{\lambda}\right| = 2$ (und $A \neq E$), muß gelten
$$\mathrm{trace}(A) = -1.$$
Das heißt, $A = \left(\begin{smallmatrix} a & b \\ c & -1-a \end{smallmatrix}\right)$ mit $b \equiv c \equiv 0 \pmod 3$, also $9 \mid b \cdot c$. Wenn wir $\det A = -a(1+a) - b \cdot c = 1$ modulo 9 betrachten, erhalten wir die Gleichung
$$a^2 + a + 1 \equiv 0 \pmod 9,$$
und eine direkte Überprüfung zeigt, daß es dafür keine Lösung gibt. Anders formuliert: Jede *endliche* Untergruppe von $\mathrm{SL}_2(\mathbb{Z})$ ist isomorph zu einer Untergruppe von $\mathrm{SL}_2(\mathbb{F}_3)$.
- $\mathrm{SL}_2(\mathbb{F}_3)$ enthält auch nur ein *einziges* Element der Ordnung 2, nämlich $\alpha := -E \pmod 3$: Denn für $X = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ folgt aus
$$X^2 = \begin{pmatrix} a^2+b\cdot c & b\cdot(a+d) \\ c\cdot(a+d) & b\cdot c+d^2 \end{pmatrix} = E$$
$a = -d$ *oder* $b = c = 0$: Im ersten Fall wäre $b \cdot c + d^2 = 1 = -\det X$ und $X \notin \mathrm{SL}_2(\mathbb{Z})$, im zweiten Fall müßte $a = \pm 1, d = \pm 1$ gelten und wegen $\det X = a \cdot d = 1$ auch $a = d$; aus $\mathrm{ord}(X) = 2$ folgt $a = d = -1$.
- Die von den Matrizen $P = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ und $Q = \left(\begin{smallmatrix} -1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$ erzeugte Untergruppe ist die Quaternionengruppe $\mathbb{Q}_8$: Denn einfaches Nachrechnen zeigt, daß P und Q beide Ordnung 4 haben und daß $P^2 = Q^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ sowie $Q \cdot P \cdot Q^{-1} = P^{-1} \iff P^2 \cdot Q \cdot P = P \cdot Q = -Q \cdot P$ gilt.
- Sei $p \in \mathbb{P}$, dann gilt
$$\mathrm{ord}\left(\mathrm{GL}_2(\mathbb{F}_p)\right) = \left(p^2 - p\right) \cdot \left(p^2 - 1\right),$$
$$\mathrm{ord}\left(\mathrm{SL}_2(\mathbb{F}_p)\right) = p \cdot \left(p^2 - 1\right).$$
Denn zunächst ist klar, daß die Determinante ein Gruppenhomomorphismus
$$\mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\star$$
mit Kern $\mathrm{SL}_2(\mathbb{F}_p)$ ist: Also gilt
$$\mathrm{ord}\left(\mathrm{GL}_2(\mathbb{F}_p)\right) = (p-1) \cdot \mathrm{ord}\left(\mathrm{SL}_2(\mathbb{F}_p)\right).$$
Die Ordnung von $\mathrm{GL}_2(\mathbb{F}_p)$ erhalten wir durch einfache Abzählung: Für $A \in \mathrm{GL}_2(\mathbb{F}_p)$ kann die erste Spalte ein beliebiger Vektor aus $\mathbb{F}_p^2 \setminus \{0\}$ sein — das ergibt $\left(p^2 - 1\right)$ verschiedene Möglichkeiten —, und die zweiter Spalte kann dann

ein beliebiger Vektor sein, der *kein* Vielfaches der ersten Spalte ist — das ergibt $\left(p^2 - p\right)$ verschiedene Möglichkeiten.

Insbesondere gilt ord $\left(\mathrm{SL}_2\left(\mathbb{F}_3\right)\right) = 3 \cdot \left(3^2 - 1\right) = 24$, also

$$\mathrm{ord}\left(G'\right) \mid 24$$

nach dem Satz von Lagrange (Satz A.3.12).

- $\mathrm{SL}_2\left(\mathbb{F}_3\right)$ enthält vier konjugierte zyklische Gruppen der Ordnung 6: Betrachte dazu

$$Y = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \in \mathrm{SL}_2\left(\mathbb{F}_3\right).$$

Durch einfaches Nachrechnen erhält man die Potenzen $Y^1, \ldots, Y^6$

$$\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Es ist also ord $(Y) = 6$, und jede Potenz von Y hat obere Dreiecksform. Sei $n \in \mathrm{SL}_2\left(\mathbb{F}_3\right)$ eine beliebiges Element aus dem *Normalisator* von $H = \langle Y \rangle \simeq C_6$,

$$n = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \iff n^{-1} = \begin{pmatrix} w & -y \\ -z & x \end{pmatrix}.$$

Dann ist

$$n \cdot Y \cdot n^{-1} = \begin{pmatrix} x \cdot z + y \cdot z - w \cdot x & -x^2 \\ z^2 & -x \cdot z + y \cdot z - w \cdot x \end{pmatrix},$$

und es folgt $z = 0$; damit folgt aber aus $\det n = x \cdot w = 1$ auch $x = w = \pm 1$, und y kann beliebig gewählt werden: Das heißt aber, der Normalisator ist *genau* die von Y erzeugte Untergruppe $H = \langle Y \rangle$,

$$N_{\mathrm{SL}_2(\mathbb{F}_3)}\left(H\right) = H.$$

Die Anzahl der konjugierten Untergruppe zu H in $\mathrm{SL}_2\left(\mathbb{F}_3\right)$ ist gleich dem *Index* des Normalisators (siehe Proposition A.3.15): $\left(\mathrm{SL}_2\left(\mathbb{F}_3\right) : N_{\mathrm{SL}_2(\mathbb{F}_3)}\left(H\right)\right) = 4$. Es gibt also vier zu H konjugierte zyklische Untergruppen H_1, H_2, H_3, H_4; jede davon enthält das *eindeutige* Element $\alpha = -E$ der Ordnung 2 aus $\mathrm{SL}_2\left(\mathbb{F}_3\right)$ sowie eine einzige (zyklische) Untergruppe der Ordnung 3, also $\left|H_i \cap H_j\right| = 2$ für $i \neq j$. Diese vier Untergruppen enthalten:

  - 8 Elemente der Ordnung 6 (zwei Erzeuger pro C_6),
  - 8 Elemente der Ordnung 3 (zwei Erzeuger pro C_3),
  - 1 Element (das einzige) der Ordnung 2,
  - das neutrale Element.

In $\mathrm{SL}_3\left(\mathbb{F}_3\right)$ gibt es also "außerhalb" dieser vier Untergruppen nur mehr 6 andre Elemente, und das sind die 6 Elemente in der Quaternionen–Untergruppe, die *nicht* Ordnung 1 oder 2 haben — diese haben dann alle Ordnung 4.

- Es gibt keine Untergruppe $H \sqsubseteq \mathrm{SL}_2\left(\mathbb{F}_3\right)$ der Ordnung 12: Denn angenommen, es gäbe ein solches H. Da in jeder Gruppe gerader Ordnung die Anzahl der

Elemente der Ordnung 2 *ungerade* ist[6], müßte H das Element $\alpha = -E$ enthalten. Da $(\mathrm{SL}_2(\mathbb{F}_3) : H) = 2$, müßte H auch alle *Quadrate* aus $\mathrm{SL}_2(\mathbb{F}_3)$ enthalten[7]: Jedes Element A der Ordnung 3 *ist* ein Quadrat, denn $A = A^3 \cdot A = \left(A^2\right)^2$, daher müßte H alle 8 Elemente der Ordnung 3 enthalten, und da die Elemente der Ordnung 3 zusammen mit α die 4 zyklischen Untergruppen der Ordnung 6 erzeugen, müßten auch die 8 Elemente der Ordnung 6 in H liegen — zusammen mit dem neutralen Element hätte H also mindestens 18 Elemente; das ist natürlich zuviel.

- Jede Untergruppe $H \sqsubseteq \mathrm{SL}_2(\mathbb{F}_3)$ der Ordnung 8 muß $\alpha = -E$ und das neutrale Element enthalten; die restlichen 6 Element müssen die 6 Elemente der Ordnung 4 aus der Quaternionen–Untergruppe sein (denn es gibt ja kein Element der Ordnung 8).
- Jede Untergruppe $H \sqsubseteq \mathrm{SL}_2(\mathbb{F}_3)$ der Ordnung 6 muß $\alpha = -E$ und ein Element g der Ordnung 3 enthalten: $\langle g, \alpha \rangle$ ist aber bereits eine der 4 zyklischen Untergruppen.
- Jede Untergruppe $H \sqsubseteq \mathrm{SL}_2(\mathbb{F}_3)$ der Ordnung 4 kann nicht die *Kleinsche Vierergruppe* $\mathbb{Z}_2 \times \mathbb{Z}_2$ sein, denn diese enthält zwei verschiedene Elemente der Ordnung 2.
- Insgesamt haben wir damit also gezeigt: $\mathrm{SL}_2(\mathbb{F}_3)$ enthält
  - *keine* Untergruppe der Ordnung 12,
  - eine *eindeutige* Untergruppe der Ordnung 8,
  - *keine* nicht–abelsche Untergruppe der Ordnung 6 (also nicht die D_6),
  - zyklische Untergruppen der Ordnung 3, 4 und 6,
  - *keine* Untergruppe, die isomorph zur *Kleinschen Vierergruppe* $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist,
  - eine *eindeutige* Untergruppe der Ordnung 2.
- $G' = G \cap \mathrm{SL}_2(\mathbb{Z})$ könnte zunächst also auch isomorph zur Quaternionengruppe $\mathbb{Q}_8$ sein. Die Betrachtung modulo 2 würde dann einen Gruppenhomomorphismus liefern:

$$\phi\colon\ G' \to \mathrm{SL}_2(\mathbb{F}_2)\text{, d.h. } G'/\ker\phi \sqsubseteq \mathrm{SL}_2(\mathbb{F}_2) \implies \frac{|G'|}{|\ker\phi|} \mid |\mathrm{SL}_2(\mathbb{F}_2)|\,.$$

Da $|\mathbb{Q}_8| = 8$ und $|\mathrm{SL}_2(\mathbb{F}_2)| = 6$, muß $|\ker\phi| \in \{4, 8\}$ gelten und daher eines der 6 Elemente der Ordnung 4 im Kern von ϕ liegen: Sei A solch ein Element. Die Eigenwerte von A sind dann $\pm\mathbb{i}$, und daher ist $\mathrm{trace}(A) = 0$, also

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \text{ für } a, b, c \in \mathbb{Z};\ a \text{ ungerade und } b, c \text{ gerade.}$$

Da $A \in \ker\phi$, gilt $4 \mid b \cdot c$, und $\det A = 1$ bedeutet

$$-a^2 - b \cdot c = 1 \implies a^2 \equiv -1 \pmod 4,$$

[6] Denn sei G eine Gruppe gerader Ordnung, dann ist $M = \{g \in G\colon\ g^{-1} \neq g\}$ eine Menge *gerader* Kardinalität, und $G \setminus (M \cup \{\mathbb{n}_G\})$ ist eine Menge *ungerader* Kardinalität.

[7] Denn $H \lhd \mathrm{SL}_2(\mathbb{F}_3)$ und $\phi\colon\ \mathrm{SL}_2(\mathbb{F}_3) \to \mathrm{SL}_2(\mathbb{F}_3)/H \simeq \mathbb{Z}_2$ ist ein Homomorphismus, also $\phi(g^2) = \phi(g) + \phi(g) = 0 \in \mathbb{Z}_2$ und $g^2 \in \ker\phi = H$.

und diese Kongruenzengleichung hat keine Lösung. Aus demselben Grund kann G' auch nicht isomorph zu *ganz* $\mathrm{SL}_2(\mathbb{F}_3)$ sein (sonst gäbe es ja eine Untergruppe, die isomorph zu $\mathbb{Q}_8$ wäre).

- Jede endliche Untergruppe $G' \subseteq \mathrm{SL}_2(\mathbb{Z})$ ist also zyklisch mit Ordnung $1, 2, 3, 4$ oder 6 und ist in $\mathrm{GL}_2(\mathbb{Z})$ zu einer der 5 zyklischen Gruppen $\langle E\rangle$, $\langle -E\rangle$, $\langle U\rangle$, $\langle V\rangle$ oder $\langle W\rangle$ konjugiert.
- Die endlichen Untergruppen $G \subseteq \mathrm{GL}_2(\mathbb{Z})$, die *nicht* Untergruppen von $\mathrm{SL}_2(\mathbb{Z})$ sind, sind die Diedergruppen D_1, D_2, D_3, D_4 oder D_6. Denn $G' = G \cap \mathrm{SL}_2(\mathbb{Z}) \sqsubseteq \mathrm{SL}_2(\mathbb{Z})$ ist dann eine der Gruppen C_1, C_2, C_3, C_4 oder C_6. Falls $G \neq G'$, ist $(G : G') = 2$ und damit[8] $G' \lhd G$. Sei dann $x \in G \setminus G'$, dann ist $\det x = -1$ und daher $\mathrm{ord}_G(x) = 2$. Die Nebenklasse $x \cdot G'$ für $x \notin G'$ enthält dann *nur* Matrizen mit Determinante -1, und diese haben *alle* Ordnung 2: Sei also y ein Erzeuger der zyklischen Gruppe G', dann ist auch $(x \cdot y)^2 = 1$, also
$$x \cdot y \cdot x^{-1} = y^{-1}$$
und G ist isomorph zu einer Diedergruppe. □

BEMERKUNG 1.4.10. *Die Quaternionengruppe $\mathbb{Q}_8$ hat ihren Namen von der Tatsache, daß sie auf der Teilmenge $\{\pm 1, \pm i, \pm j, \pm k\}$ der Quaternionenalgebra $\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ realisiert wird, wo bekanntlich die Multiplikation durch*
$$i^2 = -1 = j^2,\ i \cdot j = k = -j \cdot i.$$
gegeben ist: Dann ist auch $k^2 = i \cdot j \cdot i \cdot j = -i^2 \cdot j^2 = -1$, und $i, -i, j, -j, k, -k$ haben alle Ordnung 4.
Wir haben gesehen, daß man die Gruppe Q_8 nicht als Untergruppe von $\mathrm{GL}_2(\mathbb{Z})$ realisieren kann; man kann sie aber sehr wohl als Untergruppe von $\mathrm{GL}_2(\mathbb{C})$ realisieren:
$$i = \left(\begin{smallmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{smallmatrix}\right),\ j = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right),\ k = \left(\begin{smallmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{smallmatrix}\right).$$

Sei also G eine der 13 arithmetischen Ornamentklassen: Die Ornamentgruppen Γ entstehen daraus durch Erweiterungen der kurzen exakten Sequenz
$$\{\mathbb{m}\} \to \mathbb{Z}^2 \xrightarrow{\iota} \Gamma \to G \to \{\mathbb{m}\}.$$
Für alle Fälle außer $G = D_1, D_2, D_4$ gibt es nur eine einzige Erweiterung, für D_1 und D_4 gibt es jeweils genau 2, und für D_2 genau 3 Erweiterungen: Das sind insgesamt also $10 + 2 + 3 + 2 = 17$ Gruppen.
Bisher wurden alle kristallographischen Gruppen in den Dimensionen $1 \leq n \leq 6$ klassifiziert: Die folgende Tabelle gibt ihre Anzahl s_n wieder, wobei a_n die Anzahl der arithmetischen Ornamentklassen bezeichnet.

n	a_n	s_n	Jahr
1	2	2	1891
2	13	17	1891
3	73	219	1885
4	710	4783	1978
5	6079	222018	2000
6	85311	28927922	2000

[8] Kann man auch so sehen: $\det\colon G \to \{1, -1\} \simeq \mathbb{Z}_2$ ist ein Homomorphismus mit Kern G'.

KAPITEL 2

Polynomringe und Gröbnerbasen

2.1. Polynomringe: Teilbarkeit, Nullstellen

Sei im folgenden $\mathbb{K}$ ein Körper. Wir wissen: Der Polynomring $\mathbb{K}[x]$ ist

- ein *euklidischer Ring* (mit euklidischer Norm $\mathbf{N} \sim \deg$, siehe dazu Lemma A.3.75),
- also ein *Hauptidealbereich* (siehe Satz A.3.56),
- also ein *faktorieller Ring*[1] (siehe Satz A.3.53);

seine Einheitengruppe $\mathbb{K}[x]^\star$ ist $\mathbb{K}^\star$ (siehe Proposition A.3.73): Jedes $c \in \mathbb{K}^\star$ teilt jedes $p \in \mathbb{K}[x]$. Wenn wir in $\mathbb{K}[x]$ die Äquivalenzrelation[2]

$$p \simeq q :\Longleftrightarrow \text{ es gibt ein } c \in \mathbb{K}^\star \text{ sodaß } p(x) = c \cdot q(x)$$

betrachten, dann enthält jede Äquivalenzklasse genau ein *monisches* Polynom (i.e., mit führendem Koeffizienten 1), das wir als "kanonischen Repräsentanten" ansehen können: Eingeschränkt auf monische Polynome induziert Teilbarkeit dann eine Halbordnung, denn in $\mathbb{K}[x]$ gilt ja allgemein

$$p \mid q \text{ und } q \mid p \implies q = c \cdot p \text{ für ein } c \in \mathbb{K}^\star,$$

also *Antisymmetrie* auf monischen Polynomen, und Reflexivität ($p \mid p$) und Transitivität ($p \mid q$ und $q \mid r \implies p \mid r$) gilt ja sowieso. Diese Halbordnung ist "kompatibel" mit der euklidischen Norm, die durch die Gradfunktion deg gegeben ist, in folgendem Sinn:

$$p \mid q \implies \deg p \leq \deg q.$$

DEFINITION 2.1.1 (Größter gemeinsamer Teiler). *Seien $p_1, \ldots, p_n \in \mathbb{K}[x]$. Ein* gemeinsamer Teiler *von $p_1, \ldots, p_n$ ist ein Polynom d, das alle diese p_i teilt: $d \mid p_i$ für $1 \leq i \leq n$. Sei d ein gemeinsamer Teiler, dann gilt $p_i \in (\!(d)\!)$ für $1 \leq i \leq n$, also $(\!(p_1, \ldots, p_n)\!) \subseteq (\!(d)\!)$. Da $\mathbb{K}[x]$ ein Hauptidealbereich ist, ist aber $(\!(p_1, \ldots, p_n)\!) = (\!(s)\!)$, und für dieses s gilt also:*

$$(s \mid p_i \text{ für } 1 \leq i \leq n) \text{ und } (d \mid p_i \text{ für } 1 \leq i \leq n \implies d \mid s).$$

Dieses Polynom s heißt dann ein größter gemeinsamer Teiler *von $p_1, \ldots, p_n$. Sei c der führende Koeffizient von s, dann ist $\tilde{s} := c^{-1} \cdot s$ monisch und es gilt $(\!(s)\!) = (\!(\tilde{s})\!)$: Damit wird die Sache eindeutig, und wir können von* dem *größten gemeinsamen Teiler sprechen:*

$$\mathrm{ggT}(p_1, \ldots, p_n) = \tilde{s}.$$

Wenn $\mathrm{ggT}(p_1, p_2) = 1$ *gilt, dann nennen wir p_1 und p_2* teilerfremd.

[1] Englisch: *Unique Factorization Domain*.

[2] Diese Relation ist offensichtlich reflexiv, symmetrisch und transitiv.

Genau wie im Ring $\mathbb{Z}$ kann man den ggT (p, q) mit dem *Euklidischen Algorithmus* konstruieren:

if $\deg p < \deg q$ **then**
  $p \leftrightarrow q$ `/* Vertausche p und q */`
end if
`/* Ab hier gilt also:` $\deg p \geq \deg q$ `*/`
while $q \neq 0$ **do**
  $p = d \cdot q + r$ `/* Polynomdivision mit Rest */`
  $p \leftarrow q$
  $q \leftarrow r$
end while
return p

BEISPIEL 2.1.2. *Betrachte* $x^5 + x + 1$ *und* $x^4 + x^3 + x + 1$ *in* $\mathbb{F}_2[x]$. *Dann liefert der Euklidische Algorithmus:*

$$\begin{aligned} x^5+x+1 &= \left(x^4+x^3+x+1\right)\cdot(x+1) + x^3+x^2+x \\ x^4+x^3+x+1 &= \left(x^3+x^2+x\right)\cdot x + x^2+x+1 \\ x^3+x^2+x &= \left(x^2+x+1\right)\cdot x+0, \end{aligned}$$

also ggT $\left(x^5 + x + 1, x^4 + x^3 + x + 1\right) = x^2 + x + 1 \in \mathbb{F}_2[x]$.

DEFINITION 2.1.3. *Sei R ein Ring, sei* $q \in R[x]$. *Ein* $\alpha \in R$ *mit der Eigenschaft* $q(\alpha) = \mathbf{0}$ *heißt* Nullstelle *des Polynoms q. Die Menge aller Nullstellen (*Nullstellenmenge*; oder auch "*Verschwindungsmenge*") eines Polynoms q bezeichnen wir mit* $V(q)$.

LEMMA 2.1.4. *Sei R ein* unitärer Ring *(also ein Ring mit Einselement* $\mathbf{1}$*), sei* $q \in R[x]$ *und sei* $\alpha \in R$ *eine Nullstelle von q. Dann gilt* $(x - \alpha) \mid q$, *d.h., es gibt ein* $q^\star \in \mathbb{K}[x]$ *mit* $q(x) = (x - \alpha) q^\star(x)$, *wobei* $\deg q^\star \leq \deg q - 1$*: Wir schreiben für dieses* $q^\star$ *naheliegenderweise* $q / (x - \alpha)$.

BEWEIS. Division mit Rest ergibt

$$q(x) = (\mathbf{1} \cdot x - \alpha) \cdot s(x) + r(x),$$

wobei $\deg r < 1$, also $r \equiv c \in \mathbb{K}$ konstant. Nun wende ev_α (siehe Definition A.3.70) auf diese Gleichung an; es folgt $q(\alpha) = 0 = 0 + r$ und $q^\star(x) = s(x)$. □

Wie in jedem Ring (siehe Definition A.3.46), heißt ein Polynom $f \in \mathbb{K}[x]$ *irreduzibel*, wenn für jede Zerlegung $f = g \cdot h$ (mindestens) einer der Faktoren g oder h in der Einheitengruppe $\mathbb{K}[x]^\star$ liegt. Wir listen einige wohlbekannte Tatsachen auf:

PROPOSITION 2.1.5. *Sei* $f \in \mathbb{K}[x]$. *Dann gilt:*

- *Das Hauptideal* $((f))$ *ist maximal* $\iff$ *f ist irreduzibel* $\iff$ *Der Quotientenring* $\mathbb{K}[x] / ((f))$ *ist ein Körper.*
- $f \in \mathbb{K}[x]^\star \iff \deg f = 0$*: Wenn f* nicht *irreduzibel ist, dann gibt es also eine Zerlegung* $f = g \cdot h$ *mit* $0 < \deg g, \deg h < \deg f$.
- $\deg f = 1 \implies$ *f irreduzibel.*

- *f irreduzibel und* $\deg f > 1 \implies V(f) = \emptyset$.
- *Wenn* $\deg f \in \{2, 3\}$, *dann ist f irreduzibel* $\iff V(f) = \emptyset$.

Ohne Beweis. □

DEFINITION 2.1.6. *Der Ring* $\mathbb{K}[x]$ *der Polynome mit Koeffizienten in* $\mathbb{K}$ *hat zugleich auch die Struktur eines* Vektorraums *über* $\mathbb{K}$*: Auf diesem Vektorraum ist die* formale Ableitung *definiert als der* lineare *Operator* D, *der auf der Standardbasis*

$$\{x^n : n \in \mathbb{N}_0\} = \left\{\mathbf{1}, x, x^2, \dots\right\}$$

so gegeben ist:

$$\mathrm{D}\,\mathbf{1} = \mathbf{0} \text{ und } \mathrm{D}\,x^n := \underbrace{(\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1})}_{n} \cdot x^{n-1} \text{ für } n \in \mathbb{N}.$$

LEMMA 2.1.7. *Sei* $\mathbb{K}$ *ein Körper, seien* $q_1, q_2 \in \mathbb{K}[x]$. *Dann gilt die* Produktregel *für die formale Ableitung:*

$$\mathrm{D}(q_1 \cdot q_2) = (\mathrm{D}\,q_1) \cdot q_2 + q_1 \cdot (\mathrm{D}\,q_2). \tag{2.1}$$

BEWEIS. Daß die Produktregel für zwei Elemente der Standardbasis $q_1 = x^m$, $q_2 = x^n$ gültig ist, ergibt sich sofort aus der Definition der formalen Ableitung. Für allgemeine Polynome $q_1 = \sum_{i=0}^{m} \lambda_i x^i$ und $q_2 = \sum_{j=0}^{n} \mu_j x^j$ folgt die Behauptung durch Koeffizientenvergleich: Denn dann ist definitionsgemäß

$$\mathrm{D}\,q_1 = \sum_{i=0}^{m} i \cdot \lambda_i \cdot x^{i-1} \text{ und } \mathrm{D}\,q_2 = \sum_{j=0}^{n} j \cdot \mu_j \cdot x^j,$$

und für alle $n \in \mathbb{N}$ ist der Koeffizient $[\![x^{n-1}]\!]$ von x^{n-1} auf der linken Seite von (2.1) gegeben als

$$n \cdot \sum_i \lambda_i \cdot \mu_{n-i},$$

und auf der rechten Seite von (2.1) gegeben als

$$\sum_i i \cdot \lambda_i \cdot \mu_{n-i} + \sum_j j \cdot \lambda_{n-j} \cdot \mu_j.$$

Diese Ausdrücke sind identisch (Indextransformation $j \to (n - j)$ in der letzten Summe). □

DEFINITION 2.1.8. *Sei R ein unitärer Ring, sei $q \in R[x]$ mit Nullstelle $\alpha \in R$. Wenn α auch eine Nullstelle von $q/(x - \alpha)$ ist, dann heißt α eine* mehrfache Nullstelle *von q.*

Nach Lemma 2.1.4 folgt dann $(x - \alpha)^2 \mid q(x)$: Die größte Zahl $n \in \mathbb{N}$, für die $(x - \alpha)^n \mid q(x)$, heißt Vielfachheit *der Nullstelle α von q: Wir schreiben $n = \|\alpha\|_q$. Natürlich gilt dann $\|\alpha\|_q \leq \deg q$.*

LEMMA 2.1.9. *Sei R ein* Integritätsbereich, *und sei $q \in R[x]$. Dann besitzt q höchstens* $\deg q$ *Nullstellen (gezählt mit ihrer Vielfachheit).*

BEWEIS. Seien $\alpha_1, \alpha_2, \ldots$ die *verschiedenen* Nullstellen von q. Dann folgt aus

$$0 = q(\alpha_2) = \underbrace{(\alpha_2 - \alpha_1)^{\|\alpha_1\|_q}}_{\neq 0} \cdot q^\star(\alpha_2)$$

zunächst $q^\star(\alpha_2) = 0$ (weil R nullteilerfrei ist), also nach Lemma 2.1.4 $q^\star(x) = (x - \alpha_2)^{\|\alpha_2\|_q} \cdot q^{\star\star}(x)$, u.s.f: Man erhält also

$$q(x) = q^{[\star]} \cdot \prod_i (x - \alpha_i)^{\|\alpha_i\|_q} \text{ mit } V\left(q^{[\star]}\right) = \emptyset,$$

und natürlich gilt dann $\sum_i \|\alpha_i\|_q \leq \deg q$. □

DEFINITION 2.1.10. *Ein Polynom $p \in \mathbb{K}[x]$ heißt* separabel, *wenn es quadratfrei ist, also wenn*

$$q^2 \mid p \implies q \in \mathbb{K}^\star.$$

Ein separables Polynom hat also insbesondere keine mehrfachen Nullstellen.

LEMMA 2.1.11. *Seien $p, q \in \mathbb{K}[x]$. Dann gilt:*

$$q^2 \mid p \implies q \mid \mathrm{D}\, p.$$

Insbesondere gilt also:

$$\mathrm{ggT}(p, \mathrm{D}\, p) = 1 \implies p \text{ ist separabel.}$$

BEWEIS. Aus $p = q^2 \cdot r$ folgt gemäß der Produktregel

$$\mathrm{D}\, p = 2 \cdot q \cdot r \cdot \mathrm{D}\, q + q^2 \cdot \mathrm{D}\, r = q \cdot (2 \cdot r \cdot \mathrm{D}\, q + q \cdot \mathrm{D}\, r),$$

und die Behauptung folgt. □

LEMMA 2.1.12. *Sei $\mathbb{K}$ ein Körper, sei $q \in \mathbb{K}[x]$ mit Nullstelle $\alpha \in \mathbb{K}$. α ist genau dann eine* mehrfache *Nullstelle von q, wenn α auch eine Nullstelle von $\mathrm{D}\, q$ ist.*

BEWEIS. Wir betrachten $(\mathrm{D}\, q)(\alpha)$. Nach Lemma 2.1.4 gibt es ein $q^\star \in \mathbb{K}[x]$, sodaß $q = (x - \alpha) \cdot q^\star$, und nach Lemma 2.1.7 gilt

$$(\mathrm{D}\, q)(x) = \underbrace{(\mathrm{D}(x - \alpha))}_{\mathbf{1}} \cdot q^\star(x) + (x - \alpha) \cdot (\mathrm{D}\, q^\star)(x).$$

Wenn wir hier $x = \alpha$ setzen, ergibt sich

$$(\mathrm{D}\, q)(\alpha) = q^\star(\alpha),$$

woraus die Behauptung folgt. □

BEMERKUNG 2.1.13. *Über endlichen Körpern gibt es nicht–konstante Polynome, deren Ableitung verschwindet. Z.B. gilt für $p \in \mathbb{P}$ in $\mathbb{F}_p[x]$*

$$\mathrm{D}\, x^p = p \cdot x^{p-1} \equiv 0.$$

2.2. Polynome in mehreren Variablen

Sei $\mathbb{K}$ ein Körper, dann ist $\mathbb{K}[x]$ ein Hauptidealbereich. Wir können nun Polynome in der Variablen y betrachten, mit Koeffizienten in $\mathbb{K}[x]$:

$$\mathbb{K}[x,y] := (\mathbb{K}[x])[y],$$

und $\mathbb{K}[x,y]$ ist jedenfalls wieder ein Ring, dessen Elemente formale *endliche* Summen der Gestalt

$$\sum_{i,j\geq 0} c_{i,j} \cdot x^i \cdot y^j$$

sind. Das kann man iterieren und kommt so zu

$$\mathbb{K}[x,y,z] := (\mathbb{K}[x,y])[z],$$

oder allgemeiner zu $\mathbb{K}[x_1, x_2, \ldots, x_n]$, dem Ring der Polynome in n Variablen. Seine Elemente sind endliche formale Summen der Gestalt

$$\sum_{(i_1,\ldots,i_n)\in\mathbb{N}_0^n} \underbrace{c_{i_1,i_2,\ldots,i_n}}_{\text{Koeffizient}} \cdot \underbrace{x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n}}_{\text{Monom}},$$

und wie bei "normalen" Polynomen (siehe Definition A.3.70) haben wir *Terme*, *Koeffizienten* und *Monome*, und wir schreiben wieder

$$\left[\!\left[x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n} \right]\!\right] = c_{i_1,i_2,\ldots,i_n}.$$

Es ist klar: Das Monom $x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n}$ ist eindeutig durch das n–Tupel $v := (i_1, i_2, \ldots, i_n) \in \mathbb{N}_0^n$ bestimmt, und wir schreiben abkürzend auch

$$x^v := x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n}$$

2.2.1. Polynomiale Gleichungssysteme. Systeme von Polynomgleichungen

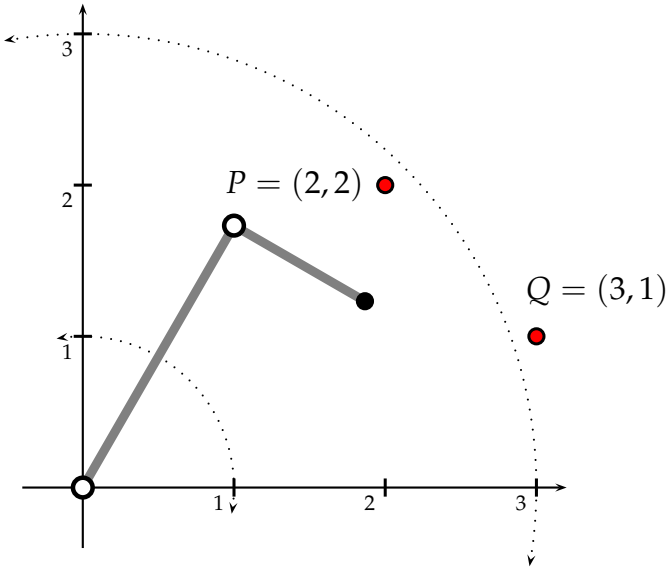
$$f_1(x_1,\ldots,x_n) = 0, \ldots, f_m(x_1,\ldots,x_n) = 0 \tag{2.2}$$

in mehreren Variablen (also $f_i \in \mathbb{K}[x_1,\ldots,x_n]$) treten in vielen Anwendungsbereichen in ganz natürlicher Weise auf, und Methoden der algebraischen Geometrie und der Computeralgebra werden verwendet, um diese Gleichungen zu lösen oder zu vereinfachen.

Wir wollen hier nur ein ganz einfaches illustrierendes Beispiel geben (siehe Abbildung 1): Gegeben sei ein Roboterarm, der aus zwei starren Stangen der Länge 2 und 1 besteht, die durch ein Drehgelenk verbunden und im Koordinatenursprung $(0,0)$ drehbar befestigt sind, sodaß sich der Arm in der Ebene $\mathbb{R}^2$ bewegen kann. Bezeichnen wir die Koordinaten des Gelenks, das die Stangen verbindet, mit (x,y), und die Koordinaten des "freien Endpunkts" dieses Gestänges mit (z,w), so ist der Zustand des Armes vollständig durch die Koordinaten $(x,y,z,w) \in \mathbb{R}^4$ beschrieben. Klarerweise können nur bestimmte Quadrupel $(x,y,z,w) \in \mathbb{R}^4$ als Zustand auftreten:

$$x^2 + y^2 - 4 = 0,$$
$$(x-z)^2 + (y-w)^2 - 1 = 0.$$

ABBILDUNG 1. Illustration: "Roboterarm" mit zwei Gelenken.



Wenn wir jetzt einen Punkt (z, w) in der Ebene vorgeben und wissen wollen, ob und wie der Roboterarm ihn erreichen kann, so müssen wir die reellen Lösungen dieses Gleichungssystems in x und y bestimmen. In diesem überaus einfachen Fall ist die Sache geometrisch natürlich durchsichtig: Sei $r = \sqrt{z^2 + w^2}$ der Abstand des vorgegebenen Punktes vom Koordinatenursprung, dann gibt es

- überhaupt keine Möglichkeit, den Punkt zu erreichen, wenn $r < 1$ oder $r > 3$ ist,
- genau eine Möglichkeit, wenn $r = 1$ oder $r = 3$ ist,
- und genau zwei Möglichkeiten, wenn $1 < r < 3$ ist.

Aber es ist klar, daß bei komplexeren Fragestellungen die Sache rasch undurchsichtig werden kann.

DEFINITION 2.2.1. *Sei R ein kommutativer Ring mit Eins und $I \sqsubseteq R[x_1, \ldots, x_n]$. Die* Nullstellenmenge *oder* Verschwindungsmenge $V(I)$ *von I ist die Menge aller Punkte $\xi = (\xi_1, \ldots, \xi_n) \in R^m$, für die*

$$f(\xi) = 0 \text{ für alle } f \in I,$$

also

$$V(I) := \{\xi = (\xi_1, \ldots, \xi_n) \in R^n : \ f(\xi) = 0 \text{ für alle } f \in I\}.$$

PROPOSITION 2.2.2. *Sei R ein kommutativer Ring mit Eins und $I \sqsubseteq R[x_1, \ldots, x_n]$ ein* endlich erzeugtes *Ideal, also*

$$I = ((f_1, \ldots, f_m)) \text{ mit } f_i \in R[x_1, \ldots, x_n] \text{ für } i \in [m].$$

Dann ist die Lösungsmenge *L des Systems von Polynomgleichungen*

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0,$$

also

$$L = \{\xi = (\xi_1, \ldots, \xi_n) \in R^n : \ f_i(\xi) = 0 \text{ für alle } i \in [m]\},$$

identisch mit der Verschwindungsmenge $V(I)$.

BEWEIS. Sei $\xi \in L$ und $f \in I$: Dann ist f eine "*Polynomialkombination*"

$$f = a_1 \cdot f_1 + \cdots + a_m \cdot f_m,$$

also ein Analogon zu einer "Linearkombination" (wie in der Linearen Algebra), wobei die Koeffizienten a_i aber keine Skalare sind, sondern selbst wieder Polynome, und klarerweise ist dann also $\xi \in V(I)$: Also ist $L \subseteq V(I)$.
Umgekehrt gilt für jedes $\xi \in V(I)$ insbesondere $f_i(\xi) = 0$ für alle $i \in [m]$ (da ja $f_i \in I$): Also ist $V(I) \subseteq L$. □

Mit dieser einfachen Beobachtung können wir die Umformung eines gegebenen Gleichungssystems

$$f_1(x_1, \ldots, x_n) = 0, \ldots, f_m(x_1, \ldots, x_n) = 0$$

in ein *äquivalentes Gleichungssystem* (also eines mit derselben Lösungsmenge)

$$g_1(x_1, \ldots, x_n) = 0, \ldots, g_k(x_1, \ldots, x_n) = 0$$

(solche Umformungen kennen wir aus der Linearen Algebra, z.B. *Gauß–Elimination*) abstrakt so beschreiben: Wir suchen ein alternatives *Erzeugendensystem* $g_1, \ldots, g_k$, sodaß gilt

$$((f_1, \ldots, f_m)) = ((g_1, \ldots, g_k)).$$

2.3. Ideale in Polynomringen in mehreren Variablen

Polynomringe $\mathbb{K}[x_1, x_2, \ldots, x_n]$ sind für $n > 1$ *keine* euklidischen Ringe und *keine* Hauptidealbereiche, d.h.: Ein Ideal $I \sqsubseteq \mathbb{K}[x_1, x_2, \ldots, x_n]$ ist zwar immer *endlich erzeugt* (nach Hilberts Basissatz, den wir hier als Korollar 2.7.12 beweisen werden), also $I = ((f_1, \ldots, f_m))$, aber es ist nicht jedes Ideal ein *Hauptideal*, also i.a. nicht $I = ((f))$. Und diese Tatsache hat folgende Konsequenzen:

- Es ist i.a. gar nicht so leicht festzustellen, ob zwei Ideale I_1, I_2 identisch sind: Denn auch wenn $I_1 = ((f_1, \ldots, f_m))$ und $I_1 = ((g_1, \ldots, g_n))$ beide endlich erzeugt sind, sind die Erzeugendensysteme ("Ideal–Basen") $\{f_1, \ldots, f_m\}$ bzw. $\{g_1, \ldots, g_n\}$ *keineswegs* eindeutig, und es kann recht kompliziert werden, die Gleichheit (oder Ungleichheit) der Ideale nachzuweisen: Dazu muß jedes $f_i \in ((g_1, \ldots, g_n))$ sein, und umgekehrt auch jedes $g_j \in ((f_1, \ldots, f_m))$.
- Im Zusammenhang damit steht die Frage, alle *gemeinsamen* Nullstellen von Polynomen $f_1, \ldots, f_m$ zu finden: Wenn $((f_1, \ldots, f_m)) = ((g_1, \ldots, g_n))$, können wir stattdessen die gemeinsamen Nullstellen der Polynome $g_1, \ldots, g_n$ bestimmen (was wir natürlich nur dann versuchen werden, wenn das System $g_1 = 0, \ldots, g_n = 0$ "einfacher" zu behandeln ist als das ursprüngliche System $f_1 = 0, \ldots, f_m = 0$).

Wir bräuchten also vor allem eine Methode um festzustellen, ob ein Polynom f in einem Ideal $I = ((f_1, \ldots, f_m))$ enthalten ist: In einem euklidischen Polynomring wäre $I = ((g))$ ein *Hauptideal*, und die Frage "$f \in ((q))$?" läßt sich durch Division mit Rest ganz leicht beantworten: Sei $f = g \cdot q + r$ (Division mit Rest), dann ist

$$f \in ((g)) \iff r \equiv \mathbf{0}.$$

Wir brauchen also einen "Ersatz" für Division mit Rest: Die funktioniert ja (sehr salopp gesprochen) so, daß vom Dividenden Schritt für Schritt der Term höchsten Grades entfernt wird, bis der Grad des Divisors höher ist als der des Dividenden. Ein erstes Problem bei Polynomen in mehreren Variablen ist aber, daß gar nicht klar ist, welches der "Term höchsten Grades" ist; z.B. bei $f = x^3 + xy^2 + xyz \in \mathbb{K}[x, y, z]$.

2.4. Monomordnungen

Bei Polynomen in einer Variablen ist es naheliegend, die Monome x^i entweder "in i aufsteigend" oder "in i absteigend" anzuordnen, also

$$p = c_0 + c_1 \cdot x + \cdots + c_n \cdot x^n$$

oder

$$p = c_n \cdot x^n + c_{n-1} \cdot x^{n-1} + \cdots + c_1 \cdot x + c_0$$

zu schreiben. Die Monome $x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n}$ werden hingegen durch n–Tupel aus $\mathbb{N}_0^n$ bestimmt, für die es keine solche "offensichtliche kanonische Ordnung" gibt: Es gibt mehrere Möglichkeiten, $\mathbb{N}_0^n$ zu ordnen.

DEFINITION 2.4.1 (Gesamtgrad). *Auf $\mathbb{N}_0^n$ können wir die Einschränkung der* 1*–Norm auf $\mathbb{R}^n$ betrachten:*

$$\|.\| : \mathbb{N}_0^n \to \mathbb{N}_0;\ \| (i_1, \ldots, i_n) \|_1 = i_1 + \cdots + i_n.$$

Für $v = (i_1, \ldots, i_n)$ betrachten wir das Monom x^v und nennen $\|v\|$ dann den Gesamtgrad *des Monoms x^v.*

DEFINITION 2.4.2 (Termordnung oder Monomordnung). *$(\mathbb{N}_0)^n$ ist eine Halbgruppe bezüglich der komponentenweisen Addition, mit Nullelement $\mathbf{0} = (0, 0, \ldots, 0)$. Eine partielle Ordnung $\preceq$ auf $\mathbb{N}_0^n$ heißt* Termordnung *oder* Monomordnung, *falls gilt:*

- *$\preceq$ ist eine* Totalordnung *(siehe Definition A.1.2),*
- *$\mathbf{0} \preceq v$ für alle $v \in \mathbb{N}_0^n$,*
- *$v_1 \preceq v_2 \implies v_1 + v \preceq v_2 + v$ für alle $v \in \mathbb{N}_0^n$.*

2.4.1. Verschiedene Monomordnungen. Es gibt mehrere Monomordnungen:

DEFINITION 2.4.3 (Monomordnungen). *Die* lexikographische Ordnung *auf $\mathbb{N}_0^n$ ist wie folgt definiert:*

$$(a_1, \ldots, a_n) \prec_{lex} (b_1, \ldots, b_n) :\Longleftrightarrow\ a_1 = b_1, \ldots, a_{k-1} = b_{k-1}; a_k < b_k$$

für ein $k \in [n]$.
Die umgekehrt lexikographische Ordnung *auf $\mathbb{N}_0^n$ ist wie folgt definiert:*

$$(a_1, \ldots, a_n) \prec_{ulex} (b_1, \ldots, b_n) :\Longleftrightarrow\ a_n = b_n, \ldots, a_{k+1} = b_{k+1}; a_k < b_k$$

für ein $k \in [n]$.
Die graduierte lexikographische Ordnung *auf $\mathbb{N}_0^n$ ist wie folgt definiert:*

$$a \prec_{grlex} b :\Longleftrightarrow\ \|a\| < \|b\| \text{ oder } (\|a\| = \|b\| \text{ und } a \prec_{lex} b)\,.$$

Die graduierte umgekehrt lexikographische Ordnung *auf* $\mathbb{N}_0^n$ *ist wie folgt definiert:*

$$a \prec_{grulex} b :\Longleftrightarrow \|a\| < \|b\| \text{ oder } (\|a\| = \|b\| \text{ und } a \prec_{ulex} b).$$

BEISPIEL 2.4.4. *In* $\mathbb{K}[x_1, x_2, x_3]$ *haben wir*

$$\begin{aligned}\alpha = (0,4,0): &\ x^\alpha = x_1^4\\ \beta = (1,1,2): &\ x^\beta = x_1 x_2 x_3^2\\ \gamma = (1,2,1): &\ x^\gamma = x_1 x_2^2 x_3\\ \delta = (3,0,0): &\ x^\delta = x_1^3\end{aligned}$$

Dann gilt $\alpha \prec_{lex} \beta \prec_{lex} \gamma \prec_{lex} \delta$ *und* $\delta \prec_{grlex} \alpha \prec_{grlex} \beta \prec_{grlex} \gamma$ *und* $\delta \prec_{grulex} \beta \prec_{grulex} \gamma \prec_{grulex} \alpha$

Es ist leicht zu sehen:

PROPOSITION 2.4.5. *Die in Definition 2.4.3 vorgestellten partiellen Ordnungen sind Monomordnungen auf* $\mathbb{N}_0^n$.
Auf $\mathbb{N}_0^1$ *gibt es nur eine Monomordnung, nämlich die "übliche" Ordnung.*

Ohne Beweis. □

Sobald wir eine Monomordnung auf $\mathbb{N}_0^n$ festgelegt haben, können wir die Monome eines Polynoms $f \in S$ eindeutig anordnen:

BEISPIEL 2.4.6. *Sei Polynom* $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z$ *in* $\mathbb{Q}[x, y, z]$ *gegeben. Dann können wir die Terme von* f *wie folgt absteigend ordnen:*

$$\begin{aligned}\text{für } \prec_{lex}: f &= 4x^3 + 7xy^2z + 4xyz^2 - 5y^4,\\ \text{für } \prec_{grlex}: f &= 7xy^2z + 4xyz^2 - 5y^4 + 4x^3,\\ \text{für } \prec_{grulex}: f &= -5y^4 + 7xy^2z + 4xyz^2 + 4x^3.\end{aligned}$$

DEFINITION 2.4.7. *Sei* $f = \sum_{\alpha \in \mathbb{N}_0^n} c_\alpha x^\alpha$ *ein von Null verschiedenes Polynom in* $\mathbb{K}[x_1, x_2, \ldots, x_n]$ *und sei* $\prec$ *eine (beliebige, aber feste) Monomordnung.*
Der Multigrad *von* f *ist*

$$\operatorname{mdeg}(f) = \max_{\prec} \{\alpha \in \mathbb{N}_0^n : \ c_\alpha \neq 0\}.$$

Der Leitkoeffizient *(oder* führende Koeffizient*) von* f *ist*

$$\operatorname{lc}(f) = c_{\operatorname{mdeg}(f)}.$$

Das führende Monom *von* f *ist*

$$\operatorname{lm}(f) = x^{\operatorname{mdeg}(f)}.$$

Der führende Term *von* f *ist*

$$\operatorname{lt}(f) = \operatorname{lc}(f) \cdot \operatorname{lm}(f).$$

Für das Nullpolynom definieren wir $\operatorname{mdeg}(\mathbf{0}) = -\overline{\infty} := \left(\underbrace{-\infty, \ldots, -\infty}_{n\text{–mal}}\right)$.

Dann können wir die Schreibweise aus Definition A.3.70 genau nachahmen: Sei $f = \sum c_{i_1,i_2,\ldots,i_n} \cdot x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n}$, dann ist

$$\left[\!\left[x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n} \right]\!\right] f = \begin{cases} c_{i_1,i_2,\ldots,i_n} \text{ für } \mathbf{0} \preceq (i_1,\ldots,i_n) \preceq \operatorname{mdeg} f, \\ 0 \text{ sonst.} \end{cases}$$

BEISPIEL 2.4.8. *Sei* $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z \in \mathbb{Q}[x,y,z]$*:*

Ordnung	$\prec_{lex}$	$\prec_{grlex}$	$\prec_{grulex}$
$\operatorname{mdeg}(f)$	$(3,0,0)$	$(1,2,1)$	$(0,4,0)$
$\operatorname{lc}(f)$	4	7	-5
$\operatorname{lm}(f)$	x^3	xy^2z	y^4
$\operatorname{lt}(f)$	$4x^3$	$7xy^2z$	$-5y^4$

PROPOSITION 2.4.9. *Sei R ein Integritätsbereich, $\prec$ eine Monomordnung auf $\mathbb{N}_0^n$ und $f, g \in R[x_1,\ldots,x_n]$. Dann gilt:*

(1) $\operatorname{mdeg}(f \cdot g) = \operatorname{mdeg} f + \operatorname{mdeg} g$.
(2) $\operatorname{mdeg}(f+g) \prec \max_{\prec}\{\operatorname{mdeg} f, \operatorname{mdeg} g\}$*; falls* $\operatorname{mdeg} f \neq \operatorname{mdeg} g$*, so gilt sogar* $\operatorname{mdeg}(f+g) = \max_{\prec}\{\operatorname{mdeg} f, \operatorname{mdeg} g\}$.

BEWEIS. Sei $x^\alpha = \operatorname{lm}(f)$ und $x^\beta = \operatorname{lm}(g)$. Für jedes Monom x^γ in $h = f \cdot g$ gilt $\gamma = \alpha' + \beta'$ für ein Monom $x^{\alpha'}$ bzw. $x^{\beta'}$, das in f bzw. in g vorkommt. Es ist aber für die Monomordnung $\prec$:

$$\gamma = \alpha' + \beta' \preceq \alpha + \beta' \preceq \alpha + \beta,$$

weil $\alpha' \preceq \alpha$ und $\beta' \preceq \beta$. Da R keine Nullteiler hat, kommt das Monom $x^{\alpha+\beta}$ in h tatsächlich vor.
Die zweite Behauptung ist klar. □

2.5. Dicksons Lemma

SATZ 2.5.1 (Dicksons Lemma). *Sei $n \in \mathbb{N}$. Betrachte auf $\mathbb{N}_0^n$ die* Produktordnung *(in bezug auf die "normale" Ordnung von $\mathbb{N}_0$; siehe Definition A.1.4)*

$$(x_1,\ldots,x_n) \leq (y_1,\ldots,y_n) :\Longleftrightarrow\ x_i \leq y_i \text{ für alle } i \in [n].$$

Dann wird jedes Ordnungsideal I von der Menge M seiner minimalen Elemente

$$M = \{m \in I\colon\ m \text{ ist minimal in } I\} \subseteq I$$

(siehe Definition A.1.2) erzeugt, und diese Menge ist nicht–leer und endlich*: $0 < |M| < \infty$.*

BEWEIS. Sei $x_0 \in I$ beliebig: Wenn x_0 nicht minimal ist, dann gibt es definitionsgemäß (siehe Definition A.1.2) ein Element $x_1 \in I$ mit $x_1 < x_0$ in der Produktordnung, und daraus folgt $\|x_1\| < \|x_0\|$. Wenn x_1 auch nicht minimal ist, wiederholen wir diese Argumentation und erhalten so eine absteigende Kette $x_0 > x_1 > x_2 > \cdots$, die in der 1–Norm monoton fällt: Diese Folge muß also *endlich* sein und in einem *minimalen* Element m_x von I enden, und (definitionsgemäß; siehe Definition A.1.5) wird I von der Menge M der minimalen Elemente erzeugt.

Es ist klar: Je zwei verschiedene Elemente $z_1, z_2 \in M$ sind *unvergleichbar* in der Produktordnung:

$$z_1 \not\preceq z_2 \text{ und } z_2 \not\preceq z_1.$$

Angenommen, M wäre unendlich. Dann können nicht alle Koordinaten der Elemente in M beschränkt sein, denn

$$x \leq (c_1, \ldots, c_n) \text{ für alle } x \in M \text{ (in der Produktordnung)}$$

würde bedeuten, daß $|M| \leq (c_1 + 1) \cdots (c_n + 1) < \infty$, im Widerspruch zu unserer Annahme.

O.B.d.A. sei also die Projektion von M auf die erste Koordinate eine unbeschränkte Teilmenge von $\mathbb{N}_0$. Dann gibt es eine unendliche Folge $A_1 = (a_i)_{i=1}^{\infty} \subseteq M$, die in der ersten Koordinate *streng monoton* wächst. In A_1 (als Menge betrachtet) kann natürlich noch eine andere Koordinate unbeschränkt sein: O.B.d.A. finden wir in diesem Fall eine unendliche *Teilfolge* $A_2 \subseteq A_1$, die auch in der zweiten Koordinate streng monoton wächst, u.s.f. O.B.d.A. finden wir so eine unendliche Folge $A_k = (z_i)_{i=1}^{\infty}$ in M, die in den ersten k Koordinaten streng monoton wächst, aber in den letzten $(n-k)$ Koordinaten beschränkt bleibt; $1 \leq k \leq n$. Dann ist aber die Projektion von A_k auf die letzten $(n-k)$ Koordinaten eine *endliche* Menge in $\mathbb{N}_0^{n-k}$, und es muß ein $i_1 < i_2$ geben, sodaß die Projektionen von z_{i_1} und z_{i_2} auf die letzten $(n-k)$ Koordinaten übereinstimmen (wenn $n = k$, so gilt dies *für alle* i_1, i_2). Es ist dann aber

$$z_{i_1} \leq z_{i_2} \text{ in der Produktordnung auf } \mathbb{N}_0^n$$

nach Konstruktion von A_k, aber

$$z_{i_1} \neq z_{i_2} \text{ (da } A_k \text{ in den } k > 0 \text{ ersten Koordinaten streng monoton).}$$

Also ist $z_{i_1} < z_{i_2}$, ein Widerspruch. □

KOROLLAR 2.5.2. *Jede Monomordnung $\preceq$ auf $\mathbb{N}_0^n$ ist eine Wohlordnung.*

BEWEIS. Sei $S \subseteq \mathbb{N}_0^n$ beliebig, sei O das von S (in der Produktordnung) erzeugte Ordnungsideal: Nach Dicksons Lemma 2.5.1 wird O von einer endlichen Menge $M = \{m_1, \ldots, m_k\}$ erzeugt, und es gilt $M \subseteq S$ (siehe Definition A.1.5). Für $v \in S$ beliebig gilt also (in der Produktordnung) $v \geq m_i$ für ein i, und nach Definition der Produktordnung ist

$$v = m_i + w$$

für ein $w \in \mathbb{N}_0^n$. Nach Definition einer Monomordnung gilt immer

$$w \succeq \mathbf{0},$$

und daraus folgt (gleichfalls nach Definition einer Monomordnung)

$$w + m_i \succeq m_i,$$

also $v \succeq m_i$. Daher ist das (in der Monomordnung) kleinste Element (in einer Totalordnung eindeutig!) in der (endlichen!) Menge M zugleich das kleinste Element von S. □

2.6. Divisionsalgorithmus für Polynome in mehreren Variablen

PROPOSITION 2.6.1. *Sei R ein Integritätsbereich, sei $\prec$ eine Monomordnung auf $\mathbb{N}_0^n$, und seien $f; f_1, \ldots, f_m \in R[x_1, \ldots, x_n] \setminus \mathbf{0}$, wobei es auf die* Ordnung *der Polynome f_i ankommt, also*

$$(f_1, \ldots, f_m) \in (R[x_1, \ldots, x_n] \setminus \mathbf{0})^m .$$

Dann gibt es Polynome $a_1, \ldots, a_m; r \in R[x_1, \ldots, x_n]$, sodaß

$$f = a_1 \cdot f_1 + \cdots + a_m \cdot f_m + r,$$

sodaß entweder $r = \mathbf{0}$ gilt, oder keiner der Terme von r durch einen der führenden Terme $\operatorname{lt} f_1, \ldots, \operatorname{lt} f_2$ teilbar ist. Falls $a_i \cdot f_i \neq \mathbf{0}$, gilt außerdem

$$\operatorname{mdeg}(a_i \cdot f_i) \preceq \operatorname{mdeg} f.$$

BEWEIS. Die behaupteten Polynome $a_1, \ldots, a_m; r$ kann man mit dem folgenden *Divisionsalgorithmus* erhalten. In jedem Schritt gilt dabei

$$f = a_1 \cdot f_1 + \cdots a_m \cdot f_m + (r + s), \tag{2.3}$$

mit einer "Hilfsvariablen" s:

```
/* Starte mit a_1 = ··· a_m = r = Nullpolynom und s = f */
a_1 ← ··· a_m ← r ← 0
s ← f
/* In jedem Schritt gilt (2.3): */
while s ≠ 0 do
  if (lt f_i | lt s) für ein i then
    Wähle das kleinste solche i (die f_i sind geordnet!)
    s ← s − (lt s / lt f_i) · f_i
    a_i ← a_i + lt s / lt f_i
  else
    r ← r + lt(s) /* t Term von r ⟹ lt(f_i) ∤ t! */
    s ← s − lt(s)
  end if
end while
/* Ende des Algorithmus: Rückgabe der Werte a_1,...,a_m;r */
return a_1,...,a_m;r
```

Wir müssen zeigen, daß dieser Algorithmus *abbricht*. Das Hilfspolynom s wird in jedem Schritt seines führenden Terms beraubt, also bilden die Multigrade $\operatorname{mdeg} s$ im Laufe des Algorithmus eine absteigende Kette in bezug auf die *Wohlordnung* $\preceq$, d.h.:

$$\underbrace{\operatorname{mdeg} s}_{\text{zu Beginn}} \succ \underbrace{\operatorname{mdeg} s}_{\text{Schritt 1}} \succ \underbrace{\operatorname{mdeg} s}_{\text{Schritt 2}} \succ \cdots$$

In einer *Wohlordnung* kann es aber keine unendlich langen strikt absteigenden Ketten geben: Denn eine solche Kette wäre eine Menge, die kein minimales Element hat. Also bricht der Algorithmus immer nach endlich vielen Schritten ab.

Zu Beginn des Algorithmus ist $a_i = 0$ und $s = f$, also $\operatorname{mdeg} a_i = -\overline{\infty}$ und $\operatorname{mdeg} s \preceq \operatorname{mdeg} f$. Im Wiederholungsschritt hat man

Monomordnung!

$$\operatorname{mdeg}\left(\left(a_i + \frac{\operatorname{lt} s}{\operatorname{lt} f_i}\right) \cdot f_i\right) \preceq \max\left\{\operatorname{mdeg}\left(a_i \cdot f_i\right), \operatorname{mdeg}\left(s\right)\right\}$$

(siehe Proposition 2.4.9). Das heißt aber, die Polynome $a_i \cdot f_i$ können im Multigrad höchstens auf den des Hilfspolynoms s steigen, und $\operatorname{mdeg} s \preceq \operatorname{mdeg} f$ während des gesamten Algorithmus. □

BEISPIEL 2.6.2. *Sei $S = \mathbb{Q}[x, y]$ mit der lexikographischen Ordnung als Monomordnung. Wir wollen den Divisionsalgorithmus für die Polynome $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ und $f_2 = y^2 - 1$ in S durchführen, die alle bereits "nach absteigendem Multigrad" hingeschrieben sind. Es gilt:*

$$\operatorname{lt}(f_1) = xy, \operatorname{lt}(f_2) = y^2$$

Der Algorithmus beginnt mit $a_1 = a_2 = r = 0$ und $s = x^2y + xy^2 + y^2$.
Wir finden $(\operatorname{lt}(f_1) = xy) \mid \left(\operatorname{lt}(s) = x^2y\right)$ und setzen also:

$$a_1 = a_1 + \frac{x^2y}{xy} = x,$$
$$s = s - \frac{x^2y}{xy}(xy - 1) = xy^2 + x + y^2.$$

Nun finden wir wieder $(\operatorname{lt}(f_1) = xy) \mid \left(\operatorname{lt}(s) = xy^2\right)$ und setzen also:

$$a_1 = a_1 + \frac{xy^2}{xy} = x + y,$$
$$s = s - \frac{xy^2}{xy}(xy - 1) = x + y^2 + y.$$

Nun finden wir keinen Index i mit $\operatorname{lt}(f_i) \mid \operatorname{lt}(s)$, also setzen wir:

$$r = 0 + \operatorname{lt}(s) = x,$$
$$s = s - \operatorname{lt}(s) = y^2 + y.$$

Nun finden wir $\left(\operatorname{lt}(f_2) = y^2\right) \mid \left(\operatorname{lt}(s) = y^2\right)$ und setzen also:

$$a_2 = a_2 + \frac{y^2}{y^2} = 1,$$
$$s = s - \frac{y^2}{y^2}\left(y^2 - 1\right) = y + 1.$$

Nun finden wir keinen Index i mit $\operatorname{lt}(f_i) \mid \operatorname{lt}(s)$, also setzen wir:

$$r = r + \operatorname{lt}(s) = x + y,$$
$$s = s - \operatorname{lt}(s) = 1.$$

Wiederum finden wir keinen Index i mit $\operatorname{lt}(f_i) \mid \operatorname{lt}(s)$, also setzen wir:

$$r = r + 1 = x + y + 1,$$
$$s = s - 1 = 0.$$

Der Algorithmus bricht also ab und liefert $a_1 = x + y$, $a_2 = 1$ und $r = x + y + 1$.

DEFINITION 2.6.3. *Das Polynom r, das wir bei der multivariaten Division von f durch das (geordnete!) Tupel von Polynomen $(f_1, \ldots, f_s)$ erhalten, heißt der* Rest *von f; die Polynome $q_1, \ldots, q_s$ heißen* Quotienten. *Wir schreiben*

$$r = f \pmod{f_1, \ldots, f_s}.$$

Klarerweise gilt:

$$f = 0 \pmod{f_1, \ldots, f_s} \implies f \in ((f_1, \ldots, f_s))$$

Die Umkehrung gilt allerdings i.a. *nicht*, wie das folgende Beispiel zeigt:

BEISPIEL 2.6.4. *Sei $f = xy^2 - x$ und $f_1 = xy + 1$, $f_2 = y^2 - 1$ in $\mathbb{Q}[x, y]$ mit der lexikographischen Ordnung. Dann ist $f = x \cdot f_2$, also $f \in ((f_1, f_2))$, aber $f = -(x + y) \neq 0 \pmod{f_1, f_2}$, denn der Divisionsalgorithmus liefert*

$$xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) - (x + y).$$

Wir werden aber sehen: Wenn man ein "gutes" Erzeugendensystem für ein Ideal $I = ((f_1, \ldots, f_s))$ findet, dann gilt tatsächlich auch

$$f \in ((f_1, \ldots, f_s)) \implies f = 0 \pmod{f_1, \ldots, f_s}.$$

2.7. Monomideale, Gröbner Basen & Buchberger–Algorithmus

Bis zum Ende dieses Kapitels verwenden wir die Abkürzung $S := \mathbb{K}[x_1, \ldots, x_n]$ ($n \in \mathbb{N}$, $\mathbb{K}$ ein Körper).

2.7.1. Monomideale.

DEFINITION 2.7.1. *Für ein n–Tupel $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ verwenden wir die abkürzende Notation*

$$x^\alpha := x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Ein Ideal $I \subseteq S$ heißt Monomideal, *falls es eine Teilmenge $A \subseteq \mathbb{N}_0^n$ gibt mit $I = ((x^A)) = ((\{x^\alpha : \alpha \in A\}))$.*

BEISPIEL 2.7.2. *Sei zum Beispiel $S = \mathbb{K}[x, y]$ und $A = \{(4, 2), (3, 4), (2, 5)\} \subset \mathbb{N}_0^2$. Dann ist $I = ((x^4y^2, x^3y^4, x^2y^5)) \sqsubseteq S$ das zu A gehörende Monomideal $((x^A))$.*
$((x^2 - y, x^2 + y)) = ((x^2, y))$ ist ein Monomideal in S, $((x + y, y^2 - 1))$ hingegen nicht (siehe Beispiel 2.7.6).

Das folgende "unscheinbare" Lemma erweist sich als sehr leistungsstark für unsere Zwecke:

LEMMA 2.7.3. *Für Monome x^α, x^β gilt:*

$$x^\alpha \mid x^\beta \iff \exists \gamma \in \mathbb{N}_0^n : \beta = \alpha + \gamma.$$

Sei $I = ((x^A))$ ein Monomideal von S und $\beta \in \mathbb{N}_0^n$. Dann gilt $x^\beta \in I$ genau dann, wenn es ein $\alpha \in A$ gibt mit $x^\alpha \mid x^\beta$.

BEWEIS. Die Behauptung über Teilbarkeit von Monomen ist klar. Wir wenden uns der Äquivalenz zu:
($\Longleftarrow$): $x^\alpha \in I$ und $\gamma := \beta - \alpha \in \mathbb{N}_0^n \implies x^\beta = x^\alpha \cdot x^{\beta-\alpha} \in I$.
($\Longrightarrow$): $x^\beta \in I \implies x^\beta = \sum_{\alpha\in A} p_\alpha \cdot x^\alpha$, wobei nur endlich viele $p_\alpha \neq 0$ sind. Mit Koeffizientenvergleich folgt dann

$[\![x^\gamma]\!]\ p = 0$ wenn $\gamma \notin \mathbb{N}_0^n$

$$\left[\!\left[x^\delta\right]\!\right] \sum_{\alpha\in A} p_\alpha \cdot x^\alpha = \sum_{\alpha\in A} \left[\!\left[x^{\delta-\alpha}\right]\!\right] p_\alpha = [\delta = \beta]\,;$$

es muß also zumindest ein α geben mit $[\![x^{\beta-\alpha}]\!]\ p_\alpha \neq 0$: Dann ist aber $\gamma = \beta - \alpha \in \mathbb{N}_0$, also $x^\alpha \mid x^\beta$. □

LEMMA 2.7.4. *Sei $I = ((x^A))$ ein Monomideal ($A \subseteq \mathbb{N}_0^n$); sei $f \in S$. Dann sind die folgenden Aussagen äquivalent.*

(1) *Es gilt $f \in I$.*
(2) *Jeder Term von f liegt in I.*
(3) *f ist eine Linearkombination von Monomen in I mit Koeffizienten in $\mathbb{K}$.*

BEWEIS. Die Implikationen (2) $\implies$ (3) $\implies$ (1) sind klar und gelten für jedes Ideal von S.
$f \in I \implies f = \sum_{\alpha\in A} p_\alpha \cdot x^\alpha$, wobei nur endlich viele $p_\alpha \neq 0$ sind. Der Koeffizient von Monom x^δ in f ist dann

$$\left[\!\left[x^\delta\right]\!\right] f = \sum_{\alpha\in A} \left[\!\left[x^{\delta-\alpha}\right]\!\right] p_\alpha;$$

und wenn dieser Koeffizient nicht Null ist (verschwindende Terme $= 0$ liegen sowieso in I), muß es mindestens ein δ geben mit $[\![x^{\delta-\alpha}]\!]\ p_\alpha \neq 0$: Dann ist aber $\delta - \alpha \in \mathbb{N}_0^n$, also $x^\alpha \mid x^\delta \implies x^\delta \in I$: Also ist jeder (nichtverschwindende) Term von f in I, und die Implikation (1) $\implies$ (2) ist gezeigt. □

KOROLLAR 2.7.5. *Ein Ideal $I \sqsubseteq S$ ist genau dann ein Monomideal, wenn für alle $f \in I$ schon jeder Term von f in I liegt.*

BEWEIS. Es ist nur mehr eine Richtung zu zeigen (die andere ist durch Lemma 2.7.4 schon erledigt).
Sei also I ein Ideal, bei dem aus $f \in I$ schon folgt: Jeder Term von f ist in I. Sei $A = \{\operatorname{mdeg} t\colon\ t \text{ ist ein Term von } f \text{ für ein } f \in I\}$: $A \subseteq \mathbb{N}_0^n$ ist also die Menge aller Exponenten von allen Monomen in I, und die Voraussetzung besagt: $x^A \subset I$. Dann ist A ein *Ordnungsideal* in $\mathbb{N}_0^n$, also nach Dicksons Lemma 2.5.1 von endlich vielen Elementen $\{\alpha_1, \ldots, \alpha_m\}$ erzeugt (als Ordnungsideal in $\mathbb{N}_0^n$ mit der Produktordnung). Sei $f \in I$ beliebig: Dann ist *jeder* Term von f ein Vielfaches eines Elements aus $\{x^{\alpha_1}, \ldots, x^{\alpha_m}\} \subseteq I$; f ist also eine $\mathbb{K}$–Linearkombination von Vielfachen aus $\{x^{\alpha_1}, \ldots, x^{\alpha_m}\}$. Also gilt $f \in ((x^{\alpha_1}, \ldots, x^{\alpha_m}))$ für alle $f \in I$, d.h., I ist das Monomideal $((x^{\alpha_1}, \ldots, x^{\alpha_m}))$. □

BEISPIEL 2.7.6. *Sei $I = ((x + y, y^2 - 1))$ in $\mathbb{Q}[x, y]$. Dann ist $x + y \in I$, aber $x \notin I$, $y \notin I$: Also ist I kein Monomideal.*

KOROLLAR 2.7.7. *Zwei Monomideale stimmen genau dann überein, wenn sie die gleichen Monome enthalten.*

2.7.2. Hilberts Basissatz. Sei ab nun eine Monomordnung $\preceq$ auf $\mathbb{N}_0^n$ festgelegt: Damit hat jedes $f \in S$ einen eindeutigen führenden Term $\mathrm{lt}(f)$.

DEFINITION 2.7.8. *Sei $P \subseteq S$. Wir definieren*

$$\mathrm{lt}(P) := \{\mathrm{lt}(f) : \ f \in P\},$$
$$\mathrm{lm}(P) := \{\mathrm{lm}(f) : \ f \in P\}.$$

Sei $I = (\!(f_1, \ldots, f_n)\!) \sqsubseteq S$ ein endlich erzeugtes Ideal: Dann gilt natürlich

$$(\!(\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_n))\!) \subseteq (\!(\mathrm{lt}(I))\!),$$

aber im allgemeinen *nicht* Gleichheit:

BEISPIEL 2.7.9. *Sei $I = (\!(f_1, f_2)\!)$ mit $f_1 = x^3 - 2xy$ und $f_2 = x^2y + x - 2y^2$ in S mit der Ordnung $\prec_{grlex}$. Dann ist $x^2 \in (\!(\mathrm{lt}(I))\!)$, denn*

$$x^2 = -y \cdot f_1 + x \cdot f_2 = x(x^2y + x - 2y^2) - y(x^3 - 2xy) \in I.$$

Aber $x^2 \notin (\!(\mathrm{lt}(f_1), \mathrm{lt}(f_2))\!) = (\!(x^3, x^2y)\!)$, denn x^2 ist nicht teilbar durch x^3 oder x^2y, sodaß $x^2 \notin (\!(x^3, x^2y)\!)$ wegen Lemma 2.7.3.

Jedoch gilt folgendes:

PROPOSITION 2.7.10. *Sei $I \subseteq S$ ein Ideal. Dann ist $(\!(\mathrm{lt}(I))\!)$ ein Monomideal, und es gibt $g_1, \ldots, g_s \in I$ mit $(\!(\mathrm{lt}(I))\!) = (\!(\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s))\!)$.*

BEWEIS. Klarerweise ist $(\!(\mathrm{lm}(I))\!)$ ein *Monomideal*: Da $\mathrm{lm}(g)$ und $\mathrm{lt}(g)$ sich nur durch eine Konstante ungleich Null unterscheiden, ist $(\!(\mathrm{lt}(I))\!) = (\!(\mathrm{lm}(I))\!)$ also auch ein Monomideal.
Nach Dicksons Lemma 2.5.1 ist $\mathrm{lm}(I)$ (interpretiert als Ordnungsideal in $\mathbb{N}_0^n$) endlich erzeugt: Es gibt also eine endliche Menge von Monomen

$$\{\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\} \subseteq \mathrm{lm}(I),$$

sodaß $\mathrm{lm}(I) \subseteq (\!(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_m))\!)$: Also folgt die Behauptung. □

Wir kombinieren dies mit folgender Beobachtung:

LEMMA 2.7.11. *Sei $I \sqsubseteq S$ ein Ideal und $P = \{f_1, \ldots, f_s\} \subseteq I$ eine* endliche *Menge mit $(\!(\mathrm{lt}(I))\!) = (\!(\mathrm{lt}(P))\!)$: Dann folgt $(\!(P)\!) = I$.*

BEWEIS. $(\!(P)\!) \subseteq I$ ist natürlich klar. Wir müssen also $I \subseteq (\!(P)\!)$ zeigen.
Sei $f \in I$ beliebig. Dann liefert der multivariate Divisionsalgorithmus

$$f = q_1 \cdot f_1 + \cdots + q_s \cdot f_s + r$$

mit $q_1, \ldots, q_s, r \in S$, und entweder $r = 0$, oder kein Term von r ist durch ein $\mathrm{lt}(f_i)$ teilbar. Dann ist aber

$$r = f - q_1 \cdot f_1 - \cdots - q_s \cdot f_s \in I,$$

und es folgt (natürlich)

$$\mathrm{lt}(r) \in \mathrm{lt}(I) \subseteq (\!(\mathrm{lt}(I))\!) = (\!(\mathrm{lt}(P))\!) = (\!(\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s))\!).$$

Nach Lemma 2.7.3 gilt dann aber $\mathrm{lt}(f_i) \mid \mathrm{lt}(r)$ für ein $i \in [s]$: Also ist $r = 0$, und wir erhalten $f \in (\!(f_1, \ldots, f_s)\!) = (\!(P)\!)$, also $I \subseteq (\!(P)\!)$. □

Damit erhalten wir (eine Variante von) *Hilberts Basissatz*:

KOROLLAR 2.7.12 (Hilberts Basissatz). *Jedes Ideal $I \subseteq S$ ist endlich erzeugt. (Das ist äquivalent dazu, daß $S = \mathbb{K}[x_1, x_2, \ldots, x_n]$ noethersch ist; siehe Proposition A.3.51.)*

BEWEIS. Das Nullideal $I = \{\mathbf{0}\} \sqsubseteq S$ wird durch $\mathbf{0}$ erzeugt: $I = ((\mathbf{0}))$.
Für alle anderen Ideale $I \sqsubseteq S$ betrachten wir das Ideal $((\mathrm{lt}(I)))$: Dies ist ein *endlich erzeugtes Monomideal* (Proposition 2.7.10), also $((\mathrm{lt}(I))) = ((\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)))$ für $\{f_1, \ldots, f_s\} \subseteq I$. Die Behauptung folgt also aus Lemma 2.7.11. □

2.7.3. Gröbnerbasen.

DEFINITION 2.7.13. *Sei $I \subseteq S$ eine Ideal. Eine endliche Teilmenge $G \subseteq I$ heißt* Basis *für I, wenn $I = ((G))$.*
Eine endliche Teilmenge $G \subseteq I$ heißt Gröbnerbasis *für I, falls $((\mathrm{lt}(G))) = ((\mathrm{lt}(I)))$ gilt.*

Gemäß Lemma 2.7.11 ist jede Gröbnerbasis tatsächlich eine Basis, und die bisherigen Überlegungen besagen:

KOROLLAR 2.7.14. *Jedes Ideal $I \subseteq S$ hat eine Gröbnerbasis.*

BEWEIS. Siehe den Beweis von Korollar 2.7.12! □

BEISPIEL 2.7.15. *Sei $I = ((f_1 = x^3 - 2xy, f_2 = x^2y + x - 2y^2))$ in $\mathbb{K}[x, y]$, mit der Monomordnung $\prec_{grlex}$. Dann ist $\{f_1, f_2\}$* keine *Gröbnerbasis (vergleiche Beispiel 2.7.9), die Menge*

$$G = \left\{f_1, f_2, x^2, 2xy, x - 2y^2\right\}$$

hingegen schon.

BEISPIEL 2.7.16. *Sei $\mathbb{K}$ ein Körper mit Charakteristik 0. Sei*

$$I = ((g_1 = x + z, g_2 = y - z)) \sqsubseteq \mathbb{K}[x, y, z]$$

mit der Monomordnung $\prec_{lex}$. Dann ist $G = \{g_1, g_2\}$ eine Gröbnerbasis von I. Um dies direkt aus der Definition abzuleiten, müssen wir zeigen, daß

$$((\mathrm{lt}(I))) \subseteq ((\mathrm{lt}(G))) = ((\mathrm{lt}(g_1), \mathrm{lt}(g_2))) = ((x, y))$$

gilt, d.h., daß der führende Term von jedem Polynom $f \in I \setminus 0$ in $((x, y))$ liegt. Wegen Lemma 2.7.3 ist das äquivalent damit, daß der führende Term von jedem $f \in I \setminus 0$ entweder durch x oder y teilbar ist. Angenommen, es gibt ein $f \in I \setminus 0$, für das $\mathrm{lt}(f)$ weder durch x noch durch y teilbar ist. Dann muß f ein Polynom in einer Variablen *(nämlich in z) sein (wegen $x \succ y \succ z$). Es muß auf allen Punkten in $V(I)$ verschwinden, wegen $f \in I$. Aber $(-t, t, t)$ ist ein Punkt in $V(I)$ für alle $t \in \mathbb{K}$, denn $g_1(-t, t, t) = g_2(-t, t, t) = 0$, daher müßte gelten $f(t) = 0$ für alle $t \in \mathbb{K}$. Wegen Charakteristik von $\mathbb{K} = 0$ bedeutet das aber: f hat unendlich viele verschiedene Nullstellen, also $f = 0$ (siehe Satz A.3.81): Widerspruch.*

Eine Gröbnerbasis hat insbesondere folgende Eigenschaft, die für unsere Zwecke wichtig ist:

PROPOSITION 2.7.17. *Sei $I \sqsubseteq S$ ein Ideal, $f \in S$ und $G = \{g_1, \dots, g_s\}$ eine Gröbnerbasis von I. Dann existiert ein* eindeutiges *$r \in S$, sodaß $f - r \in I$ und entweder $r = 0$ ist oder kein Term von r durch irgendeinen Term $\operatorname{lt}(g_1), \dots, \operatorname{lt}(g_s)$ teilbar ist.*
Insbesondere hängt der Rest r bei der multivariaten Division von f durch G also nicht *von der Reihenfolge der Elemente aus G ab. Wir schreiben daher*

$$r = f \pmod{G}.$$

BEWEIS. *Ein* solches r erhalten wir mit dem multivariaten Divisionsalgorithmus. Angenommen, es gäbe ein weiteres $r' \neq r$ mit derselben Eigenschaft. Dann ist

$$(f - r') - (f - r) = r - r' \in I \setminus \{\mathbf{0}\} = ((g_1, \dots, g_s)) \setminus \{\mathbf{0}\},$$

aber weil G eine Gröbnerbasis ist, gilt $\operatorname{lt}(r - r') \in ((\operatorname{lt}(I))) = ((\operatorname{lt}(G)))$, und nach Lemma 2.7.3 gilt $\operatorname{lt}(g_i) \mid \operatorname{lt}(r - r')$ für ein $i \in [s]$: Widerspruch.
Insbesondere kommt bei *jeder* multivariaten Division (mit beliebiger Reihenfolge der Elemente aus G) immer derselbe Rest r heraus. □

Wenn wir eine Gröbnerbasis G für ein Ideal I haben, können wir also durch multivariate Division durch G feststellen, ob ein Polynom f zu I gehört.

KOROLLAR 2.7.18. *Sei $I \sqsubseteq S$ ein Ideal und $G = \{g_1, \dots, g_s\}$ eine Gröbnerbasis von I. Für jedes Polynom $f \in S$ gilt*

$$f \in I \iff f = \mathbf{0} \pmod{G}.$$

BEWEIS. Aus $r = 0$ folgt natürlich $f \in I$. Ist umgekehrt $f = f + \mathbf{0} \in I$, dann ist also $r = \mathbf{0}$ der (nach Proposition 2.7.17 *eindeutige*) Rest von f bei Division durch G. □

Wir wissen zwar jetzt, daß jedes Ideal $I \sqsubseteq S$ eine Gröbnerbasis besitzt, aber es fehlt uns noch ein Verfahren, um eine solche Basis zu konstruieren.

2.7.4. Buchbergers Algorithmus. Betrachten wir irgendeine Basis F von I; $F = \{f_1, \dots, f_s\}$. Wenn *F keine* Gröbnerbasis ist, dann liegt das daran, daß "Polynomialkombinationen"

$$a_1 \cdot f_1 + \cdots + a_s \cdot f_s \text{ für } a_1, \dots, a_s \in S$$

existieren, deren führende Terme *nicht* in $((\operatorname{lt}(F)))$ liegen. Zum Beispiel könnten sich die führenden Terme in einer geeigneten Kombination

$$\lambda \cdot x^\alpha \cdot f_i - \mu \cdot x^\beta \cdot f_j$$

wegkürzen, sodaß nur kleinere Terme "überleben" und der neue führende Term nicht mehr durch irgendein $\operatorname{lt}(f_i)$ teilbar ist.

BEISPIEL 2.7.19. *Sei $I = ((f_1 = x^3 - 2xy, f_2 = x^2y + x - 2y^2))$ in S mit der Ordnung $\prec_{grlex}$ (wie in Beispiel 2.7.9). Dann ist*

$$-y \cdot f_1 + x \cdot f_2 = x^2$$

eine "Polynomialkombination", deren führender Term x^2 weder durch $\operatorname{lt}(f_1) = x^3$ noch durch $\operatorname{lt}(f_2) = x^2y$ teilbar ist.

Sei $F = (f_1, \ldots, f_m)$ in $S \setminus \{\mathbf{0}\}$: Wenn F eine Gröbnerbasis für $I = ((f_1, \ldots, f_m))$ ist, dann müßte es für jedes $f \in I$ eine Darstellung als "Polynomialkombination"

$$f = a_1 \cdot f_1 + \cdots a_m \cdot f_m,\ a_i \in S, \tag{2.4}$$

geben mit der *zusätzlichen* Eigenschaft

$$\mathrm{lt}\,(f_i) \mid \mathrm{lt}\,(f) \text{ für ein } i \in [m]$$

(nach Definition einer Gröbnerbasis gilt ja $((\mathrm{lt}\,(I))) = ((\mathrm{lt}\,(F)))$).

DEFINITION 2.7.20. *Sei $F = (f_1, \ldots, f_m)$ in $S \setminus \{\mathbf{0}\}$. Ein Polynom $f \in S$ heißt* nullreduziert *modulo F, falls es Polynome $a_1, \ldots, a_m \in S$ gibt mit*

$$f = a_1 \cdot f_1 + \cdots + a_m \cdot f_m,$$

wobei $a_i \neq \mathbf{0} \implies \mathrm{lm}\,(a_i \cdot f_i) \mid \mathrm{lm}\,(f)$ (woraus natürlich $\mathrm{lt}\,(f_i) \mid \mathrm{lt}\,(f)$ folgt). Wir schreiben dafür:

$$f \to_F 0.$$

BEMERKUNG 2.7.21. *$f \to_F 0$ bedeutet: $f \in ((F))$ ist durch eine "Polynomialkombination" darstellbar mit der* zusätzlichen Eigenschaft, *daß kein "Wegkürzen führender Terme" stattfindet. Aus den Eigenschaften des multivariaten Divisionsalgorithmus' folgt*

$$f = 0 \pmod F \implies f \to_F 0,$$

aber die Umkehrung gilt i.a. nicht: Sei z.B. $S = \mathbb{Q}[x, y]$ mit Monomordnung $\prec_{lex}$, dann ist das Polynom $f = x^3y + x^2y + x + y^2$ modulo $F = \left(x^2 + y, x^2y + 1\right)$ nullreduziert, denn es läßt sich darstellen als

$$f = x^3y + x^2y + x + y^2 = y \cdot \underbrace{\left(x^2 + y\right)}_{f_1} + x \cdot \underbrace{\left(x^2y + 1\right)}_{f_2}.$$

Aber multivariate Division liefert

$$f = (xy + y) \cdot f_1 + \mathbf{0} \cdot f_2 + \left(-xy^2 + x\right),$$

also $f = \left(-xy^2 + x\right) \pmod F$.

PROPOSITION 2.7.22. *Sei $F = (f_1, \ldots, f_m)$ in $S \setminus \{\mathbf{0}\}$, sei $I = ((f_1, \ldots, f_m))$.*
Wenn $f \to_F 0$ für alle $f \in I$ gilt, dann ist F eine Gröbnerbasis für I.
Wenn F eine Gröbnerbasis für I ist, dann ist

$$f \to_F 0 \iff f = 0 \pmod{f_1, \ldots, f_m} \text{ für alle } f \in I.$$

BEWEIS. Sei $f \in I$ beliebig. $f \to_F 0$ bedeutet, daß es (mindestens) ein f_i gibt, sodaß

$$\mathrm{lt}\,(f_i) \mid \mathrm{lt}\,(f) \implies \mathrm{lt}\,(f) \in ((\mathrm{lt}\,(F))),$$

also $((\mathrm{lt}\,(I))) \subseteq ((\mathrm{lt}\,(F)))$. Nach Definition heißt das aber: F ist eine Gröbnerbasis für I.
$f = 0 \pmod{f_1, \ldots, f_m} \implies f \to_F 0$ ergibt sich aus dem Divisionsalgorithmus; und wenn F eine Gröbnerbasis ist, dann folgt aus Proposition 2.7.17 ("Eindeutigkeit des Rests" modulo F)

$$f \to_F 0 \implies f = 0 \pmod F;$$

unabhängig von der Reihenfolge der f_i. □

Wir führen nun folgende Abkürzungen für die "Polynomialkombination" (2.4) ein:

$$\begin{aligned} \mathrm{lt}(f) &= a \cdot x^v, a \in \mathbb{K}^\star, && (2.5)\\ \mathrm{lt}(a_i) &= c_i \cdot x^{u_i}, c_i \in \mathbb{K}^\star, i \in [m], && (2.6)\\ \mathrm{lt}(f_i) &= d_i \cdot x^{v_i}, d_i \in \mathbb{K}^\star, i \in [m], && (2.7)\\ \delta &:= \max_\prec \{u_i + v_i : \ i \in [m]\}. \end{aligned}$$

Wegen $\mathrm{lt}(a_i \cdot f_i) = \mathrm{lt}(a_i) \cdot \mathrm{lt}(f_i)$ kann $v \succ v_i + u_i$ nicht für alle $i \in [m]$ gelten: Es ist also $v \preceq \delta$. O.B.d.A. können wir annehmen, daß

$$\delta = u_1 + v_1 = \cdots = u_r + v_r$$

für $r \in [m]$. Wenn $v = \delta$, dann gilt

$$\mathrm{lt}(f) = a \cdot x^v = \left(\underbrace{c_1 \cdot d_1 + \cdots + c_r \cdot d_r}_{\neq 0} \right) x^\delta,$$

woraus sofort

$$d_1 \cdot x^{v_1} = \mathrm{lt}(f_1) \mid \mathrm{lt}(f) = a \cdot x^v.$$

folgt. Ist hingegen $v \prec \delta$, dann entsteht dies durch "Wegkürzen" der Terme mit Multigrad δ auf der rechten Seite von (2.4); d.h.,

$$c_1 \cdot d_1 + \cdots + c_r \cdot d_r = 0,$$

und es folgt *nicht* zwingend $\mathrm{lt}(f_i) \mid \mathrm{lt}(f)$ für ein $i \in [m]$.
Sei

$$\begin{aligned} C &:= \mathrm{lt}(a_1) \cdot f_1 + \cdots + \mathrm{lt}(a_r) \cdot f_r \\ &= c_1 \cdot x^{u_1} \cdot f_1 + \cdots + c_r \cdot x^{u_r} \cdot f_r, \end{aligned}$$

dann können wir (2.4) schreiben als

$$\begin{aligned} f = C + (a_1 - \mathrm{lt}(a_1)) \cdot f_1 + \cdots + (a_r - \mathrm{lt}(a_r)) \cdot f_r \\ + a_{r+1} \cdot f_{r+1} + \cdots a_m \cdot f_m. \end{aligned} \quad (2.8)$$

Das heißt: f ist die Summe von C und weiteren Polynomen mit Multigrad $\prec \delta$.
Wenn $c_1 \cdot d_1 + \cdots c_r \cdot d_r \neq 0$, dann gibt es kein "Wegkürzen führender Terme" und $\mathrm{lt}(f)$ ist durch $\mathrm{lt}(f_i)$ teilbar für ein $i \in [r]$.
Wenn hingegen $c_1 \cdot d_1 + \cdots c_r \cdot d_r = 0$, dann setze $g_i := \frac{1}{d_i} \cdot x^{u_i} \cdot f_i$ und schreibe C "teleskopierend":

$$\begin{aligned} C &= c_1 \cdot d_1 \cdot g_1 + \cdots + c_r \cdot d_r \cdot g_r \\ &= c_1 \cdot d_1 \cdot (g_1 - g_2) + (c_1 \cdot d_1 + c_2 \cdot d_2) \cdot (g_2 - g_3) + \cdots \\ &\quad \cdots + (c_1 \cdot d_1 + \cdots + c_{r-1} \cdot d_{r-1}) \cdot (g_{r-1} - g_r) + \\ &\quad + \underbrace{(c_1 \cdot d_1 + \cdots + c_r \cdot d_r)}_{=0} \cdot g_r. \end{aligned} \quad (2.9)$$

C ist also eine "Polynomialkombination" der Polynome

$$g_i - g_j = \frac{1}{d_i} \cdot x^{u_i} \cdot f_i - \frac{1}{d_j} \cdot x^{u_j} \cdot f_j \text{ mit } i, j \in [r],$$

wobei $u_i + v_i = u_j + v_j$: Das heißt aber, die führenden Terme in $g_i - g_j$ kürzen einander weg, es ist also $\operatorname{mdeg}(g_i - g_j) \prec u_i + v_i = \delta$.

DEFINITION 2.7.23. *Seien x^α, x^β zwei Monome in S; für $\alpha = (\alpha_1, \ldots, \alpha_n)$ und $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}_0^n$. Dann ist auch*

$$\gamma = (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\})$$

in $\mathbb{N}_0^n$, und wir bezeichnen x^γ als kleinstes gemeinsames Vielfaches *von x^α und x^β:*

$$\operatorname{kgV}\left(x^\alpha, x^\beta\right) := x^\gamma.$$

Sei also $x^{w_{i,j}} = \operatorname{kgV}(x^{v_i}, x^{v_j})$: Dann ist $\xi := u_i + v_i - w_{i,j} \in \mathbb{N}_0^n$ und

$$g_i - g_j = x^\xi \cdot \left(\frac{x^{w_{i,j}} \cdot f_i}{d_i \cdot x^{v_i}} - \frac{x^{w_{i,j}} \cdot f_j}{d_j \cdot x^{v_j}} \right),$$

und die führenden Terme in

$$\frac{x^{w_{i,j}} \cdot f_i}{d_i \cdot x^{v_i}} - \frac{x^{w_{i,j}} \cdot f_j}{d_j \cdot x^{v_j}}$$

kürzen einander weg.

DEFINITION 2.7.24. *Seien $f, g \in S$, $f, g \neq \mathbf{0}$, und sei $x^\gamma = \operatorname{kgV}(\operatorname{lm}(f), \operatorname{lm}(g))$. Dann ist das* S–Polynom *von f und g definiert als*

$$S(f, g) := \frac{x^\gamma}{\operatorname{lt}(f)} \cdot f - \frac{x^\gamma}{\operatorname{lt}(g)} \cdot g.$$

Offensichtlich ist $S(f, g) \in (\!(f, g)\!)$, und $S(f, g) = -S(g, f)$.

BEISPIEL 2.7.25. *Seien $f, g \in \mathbb{Q}[x, y]$ mit der Monomordnung $\prec_{grlex}$,*

$$f = x^3y^2 - x^2y^3 + x,$$
$$g = 3x^4y + y^2.$$

Dann ist $\gamma = (4, 2)$ (gemäß Definition 2.7.24) und

$$\begin{aligned} S(f, g) &= \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g \\ &= x \cdot f - \frac{1}{3}y \cdot g \\ &= -x^3y^3 + x^2 - \frac{1}{3}y^3. \end{aligned}$$

LEMMA 2.7.26. *Sei $F = (f_1, \ldots, f_m)$ in $S \setminus \{\mathbf{0}\}$, und sei $I = (\!(f_1, \ldots, f_m)\!)$. Wenn $S(f_i, f_j) \to_F 0$ für alle $i \neq j \in [m]$ gilt, dann folgt $f \to_F 0$ für alle $f \in I$.*

BEWEIS. Sei $f \in I$. Angenommen, wir haben für f eine "Polynomialkombination" wie in (2.4), in der sich führende Terme wegkürzen. Aus den Überlegungen zu (2.4) und (2.9) ergibt sich (unter Verwendung der dort eingeführten Notation und der Definition des S–Polynoms):

$$C = b_1 \cdot x^{\xi_1} \cdot S(f_1, f_2) + \cdots + b_{r-1} \cdot x^{\xi_{r-1}} \cdot S(f_{r-1}, f_r) \tag{2.10}$$

mit $b_i \in \mathbb{K}$ und $\operatorname{mdeg}\left(x^{\xi_i} \cdot S(f_i, f_{i+1})\right) \prec \delta$.
Aus $S(f_i, f_j) \to_F 0$ folgt

$$S(f_i, f_j) = e_1^{i,j} \cdot f_1 + \cdots e_m^{i,j} \cdot f_m$$

mit $e_k^{i,j} \in S$, wobei $\operatorname{lt}\left(e_k^{i,j} \cdot f_k\right) \mid \operatorname{lt} S(f_i, f_j)$ gilt, also

$$\operatorname{lm}\left(e_k^{i,j} \cdot f_k\right) \preceq \operatorname{lm}\left(S(f_i, f_j)\right) \prec x^\delta \text{ für alle } k \in [m].$$

Wenn wir diese Darstellung in (2.10) und den dadurch erhaltenen Ausdruck für C in (2.8) einsetzen, erhalten wir:

$$\begin{aligned}
f &= b_1 \cdot x^{\xi_1}\left(e_1^{1,2} \cdot f_1 + \cdots e_m^{1,2} \cdot f_m\right) + \cdots \\
&\quad + b_{r-1} \cdot x^{\xi_{r-1}}\left(e_1^{r-1,r} \cdot f_1 + \cdots e_m^{r-1,r} \cdot f_m\right) \\
&\quad + (a_1 - \operatorname{lt}(a_1)) \cdot f_1 + \cdots + (a_r - \operatorname{lt}(a_r)) \cdot f_r \\
&\quad + a_{r+1} \cdot f_{r+1} + \cdots + a_m \cdot f_m \\
&= \left(b_1 \cdot x^{\xi_1} \cdot e_1^{1,2} + \cdots + b_{r-1} \cdot x^{\xi_{r-1}} \cdot e_1^{r-1,r} + (a_1 - \operatorname{lt}(a_1))\right) \cdot f_1 + \cdots \\
&\quad + \left(b_1 \cdot x^{\xi_1} \cdot e_m^{1,2} + \cdots + b_{r-1} \cdot x^{\xi_{r-1}} \cdot e_m^{r-1,r} + a_m\right) \cdot f_m.
\end{aligned}$$

Das heißt, es gibt eine *andere* Darstellung von f als "Polynomialkombination"

$$f = h_1 \cdot f_1 + \cdots + h_m \cdot f_m$$

mit $\max_\prec \{\operatorname{lm}(h_i \cdot f_i) : \ i \in [m]\} \prec \delta$.
Wenn sich in dieser Darstellung *wieder* führende Termen wegkürzen, dann wiederholen wir die obige Konstruktion: Da $\prec$ eine *Wohlordnung* ist, muß dies nach endlich vielen Schritten abbrechen, und wir erhalten eine Darstellung

$$f = b_1 \cdot f_1 + \cdots + b_m \cdot f_m,$$

in der der maximale Multigrad (in bezug auf $\prec$) der Summanden auf der rechten Seite gleich $\operatorname{mdeg}(f)$ ist, also $f \to_F 0$. □

Damit erhalten wir:

SATZ 2.7.27 (Buchbergers Kriterium). *Eine endliche Menge $F = \{f_1, \ldots, f_m\} \subseteq S \setminus \{\mathbf{0}\}$ ist genau dann eine Gröbnerbasis für das Ideal $I = (\!(F)\!)$, wenn*

$$S(f_i, f_j) \to_F 0 \textit{ für alle } i \neq j \in [m].$$

Das ist äquivalent mit

$$S(f_i, f_j) = 0 \pmod F \textit{ für alle } i \neq j \in [m].$$

BEWEIS. Die erste Aussage folgt aus Lemma 2.7.26 und Proposition 2.7.22.
Die zweite Aussage ergibt sich aus Proposition 2.7.22: Aus $S\left(f_i, f_j\right) = 0 \pmod F$ folgt ja (immer) $S\left(f_i, f_j\right) \to_F 0$, und wenn F eine Gröbnerbasis ist, dann gilt auch die Umkehrung. □

Buchbergers Algorithmus ist nun einfach:

```
/* Sei F = (f_1, ..., f_m) eine Basis von I = ((F)) */
G ← F
while ∃ (i < j) : S(f_i, f_j) ≠ 0 (mod G) do
  G ← G ∪ S(f_i, f_j)
end while
return G
```

SATZ 2.7.28. *Buchbergers Algorithmus bricht nach endlich vielen Schritten ab (und liefert dann eine Gröbnerbasis).*

BEWEIS. Sei $(G_0 = F, G_1, \dots)$ die (möglicherweise nicht abbrechende!) Folge der Basen für das Ideal I, die im Wiederholungsschritt von Buchbergers Algorithmus erzeugt werden. Dann ist

$$(((\operatorname{lt} G_0)), ((\operatorname{lt} G_1)), \dots)$$

eine *aufsteigende Kette* von *Monomidealen* in $S = \mathbb{K}[x_1, \dots, x_n]$, denn $G_{i+1} = G_i \cup \{r\}$, wobei $S\left(f_i, f_j\right) \equiv r \neq \mathbf{0} \pmod{G_i}$ (Rest aus Divisionsalgorithmus!) ist und (daher!) $\operatorname{lt}(r) \notin ((\operatorname{lt}(G_i)))$ gilt.
Nach Hilberts Basissatz (siehe Korollar 2.7.12) ist aber $\mathbb{K}[x_1, \dots, x_n]$ ein *noetherscher* Ring, d.h., diese aufsteigende Kette von Idealen wird *stationär*. □

BEISPIEL 2.7.29. *Sei $F = (f_1, f_2) = \left(x^3 - 2xy, x^2y - 2y^2 + x\right)$ in $\mathbb{K}[x, y]$ mit der Monomordnung $\prec_{grlex}$.*
Es ist $S(f_1, f_2) = -x^2 = 0 \cdot f_1 + 0 \cdot f_2 + \left(-x^2\right)$, also

$$S(f_1, f_2) \neq 0 \pmod{f_1, f_2}.$$

Sei also $f_3 = -x^2$ und betrachten wir ab nun $G = (f_1, f_2, f_3)$. Nun ist

$$S(f_1, f_2) = 0 \pmod{f_1, f_2, f_3},$$

aber

$$S(f_1, f_3) = -2xy \neq 0 \pmod{f_1, f_2, f_3}.$$

und

$$S(f_2, f_3) = -2y^2 + x \neq 0 \pmod{f_1, f_2, f_3}.$$

Sei also $f_4 = -2xy$ und $f_5 = -2y^2 + x$, und betrachten wir ab nun $G = (f_1, \cdots, f_5)$: Wie man leicht nachprüft, bricht Buchbergers Algorithmus nun ab; also ist

$$G = \left\{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\right\}$$

die gesuchte Gröbnerbasis für $((F))$.

BEMERKUNG 2.7.30. *Die Berechnung einer Gröbnerbasis "in der Praxis" ist ein hartes Problem im Sinne der Komplexitätstheorie: Die Laufzeit der besten bekannten Algorithmen ist (im worst case)* exponentiell.

2.7.5. Reduzierte Gröbnerbasen. Eine Gröbnerbasis für ein Ideal ist nicht eindeutig: Insbesondere kann man eine Gröbnerbasis "vergrößern", indem man ein Polynom aus dem Ideal hinzufügt, das nicht zur Basis gehört.

LEMMA 2.7.31. *Sei G eine Gröbnerbasis für das Ideal $I \subseteq S$. Sei $p \in G$ ein Polynom mit* $\operatorname{lt}(p) \in ((\operatorname{lt}(G \setminus \{p\})))$. *Dann ist $G \setminus \{p\}$ ebenfalls eine Gröbnerbasis für I.*

BEWEIS. Nach Voraussetzung ist

$$((\operatorname{lt}(G \setminus \{p\}))) = ((\operatorname{lt}(G))) = ((\operatorname{lt} I)).$$

Nach Definition ist dann aber $G \setminus \{p\}$ eine Gröbnerbasis für I. □

DEFINITION 2.7.32. *Eine Gröbnerbasis G für ein Ideal $I \sqsubseteq S$ heißt* minimal, *falls*

(1) $\operatorname{lc}(p) = 1$ *für alle $p \in G$.*
(2) $\operatorname{lt}(p) \notin ((\operatorname{lt}(G \setminus \{p\})))$ *für alle $p \in G$.*

BEISPIEL 2.7.33. *Sei $I = ((x^3 - 2xy, x^2y - 2y^2 + x)) \sqsubseteq \mathbb{K}[x, y]$ mit Monomordnung $\prec_{grlex}$. Dann ist die Gröbnerbasis*

$$G = \left\{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\right\}$$

nicht minimal, aber

$$G' = \left\{x^2, xy, y^2 - \frac{1}{2}x\right\}$$

schon: G' entsteht aus G durch Normieren und Entfernen "überflüssiger" Elemente im Sinne von Lemma 2.7.31.
Eine minimale Gröbnerbasis muß nicht eindeutig sein: Für jedes $\lambda \in \mathbb{K}$ ist

$$G_\lambda = \left\{x^2 + \lambda xy, xy, y^2 - \frac{1}{2}x\right\}$$

eine minimale Gröbnerbasis von I.

DEFINITION 2.7.34. *Eine Gröbnerbasis G für ein Ideal $I \subseteq S$ heißt* reduziert, *falls*

(1) $\operatorname{lc}(p) = 1$ *für alle $p \in G$.*
(2) *Für alle $p \in G$ liegt* kein Term *von p in* $((\operatorname{lt} G \setminus \{p\}))$.

Natürlich ist eine reduzierte Gröbnerbasis auch minimal.

PROPOSITION 2.7.35. *Sei $I \sqsubseteq S$ ein von Null verschiedenes Ideal. Dann besitzt I eine eindeutige reduzierte Gröbnerbasis.*

BEWEIS. Jedes Ideal $I \neq \{\mathbf{0}\}$ hat eine Gröbnerbasis H nach Korollar 2.7.14, und nach Lemma 2.7.31 ist klar, daß man daraus eine minimale Gröbnerbasis $G = \{f_1, \ldots, f_m\}$ gewinnen kann. Wir konstruieren daraus eine neue Basis, indem wir Elemente der Basis sukzessive durch ihre Reste bei Division durch die übrigen Basiselemente ersetzen, also:

$$\begin{aligned}
f_1 &\mapsto f_1', \text{ wobei } f_1' = f_1 \pmod{f_2, f_3, \ldots, f_m},\\
f_2 &\mapsto f_2', \text{ wobei } f_2' = f_2 \pmod{f_1', f_3, \ldots, f_m},\\
&\vdots\\
f_m &\mapsto f_m', \text{ wobei } f_m' = f_m \pmod{f_1', f_2', \ldots, f_{m-1}'}.
\end{aligned}$$

Es ist klar: $G' = \{f_1', \ldots, f_m'\}$ ist eine Basis von I. Da G *minimale Gröbnerbasis* war, ist $\mathrm{lt}\left(f_i'\right) = \mathrm{lt}\left(f_i\right)$ (im Divisionsalgorithmus "wandert" $\mathrm{lt}\left(f_i\right)$ sofort in den Rest, weil kein $\mathrm{lt}\left(f_j\right)$ für $j \neq i$ ein Teiler ist), also ist $\mathrm{lt}\left(G\right) = \mathrm{lt}\left(G'\right)$, und da G eine Gröbnerbasis war, ist auch G' eine (nach Definition). Überdies ist kein Term von f_j' durch ein $\mathrm{lt}\left(f_j'\right) = \mathrm{lt}\left(f_j\right)$ teilbar für $i \neq j$ (siehe Divisionsalgorithmus Proposition 2.6.1), also ist G' tatsächlich reduziert.

Seien $\{f_1, \ldots, f_m\}$ und $\{g_1, \ldots, g_{m'}\}$ zwei reduzierte Gröbnerbasen: Da $g_1 \in I$, gibt es ein f_j mit $\mathrm{lt}\left(f_j\right) \mid \mathrm{lt}\left(g_1\right)$, und da $f_j \in I$, gibt es ein g_i mit $\mathrm{lt}\left(g_i\right) \mid \mathrm{lt}\left(f_j\right)$. Daraus folgt $\mathrm{lt}\left(g_i\right) \mid \mathrm{lt}\left(g_1\right)$, also $i = 1$. $\mathrm{lt}\left(g_1\right)$ und $\mathrm{lt}\left(f_j\right)$ unterscheiden sich also nur um eine Einheit, und weil beide Koeffizient 1 haben, sind sie gleich.

Daraus folgt: $\{\mathrm{lt}\left(g_1\right), \ldots, \mathrm{lt}\left(g_{m'}\right)\}$ ist eine Permutation von $\{\mathrm{lt}\left(f_1\right), \ldots, \mathrm{lt}\left(f_m\right)\}$, insbesondere also $m = m'$. O.B.d.A. können wir also annehmen: $\mathrm{lt}\left(g_i\right) = \mathrm{lt}\left(f_i\right)$ für $i \in [m]$.

Es gilt dann aber sogar $g_i = f_i$: Denn in der Differenz $f_i - g_i$ fallen die führenden Terme weg, und nach Definition einer reduzierten Gröbnerbasis ist keiner der übrigen Terme durch einen der führenden Terme aus

$$\{\mathrm{lt}\left(f_1\right), \ldots, \mathrm{lt}\, f_m\} \setminus \{\mathrm{lt}\left(f_i\right)\} = \{\mathrm{lt}\left(g_1\right), \ldots, \mathrm{lt}\, g_m\} \setminus \{\mathrm{lt}\left(g_i\right)\}$$

teilbar, und (natürlich) auch nicht durch $\mathrm{lt}\left(f_i\right)$; also erscheint $f_i - g_i$ als *Rest* bezüglich der multivariaten Division durch $(f_1, \ldots, f_m)$:

$$f_i - g_i = \sum_k \mathbf{0} \cdot f_k + (f_i - g_i) \text{ (Divisionsalgorithmus).}$$

Da $f_i - g_i \in I$, gilt aber

$$f_i - g_i \equiv 0 \pmod{f_1, \ldots, f_m},$$

also muß dieser (nach Proposition 2.7.17 eindeutige!) Rest Null sein, d.h.: $f_i = g_i$. □

BEISPIEL 2.7.36. *Wir bestimmen die reduzierte Gröbnerbasis von* $((f_1, f_2, f_3)) = ((x^2y - 1, x + yz, y^2 - z))$ *in bezug auf die Ordnung* $\prec_{lex}$.
Als erstes bestimmen wir $f_1 = r \pmod{f_2, f_3}$*:*

$$x^2y - 1 = \left(xy - yz^2\right) \cdot (x + yz) + \left(yz^2\right) \cdot \left(y^2 - z\right) + yz^3 - 1$$

Das S–Polynom

$$S\left(y^2 - z, yz^3 - 1\right) = y - z^4$$

ist nicht Null, unser "Gröbnerbasis-Zwischenstand" ist also:

$$\left(x + yz, y^2 - z, yz^3 - 1, y - z^4\right).$$

Wir reduzieren

$$y^2 - z = \left(y + z^4\right) \cdot \left(y - z^4\right) + z^8 - z$$
$$yz^3 - 1 = z^3\left(y - z^4\right) + z^7 - 1$$

und erhalten als neuen Zwischenstand:

$$\left(x + yz, y - z^4, z^7 - 1\right).$$

Noch einmal reduzieren liefert

$$x + yz = z\left(y - z^4\right) + x + z^5,$$

und nun haben wir tatsächlich die reduzierte Gröbnerbasis gefunden:

$$\left(x + z^5, y - z^4, z^7 - 1\right).$$

2.7.6. Gröbnerbasen und Systeme von Polynomgleichungen. Die Lösungsmenge eines Systems von n Polynomgleichungen

$$f_1 = 0, \ldots, f_n = 0$$

ist gleich der Nullstellenmenge $V(I)$ des von diesen Polynomen erzeugten Ideals $I = (\!(f_1, \ldots, f_n)\!)$. Sei $g_1, \ldots, g_m$ eine Gröbnerbasis von I, dann ist das Gleichungssystem

$$g_1 = 0, \ldots, g_m = 0$$

also äquivalent zum obigen.
Angenommen, ein System von Polynomgleichungen in den Variablen $\{x_1, \ldots, x_s\}$ zerfiele in nichtleere "Teilsysteme" von Polynomgleichungen

- in der Variable x_1,
- in den Variablen x_1, x_2,
- ...
- in den Variablen $x_1, \ldots, x_{n-1}$,
- in den Variablen $x_1, \ldots, x_{n-1}, x_n$.

Dann könnte man (ganz analog zur *Gauß–Elimination* für lineare Gleichungssysteme) einfach sukzessive Polynomgleichungen in nur *einer* Variablen lösen und die erhalten Lösungen dann in das nächste "Teilsystem" einsetzen.
Ein solches "zerfallendes" System von Polynomgleichungen würden wir erhalten, wenn wir für das erzeugte Ideal I folgende Durchschnitte bestimmen könnten:

- $I \cap \mathbb{K}[x_1]$,
- $I \cap \mathbb{K}[x_1, x_2]$,
- ...,
- $I \cap \mathbb{K}[x_1, \ldots, x_{s-1}]$,
- $I \cap \mathbb{K}[x_1, \ldots, x_{s-1}, x_s]$.

SATZ 2.7.37. *Sei $G = \{f_1, \ldots, f_m\}$ eine Gröbnerbasis für I in bezug auf die Monomordnung $\prec_{lex}$, wobei die Variablenordnung $x_n > x_{n-1} > \cdots > x_1$ ist. Dann ist $G \cap \mathbb{K}[x_1, \ldots, x_i]$ eine Gröbnerbasis von $I \cap \mathbb{K}[x_1, \ldots, x_i]$ für $i \in [n]$.*

BEWEIS. Sei $G' := G \cap \mathbb{K}[x_1, \ldots, x_i]$ und $f \in I' := I \cap \mathbb{K}[x_1, \ldots, x_i]$. Multivariate Division liefert

$$f = a_1 \cdot f_1 + \cdots + a_m \cdot f_m,$$

wobei

$$\operatorname{lt} a_j \cdot f_j \preceq \operatorname{lt} f$$

wann immer $a_j \cdot f_j \neq 0$ (siehe Proposition 2.6.1). Es ist dann aber jedes solche $f_j \in \mathbb{K}[x_1, \ldots, x_i]$ wegen

$$\operatorname{lt} f_j \preceq \operatorname{lt} f \prec x_{i+1},$$

also ist G' eine *Basis* für I'.
Diese Überlegung zeigt auch, daß für $f \in I'$ beliebig gilt:

$$f = 0 \pmod{G} \implies f = 0 \pmod{G'}.$$

Das gilt dann insbesondere für alle S–Polynome, die man aus den Polynomen von G' bilden kann: Nach Buchbergers Kriterium Satz 2.7.27 ist G' also eine *Gröbnerbasis*. □

BEISPIEL 2.7.38. *Für das Gleichungssystem*

$$x^2y - 1 = 0, x + yz = 0, y^2 - z = 0$$

haben wir schon im vorigen Beispiel die reduzierte Gröbnerbasis bestimmt: Das Gleichungssystem ist äquivalent zu

$$x + z^5 = 0, y - z^4 = 0, z^7 - 1 = 0,$$

das wir nun durch "Elimination" leicht lösen können. Aus der letzten Gleichung sehen wir

$$z = \mathrm{e}^{\mathrm{i}\frac{2\pi}{7}k} \text{ für } k = 0, \ldots, 6.$$

Durch Einsetzen in die beiden anderen Gleichungen erhalten wir sofort die Lösungsmenge

$$\left\{ \left(-\mathrm{e}^{5\mathrm{i}\frac{2\pi}{7}k}, \mathrm{e}^{4\mathrm{i}\frac{2\pi}{7}k}, \mathrm{e}^{\mathrm{i}\frac{2\pi}{7}k} \right) : \ k = 0, 1, \ldots, 6 \right\}.$$

KAPITEL 3

Endliche Körper und Codierungstheorie

3.1. Endliche Körper

3.1.1. Einheitswurzeln und zyklotomische Polynome.

DEFINITION 3.1.1. *Sei $n \in \mathbb{N}$: Eine komplexe Zahl ζ heißt n–te* Einheitswurzel, *falls $\zeta^n = 1$. In Polarkoordinaten ist $\zeta = r\mathrm{e}^{\mathrm{i}\vartheta}$ mit $r = 1$ und $\vartheta = \frac{m \cdot 2\pi}{n}$ für ein m in $\{0, 1, \ldots, n-1\}$. Gilt zusätzlich $\zeta^k \neq 1$ für $1 \leq k < n$, so heißt ζ* primitive *n–te Einheitswurzel.*

LEMMA 3.1.2. *ζ ist primitive n–te Einheitswurzel genau dann, wenn $\zeta = \mathrm{e}^{\frac{2m\pi\mathrm{i}}{n}}$ mit $1 \leq m \leq n$ und $\mathrm{ggT}(m, n) = 1$. Wenn ζ eine primitive n–te Einheitswurzel ist und $\zeta^k = 1$ gilt, so folgt $n \mid k$.*

BEWEIS. Sei $\zeta = \mathrm{e}^{\frac{m \cdot 2\pi\mathrm{i}}{n}}$, und sei $d = \mathrm{ggT}(m, n)$. $\zeta^k = 1$ gilt genau dann wenn

$$\frac{k \cdot m \cdot 2\pi}{n} = \lambda \cdot 2\pi \text{ für ein } \lambda \in \mathbb{Z}.$$

Das ist gleichbedeutend damit, daß $(k \cdot m)$ ein *gemeinsames* Vielfaches von n und m ist, also

$$\mathrm{kgV}(m, n) \mid (k \cdot m).$$

Das *kleinste* $k_0 \in \mathbb{N}$, das dies erfüllt, ist $k_0 = \frac{n}{d}$ (denn dann ist $(k_0 \cdot m) = \frac{m \cdot n}{\mathrm{ggT}(m,n)} = \mathrm{kgV}(m, n)$). ζ ist *primitive* Einheitswurzel genau dann, wenn dieses kleinste $k_0 \in \mathbb{N}$ gleich n ist, also $d = 1$.

Wenn $d = 1$, dann ist $\mathrm{kgV}(m, n) = (m \cdot n)$, und aus $(m \cdot n) \mid (k \cdot m)$ folgt $n \mid k$. □

BEMERKUNG 3.1.3. *Die n–ten Einheitswurzeln bilden eine (zyklische) Gruppe $C_n \simeq \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.*

DEFINITION 3.1.4. *Sei $n \in \mathbb{N}$: Das n–te* zyklotomische Polynom $\Phi_n(x) \in \mathbb{C}[x]$ *ist gegeben als*

$$\Phi_n(x) := \prod_{\substack{1 \leq m \leq n \\ \mathrm{ggT}(m,n)=1}} \left(x - \mathrm{e}^{\frac{2m\pi\mathrm{i}}{n}}\right).$$

Es gilt offensichtlich: Φ_n ist normiert *(d.h., hat führenden Koeffizienten 1) und hat* Grad $\varphi(n)$.

BEMERKUNG 3.1.5. *Die ersten 10 zyklotomischen Polynome sind:*

$x-1$	x^2-x+1
$x+1$	$x^6+x^5+x^4+x^3+x^2+x+1$
x^2+x+1	x^4+1
x^2+1	x^6+x^3+1
$x^4+x^3+x^2+x+1$	$x^4-x^3+x^2-x+1$

Die Koeffizienten der zyklotomischen Polynom sind *nicht* immer ± 1 (zum Beispiel ist $\Phi_{105}(x) = x^{48}+x^{47}+\cdots-2x^7-x^6-x^5+x^2+x+1$), jedoch sind sie immer ganzzahlig:

PROPOSITION 3.1.6. *Für alle $n \in \mathbb{N}$ gilt:*

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

$$\Phi_n(x) \in \mathbb{Z}[x] \tag{ii}$$

BEWEIS. Wir zeigen zuerst (i): Man sieht sofort, daß die Polynome auf der linken und auf der rechten Seite der Gleichung beide *normiert* sind.
Wir betrachten nun die n–ten Einheitswurzeln als Elemente der zyklischen Gruppe $\mathbb{Z}_n$. Dann hat jede Einheitswurzel eine *Ordnung* d mit $d|n$ und es gilt:

- Eine n–te Einheitswurzel der Ordnung d ist (natürlich) *primitive* d–te Einheitswurzel,
- Eine *primitive* d–te Einheitswurzel mit $d \mid n$ ist (natürlich) eine n–te Einheitswurzel.

Daher haben die Polynome auf der linken und auf der rechten Seite der Gleichung auch genau dieselben Nullstellen; sie sind also gleich.
Nun zu (ii): Wir beweisen die Behauptung mit Induktion nach n. Der Induktionsanfang ist klar: $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Für den Induktionsschritt sei nun $n > 1$. Wir definieren $f := \prod_{\substack{d<n \\ d|n}} \Phi_d$, dann ist f nach Induktionsvoraussetzung ein normiertes Polynom in $\mathbb{Z}[x]$. Mit Polynomdivision (in $\mathbb{Z}[x]$!) erhalten wir

$$x^n - 1 = g \cdot f + r$$

mit $g, r \in \mathbb{Z}[x]$ und $r \equiv 0$ oder $\deg r < \deg f$. Nach (i) gilt aber (in $\mathbb{C}[x]$!)

$$x^n - 1 = \Phi_n \cdot f,$$

und durch Subtraktion dieser Gleichungen ergibt sich (in $\mathbb{C}[x]$!) die Polynomidentität

$$0 = (g - \Phi_n) \cdot f + r,$$

die nur richtig sein kann für $g = \Phi_n$ und $r = 0$. □

Wir verallgemeinern nun das Konzept der primitiven Einheitswurzeln vom Körper $\mathbb{C}$ auf eine allgemeinere Klasse von Ringen.

DEFINITION 3.1.7. *Sei R ein kommutativer Ring mit $\mathbf{1}$, sei $n \in \mathbb{N}$. $\alpha \in R$ heißt primitive n–te Einheitswurzel, falls $\alpha^n = \mathbf{1}$, aber $\alpha^k \neq \mathbf{1}$ für $k = 1, 2, \ldots, n-1$.*

LEMMA 3.1.8. *Sei R ein Integritätsbereich*[1] *und $\alpha \in R$. Ist $\Phi_n(\alpha) = \mathbf{0}$ und α* keine *mehrfache Nullstelle von $x^n - 1$ in $R[x]$, dann ist α eine primitive n–te Einheitswurzel in R.*

BEWEIS. Alles folgt aus der Tatsache, dass die Faktorisierung

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

aus Proposition 3.1.6 auch in $R[x]$ gültig ist[2]. Denn natürlich folgt dann aus $\Phi_n(\alpha) = \mathbf{0}$ sofort $\alpha^n - \mathbf{1} = \mathbf{0}$. Wenn α eine *primitive* d–te Einheitswurzel für ein $d < n$ ist, muß $d \mid n$ gelten[3] und es folgt:

$$x^d - 1 = \prod_{e|d} \Phi_e(x) \text{ hat } \textit{auch} \text{ Nullstelle } \alpha.$$

Da R nullteilerfrei ist, muß es ein e' mit $e' \mid d$ geben, sodaß $\Phi_{e'}(\alpha) = \mathbf{0}$: Da $e \mid d \mid n$, ist α dann aber eine mehrfache (mindestens doppelte) Nullstelle ($\Phi_n(\alpha) = \Phi_{e'}(\alpha) = \mathbf{0}$ mit $e' < n$) von $x^n - 1$. □

SATZ 3.1.9. *Sei $\mathbb{K}$ ein Körper und $G \subseteq \mathbb{K}^\star$ eine* endliche *Untergruppe der multiplikativen Gruppe $\mathbb{K}^\star := (\mathbb{K} \setminus \{\mathbf{0}\}, \cdot)$. Dann ist G zyklisch.*

BEWEIS. Sei n die Ordnung der Gruppe G: $n = |G|$. Betrachte das Polynom

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \in \mathbb{K}[x].$$

Die Nullstellen der linken Seite sind *genau* die Elemente $\alpha \in G$, da $\alpha^n = \alpha^{|G|} = \mathbf{1}$ für alle $\alpha \in G$ gilt[4] und es nach Satz A.3.81 keine weiteren Nullstellen geben kann. Alle diese Nullstellen sind *einfach*, und somit hat insbesondere $\Phi_n(x)$ genau $\varphi(n) > 0$ Nullstellen. Diese sind nach Lemma 3.1.8 primitive n–te Einheitswurzeln in K und somit Erzeuger von G. □

BEMERKUNG 3.1.10. *Als (sehr einfache) Anwendung dieses Satzes erhält man, daß für $p \in \mathbb{P}$ die multiplikative Gruppe $\mathbb{F}_p^\star$ zyklisch ist, mit $\varphi(p-1)$ Erzeugern.*

3.1.2. Endliche Körper. Aus der Zahlentheorie wissen wir, daß für $p \in \mathbb{P}$ $\mathbb{F}_p := \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper ist. Wir wollen nun allgemeinere endliche Körper untersuchen.

LEMMA 3.1.11. *Sei $\mathbb{K}$ ein endlicher Körper. Dann gibt es eine Primzahl $p \in \mathbb{P}$ und eine natürliche Zahl $n \in \mathbb{N}$ sowie ein irreduzibles Polynom $f \in \mathbb{F}_p[x]$ vom Grad n, sodaß*

$$\mathbb{K} \simeq \mathbb{F}_p[x] / ((f)).$$

[1] Also ein kommutativer Ring mit Eins, der keine Nullteiler besitzt.

[2] Denn R enthält ein homomorphes Bild von $\mathbb{Z}$, siehe Definition A.3.61.

[3] Denn sonst wäre $n = d \cdot k + r$ (Division mit Rest in $\mathbb{Z}$) mit $0 < r < d$ und $\alpha^r = \alpha^{n-d\cdot k} = \underbrace{\alpha^n}_{\mathbf{1}} \underbrace{\left(\alpha^d\right)^{-k}}_{\mathbf{1}} = \mathbf{1}$, im Widerspruch zur Annahme (α primitive d–te Einheitswurzel).

[4] Die Ordnung eines Elements einer endlichen Gruppe ist stets ein Teiler der Gruppenordnung nach dem Satz von Lagrange (Satz A.3.12 im Anhang).

Insbesondere gilt $|\mathbb{K}| = p^n$.

BEWEIS. Betrachte den Homomorphismus $\kappa : \mathbb{Z} \to \mathbb{K}$, der 1 auf $\mathbf{1}_K$ abbildet, also:

$$\kappa(n) = \kappa\left(\underbrace{1+1+\cdots+1}_{n\times 1}\right) = \kappa(\mathbf{1}) + \kappa(\mathbf{1}) + \cdots + \kappa(\mathbf{1}) =: n\mathbf{1}_k$$

Da $|\mathbb{K}| < \infty$, ist die Abbildung κ nicht injektiv, und für den Homomorphismus zwischen den additiven Gruppen (also $\kappa : (\mathbb{Z}, +) \to (\mathbb{K}, +)$) gilt $\ker\kappa \subseteq \mathbb{Z} \neq \{0\} \implies \ker\kappa = m \cdot \mathbb{Z}$ für ein $m \in \mathbb{N}$. Hätte m einen nichttrivialen Teiler d, dann wäre $\kappa(m) = \kappa(d)\,\kappa(m/d) = \mathbf{0}_{\mathbb{K}}$ und somit bereits $\kappa(d) = \mathbf{0}_{\mathbb{K}}$ oder $\kappa(m/d) = \mathbf{0}_{\mathbb{K}}$ (da $\mathbb{K}$ nullteilerfrei): Also ist $m = p \in \mathbb{P}$ prim, und der Körper $\mathbb{F}_p$ erscheint als *Teilring* in $\mathbb{K}$: $\mathbb{F}_p \sqsubseteq \mathbb{K}$.

Nach Satz 3.1.9 ist $\mathbb{K}^\star$ eine zyklische Gruppe mit einem Erzeuger γ, also:

$$\alpha \in \mathbb{K} \implies \alpha = \mathbf{0}_{\mathbb{K}} \text{ oder } \alpha = \gamma^n \text{ für ein } n \in \mathbb{N}.$$

Daher ist der Ringhomomorphismus (*Evaluation* bei γ)

$$\mathrm{ev}_\gamma : \mathbb{F}_p[x] \to \mathbb{K},$$

der durch $\mathrm{ev}_\gamma(q) := q(\gamma)$ definiert ist, *surjektiv* (denn $\mathbf{0} \in \mathbb{F}_p[x]$ und $x^n \in \mathbb{F}_p[x]$ für alle $n \in \mathbb{N}$). Der Kern von ev_γ ist ein *Hauptideal* $(f) \subset \mathbb{F}_p[x]$ (denn $\mathbb{F}_p[x]$ ist ein euklidischer Ring gemäß Lemma A.3.75 und daher ein *Hauptidealring* gemäß Satz A.3.56) und somit ist

$$\mathbb{F}_p[x] / ((f)) \simeq \mathbb{K}$$

nach dem *Isomomorphiesatz* (siehe Korollar A.3.41). Da $\mathbb{K}$ ein *Körper* ist, muß $((f))$ ein maximales Ideal sein (siehe Proposition A.3.66), also muß f irreduzibel sein (siehe Satz A.3.48). Sei $n = \deg f$: Dann ist klarerweise $|\mathbb{K}| = p^n$ (siehe Proposition A.3.84). □

KOROLLAR 3.1.12. *Sei* $p \in \mathbb{P}$ *und* $\mathbb{K}$ *ein endlicher Körper mit* p^n *Elementen. Dann gilt in* $\mathbb{K}[x]$ *die Faktorisierung:*

$$x^{p^n} - x = \prod_{\alpha\in\mathbb{K}} (x - \alpha).$$

BEWEIS. Nach Satz 3.1.9 ist die multiplikative Gruppe $\mathbb{K}^\star$ zyklisch mit Ordnung $p^n - 1$, also ist *jedes* Element $\alpha \in \mathbb{K}$ Nullstelle von $x^{p^n} - x$. Nach Lemma 2.1.4 gilt daher $(x - \alpha) \mid x^{p^n} - x$ für alle $\alpha \in \mathbb{K}$: Die Polynome auf der linken und rechten Seite haben also dieselben Nullstellen, denselben Grad und denselben führenden Koeffizienten: Daher sind die Polynome gleich (siehe auch Satz A.3.81). □

SATZ 3.1.13. *Ist* f *ein* irreduzibles *Polynom in* $\mathbb{F}_p[x]$, *das* Φ_{p^n-1} *teilt, dann gilt* $\deg f = n$. *Insbesondere gilt also: Für alle* $p \in \mathbb{P}$, $n \in \mathbb{N}$ *existiert ein irreduzibles Polynom* f *in* $\mathbb{F}_p[x]$ *vom Grad* n.

BEWEIS. Sei $f(x) \in \mathbb{F}_p[x]$ ein *irreduzibler* Teiler von Φ_{p^n-1} mit $\deg f = d$: D.h., in $\mathbb{F}_p[x]$ gilt $\Phi_{p^n-1} = f \cdot g$ für ein $g \in \mathbb{F}_p[x]$.

Da f irreduzibel ist, ist $\mathbb{K} = \mathbb{F}_p[x]/((f))$ ein Körper mit p^d Elementen, der $\mathbb{F}_p$ als Teilkörper enthält, und $\alpha = \overline{x} \in \mathbb{K}$ (d.h., α ist die *Äquivalenzklasse* des Polynoms x in $\mathbb{F}_p[x]$ in bezug auf das Ideal $((f))$) ist eine Nullstelle des Polynoms $f \in \mathbb{F}_p[x] \subseteq \mathbb{K}[x]$. Dann ist aber natürlich auch $\Phi_{p^n-1}(\alpha) = f(\alpha) \cdot g(\alpha) = 0$.

Wir betrachten die formale Ableitung in $\mathbb{K}[x]$:

$$\mathrm{D}\left(x^{p^n-1} - 1\right) = (p^n - 1)\, x^{p^n-2} = -x^{p^n-2} \text{ in } \mathbb{K}[x].$$

Ausgewertet bei $\alpha = \overline{x}$ ist das $\overline{-x^{p^n-2}} = \left((-1) \cdot \overline{-x}^{p^n-2}\right) \neq 0$ in $\mathbb{K}$, daher ist (siehe Lemma 2.1.12) α *keine* mehrfache Nullstelle von $\left(x^{p^n-1} - 1\right)$ und somit nach Lemma 3.1.8 eine *primitive* (p^n-1)–te Einheitswurzel in $\mathbb{K}$. α erzeugt also eine (zyklische) Untergruppe der Ordnung $(p^n - 1)$ in der (ebenfalls zyklischen, nach Satz 3.1.9) Gruppe $\mathbb{K}^\star$, die die Ordnung $\left(p^d - 1\right)$ hat: Nach dem Satz von Lagrange (Satz A.3.12 im Anhang) muß also $(p^n - 1) \mid \left(p^d - 1\right)$ gelten, und das ist äquivalent mit $n \mid d$ (siehe Lemma A.3.76).

Betrachten wir nun die Menge $R = \left\{\xi \in \mathbb{K} : \xi^{p^n} = \xi\right\}$. Aus dem kleinen Satz von Fermat A.2.3 folgt

$$a^p \equiv a \pmod{p} \text{ für alle } a \in \mathbb{F}_p,$$

also ist $\mathbb{F}_p \subseteq R$ (denn $a^{p^n} = a^{p \cdot p^{n-1}} = (a^p)^{p^{n-1}} = a^{p^{n-1}}$). R ist ein *Teilkörper* von $\mathbb{K}$ ($R \sqsubseteq \mathbb{K}$), denn R enthält natürlich $\mathbf{0}$ und $\mathbf{1}$ sowie neben den multiplikativen Inversen (klar!) auch die additiven, denn

$$(-\xi)^{p^n} = (-1)^{p^n} \cdot (\xi)^{p^n} = -(\xi)^{p^n} = -\xi,$$

und ist abgeschlossen unter der Addition und Multiplikation in $\mathbb{K}$, d.h., für alle $\xi, \eta \in R$ gilt

$$\begin{aligned} \xi^{p^n} + \eta^{p^n} &= (\xi + \eta)^{p^n} \text{ (siehe Lemma A.3.64),} \\ (\xi \cdot \eta)^{p^n} &= \xi^{p^n} \cdot \eta^{p^n}. \end{aligned}$$

Da $\alpha^{p^n-1} = \mathbf{1}$, ist natürlich $\alpha \in R$ und somit auch $\{\alpha, \alpha^2, \dots\} \subseteq R$: Dann ist aber auch

$$\mathbb{K} = \left\{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} : a_i \in \mathbb{F}_p\right\} \sqsubseteq R,$$

also $\mathbb{K} = R$. Nach Satz 3.1.9 ist die multiplikative Gruppe $\mathbb{K}^\star$ der Ordnung $p^d - 1$ zyklisch, es gibt also eine primitive Einheitswurzel $\zeta \in \mathbb{K}$ der Ordnung $p^d - 1$: $\zeta^{p^d-1} = 1$; wegen $\zeta \in R$ gilt aber auch $\zeta^{p^n-1} = 1$, also $p^d - 1 \mid p^n - 1$, und das ist äquivalent mit $d \mid n$ (siehe Lemma A.3.76).

Es ist also $d = n$ und die Behauptung ist gezeigt. □

BEMERKUNG 3.1.14. *Sei $\Phi_{p^n-1} = f_1 \cdot f_2 \cdots f_r$ eine Zerlegung in irreduzible Polynome $f_i \in \mathbb{F}_p[x]$: Dann folgt aus dem obigen Satz* $\deg f_i = n$, *also* $n \mid \varphi(p^n - 1)$.

SATZ 3.1.15. *Für $p \in \mathbb{P}$, $n \in \mathbb{N}$ existiert genau ein endlicher Körper mit p^n Elementen, den wir mit $\mathbb{F}_{p^n}$ bezeichnen. Genauer gesagt: Je zwei endliche Körper $\mathbb{K}, \mathbb{K}'$ mit p^n Elementen sind isomorph: $\mathbb{K} \simeq \mathbb{K}'$.*

BEWEIS. Nach Satz 3.1.13 gibt es ein irreduzibles Polynome $f \in \mathbb{F}_p[x]$ mit $\deg f = n$; betrachte den Körper $\mathbb{K}_f = \mathbb{F}_p[x]/((f))$ mit p^n Elementen. Nach *Konstruktion* ist $\alpha = \overline{x} \in \mathbb{K}_f$ eine Nullstelle von $f \in \mathbb{K}_f[x]$. Die Menge

$$I := \left\{ g \in \mathbb{F}_p[x] : g(\alpha) = \mathbf{0}_{\mathbb{K}_f} \right\}$$

ist eine *Teilmenge* in $\mathbb{K}_f[x]$; sie ist aber offensichtlich auch ein *Ideal* in $\mathbb{F}_p[x]$, und es gilt $f \in I$. Da $\mathbb{K}_f = \mathbb{F}_p[x]/((f))$ ein Körper (siehe Proposition A.3.66) ist, ist $((f))$ ein *maximales* Ideal, also muß $I = ((f))$ gelten. Es ist aber auch $x^{p^n} - x \in I$, denn $\zeta^{p^n-1} = 1$ gilt ja für *jedes* $\zeta \in \mathbb{K}_f^\star$ (also insbesondere für α), also gilt $f \mid \left(x^{p^n} - x\right)$ in $\mathbb{F}_p[x]$.
Wir wollen zeigen: Ein *beliebiger* endlicher Körper $\mathbb{K}$ mit p^n Elementen ist isomorph zu $\mathbb{K}_f$. Nach Korollar 3.1.12 gilt in $\mathbb{K}[x]$ die Faktorisierung

$$x^{p^n} - x = \prod_{\beta \in \mathbb{K}} (x - \beta),$$

also muß $f \in \mathbb{F}_p[x] \subseteq \mathbb{K}[x]$ eine Nullstelle $\beta \in \mathbb{K}$ haben (denn $f \mid \left(x^{p^n} - x\right)$).
Wir betrachten die *Evaluation*

$$\mathrm{ev}_\beta : \mathbb{F}_p[x] \to \mathbb{K}, \text{ gegeben durch } q(x) \mapsto q(\beta) \in \mathbb{K}$$

(Auswertung des Polynoms q an der Stelle β): ev_β ist sichtlich ein (nichttrivialer) Homomorphismus mit $((f)) \subseteq \ker \mathrm{ev}_\beta$, und da $((f))$ ein *maximales* Ideal ist (und $\ker \mathrm{ev}_\beta$ nicht ganz $\mathbb{F}_p[x]$ ist), ist $((f)) = \ker \mathrm{ev}_\beta$. Daher induziert ev_β einen Ringisormorphismus $\mathbb{F}_p[x]/((f)) \to \operatorname{img} \mathrm{ev}_\beta \subseteq \mathbb{K}$, also insbesondere eine injektive Abbildung: Da aber $\left|\mathbb{K}_f\right| = |\mathbb{K}| = p^n$, ist $\operatorname{img} \mathrm{ev}_\beta = \mathbb{K}$ und die Behauptung ist gezeigt. □

Wir wissen bereits:

$$x^{p^n} - x = x\left(x^{p^n-1} - 1\right) = x \prod_{d \mid p^n-1} \Phi_d$$

hat einen irreduziblen Teiler vom Grad n. Wie sieht die vollständige Faktorisierung aus?

BEISPIEL 3.1.16. *In $\mathbb{F}_2$ gilt $x^4 - x = x(x+1)\left(x^2+x+1\right)$, und in $\mathbb{F}_3$ gilt $x^9 - x = x(x+1)(x-1)\left(x^2+1\right)\left(x^2+x-1\right)\left(x^2-x-1\right)$.*

SATZ 3.1.17. *Das Polynom $x^{p^n} - x \in \mathbb{F}_p[x]$ ist das Produkt aller* monischen *(i.e., führender Koeffizient ist 1) irreduziblen Polynome $f \in \mathbb{F}_p[x]$ vom Grad d für $d \mid n$.*

BEWEIS. Sei $f \in \mathbb{F}_p[x]$ ein monisches irreduzibles Polynom vom Grad d: Dann ist $\mathbb{K} = \mathbb{F}_p[x]/((f))$ ein Körper mit p^d Elementen. Sei $\alpha := \overline{x} \in \mathbb{K}$, dann gilt nach Konstruktion $\alpha^{p^d-1} - \mathbf{1} = \mathbf{0}$ in $\mathbb{K}$, und $((f)) = \left\{ q \in \mathbb{F}_p[x] : q(\alpha) = \mathbf{0} \right\}$

(wie im Beweis von Satz 3.1.15: $((f)) \subseteq \ker \mathrm{ev}_\alpha \implies ((f)) = \ker \mathrm{ev}_\alpha$, weil $((f))$ *maximal* ist).

- *Wenn* $d \mid n$, dann folgt zunächst $p^d - 1 \mid p^n - 1$ (siehe Lemma A.3.76) und damit $\alpha^{p^n-1} = \mathbf{1}$ in $\mathbb{K}$: Das bedeutet aber $x^{p^n} - x \in \ker \mathrm{ev}_\alpha = ((f))$, d.h., $f \mid \left(x^{p^n} - x\right)$.
- *Wenn* $f \mid \left(x^{p^n} - x\right)$, dann gilt für $R = \left\{\xi \in \mathbb{K} : \xi^{p^n} = \xi\right\} \sqsubseteq \mathbb{K}$ (vergleiche den Beweis von Satz 3.1.13) schon $R = \mathbb{K}$ (denn $\alpha \in R$ wegen $f \mid \left(x^{p^n} - x\right)$, und somit $\alpha^k \in R$ für alle $k \in \mathbb{Z}$). Sei γ ein erzeugendes Element der zyklischen Gruppe $\mathbb{K}^\star$, also $\mathrm{ord}_{\mathbb{K}^\star}(\gamma) = p^d - 1$; wegen $\gamma \in R$ gilt aber auch $\gamma^{p^n-1} = 1$, es folgt also zunächst $p^d - 1 \mid p^n - 1$ und somit $d \mid n$ (nach Lemma A.3.76). Insgesamt gilt also für jedes monische irreduzible Polynom $f \in \mathbb{F}_p[x]$:

$$f \mid x^{p^n} - x \iff \deg f \mid n.$$

Wir haben also gezeigt: Seien $f_1, \ldots, f_r$ die verschiedenen monischen irreduziblen Polynome, deren Grade Teiler von n sind, dann ist

$$x^{p^n} - x = f_1^{n_1} \cdot f_2^{n_2} \cdots f_r^{n_r}$$

mit $n_i \geq 1$, $1 \leq i \leq r$. Wir wollen noch zeigen: $n_i = 1$. Das ergibt sich aber sofort aus Lemma 2.1.12, denn aus

$$\left(\mathrm{D}\left(x^{p^n} - x\right)\right) = p^n \cdot x^{p^n-1} - 1 \equiv -1 \neq \mathbf{0} \text{ in } \mathbb{F}_p[x]$$

folgt, daß $x^{p^n} - x$ keine mehrfachen Nullstellen haben kann, also kann kein Faktor f_i (der ja eine Nullstelle *hat*!) mehrfach auftreten. □

BEMERKUNG 3.1.18. *Sei* N_d *die* Anzahl *der monischen irreduziblen Polynome vom Grad* d *in* $\mathbb{F}_p[x]$*, dann ergibt sich aus der Betrachtung der Grade in Satz 3.1.17 sofort:*

$$p^n = \sum_{d \mid n} d \cdot N_d. \tag{3.1}$$

Es gilt $N_1 = p$*, denn die Polynome* $x, x-1, \ldots, x-(p-1)$ *sind* alle *monisch und irreduzibel in* $\mathbb{F}_p[x]$*, und für* $q \in \mathbb{P}$ *erhält man aus* (3.1) $p^q = q \cdot N_q + N_1 = q \cdot N_q + p$ *sofort* $N_q = \frac{p^q - p}{q}$*. Allgemein ergibt sich* N_n *durch* Möbiusinversion *(siehe Satz A.2.5) aus* (3.1)*:*

$$N_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \cdot p^d. \tag{3.2}$$

Zum Beispiel ist $N_2 = \frac{1}{2}\left(-p + p^2\right)$, $N_3 = \frac{1}{3}\left(-p + p^3\right)$ *und* $N_6 = \frac{1}{6}\left(p - p^2 - p^3 + p^6\right)$.

3.1.3. Faktorisierung von Polynomen über $\mathbb{Z}_p$ ($p \in \mathbb{P}$). *Faktorisierung* ist im allgemeinen schwierig, vergleichsweise sehr einfach ist hingegen die Bestimmung des größten gemeinsamen Teilers: Wir werden in diesem Abschnitt sehen, wie wir das verwenden können. Zunächst noch ein einfache Beobachtung:

PROPOSITION 3.1.19. *Sei* $f \in \mathbb{F}_p[x]$*:*

- *Falls* $\deg f \in \{2, 3\}$*, dann ist* f *irreduzibel genau dann, wenn* f keine *Nullstelle in* $\mathbb{F}_p$ *hat.*

- *Wenn es ein irreduzibles Polynom g gibt mit $g^2 \mid f$, dann gilt $g \mid \mathrm{ggT}(f, \mathrm{D}(f))$.*

BEWEIS. Die erste Behauptung ist klar: f ist genau dann reduzibel, wenn f einen Linearfaktor $(x-\alpha)$ und somit eine Nullstelle besitzt.
Für die zweite Behauptung verwenden wir die Produktregel (siehe Lemma 2.1.7): Sei $f = g^2 \cdot g^\star$, dann ist

$$\mathrm{D}(f) = \mathrm{D}\left(g^2 \cdot g^\star\right) = 2 \cdot g \cdot g^\star + g^2 \cdot \mathrm{D}(g^\star),$$

woraus die Behauptung folgt. □

3.1.3.1. *Elementare Ansätze.* Satz 3.1.17 liefert uns eine einfache Methode zur (i.A. nicht vollständigen) Faktorisierung eines Polynoms $f \in \mathbb{F}_p[x]$, die wir folgendermaßen algorithmisch fassen können:

```
/* Abdividieren von Linearfaktoren */
while ∃α ∈ F_p: f(α) = 0 do
  f ← f/(x − α)
end while
/* Abdividieren von quadratischen Faktoren */
q ← ggT(D(f), f)
if deg q > 0 then
  f ← f/q^2
end if
/* q ist i.A. nicht irreduzibel; ab hier gilt aber jedenfalls: f ist
quadratfrei und hat keinen Linearfaktor. */
m = ⌊deg f / 2⌋
/* Sukzessives Abdividieren des Produkts aller (verschiedenen!) irreduziblen
Teiler von f mit Grad d (gemäß Satz 3.1.17). */
for d = 2 to m do
  q = ggT(f, x^(p^d) − x)
  f ← f/q
end for
```

BEISPIEL 3.1.20. *Sei* $f(x) = x^{16} + x^{15} + 2x^{12} + x^{11} + x^{10} + x^9 + x^8 + 2x^7 + x^6 + 2x^4 + 2x^2 + 2x + 1 \in \mathbb{F}_3[x]$.
Es gilt $f(1) = 0$, *und* $g = f/(x-1) = x^{15} + 2x^{14} + 2x^{13} + 2x^{12} + x^{11} + 2x^{10} + x^8 + 2x^7 + x^6 + 2x^5 + 2x^4 + x^3 + x^2 + 2$ *hat keine Nullstelle mehr.*
Es gilt $D(g) = x^{13} + 2x^{12} + 2x^{10} + 2x^9 + 2x^7 + 2x^6 + x^4 + 2x^3 + 2x$, *und mit dem euklidischen Algorithmus erhalten wir* $q = \mathrm{ggT}(g, D(g)) = x^2 + x + 2$*: Da alle Linearfaktoren schon abdividiert wurden, hat* q *keine Nullstelle und muß (da* $\deg q \leq 3$*) bereits irreduzibel sein.*
Wir fahren also mit $h = g/q^2 = x^{11} + x^8 + x^7 + x^6 + x^5 + x^4 + 2x^3 + 2x^2 + x + 2$ *fort, das* quadratfrei *ist. Jetzt holen wir uns das* Produkt *der irreduziblen Teiler von* h *mit Grad 3:* $q = \mathrm{ggT}\left(h, x^{27} - x\right) = x^3 + 2x^2 + 1$*; das ist also sichtlich auch ein* irreduzibler *Teiler von* h*.*
Der Rest $r = h/q = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 2$ *ist das Produkt von* 2 *irreduziblen Polynomen vom Grad* 4*, denn der euklidische Algorithmus liefert*

$\operatorname{ggT}\left(r, x^{81}-x\right) = r$: *Wir haben damit zwar die vollständige Faktorisierung in irreduzible Teiler*

$$f(x)=(x+2)\left(x^2+x+2\right)^2\left(x^3+2x^2+1\right)\left(x^4+2x^3+x^2+1\right)\left(x^4+2x^3+2x^2+x+2\right)$$

nicht geschafft, sind aber doch recht weit gekommen.

3.1.3.2. *Der Berlekamp–Algorithmus.* In der Computeralgebra, einem Teilgebiet der Mathematik, ist der *Berlekamp–Algorithmus* eine Methode zur Faktorisierung von Polynomen über einem endlichen Körper, die 1967 von Elwyn Berlekamp entwickelt wurde. Er ist in den meisten Computeralgebrasystemen implementiert und war der führende Faktorisierungsalgorithmus bis zur Entwicklung des *Cantor–Zassenhaus–Algorithmus*, einer probabilistischen Variante des Berlekamp–Algorithmus, aus dem Jahre 1981.

Gesucht ist eine Faktorisierung von $f(x) \in \mathbb{F}_p[x]$ mit $\deg f(x) = n$ in irreduzible Faktoren $f(x) = g_1(x) \cdots g_r(x)$, wobei die Anzahl r der Faktoren unbekannt ist. Insbesondere kann auch $r = 1$ gelten: Dann ist $f(x)$ irreduzibel. Dabei kann man ohne Beschränkung der Allgemeinheit annehmen, dass $f(x)$ *quadratfrei* ist, weil andernfalls $\deg \operatorname{ggT}(f, \mathrm{D}(f)) > 0$ ist und daher auf diese Weise bereits ein echter Teiler gefunden wird (siehe Proposition 3.1.19).

DEFINITION 3.1.21. *Es sei R ein kommutativer unitärer Ring mit Charakteristik $p \in \mathbb{P}$*[5]*. Die Abbildung*

$$\operatorname{frob}_p R \to R : \; x \mapsto x^p$$

wird als Frobeniusabbildung *bezeichnet.*

Wegen $(a+b)^p = a^p + b^p$ in R (siehe Lemma A.3.64) ist sie ein Ringendomorphismus.

Sei $p \in \mathbb{P}$ und $f \in \mathbb{F}_p[x]$: Der Ring $R = \mathbb{F}_p[x]/((f))$ hat die Struktur eines *Vektorraums* über dem Körper $\mathbb{F}_p$, und die Frobeniusabbildung $R \to R$ ist hier eine *lineare* Abbildung, denn sie fixiert den Körper $\mathbb{F}_p$,

$$\operatorname{frob}_p(\lambda) = \lambda^p = \lambda \text{ für alle } \lambda \in \mathbb{F}_p,$$

also ist

$$\operatorname{frob}_p(a + \lambda \cdot b) = a^p + \underbrace{\lambda^p}_{=\lambda} \cdot b^p = \operatorname{frob}_p(a) + \lambda \cdot \operatorname{frob}_p(b).$$

BEISPIEL 3.1.22. *Sei $f = x^5 + x + 1 \in \mathbb{F}_2[x]$, dann ist $R = \mathbb{F}_2[x]/((f))$ ein 5–dimensionaler Vektorraum über $\mathbb{F}_2$ mit Basis $\mathcal{B} = \left\{\mathbf{1}, \alpha, \alpha^2, \alpha^3, \alpha^4\right\}$, wobei $\alpha = \overline{x}$ und $\alpha^5 = \mathbf{1} + \alpha$. Wir bestimmen die Matrix der Frobeniusabbildung* frob_2 *für diese Basis und berechnen dazu die Werte der Abbildung für die Basis $\mathcal{B}$:*

$$\operatorname{frob}_2(\mathcal{B}) = \left\{\mathbf{1}, \alpha^2, \alpha^4, \alpha^6 = \alpha \cdot (1+\alpha) = \alpha + \alpha^2, \alpha^8 = \alpha^3 + \alpha^4\right\}.$$

[5] Siehe Definition A.3.61: Der Kern der Abbildung $\mathbb{Z} \to R$, die durch $1 \mapsto \mathbf{1}_R$ gegeben ist, ist eine (additive) Untergruppe von $\mathbb{Z}$, also entweder $\{1\}$ — dann hat der Ring Charakteristik 0 — oder $m\mathbb{Z}$ — dann hat der Ring Charakteristik m.

D.h., die Matrixdarstellung in bezug auf die Basis $\mathcal{B}$ lautet:

$$[\mathrm{frob}_2]_{\mathcal{B},\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Wenn $\ker \mathrm{frob}_p \neq \{\mathbf{0}\}$, dann gibt es ein $g \neq \mathbf{0} \in \mathbb{F}_p[x]$ mit $\deg g < \deg f$ und $\mathrm{frob}_p(\overline{g}) = \overline{g}^p = \overline{\mathbf{0}}$ in $\mathbb{F}_p[x]/((f))$. (g ist nicht konstant, denn für alle $c \in \mathbb{F}_p$ gilt ja $\mathrm{frob}_p(c) = c$, also $0 < \deg g < \deg f$.) Das heißt $f \mid g^p$ in $\mathbb{F}_p[x]$. Sei nun π mit $\deg \pi > 0$ ein *irreduzibler* Teiler von f, dann gilt auch $\pi \mid g$ und $\mathrm{ggT}(f,g)$ ist ein *echter* Teiler von f, denn

$$0 < \deg \pi \leq \deg \mathrm{ggT}(f,g) \leq \deg g < \deg f.$$

Sei $\mathrm{id}\colon R \to R$ die identische Abbildung $\mathrm{id}(x) = x$: Klarerweise ist $\mathbb{F}_p \subseteq \ker\left(\mathrm{frob}_p - \mathrm{id}\right)$ (denn nach dem kleinen Satz von Fermat A.2.3 gilt $x^p = x$ für alle $x \in \mathbb{F}_p$). Sei $g \in \mathbb{F}_p[x]$ mit $0 < \deg g < \deg f$ und $\overline{g} \in \ker\left(\mathrm{frob}_p - \mathrm{id}\right)$, dann ist $\overline{g}^p = \overline{g}$ in R. Es gilt

$$x^p - x = x \cdot (x-1) \cdot (x-2) \cdots (x-p+1) \text{ in } \mathbb{F}_p[x]$$

Ausmultiplizieren und Koeffizienten vergleichen!

(denn es ist ja $\alpha^p = \alpha$ für alle $\alpha \in \mathbb{F}_p$), daher gilt auch

$$g^p - g = g \cdot (g-1) \cdot (g-2) \cdots (g-p+1) \text{ in } \mathbb{F}_p[x].$$

Sei h ein irreduzibler Teiler von f, dann gilt wegen $f \mid g^p - g$ also h teilt einen der Faktoren $g, g-1, \ldots, g-p+1$, und daher ist eines der Polynome $\mathrm{ggT}(f,g), \mathrm{ggT}(f,g-1), \ldots, \mathrm{ggT}(f,g-p+1)$ ein *echter* Teiler von f (wieder wegen $\deg g < \deg f$).

BEISPIEL 3.1.23. *Für das vorige Beispiel ist die Matrixdarstellung von* $\left(\mathrm{frob}_p - \mathrm{id}\right)$ *in bezug auf die Basis $\mathcal{B}$:*

$$A := [\mathrm{frob}_2 - \mathrm{id}]_{\mathcal{B},\mathcal{B}} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \text{ und } A \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Also gilt für $g = 1 + x + x^3 + x^4$: $f \mid g^2 - g$. Mit dem Euklidischen Algorithmus erhält man

$$\mathrm{ggT}\left(x^5 + x + 1, x^4 + x^3 + x + 1\right) = x^2 + x + 1,$$

und das ist ein Faktor von $f = x^5 + x + 1$.

Um zu entscheiden, ob f irreduzibel ist, genügt es also, die Kerne der $\mathbb{F}_p$–linearen Abbildungen frob_p und $\left(\mathrm{frob}_p - \mathrm{id}\right)$ zu untersuchen.

SATZ 3.1.24. *Sei $f \in \mathbb{F}_p[x]$ nicht konstant. Wir betrachten die Frobeniusabbildung $\mathrm{frob}_p : R \to R$ für $R = \mathbb{F}_p[x]/((f))$: Dann ist f irreduzibel genau dann, wenn $\ker \mathrm{frob}_p = \{\mathbf{0}\}$ und $\ker\left(\mathrm{frob}_p - \mathrm{id}\right) = \mathbb{F}_p$.*

BEWEIS. Wir haben bereits gesehen: Wenn $\ker \mathrm{frob}_p \neq \{\mathbf{0}\}$ oder $\ker\left(\mathrm{frob}_p - \mathrm{id}\right) \neq \mathbb{F}_p$, dann ist f reduzibel.

$A \implies B \iff (\neg B) \implies (\neg A)$

Wir müssen die Umkehrung zeigen: Sei $\ker \mathrm{frob}_p = \{\mathbf{0}\}$ und $\ker\left(\mathrm{frob}_p - \mathrm{id}\right) = \mathbb{F}_p$. Sei $a \neq \mathbf{0}$ in R beliebig: Wir wollen zeigen, daß ein multiplikatives Inverses a^{-1} existiert mit $a \cdot a^{-1} = \mathbf{1}$, denn dann ist R ein Körper, also $((f))$ ein *maximales* Ideal und f ein *irreduzibles* Polynom. Wir betrachten dazu die $\mathbb{F}_p$–lineare Abbildung

$$\phi : R \to R, x \mapsto a \cdot x$$

und wollen zeigen: $\mathbf{1} \in \mathrm{img}\,\phi$.

- Behauptung: $\ker\phi \cap \mathrm{img}\,\phi = \{\mathbf{0}\}$. Denn sei $x \in \ker\phi \cap \mathrm{img}\,\phi$, dann gibt es ein y mit $x = a \cdot y$ und es gilt $a \cdot x = 0$. Daraus folgt

$$\mathrm{frob}_p(x) = a^p \cdot y^p = a^{p-2} \cdot y^{p-1} a \cdot x = 0,$$

also ist $x \in \ker \mathrm{frob}_p$ und daher $x = 0$; damit ist die Behauptung gezeigt. Aus dem *Rangsatz* (siehe Satz A.4.3) folgt dann aber

$$\dim_{\mathbb{F}_p}(\ker\phi) + \dim_{\mathbb{F}_p}(\mathrm{img}\,\phi) = \dim_{\mathbb{F}_p}(R),$$

und das heißt

$$R = \ker\phi \oplus \mathrm{img}\,\phi.$$

(R ist *direkte* Summe von $R = \ker\phi$ und $\mathrm{img}\,\phi$.)

- Offensichtlich gilt: Wenn $x \in \ker\phi$ (bzw. $x \in \mathrm{img}\,\phi$), dann ist auch $\mathrm{frob}_p(x) \in \ker\phi$ (bzw. $\mathrm{frob}_p(x) \in \mathrm{img}\,\phi$): Denn

$$a \cdot x = 0 \implies a \cdot x^p = 0,$$
$$x = a \cdot y \implies x^p = a \cdot \left(a^{p-1} \cdot y^p\right).$$

- Wenn wir $\mathbf{1} \in R$ also (eindeutig!) schreiben als $\mathbf{1} = \alpha + \beta$ mit $\alpha \in \ker\phi$, $\beta \in \mathrm{img}\,\phi$, dann erhalten wir:

$$\alpha + \beta = \mathbf{1} = \mathrm{frob}_p(\mathbf{1}) = \mathrm{frob}_p(\alpha) + \mathrm{frob}_p(\beta) = \underbrace{\alpha^p}_{\in\ker\phi} + \underbrace{\beta^p}_{\in\mathrm{img}\,\phi},$$

und wegen der *Eindeutigkeit* der Darstellung folgt $\alpha^p = \alpha$ und $\beta^p = \beta$. Das heißt, $\alpha \in \ker\left(\mathrm{frob}_p - I\right)$, also *nach Voraussetzung* $\alpha \in \mathbb{F}_p$. Da $\alpha \in \ker\phi$, muß $\alpha = \mathbf{0}$ gelten: Also ist $\beta = \mathbf{1} \in \mathrm{img}\,\phi$ und wir sind fertig. □

Aus diesen Überlegungen ergibt sich der *Berlekamp–Algorithmus*, dessen Ablauf wir anhand eines Beispiel illustrieren:

BEISPIEL 3.1.25. *Wir suchen die Faktorisierung des Polynoms*

$$f = x^7 + x^5 + 2x^3 + 2x^2 + 3x + 2 \in \mathbb{F}_5[x].$$

Wir bestimmen $\mathrm{ggT}(f, \mathrm{D}(f)) = \mathbf{1}$*:*

$$\begin{aligned}
x^7+x^5+2x^3+2x^2+3x+2 &= \left(2x^6+x^2+4x+3\right)\cdot 3x + x^5+4x^3+4x+2\\
2x^6+x^2+4x+3 &= \left(x^5+4x^3+4x+2\right)\cdot 2x + 2x^4+3x^2+3\\
x^5+4x^3+4x+2 &= \left(2x^4+3x^2+3\right)\cdot 3x+2\\
2x^4+3x^2+3 &= 2\cdot\left(x^4+4x^2+4\right)+0.
\end{aligned}$$

ABBILDUNG 1. Nachrichtenübertragung über einen störungsanfälligen Kanal: Die gesendete Information kommt beim Empfänger möglicherweise fehlerhaft an.

Weil $\mathrm{ggT}(f, \mathrm{D}(f)) = \mathbf{1}$*, ist* f *quadratfrei. Die Frobeniusabbildung* frob_f *nimmt auf der Basis* $\mathcal{B} = \{\mathbf{1}, \alpha, \alpha^2, \ldots, \alpha^6\}$ *des 7–dimensionalen Vektorraums* $\mathbb{F}_5[x]/((f))$ *die Werte*

$$\begin{aligned} 1, \alpha^5, 4\alpha^6 + 3\alpha^5 + 4\alpha^4 + 3\alpha^2 + 2\alpha, \alpha^6 + 2\alpha^5 + 4\alpha^4 + 4\alpha^2 + \alpha, \\ 2\alpha^6 + 3\alpha^5 + 3\alpha^3 + 2\alpha^2 + 2\alpha + 2, \\ 2\alpha^6 + 4\alpha^5 + \alpha^4 + 4\alpha^2, 2\alpha^6 + 2\alpha^5 + 4\alpha^4 + \alpha^3 + 2\alpha^2 + 3 \end{aligned}$$

an und hat daher folgende Matrixdarstellung:

$$Q := [\mathrm{frob}_5]_{\mathcal{B},\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 2 & 1 & 2 & 0 & 0 \\ 0 & 0 & 3 & 4 & 2 & 4 & 2 \\ 0 & 0 & 0 & 0 & 3 & 0 & 1 \\ 0 & 0 & 4 & 4 & 0 & 1 & 4 \\ 0 & 1 & 3 & 2 & 3 & 4 & 2 \\ 0 & 0 & 4 & 1 & 2 & 2 & 2 \end{pmatrix}$$

Die Determinante dieser Matrix ist $-306 \equiv 4 \pmod 5$*, also ist der Kern der Frobeniusabbildung trivial. Wir versuchen nun den Kern von* $Q - E$ *zu bestimmen, also den* Eigenraum *von* Q *zum* Eigenwert 1*. Durch Lösen des entsprechenden Gleichungssystems (über* $\mathbb{F}_5$*!) erhält man zwei Eigenvektoren* $v_1 = (1,0,0,0,0,0,0)$ *und* $v_2 = (0,3,1,4,1,2,1)$*. Für das zu* v_2 *gehörende Polynom* $g(x) := x^6 + 2x^5 + x^4 + 4x^3 + x^2 + 3x$ *gilt also* $f \mid g^5 - g$*, und eines der Polynome* $\mathrm{ggT}(f, g - s)$*,* $s \in \mathbb{F}_5$*, ist ein Teiler von* f*: Für* $s = 2$ *liefert der Euklidische Algorithmus*

$$\begin{aligned} x^7+x^5+2x^3+2x^2+3x+2 &= \left(x^6+2\,x^5+x^4+4x^3+x^2+3x+3\right)\cdot(x+3)+4x^5+3x^4+4x^3+x^2+x+3 \\ x^6+2x^5+x^4+4x^3+x^2+3x+3 &= \left(4\,x^5+3x^4+4x^3+x^2+x+3\right)\cdot 4x+2x^2+x+3 \\ 4x^5+3x^4+4x^3+x^2+x+3 &= \left(2\,x^2+x+3\right)\cdot\left(2x^3+3x^2+1\right)+0, \end{aligned}$$

und wir erhalten die Faktorisierung

$$f = \left(3x^5 + x^4 + 3x^3 + 2x^2 + 3x + 4\right) \cdot \left(2x^2 + x + 3\right).$$

Der quadratische Faktor hat keine Nullstelle in $\mathbb{F}_5$ *und ist daher irreduzibel (siehe Proposition 3.1.19), und für den anderen Faktor kann man (analog zur obigen Vorgangsweise) nachweisen, daß er irreduzibel ist: Die Zerlegung ist also gefunden.*

3.2. Codierungstheorie

Codierungstheorie beschäftigt sich mit dem Problem, daß Nachrichten, die über einen störungsanfälligen Kanal (zum Beispiel über Internet) übertragen werden, durch Fehler verfälscht werden können, die man nicht vermeiden kann (siehe Abbildung 1): Die Aufgabe besteht hier also darin, durch das "Mitübertragen" zusätzlicher Informationen ("*Redundanz*") zu gewährleisten, daß Übertragungsfehler *erkannt* oder sogar *korrigiert* werden können; und das unter der naheliegenden weiteren Anforderung, daß die redundanten Zusatzinformationen möglichst sparsam konzipiert werden.

BEISPIEL 3.2.1. *Betrachten wir die Übertragung von Buchstaben über eine Netzwerkleitung: Buchstaben werden üblicherweise als achtstellige Binärzahlen (Bytes:* 8 Bits $=$ 1 Byte*) codiert. Wenn wir Fehler erkennbar machen wollen, könnten wir ganz einfach jedes Byte doppelt senden.*

Natürlich erkennt dann der Empfänger der Botschaft, daß ein Fehler passiert ist, wenn das erste und das zweite übertragene Byte nicht übereinstimmen: Allerdings kann er den Fehler nicht korrigieren, denn er weiß ja nicht, ob das erste oder das zweite Byte fehlerhaft ist.

Außerdem bedeutet diese einfache Codierung eine Verdoppelung der Datenmenge, die übertragen wird: Die Redundanz ist hier also genau so groß wie die eigentliche Nachricht. Wir werden sehen, dass es wesentlich sparsamere Codierungsmethoden gibt, die die Erkennung eines Fehlers gewährleisten.

BEMERKUNG 3.2.2. *Klarerweise wird ein "Doppelfehler" der Gestalt, daß das erste und zweite Byte zwar über einstimmen, aber beide fehlerhaft sind, in diesem Beispiel nicht erkannt: Dieser prinzipielle Mangel gilt für alle Kodierungsmethoden, die wir in der Folge betrachten werden. Da aber in der Praxis die Wahrscheinlichkeiten für* einen *Fehler schon gering sind, ist die Wahrscheinlichkeit für zwei Fehler relativ verschwindend: Das Interesse in der Nachrichtentechnik für Kodierungsmethoden, die die Fehlerwahrscheinlichkeit deutlich reduzieren, ist jedenfalls sehr groß.*

BEISPIEL 3.2.3 (ISBN–Code). *Ein einfaches Beispiel aus der Praxis ist der* ISBN–Code*: ISBN steht für* International Standard Book Number *und ist ein* 10*-stelliger Zahlencode $z_{10}z_9 \cdots z_2z_1$, der jedes Buch international erkennbar macht. Dabei sind $z_i \in \{0, 1, 2, \ldots, 9\}$ für $2 \leq i \leq 10$ und $z_1 \in \{0, \ldots, 9, X\}$ (wobei der Buchstabe X für die Zahl* 10 *steht). Die ersten* 9 *Ziffern kennzeichnen das Erscheinungsland, den Verlag, und den Buchtitel. Die letzte Ziffer ist das redundante Prüfzeichen: z_1 wird so gewählt, daß gilt*

$$S = \sum_{i=1}^{10} i \cdot z_i = 1 \cdot z_1 + 2 \cdot z_2 + \cdots 10 \cdot z_{10} \equiv 0 \mod 11 \text{ (mit } X = 10\text{)}.$$

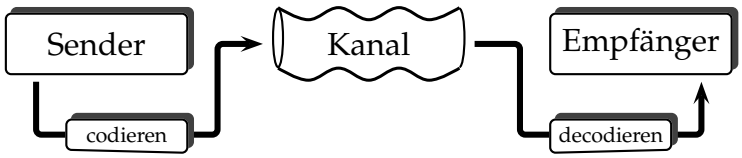
Betrachten wir zum Beispiel die ISBN-Nummer

3-540-20521-7

Die letzte Ziffer 7 *ist ein korrektes Prüfzeichen, da*

$$10 \cdot 3 + 9 \cdot 5 + 8 \cdot 4 + 7 \cdot 0 + 6 \cdot 2 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 2 + 2 \cdot 1 + 1 \cdot 7 = 154$$

ABBILDUNG 2. Codierte Nachrichtenübertragung über einen störungsanfälligen Kanal: Die gesendete Information wird vom Sender *codiert* und vom Empfänger wieder *decodiert*.



tatsächlich durch 11 *teilbar ist. Die Redundanz ist hier recht gering (1 zusätzliches Zeichen entspricht* $1/9$ *der eigentlichen Nachricht), und die zwei häufigsten Übertragungsfehler beim Lesen oder Abtippen werden erkannt:*

(1) *Genau eine Ziffer ist falsch.*
(2) *Genau zwei Ziffern sind vertauscht.*

Ad (1)*: Wenn statt der Ziffer* z_j $y_j \neq z_j$ *übermittelt wird, dann gilt* $(y_j - z_j) \not\equiv 0 \mod 11$ *wegen* $1 \leq |y_j - z_j| \leq 10$*. Deshalb gilt für die gewichtete Summe*

$$\begin{aligned} S &= j \cdot y_j + \sum_{i=1, i\neq j}^{10} i \cdot z_i = j\,(y_j - z_j) + \sum_{i=1}^{10} i \cdot z_i \\ &\equiv j(y_j - z_j) \not\equiv 0 \mod 11. \end{aligned}$$

Wäre also in unserem Beispiel die erste Ziffer verfälscht worden und wir hätten

`8-540-20521-7`

erhalten, so wüßten wir wegen $S = 204$ *sofort, daß die Zahl fehlerhaft ist, denn* 204 *ist nicht durch* 11 *teilbar.*

Ad (2)*: Angenommen, die Ziffern* z_j *und* z_k *mit* $z_j \neq z_k$ *werden vertauscht. Dann ist* $(k-j)(z_j - z_k) \not\equiv 0 \mod 11$ *wegen* $1 \leq |j-k| \leq 9$*. Deshalb gilt für die gewichtete Summe*

$$\begin{aligned} S &= j \cdot z_k + k \cdot z_j + \sum_{i=1, i\neq j,k}^{10} i \cdot z_i = (k-j)\,(z_j - z_k) + \sum_{i=1}^{10} i \cdot z_i \\ &\equiv (k-j)\,(z_j - z_k) \not\equiv 0 \mod 11. \end{aligned}$$

Wären also in unserem Beispiel die zweite und dritte Ziffer vertauscht worden und wir hätten

`3-450-20521-7`

erhalten, erkennen wir den Fehler wegen $S = 153 \not\equiv 0 \mod 11$.

Wir illustrieren nun anhand eines Beispiels, in welchem Sinn eine Codierung nicht nur das *Erkennen*, sondern auch die *Korrektur* von Fehlern möglich machen kann:

BEISPIEL 3.2.4. *Angenommen, wir wollen* 2–Bit *Nachrichten senden, also* 00, 10, 01 *und* 11. *Das* Codieren *besteht einfach in drei Wiederholungen der eigentlichen Nachricht, d.h.,*

$$\begin{aligned} 00 &\to 000000, \\ 10 &\to 101010, \\ 01 &\to 010101, \\ 11 &\to 111111. \end{aligned}$$

Das Decodieren *einer empfangenen Nachricht v besteht darin, daß in der Liste der* 4 *Codewörter jenes gewählt wird, das sich von v in der geringsten Anzahl von Bits unterscheidet: Wenn wir also z.B.* 101011 *empfangen, sehen wir sofort, daß ein Fehler passiert ist und gehen davon aus, daß die Nachricht eigentlich* 101010 *lauten sollte.*

Man kann leicht nachprüfen, daß so alle Fehler korrigiert werden können, die durch die Übertragung von genau einem *falschen Bit entstehen.*

3.2.1. Grundlegende Definitionen. Die Codierungstheorie beschäftigt sich mit der Erkennung/Korrektur von Fehlern, die bei der Datenübertragung entstehen: Es geht hier also *nicht* um die *Verschlüsselung* der Daten zum Schutz vor unerlaubtem Zugriff — damit beschäftigt sich die *Kryptographie*.

DEFINITION 3.2.5. *Sei F eine Menge mit $|F| = q < \infty$, die wir im Zusammenhang mit Codierung auch als* Alphabet *bezeichnen. Eine nichtleere Teilmenge $C \subseteq F^n = \{(u_1, \cdots, u_n) : u_i \in F\}$ heißt eine* Code *der Länge n über dem Alphabet F. (Solche Codes heißen auch* Blockcodes*: Jedes Wort hat dieselbe Länge.) Die n–Tupel in F^n bezeichnen wir in diesem Zusammenhang auch als* Worte*, und die n–Tupel in C als* Codeworte*.*

In der Computertechnik besonders wichtig ist der Fall $q = 2$: Man spricht dann von binären Codes*.*

Ein Code C mit m Wörtern der Länge n kann als $(m \times n)$-Matrix geschrieben werden, deren Zeilen die Codewörter sind.

BEISPIEL 3.2.6. *Es ist*

$$C = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

ein binärer Code mit 4 *Wörtern der Länge* 2*. Codiert man ein* 2*-Bit Wort mit einem weiteren Bit so, daß die Quersumme gerade wird, erhält man einen binären Code der Länge* 3*:*

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Dieser Code gewährleistet, daß ein Fehler erkannt wird, wenn genau 1 *Bit falsch übertragen wird.*

In der Praxis wird $F = \{0, 1, \ldots, q-1\}$ betrachtet und F mit $\mathbb{Z}/q\mathbb{Z}$ identifiziert: Damit hat $F = \mathbb{Z}/q\mathbb{Z}$ die Struktur eines Rings. In den folgenden Betrachtungen gehen wir davon aus, daß $q = p^k$ eine *Primzahlpotenz* ist: Dann hat $F = \mathbb{F}_q$ die Struktur eines (endlichen) Körpers, und $\mathbb{F}_q^n$ hat die Struktur eines *Vektorraums* über $\mathbb{F}_q$.

DEFINITION 3.2.7 (Hamming–Distanz). *Sei q eine Primzahlpotenz, sei $n \in \mathbb{N}$. Im Vektorraum $V = \mathbb{F}_q^n$ ist die* Hamming–Distanz $d : V \times V \to \mathbb{N}_0$ *wie folgt definiert: Seien $x = (x_1, \ldots, x_n)$ und $(y = (y_1, \ldots, y_n)$ zwei Vektoren in V, dann ist*

$$d(x, y) := \text{ Anzahl der Indizes } i \text{ mit } x_i \neq y_i.$$

Es gilt (natürlich)

$$d(x + z, y + z) = d(x, y) \text{ (d ist translationsinvariant)}$$

und

$$0 \leq d(x, y) \leq n$$

für alle $x, y \in V$.

LEMMA 3.2.8. *Die Hamming–Distanz ist eine* Metrik *auf $V = \mathbb{F}_q^n$:*

(1) $d(x, y) = 0$ *genau dann wenn $x = y$.*
(2) $d(x, y) = d(y, x)$ *für alle $x, y \in V$.*
(3) $d(x, y) \leq d(x, z) + d(z, y)$ *für alle $x, y, z \in V$.*

BEWEIS. Für die Dreiecksungleichung überlege: $d(x, y)$ ist die kleinste Anzahl von Koordinatenänderungen, die nötig ist, um x in y überzuführen. □

BEMERKUNG 3.2.9. *Über $\mathbb{F}_2$ erscheint die Hamming–Distanz als das Quadrat des Euklidischen Abstandes:*

$$d(x, y) = \sum_{i=1}^{n} (x_i - y_i)^2.$$

DEFINITION 3.2.10. *Sei $C \subseteq \mathbb{F}_q^n$. Die* Minimaldistanz *von C ist definiert als*

$$d(C) = \min \{d(x, y) : x, y \in C, x \neq y\}.$$

Das Gewicht $\mathbf{w}(x)$ *von $x \in \mathbb{F}_q^n$ ist definiert als die Anzahl der Koordinaten in $x = (x_1, \ldots, x_n)$ mit $x_i \neq 0$.*

BEISPIEL 3.2.11. *Der binäre Code C_1 aus Beispiel 3.2.6 hat die Minimaldistanz $d(C_1) = 2$: Es gilt $d(x, y) = 2$ für alle $x \neq y \in C_1$, und außerdem $\mathbf{w}(x) = 2$ für alle $x \in C_1 \setminus \mathbf{0}$.*

DEFINITION 3.2.12 (Decodieren mit Hamming–Distanz). *Sei $C \subseteq \mathbb{F}_q^n$ ein Code, sei $s = (s_1, \ldots, s_n) \in C$ das Codewort, das der Sender gesendet hat, und sei $r = (r_1, \ldots, r_n) \in \mathbb{F}_q^n$ das Wort, das der Empfänger erhalten hat: Jeden Buchstaben r_i, der fehlerhaft übermittelt wurde (also $r_i \neq s_i$ bezeichnen wir als* Übertragungsfehler *(oder kurz* Fehler*): Die Hamming–Distanz $d(s, r)$ ist also die Anzahl der Übertragungsfehler.*
Decodieren mit Hamming–Distanz *bedeutet: Wenn die Funktion*

$$d_r : C \to \mathbb{N}_0 : \; x \mapsto d(r, x)$$

ein eindeutiges *Minimum für $x = x_0$ hat, dann decodiert der Empfänger r als x_0: Das heißt, das empfangene Wort r wird als das* nächstgelegene *Codewort x_0 (im Sinne der Hamming–Distanz) gedeutet. (Es kann natürlich $x_0 \neq s$ gelten: Decodieren ist nicht notwendigerweise* korrekt*.)*

Wenn $r \notin C$, dann wird r korrekt als *fehlerhaft erkannt*:

$$r \notin C \implies r \neq s.$$

Umgekehrt gilt das aber nicht:

$$r \in C \not\Longrightarrow r = s :$$

Decodieren mit Hamming–Distanz würde im Fall $r \in C$, aber $r \neq s$ keinen Fehler erkennen und ein *falsches* Ergebnis liefern.

PROPOSITION 3.2.13. *Es sei $C \subseteq \mathbb{F}_q^n$ ein Code. Für das Decodieren mit Hamming–Distanz gilt:*

(1) *Ist $d(C) \geq t+1$, dann werden alle Worte mit höchstens t Übertragungsfehlern korrekt als richtig oder falsch erkannt (man sagt auch salopp: C erkennt $d(C) - 1$ Fehler).*
(2) *Ist $d(C) \geq 2t+1$, dann werden alle Worte mit höchstens t Übertragungsfehlern korrekt decodiert (man sagt auch salopp: C korrigiert $\left\lfloor \frac{d(C)-1}{2} \right\rfloor$ Fehler).*

BEWEIS. Es seien s das gesendete und r das empfangene Wort, und es sei $d(s,r) \leq t$.
Ad (1): Da $d(C) \geq t+1$, ist entweder $r = s \in C$ (und r wird korrekt als richtig erkannt) oder $r \notin C$ (und r wird korrekt als falsch erkannt).
Ad (2): Da $d(s,r) \leq t$, gilt $d(r,x) \geq t+1$ für jedes andere Codewort $x \neq s \in C$, denn andernfalls wäre

$$d(s,x) \leq d(s,r) + d(r,x) \leq t + t = 2t,$$

im Widerspruch zu $d(C) \geq 2t+1$: Also wird r richtig als s decodiert. □

BEISPIEL 3.2.14. *Der Code $C_1 \subset \mathbb{F}_2^3$*

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

aus Beispiel 3.2.6 erfüllt $d(C_1) = 2$ und erkennt daher einen *Fehler, korrigiert aber* keinen *Fehler.*
Der Code $C \subset \mathbb{F}_2^6$

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

aus Beispiel 3.2.4 erfüllt $d(C) = 3$ und korrigiert daher einen Fehler.

DEFINITION 3.2.15. *Ein (n, M, d)–Code über q ist ein Code $C \in \mathbb{F}_q^n$ mit $|C| = M$ (C umfaßt also M Wörter) und Minimaldistanz $d = d(C)$.*
$A_q(n, d)$ sei die größte Zahl M, für die ein (n, M, d)-Code über q existiert.

Es ist *qualitativ* klar: Ein (n, M, d)–Code ist dann gut, wenn er

- möglichst kleines n hat (damit die Datenübertragung sparsam ist),
- möglichst großes M hat (damit Information detailliert übertragen werden kann),
- möglichst großes d hat (damit viele Fehler erkannt bzw. korrigiert werden).

PROPOSITION 3.2.16. *Es gilt $A_q(n, 1) = q^n$ und $A_q(n, n) = q$. Allgemein gilt die (sehr grobe) Singleton–Schranke* **[14]**:

$$A_q(n, d) \leq q^{n-d+1}.$$

BEWEIS. Die erste Behauptung ist klar (Minimaldistanz 1 heißt: Die Codewörter sind paarweise verschieden).
Ist C ein (n, M, n)–Code über q, so unterscheiden sich je zwei Codewörter in allen Koordinaten. Da insbesondere die erste Koordinate nur q verschiedene Werte haben kann, folgt also sofort $A_q(n, n) \leq q$. Es gilt $A_q(n, n) = q$, weil der "Repetitions–Code" der Länge n über q, der aus den Worten $(i, i, \ldots, i)$ für $0 \leq i \leq q-1$ besteht, ein Code mit Minimaldistanz n und q Wörtern ist.
Es sei C ein (n, M, d)-Code über q. Löschen wir die letzten $d-1$ Stellen aller Codewörter, dann sind die verbleibenden Wörter der Länge $n-d+1$ noch immer paarweise verschieden (weil die Minimaldistanz d war): Also ist $M \leq q^{n-d+1}$. □

SATZ 3.2.17 (Kugelpackungsschranke). *Für $m \in \mathbb{F}_q^n$ und $r \in \mathbb{N}$ definieren wir die* Hamming–Kugel *mit Mittelpunkt m und Radius r*

$$B_H(m, r) := \left\{ v \in \mathbb{F}_q^n : d(m, v) \leq r \right\} \subseteq \mathbb{F}_q^n.$$

Es gilt die Kugelpackungsschranke

$$A_q(n, d) \leq \frac{q^n}{\left| B_H\left(m, \left\lfloor \frac{d-1}{2} \right\rfloor\right)\right|}. \tag{3.3}$$

Die Anzahl der Vektoren in einer Hamming–Kugel können wir leicht abzählen:

$$\left| B_H\left(m, \left\lfloor \frac{d-1}{2} \right\rfloor\right)\right| = \sum_{i=0}^{\left\lfloor \frac{d-1}{2} \right\rfloor} \binom{n}{i} (q-1)^i \tag{3.4}$$

BEWEIS. Sei C ein (n, M, d)-Code. Dann müssen die Kugeln $B_H\left(c, \left\lfloor \frac{d-1}{2} \right\rfloor\right)$ für $c \in C$ paarweise disjunkt sein: Denn falls es ein x gäbe mit

$$x \in B_H\left(c_1, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \cap B_H\left(c_2, \left\lfloor \frac{d-1}{2} \right\rfloor\right),$$

dann wäre

$$d(c_1, c_2) \leq d(c_1, x) + d(c_2, x) \leq 2 \left\lfloor \frac{d-1}{2} \right\rfloor \leq d - 1,$$

ein Widerspruch: Daraus folgt natürlich (3.3).
Die Anzahl der Vektoren mit Hamming–Abstand i von m ist $\binom{n}{i}(q-1)^i$ (unabhängig von m): Durch Aufsummieren folgt die zweite Behauptung in (3.4). □

DEFINITION 3.2.18. *Ein (n, M, d)–Code über q mit ungerader Minimaldistanz $d = 2t + 1$ heißt* perfekter Code, *wenn für die Schranke* (3.3) *in Satz 3.2.17 Gleichheit gilt, d.h.*

$$M = \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}.$$

3.2.2. Lineare Codes. Die Konstruktion von Codes $C \subseteq \mathbb{F}_q^n$ wird einfacher, wenn man die algebraische Struktur von $\mathbb{F}_q^n$ ausnützt:

DEFINITION 3.2.19. *Ein Code C der Länge n über $\mathbb{F}_q$ heißt* linearer Code, *wenn er ein Untervektorraum von $\mathbb{F}_q^n$ ist.*

Ist $k \leq n$ die Dimension des linearen Codes C über $\mathbb{F}_q$, so ist C ein (n, q^k, d)–Code: Wir schreiben dann kürzer $[n, k, d]_q$, oder nur $[n, k, d]$, oder überhaupt nur $[n, k]$.

Eine $(k \times n)$–Matrix über $\mathbb{F}_q$, deren Zeilen eine Basis des Untervektorraums $U = C$ bilden, heißt dann Erzeugermatrix *des linearen Codes $[n, k, d]$.*

Ist $G = \left(g_{i,j}\right)_{1,1}^{k,j}$ die Erzeugermatrix von C, dann erhält man definitionsgemäß alle Codewörter in C durch Multiplikation eines beliebigen Vektors $u \in \mathbb{F}_q^k$ mit G:

$$(u_1, \ldots, u_k) \cdot \begin{pmatrix} g_{1,1} & \cdots & g_{1,n} \\ \vdots & \cdots & \vdots \\ g_{k,1} & \cdots & g_{k,n} \end{pmatrix} = (c_1, \ldots, c_n) \in C$$

BEISPIEL 3.2.20. *Der binäre Code*

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

aus Beispiel 3.2.6 bzw. Beispiel 3.2.11 ist ein linearer $[3, 2, 2]$–Code mit Erzeugermatrix

$$G = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

PROPOSITION 3.2.21. *Für einen linearen Code $C \sqsubseteq \mathbb{F}_q^n$ gilt:*

(1) *Die Hamming–Distanz zweier Codewörter x, y aus C ist identisch mit dem Gewicht ihrer Differenz: $d(x, y) = \mathbf{w}(x - y)$.*
(2) *Die Minimaldistanz von C entspricht dem minimalen Gewicht nicht-verschwindender Codewörter aus C, d.h. es gilt*

$$d(C) = \min\{\mathbf{w}(x) : 0 \neq x \in C\}.$$

BEWEIS. Da d translationsinvariant ist, folgt

$$d(x,y) = d(x-y,0) = \mathbf{w}(x-y).$$

Da C linear ist, gilt $x, y \in C \implies x - y \in C$: Daraus folgt auch sofort die zweite Behauptung. □

Zur Bestimmung der Minimaldistanz eines linearen Codes C mit M Wörtern muß man also nur die $M-1$ Wörter ungleich Null betrachten.

BEISPIEL 3.2.22. *Es sei C der ternäre lineare Code mit Erzeugermatrix*

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Nach Definition ist

$$C = \{(c_3, c_2, c_2 + c_3, c_1, c_1 + c_3) : c_i \in \mathbb{F}_3\} \subset \mathbb{F}_3^5.$$

Man sieht leicht: Für $u \neq \mathbf{0} \in \mathbb{F}_3^3$ gilt $\mathbf{w}(u \cdot G) \geq 2$, also hat C Minimaldistanz 2 und ist ein $[5,3,2]_3$–Code.

Die Erzeugermatrix G eines linearen Codes bestimmt eine injektive lineare Abbildung $\mathbb{F}_q^k \to \mathbb{F}_q^n$: Sieht man die Elemente in $\mathbb{F}_q^k$ als die "eigentlichen Nachrichten" an, dann vermittelt diese Abbildung genau die *Codierung*. Es ist klar, daß auch für die *Decodierung* lineare Abbildungen bzw. Matrizen eine Rolle spielen werden.

PROPOSITION 3.2.23. *Sei $\mathbb{K}$ ein Körper, $n \in \mathbb{N}$. Die Abbildung $\langle .,. \rangle : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$, die durch*

$$\langle u, v \rangle := \sum_{i=1}^{n} u_i \cdot v_i$$

gegeben ist, ist eine symmetrische, nicht ausgeartete Bilinearform auf $\mathbb{K}^n$, d.h.:

- $\langle u, v \rangle = \langle v, u \rangle$,
- $\langle u, v + \lambda \cdot w \rangle = \langle u, v \rangle + \lambda \cdot \langle u, w \rangle$,
- *$u \mapsto \langle u, . \rangle$ ist eine injektive Abbildung in den Dualraum, also $\mathbb{K}^n \to \mathbb{K}^{n\star}$.*

Sie ist im allgemeinen nicht *definit:*

$$\langle u, u \rangle = 0 \text{ für } u \neq 0$$

ist möglich.

DEFINITION 3.2.24. *Sei $C \sqsubseteq \mathbb{F}_q^n$ ein linearer Code. Dann heißt*

$$C^\perp := \left\{ x \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ für alle } y \in C \right\}$$

der zu C duale Code. *$C^\perp$ ist sichtlich ein* linearer *Code*[6]*; eine Erzeugermatrix H von $C^\perp$ heißt* Kontrollmatrix *zu C. Im Falle $C = C^\perp$ nennen wir C* selbstdual.

[6] Als Lösungsmenge eines linearen Gleichungssystems!

PROPOSITION 3.2.25. *Es sei $C \sqsubseteq \mathbb{F}_q^n$ ein linearer Code der Dimension k. Dann gilt für jede Erzeugermatrix H von $C^\perp$ die* Kontrollgleichung

$$C = \left\{ y \in \mathbb{F}_q^n : H \cdot y = 0 \right\} \text{ (} y \text{ erscheint hier als Spaltenvektor).} \tag{3.5}$$

Insbesondere ist $C^\perp$ ein linearer Code der Dimension $n-k$, und die Dualisierung ist eine Involution, *d.h. $(C^\perp)^\perp = C$.*

BEWEIS. Ist G die Erzeugermatrix von C, so gilt $x \in C^\perp$ genau dann, wenn $G \cdot x = 0$ ist: Dies ist ein lineares Gleichungssystem mit k linear unabhängigen Gleichungen in n Variablen; sein Lösungsraum $C^\perp$ hat also Dimension $n-k$. Eine Kontrollmatrix H von C ist dann eine $(n-k) \times n$–Matrix, deren Zeilen eine Basis von $C^\perp$ bilden:, und es gilt $G \cdot H^t = 0$. Das Gleichungssystem $y \cdot H^t = 0 \iff H \cdot y = 0$ hat $n-k$ linear unabhängige Gleichungen in n Variablen, sein Lösungsraum hat daher Dimension k und wird von den Zeilen von G aufgespannt: Also gilt die Kontrollgleichung (3.5), und es folgt

$$C = \left\{ y \in \mathbb{F}_q^n : \langle y, x \rangle = 0 \text{ für alle } x \in C^\perp \right\},$$

d.h., $(C^\perp)^\perp = C$. □

BEISPIEL 3.2.26. *Sei $C \sqsubseteq \mathbb{F}_2^4$ der lineare $[4,2]$–Code mit Erzeugermatrix*

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Dann ist $C^\perp$ ein linearer $[4,2]$–Code mit Erzeugermatrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

und H ist eine Kontrollmatrix zu C.
Denn $x = (x_1, x_2, x_3, x_4) \in C^\perp$ genau dann, wenn $G \cdot x = 0$, also wenn x eine Lösung des Gleichungssystems

$$\begin{aligned} x_2 + x_3 + x_4 &= 0 \\ x_1 + x_3 &= 0 \end{aligned}$$

ist. In $\mathbb{F}_2$ ist $-1 = 1$, also erhalten wir als Lösungsraum sofort

$$C^\perp = \{(x_1, x_2, x_1, x_1 + x_2) : x_i \in \mathbb{F}_2\},$$

und die Matrix H ist sichtlich eine Erzeugermatrix für $C^\perp$. Sie erfüllt die Gleichung

$$G \cdot H^t = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

und es gilt die Kontrollgleichung

$$C = \left\{ x \in \mathbb{F}_q^n : H \cdot x = 0 \right\} = \{(x_1, x_2, x_1 + x_2, x_2) : x_i \in \mathbb{F}_2\}.$$

Aus der Kontrollmatrix eines Codes C erkennt man ganz leicht seine Minimaldistanz $d(C)$:

PROPOSITION 3.2.27. *Für $k \in \mathbb{N}$ sei $C \sqsubseteq \mathbb{F}_q^n$ ein linearer $[n,k]$–Code mit Kontrollmatrix H. Dann gilt*

$$\begin{aligned} d(C) &= \min\{\ell \geq 1 \mid \text{es gibt } \ell \text{ linear abhängige Spalten in } H\} \\ &= \max\{\ell \geq 1 \mid \text{je } \ell - 1 \text{ Spalten von } H \text{ sind linear unabhängig}\}. \end{aligned}$$

($d(C)$ ist also sozusagen ein "diametrales Gegenteil" zum Spaltenrang, der maximalen *Zahl* linear unabhängiger *Spalten.)*

BEWEIS. Sei $H = (h_1, \ldots, h_n)$, wobei h_i die i–te Spalte bezeichnet. Alle h_i haben Länge $n-k$: Da $k > 0$, ist $n - k < n$ und die Spalten sind linear abhängig.
Für *jede* Teilmenge $\{h_{i_1}, \ldots, h_{i_d}\}$ von linear abhängigen Spalten gibt es ein $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ mit der Eigenschaft $c_j \neq 0 \iff j \in \{i_1, \ldots, i_d\}$ (d.h.: $\mathbf{w}(c) = d$), sodaß gilt:

$$\sum_{j=1}^{n} c_j \cdot h_j = 0.$$

Das heißt aber: $H \cdot c = 0 \iff c \in C$; und umgekehrt gibt es für jedes $c \neq 0 \in C$ eine Teilmenge von $\mathbf{w}(c)$ linear abhängigen Spalten in H. Die Behauptung folgt also aus Proposition 3.2.21. □

BEISPIEL 3.2.28. *Die Matrix*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

erzeugt einen linearen, selbstdualen $[8,4,4]_2$–Code C: Denn es ist $G \cdot G^t = 0$, also ist C selbstdual.
Je drei Spalten der Kontrollmatrix $H = G$ sind linear unabhängig. Deshalb ist nach Proposition 3.2.27 $d(C) = 4$.

DEFINITION 3.2.29. *Sei C ein linearer $[n,k,d]$–Code in $\mathbb{F}_q^n$. Eine Erzeugermatrix G von C heißt* reduziert, *falls G die Gestalt*

$$G = (E_n|P) = \begin{pmatrix} 1 & & 0 & \\ & \ddots & & P \\ 0 & & 1 & \end{pmatrix}$$

hat, wobei P eine $(k \times (n-k))$–Matrix über $\mathbb{F}_q$ ist.
Zwei Codes C, C' aus $\mathbb{F}_q^n$ heißen äquivalent, *wenn es eine Permutation $\sigma \in \mathfrak{S}_n$ gibt mit*

$$(x_1, \ldots, x_n) \in C \Leftrightarrow (x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in C'.$$

Ist $C = C'$, so heißt ein solches $\sigma \in \mathfrak{S}_n$ eine Symmetrie von C. Die Menge aller Symmetrien von C bildet eine Gruppe, *die wir mit* $\mathrm{Sym}(C)$ *bezeichnen.*

BEISPIEL 3.2.30 (Parity Check Code). *Der lineare Code*

$$C = \left\{ (x_1, \ldots, x_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i = 0 \right\}$$

wird als Parity Check Code *bezeichnet. Er hat Dimension* $n-1$*, seine (reduzierte) Erzeugermatrix ist* $G = \left(E_{n-1} | \, (-1,\ldots,-1)^t\right)$ *und seine Minimaldistanz ist* 2 *(Proposition 3.2.21: Zwei Vektoren* $x \neq y \in C$ *können sich nicht in* nur einer *Koordinate unterscheiden).*

Für $q = 2$ *und* $n = 4$ *sieht das so aus:*

$$C = \left\{ (x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 : \sum_{i=1}^{4} x_i = 0 \right\}$$

mit reduzierter Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

BEISPIEL 3.2.31 (Repetitionscode). *Der* Repetitionscode

$$C = \left\{ (x_1,\ldots,x_n) \in \mathbb{F}_q^n : x_1 = \cdots = x_n \right\}$$

ist ein linearer $[n,1,n]$*–Code mit Erzeugermatrix* $G = (1,\ldots,1)$*. Der duale Code* $C^\perp$ *ist*

$$\begin{aligned} C^\perp &= \left\{ x \in \mathbb{F}_q^n : G \cdot x^t = 0 \right\} \\ &= \left\{ (x_1,\ldots,x_n) \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i = 0 \right\}, \end{aligned}$$

also der Parity Check Code *der Länge n. Daher ist die Kontrollmatrix H zu C die* $(n-1) \times n$*–Matrix*

$$H = \left(I_{n-1} \mid (-1,\ldots,-1)^t\right) = \begin{pmatrix} 1 & & 0 & -1 \\ & \ddots & & \vdots \\ 0 & & 1 & -1 \end{pmatrix}.$$

Die linearen Abhängigkeiten von Spalten einer Kontrollmatrix ändern sich natürlich nicht unter einer Basistransformation:

PROPOSITION 3.2.32. *Zu jedem linearen Code C in* $\mathbb{F}_q^n$ *gibt es einen äquivalenten linearen Code mit reduzierter Erzeugermatrix (in bezug auf eine geeignet gewählte Basis).*

BEWEIS. Es seien C ein linearer Code der Dimension k und G seine Erzeugermatrix. G hat *Spaltenrang* (= Zeilenrang) k, also gibt es eine *Permutationsmatrix* $Q \in GL_n\left(\mathbb{F}_q\right)$, sodaß die ersten k Spalten von $G' = G \cdot Q$ *linear unabhängig* sind. Also hat G' die Gestalt $(J'|P')$ mit $J' \in \mathrm{GL}_k\left(\mathbb{F}_q\right)$. Wählen wir nun die Zeilen von J' als Basis von $\mathbb{F}_q^k$, dann hat der Code $C' := \mathbb{F}_q^k \cdot G'$ eine reduzierte Erzeugermatrix (nämlich $(J')^{-1} \cdot G'$ in bezug auf diese Basis) und ist wegen $C \cdot Q = C'$ äquivalent zu C. □

DEFINITION 3.2.33. *Es sei $C \sqsubseteq \mathbb{F}_q^n$ ein linearer Code. Die Summe*

$$W_C(x,y) := \sum_{c \in C} x^{n-\mathbf{w}(c)} y^{\mathbf{w}(c)}$$

ist ein (homogenes) Polynom in $\mathbb{F}_q[x,y]$ und wird als Gewichtspolynom *von C bezeichnet. Man kann es auch in der Form*

$$W_C(x,y) = \sum_{k=0}^{n} c_n(C) \cdot x^{n-k} y^k$$

schreiben, wo $c_n(C)$ die Anzahl aller Codewörter in C vom Gewicht k ist.

BEISPIEL 3.2.34. *Es sei $C \sqsubseteq \mathbb{F}_2^7$ der binäre $[7,4,3]_2$-Code, der durch*

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

erzeugt wird. Dann gilt $W_C(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7$, denn die Liste der $2^4 = 16$ Codewörter von C, gegliedert nach ihrem Gewicht, ist

Gewicht	*Codewörter in C mit diesem Gewicht*
0	*0000000*
3	*1101000, 1010100, 0110010, 0001110, 0011001, 0100101, 1000011*
4	*0111100, 1011010, 1100110, 1110001, 1001101, 0101011, 0010111*
7	*1111111*

Also ist $c_0(C) = c_7(C) = 1$ und $c_3(C) = c_4(C) = 7$; alle andren $c_i(C)$ sind 0. Sichtlich gilt $d(C) = 3$, und der Code ist perfekt *(siehe Definition 3.2.18), denn die Kugelpackungsschranke aus Satz* 3.2.17*, wird angenommen:*

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i} = \frac{2^7}{1+7} = 16,$$

und C hat ja 16 Wörter.

Die Gewichtspolynome zu einem linearem Code C und seinem dualen Code $C^\perp$ erfüllen die folgende Identität **[11]**, die nach der englischen Mathematikerin Florence Jessie MacWilliams benannt ist:

PROPOSITION 3.2.35 (MacWilliams Identität). *Es sei C ein linearer $[n,k]_q$–Code und $C^\perp$ sein dualer $[n,n-k]_q$–Code. Dann gilt*

$$W_{C^\perp}(X,Y) = \frac{1}{q^k} W_C(X + (q-1)Y, X - Y).$$

Ohne Beweis. □

3.2.2.1. *Perfekte lineare Codes.* Zur Erinnerung: Ein Code $C \subseteq \mathbb{F}_q^n$ mit ungerader Minimaldistanz $d(C) = 2t+1$ heißt *perfekt*, falls es zu jedem Element $y \in \mathbb{F}_q^n$ *genau ein* Codewort $x \in C$ mit Abstand $d(x,y) \leq t$ gibt. Die Hamming–Kugeln $\{B_H(c,t) : c \in C\}$ mit Radius $t = (d(C)-1)/2$ um die Codewörter $c \in C$ bilden also eine *(Mengen)–Partition* von C, daher gilt

$$\left|\mathbb{F}_q^n\right| = q^n = |C| \times B_H(c,t) = |C| \times \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \tag{3.6}$$

(siehe *Kugelpackungsschranke* (3.3)). Ist C ein *linearer* $[n,k,2\cdot t+1]_q$-Code, so ist $|C| = q^k$, und die Bedingung lautet

$$q^{n-k} = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i. \tag{3.7}$$

BEISPIEL 3.2.36 (Triviale perfekte lineare Codes). *Für ungerades $n \geq 1$ ist der binäre n-fache Repetitions–Code perfekt: Denn das ist ein linearer $[n,1,n]_2$-Code mit $t = (n-1)/2$, und es gilt ja*

binomischer Lehrsatz: $(1+1)^n = \sum \binom{n}{k}$

$$2^{n-1} = \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i}.$$

Ebenso sind die triviales Code $C = \mathbb{F}_q^n$ (als $[n,n,1]$–Code) und $C = \{0\}$ (als $[n,0,\infty]$–Code: Denn $q^{n-0} = (1+(q-1))^n = \sum_{i>0} \binom{n}{i} (q-1)^i$). perfekt.

Wenn man Parameter q,n,k und $d = 2t+1$ findet, die die Bedingung (3.7) erfüllen, so ist damit *nicht* gewährleistet, daß es einen linearen $[n,k,d]_q$–Code gibt:

BEISPIEL 3.2.37. *Für $n = 90$, $k = 78$, $d = 5$ und $q = 2$ ist die Bedingung* (3.7) *erfüllt, denn es ist $n-k = 12$, $t = 2$ und $\binom{90}{2} = 4005$:*

$$2^{12} = 4096 = \sum_{i=0}^{2} \binom{90}{i} = 1 + 90 + 4005.$$

Es gibt aber keinen perfekten linearen $[90,78,5]_2$-Code.

DEFINITION 3.2.38 (Lloyd–Polynom). *Für $n,t \in \mathbb{N}$ ist das* Lloyd–Polynom $L_t(n,x) \in \mathbb{Q}[x]$ *definiert als*

$$L_t(n,x) := \sum_{j=0}^{t} (-1)^j \binom{x-1}{j} \binom{n-x}{t-j} (q-1)^{t-j}.$$

Hier ist der Binomialkoeffizient

$$\binom{x}{j} = \frac{x\cdot(x-1)\cdots(x-j+1)}{j!}$$

natürlich auch als Polynom in $\mathbb{Q}[x]$ aufzufassen.

SATZ 3.2.39. *Sei C ein perfekter Code der Länge n mit $d(C) = 2t+1$. Dann hat das Lloyd–Polynom $L_t(n,x)$* genau *t verschiedene ganzzahlige Nullstellen aus $[n] = \{1,2,\ldots,n\}$.*

Ohne Beweis. □

In Beispiel 3.2.2.1 ist $t = q = 2$, und das Lloyd Polynom ist

$$L_2(90, x) = \sum_{j=0}^{2} (-1)^j \binom{x-1}{j} \binom{90-x}{2-j} = 2x^2 - 182x + 4096.$$

Dieses Polynom hat keine ganzzahlige Nullstelle.

3.2.2.2. *Nichttriviale perfekte lineare Codes.* Tatsächlich gibt es nur drei Möglichkeiten für *nichttriviale* perfekte lineare Codes, die wir hier kurz vorstellen.

DEFINITION 3.2.40. *Sei $\ell \geq 2$ eine natürliche Zahl und $n = \frac{q^\ell - 1}{q-1}$. Ein linearer $[n, n-\ell]_q$–Code C heißt* Hamming–Code, *falls die Spalten seiner Kontrollmatrix paarweise linear unabhängig sind. Wir bezeichnen einen solchen Code mit* Ham $[n, n-\ell]$

PROPOSITION 3.2.41. *Zu jeder natürlichen Zahl $\ell \geq 2$ gibt es einen Hamming–Code der Länge $n = \frac{q^\ell - 1}{q-1}$. Er ist ein perfekter linearer $[n, n-\ell]$–Code mit Minimaldistanz $d(C) = 3$.*

BEWEIS. Wähle aus allen 1–dimensionalen Teilräumen von $\mathbb{F}_q^\ell$ jeweils einen (Spalten–)Vektor $\neq \mathbf{0}$ und bilde aus diesen $n = \frac{q^\ell - 1}{q-1}$ Vektoren eine $l \times n$–Matrix H. H ist Kontrollmatrix eines linearen $[n, n-\ell]_q$–Codes C. Nach Konstruktion sind die Spalten von H paarweise linear unabhängig, aber es gibt sicher 3 linear abhängige Spalten: Aus Satz 3.2.27 folgt $d(C) = 3$. Er erfüllt die Bedingung (3.7), denn

$$q^{n-(n-\ell)} = q^\ell = 1 + n(q-1)$$

hat natürlich die Lösung $n = \frac{q^\ell - 1}{q-1}$; C ist also perfekt. □

BEISPIEL 3.2.42. *Der lineare $[7, 4, 3]_2$–Code aus Beispiel* 3.2.34 *ist ein Hamming–Code mit Kontrollmatrix*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Die folgende Tabelle gibt einige Beispiele für die Parameter $[n, n-\ell]_q$ von Hamming-Codes.

	$q=2$	$q=3$	$q=4$	$q=5$
$\ell=2$	$[3,1]_2$	$[4,2]_3$	$[5,3]_4$	$[6,4]_5$
$\ell=3$	$[7,4]_2$	$[13,10]_3$	$[21,18]_4$	$[31,28]_5$
$\ell=4$	$[15,11]_2$	$[40,36]_3$	$[85,81]_4$	$[156,152]_5$
$\ell=5$	$[31,26]_2$	$[121,116]_3$	$[341,336]_4$	$[781,776]_5$
$\ell=6$	$[63,57]_2$	$[364,358]_3$	$[1365,1359]_4$	$[3906,3900]_5$
$\ell=7$	$[127,120]_2$	$[1093,1086]_3$	$[5461,5454]_4$	$[19531,19524]_5$
$\ell=8$	$[255,247]_2$	$[3280,3272]_3$	$[21845,21837]_4$	$[488281,488273]_5$

Der Schweizer Elektroingenieur M. Golay bemerkte die Identitäten

$$\sum_{i=0}^{3}\binom{23}{i} = 1+23+253+1771 = 2048 = 2^{23-12}$$

$$\sum_{i=0}^{2}\binom{11}{i}2^i = 1+2\cdot 11+4\cdot 55 = 1+22+220 = 243 = 3^{11-6}$$

und fand dazu tatsächlich je einen perfekten linearen Code, nämlich C_{23} und C_{11}.

BEISPIEL 3.2.43 (C_{11}). *Der ternäre* Golay–Code C_{11} *ist durch die Erzeugermatrix*

$$G = \begin{pmatrix} 1&0&0&0&0&0&0&1&2&2&1\\ 0&1&0&0&0&0&1&0&1&2&2\\ 0&0&1&0&0&0&2&1&0&1&2\\ 0&0&0&1&0&0&2&2&1&0&1\\ 0&0&0&0&1&0&1&2&2&1&0\\ 0&0&0&0&0&1&1&1&1&1&1 \end{pmatrix}$$

definiert. Es gilt $d(C_{11}) = 5$, *und* C_{11} *ist ein perfekter linearer* $[11,6,5]_3$*-Code.*

BEISPIEL 3.2.44 (C_{23}). *Der binäre* Golay–Code C_{23} *ist durch die Erzeugermatrix* $G = (I_{12} \mid P)$ *mit*

$$P = \begin{pmatrix} 1&1&0&1&1&1&0&0&0&1&0\\ 1&0&1&1&1&0&0&0&1&0&1\\ 0&1&1&1&0&0&0&1&0&1&1\\ 1&1&1&0&0&0&1&0&1&1&0\\ 1&1&0&0&0&1&0&1&1&0&1\\ 1&0&0&0&1&0&1&1&0&1&1\\ 0&0&0&1&0&1&1&0&1&1&1\\ 0&0&1&0&1&1&0&1&1&1&0\\ 0&1&0&1&1&0&1&1&1&0&0\\ 1&0&1&1&0&1&1&1&0&0&0\\ 0&1&1&0&1&1&1&0&0&0&1\\ 1&1&1&1&1&1&1&1&1&1&1 \end{pmatrix}$$

definiert. Es gilt $d(C_{23}) = 7$, *und* C_{23} *ist ein perfekter linearer* $[23,12,7]_2$*-Code.*

Es fällt auf, daß die ersten 11 Zeilen dieser Matrix "zyklisch nach links wandern" (die zwöfte Zeile ist $(1,\dots,1)$).

PROPOSITION 3.2.45. *Für die Gewichtspolynome des ternären* $[11,6,5]_3$*–Golay–Codes* C_{11} *bzw. des binären* $[23,12,7]_2$*–Golay–Codes* C_{23} *gilt:*

$$W_{C_{11}}(X,1) = 24+110X^2+330X^3+132X^5+132X^6+X^{11},$$
$$W_{C_{23}}(X,1) = 1+253X^7+506X^8+1288X^{11}+1288X^{12}+506X^{15}+253X^{16}+X^{23}.$$

Ohne Beweis. □

SATZ 3.2.46 (Tietäväinen; Leont'ev, Zinov'ev 1973). *Es sei* C *ein nichttrivialer, perfekter, linearer* $[n,k,d]_q$*-Code. Dann tritt genau einer der drei folgenden Fälle ein.*

(1) *C ist ein* $[\frac{q^\ell-1}{q-1}, \frac{q^\ell-1}{q-1} - \ell, 3]_q$*-Hamming-Code, für jedes* $\ell \geq 2$ *und jede Primzahlpotenz* q.
(2) *C ist der* $[23, 12, 7]_2$*-Golay-Code.*
(3) *C ist der* $[11, 6, 5]_3$*-Golay-Code.*

Ohne Beweis. □

3.2.3. Zyklische Codes. Tatsächlich kann man Codes mit "noch mehr algebraischer Struktur" betrachten: Gewisse Untervektorräume von $\mathbb{F}_q^n$ haben überdies die Struktur eines *Ideals* in $\mathbb{F}_q[x]/((x^n-1))$, und das kann man nutzbringend verwenden.

DEFINITION 3.2.47. *Die symmetrische Gruppe* $\mathfrak{S}_n$ *wirkt auf* $\mathbb{F}_q^n$ *durch Permutation der Koordinaten:*

$$\pi(x_1, \ldots, x_n) := \left(x_{\pi(1)}, \ldots, x_{\pi(n)}\right).$$

Sei $C \sqsubseteq \mathbb{F}_q^n$ *ein Code: Die* Symmetriegruppe $\mathrm{Sym}(C)$ *von C ist definiert als die* Untergruppe *der Permutationen* $\pi \in \mathfrak{S}_n$*, die C fixieren:*

$$\mathrm{Sym}(C) := \{\pi \in \mathfrak{S}_n : \ \pi(c) \in C \text{ für alle } c \in C\}.$$

Ein linearer Code $C \sqsubseteq \mathbb{F}_q^n$ *der Länge n heißt* zyklisch*, wenn seine Symmetriegruppe* $\mathrm{Sym}(C)$ *die zyklische Gruppe* C_n *ist, also wenn*

$$(x_1, \ldots, x_n) \in C \Leftrightarrow (x_n, x_1, \ldots, x_{n-1}) \in C$$

gilt.

BEISPIEL 3.2.48. *Der ternäre Code mit Erzeugermatrix* $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$ *ist zyklisch.*

Der binäre Code

$$C = \{(0,0,0,0), (1,0,0,1), (0,1,1,0), (1,1,1,1)\}$$

ist nicht zyklisch; er ist aber äquivalent zu einem zyklischen Code, den man durch Vertauschung der dritten und vierten Koordinate erhält.

Natürlich gibt es auch lineare Codes, die nicht *äquivalent* zu einem zylischen Code sind: Wir werden noch sehen, daß der ternäre Code $\mathrm{Ham}[4,3]$ so ein Beispiel ist.

LEMMA 3.2.49. *Sei*

$$\rho : \mathbb{F}_q^n \to \mathbb{F}_q[x]/((x^n-1)), \quad (a_0, \ldots, a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i x^i.$$

Dann ist ρ *ein* Vektorraum–Isomorphismus.
Es gelten folgende Aussagen.

(1) *Ein linearer Code* $C \sqsubseteq \mathbb{F}_q^n$ *ist genau dann zyklisch, wenn sein Bild* $\rho(C)$ *ein* Ideal *in* $\mathbb{F}_q[x]/((x^n-1))$ *ist.*
(2) *Jedes Ideal im Ring* $\mathbb{F}_q[x]/((x^n-1))$ *ist ein* Hauptideal *und wird von einem Teiler des Polynoms* $x^n - 1$ *erzeugt.*

BEWEIS. Daß ρ ein Vektorraum–Isomorphismus ist, ist leicht zu sehen: Denn die Addition von Polynomen bzw. die Multiplikation mit Skalaren entspricht ja genau den entsprechenden Operationen für die "Koeffizienten–Vektoren" der Polynome.

Ad (1): Wegen $x^n \equiv 1 \pmod{x^n - 1}$ gilt

$$\begin{aligned} x \cdot \sum_{i=0}^{n-1} a_i x^i &= a_0 x + a_1 x^2 + a_- 2x^3 + \cdots + a_{n-1} x^n \\ &\equiv a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} \pmod{x^n - 1}. \end{aligned}$$

Ein linearer Code C ist also genau dann zyklisch, wenn $x \cdot \rho(C) \sqsubseteq \rho(C)$ gilt. Das ist aber genau dann der Fall, wenn $\rho(C)$ ein Ideal in $\mathbb{F}_q[x]/((x^n - 1))$ ist[7].

Ad (2): Sei $\pi : \mathbb{F}_q[x] \to \mathbb{F}_q[x]/((x^n - 1))$ der kanonische Ring–Epimorphismus. Sei $I \sqsubseteq \mathbb{F}_q[x]/((x^n - 1))$ ein Ideal, dann haben wir also einen zusammengesetzten Ring–Epimorphismus

$$\mathbb{F}_q[x] \to \mathbb{F}_q[x]/((x^n - 1)) \to \left(\mathbb{F}_q[x]/((x^n - 1))\right)/I,$$

und wenn wir dessen Kern betrachten, sehen wir: Die Ideale in $\mathbb{F}_q[x]/((x^n - 1))$ sind die Bilder der Ideale in $\mathbb{F}_q[x]$ unter π; für ein Ideal I in $\mathbb{F}_q[x]/((x^n - 1))$ ist also $\pi^{-1}(I)$ ein Ideal in $\mathbb{F}_q[x]$. Da $\mathbb{F}_q$ ein Körper ist, ist $\mathbb{F}_q[x]$ ein Hauptidealring. Also wird $\pi^{-1}(I)$ von einem Polynom $g(x) \in \mathbb{F}_q[x]$ erzeugt: $\pi^{-1}(I) = ((g))$. Wegen $\pi(x^n - 1) = 0$ gilt dann

$$((x^n - 1)) \subseteq \pi^{-1}(I) = ((g(x))),$$

d.h. $g(x) \mid x^n - 1$ in $\mathbb{F}_q[x]$. □

Im Lichte von Lemma 3.2.49 betrachten wir ab jetzt einen zyklischen Code C immer als Ideal in $\mathbb{F}_q[x]/((x^n - 1))$.

DEFINITION 3.2.50. *Es sei $C \sqsubseteq \mathbb{F}_q[x]/((x^n - 1))$ (gedeutet, wie gesagt, als ein Ideal in $\mathbb{F}_q[x]/((x^n - 1))$) ein zyklischer Code. Sei $g(x)$ das eindeutig bestimmte* normierte *Polynom* minimalen Grades *mit $C = ((g(x)))$. Dann heißt $g(x)$ das* Erzeugerpolynom *und $h(x) = (x^n - 1)/g(x)$ das* Kontrollpolynom *von C.*

BEISPIEL 3.2.51. *Der ternäre zyklische Code aus Beispiel* 3.2.48 *hat das Erzeugerpolynom $g(x) = x + 2$ und das Kontrollpolynom $h(x) = x^2 + x + 1$. Denn in $\mathbb{F}_3[x]/((x^3 - 1))$ gilt $\operatorname{ggT}\left(1 + 2x^2, 2x + x^2\right) = 1 + 2x = x + 2$, also wird $I = ((1 + 2x^2, x + 2x^2))$ von $g(x) = x + 2$ erzeugt. Es besteht aus den Polynomen, deren Koeffizientensumme gleich Null ist in $\mathbb{F}_3$. Wegen $(x + 2)\left(x^2 + x + 1\right) = x^3 - 1$ über $\mathbb{F}_3$ ist $h(x) = x^2 + x + 1$ das Kontrollpolynom.*

[7] Denn $\rho(C)$ ist als Teilraum klarerweise eine (additive) Untergruppe von $\mathbb{F}_q[x]/((x^n - 1))$, die *abgeschlossen* ist unter der Multiplikation mit Skalaren aus dem Grundkörper $\mathbb{F}_q$; und wenn $\rho(C)$ auch abgeschlossen ist unter der Multiplikation mit x, dann auch unter der Multiplikation mit x^n, also auch unter der Multiplikation mit $\lambda_n \cdot x^n$, also auch unter der Multiplikation mit $\sum \lambda_i \cdot x^i$.

PROPOSITION 3.2.52. *Sei $C \sqsubseteq \mathbb{F}_q^n$ ein zyklischer $[n,k]$–Code mit Erzeugerpolynom g, also*

$$C \simeq (\!(g)\!) \sqsubseteq \mathbb{F}_q[x] / (\!(x^n - 1)\!)$$

im Sinne des Vektorraum–Isomorphismus aus Lemma 3.2.49. Dann hat das Erzeugerpolynom Grad $n-k$, und C hat die Basis

$$\left\{ x^j \cdot g \colon \ j = 0, 1, \ldots, k-1 \right\}$$

(als Vektorraum über $\mathbb{F}_q$; wieder im Sinne des Isomorphismus aus Lemma 3.2.49).

BEWEIS. Die Quotientenabbildung

$$\psi \colon \ \left(\mathbb{F}_q[x] / (\!(x^n - 1)\!) \right) \to \left(\mathbb{F}_q[x] / (\!(x^n - 1)\!) \right) / (\!(g)\!)$$

ist eine *lineare Abbildung*, die

- jedes Basis–Monom x^m mit $m < \deg g$ auf sich selbst abbildet,
- jedes Basis–Monom x^m mit $m \geq \deg g$ auf eine Linearkombination von Basis–Monomen x^l mit $l < \deg g$ abbildet.

Das Bild von ψ wird also aufgespannt von den linear unabhängigen Vektoren $x^0, x^1, \ldots, x^{\deg g - 1}$; daher ist

$$\dim \left(\mathbb{F}_q[x] / (\!(x^n - 1)\!) \right) / (\!(g)\!) = \deg g.$$

Im Sinne des Vektorraum–Isomorphismus aus Lemma 3.2.49 ist das gleichbedeutend mit

$$n - k = \dim \mathbb{F}_q^n / C = \deg g.$$

Daher haben die Polynome $\left\{ x^j \cdot g \colon \ j = 0, 1, \ldots, k-1 \right\}$ alle Grad kleiner n und liegen somit in $C \sqsubseteq \mathbb{F}_q[x] / (\!(x^n - 1)\!)$; ganz offensichtlich sind sie *linear unabhängig* und bilden somit eine Basis für $(\!(g)\!) \simeq C$. □

LEMMA 3.2.53. *Für einen zyklischen Code $C \sqsubseteq \mathbb{F}_q[x] / (\!(x^n - 1)\!)$ mit Kontrollpolynom $h(x)$ gilt die* Kontrollgleichung

$$f \in C \iff f \cdot h \equiv 0 \text{ in } \mathbb{F}_q[x] / (\!(x^n - 1)\!), \tag{3.8}$$

d.h.,

$$C = \left\{ f(x) \in \mathbb{F}_q[x] / (\!(x^n - 1)\!) \colon \ f \cdot h \equiv 0 \right\}.$$

BEWEIS. Da $C = (\!(g)\!)$, ist jedes Polynom $f \in C$ ein Vielfaches des Erzeugerpolynoms g: $f = a \cdot g$ für ein gewisses Polynom $a(x) \in \mathbb{F}_q[x] / (\!(x^n - 1)\!)$. Wegen $g \cdot h = x^n - 1 \equiv 0$ in $\mathbb{F}_q[x] / (\!(x^n - 1)\!)$ erfüllt f daher die Kontrollgleichung (3.8) $f(x) \cdot h(x) = 0$.

Umgekehrt gilt für jedes f mit $f \cdot h \equiv 0 \iff (x^n - 1) = g \cdot h \mid f \cdot h$ die Teilerbedingung $g \mid f$, also ist $f \in C$. □

BEISPIEL 3.2.54. *Die Kontrollgleichung für den zyklischen Code*

$$C = (\!(x + 2)\!) \sqsubseteq \mathbb{F}_3[x] / (\!(x^3 - 1)\!)$$

lautet also

$$\begin{aligned} f \cdot h &= \left(a_2x^2 + a_1x + a_0\right)\left(x^2 + x + 1\right) \\ &= a_0 + (a_0 + a_1)\,x + (a_0 + a_1 + a_2)\,x^2 + (a_1 + a_2)\,x^3 + a_2x^4 \\ &\equiv (a_0 + a_1 + a_2)\left(x^2 + x + 1\right) \quad \leftarrow x^3 \equiv 1 \pmod{x^3 - 1} \\ &\equiv 0 \pmod{x^3 - 1}. \end{aligned}$$

Also ist

$$C = \{(a_2x^2 + a_1x + a_0 \in \mathbb{F}_3[x]/(x^3 - 1) \mid a_0 + a_1 + a_2 = 0 \text{ in } \mathbb{F}_3\}.$$

(Vergleiche auch Beispiel 3.2.51.)

Sei in $\mathbb{F}_q[x]$ die Faktorisierung $x^n - 1 = f_1 \cdot f_2 \cdot \cdots \cdot f_r$ in r normierte irreduzible Faktoren. Das Polynom $x^n - 1$ hat dann 2^r normierte Teiler, und diese erzeugen insgesamt 2^r zyklische Codes in $\mathbb{F}_q^n$, die aber nicht paarweise inäquivalent sein müssen.

BEISPIEL 3.2.55. *Für $n = 4$ und $q = 3$ gibt es genau 8 zyklische Codes in $\mathbb{F}_3^4$, gegeben durch die Erzeugerpolynome*

$$1, x + 2, x + 1, x^2 + 1, x^2 + 2, x^3 + 2x^2 + x + 2, x^3 + x^2 + x + 1, x^4 - 1.$$

Die Faktorisierung ist nämlich

$$x^4 - 1 = (x + 2)\,(x + 1)\left(x^2 + 1\right),$$

und man erhält die 6 nichttrivialen Teiler

$$x + 2, x + 1, x^2 + 1, (x + 2)\,x + 1, (x + 2)\,x^2 + 1, (x + 1)\left(x^2 + 1\right).$$

Für die trivialen Teiler ist klar: Das Polynom 1 erzeugt ganz $\mathbb{F}_3^4$, das Polynom $x^4 - 1$ den $\mathbf{0}$-Code.

KOROLLAR 3.2.56. *Der Hamming–Code* $\mathrm{Ham}[4, 2]$ *über $\mathbb{F}_3$ ist nicht äquivalent zu einem zyklischen Code.*

BEWEIS. Der Hamming–Code $\mathrm{Ham}[4, 2]$ über $\mathbb{F}_3$ hat (wie alle Hamming–Codes) Minimaldistanz $d = 3$ und Dimension $k = n - \ell = \frac{3^2-1}{3-1} - 2 = 2$.
In der Liste aller ternären zyklischen Codes der Länge 4 aus Beispiel 3.2.55 müssen wir also die beiden Codes der Dimension 2 betrachten, die von $x^2 + 1$ bzw. von $x^2 + 2$ erzeugt werden.
Im Fall $g(x) = x^2 + 1$ ist das Kontrollpolynom $h(x) = x^2 + 2$, und Erzeugermatrix G bzw. Kontrollmatrix H sind gegeben durch

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$

Damit hat der Code Minimaldistanz $2 \neq 3$ nach Proposition 3.2.27.
Für $g(x) = x^2 + 2$ gilt $h(x) = x^2 + 1$ (G und H tauschen die Rollen), und der Code hat ebenso Minimaldistanz $2 \neq 3$. □

Tatsächlich kann man folgendes Resultat zeigen (siehe auch Proposition 3.2.69) das wir hier allerdings nicht beweisen:

PROPOSITION 3.2.57. *Ein Hamming–Code* $\mathrm{Ham}\,[n, n-\ell]$ *über* $\mathbb{F}_q$ *ist genau dann zu einem zyklischen Code äquivalent, wenn* $\mathrm{ggT}\,(\ell, q-1)) = 1$.

Es liegt auf der Hand, daß es zwischen Erzeugermatrix und Erzeugerpolynom bzw. zwischen Kontrollmatrix und Kontrollpolynom einen Zusammenhang gibt:

PROPOSITION 3.2.58. *Sei C ein zyklischer $[n,k]$–Code mit Erzeugerpolynom $g = \sum_{i=0}^{n-k} g_i \cdot x^i$ und Kontrollpolynom $h = \sum_{i=0}^{k} h_i \cdot x^i$. Dann ist die $k \times n$–Matrix*

$$G = \left(g_{j-i}\right)_{(1,1)}^{(k,n)} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-k-1} & g_{n-k} & \cdots & 0 \\ \vdots & & & & & & \\ 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix}$$

eine Erzeugermatrix von C, und die $(n-k) \times n$–Matrix

$$H = \left(h_{k+i-j}\right)_{(1,1)}^{(n-k,n)} = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & \cdots & 0 \\ \vdots & & & & & & \\ 0 & \cdots & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{pmatrix}$$

ist eine Kontrollmatrix von C.

BEWEIS. Gemäß Proposition 3.2.52 ist $\left\{x^j \cdot g\colon\ j = 0, 1, \ldots, k-1\right\}$ eine Basis von C: Das "sind" (im Sinne des Vektorraum–Isomorphismus aus Lemma 3.2.49) aber genau die Zeilen der angegebenen Matrix G, die daher eine Erzeugermatrix ist.

Definitionsgemäß ist $g \cdot h = x^n - 1$, also erhalten wir mit Koeffizientenvergleich

$$\sum_{l=1}^{n-k} g_l \cdot h_{m-l} = 0 \text{ für } m = 1, 2, \ldots, n-1.$$

Diese Summe ist aber exakt der Eintrag in Position $(k+j-m, j)$ (immer derselbe, für $j = 1, 2, \cdots n-k$) der Matrix $G \cdot H^t$

$$\sum_s g_{s-k-j+m} \cdot h_{k+j-s} \ \leftarrow \text{Indextransformation: } l{=}s{-}k{-}j{+}m,$$

also gilt

$$G \cdot H^t = 0.$$

Außerdem gilt (wieder mit Koeffizientenvergleich)

$$g_0 \cdot h_0 = -1,$$

also ist $h_0 \neq 0$, die Zeilen von H sind also offensichtlich linear unabhängig, und H hat daher Rang $n-k$: H ist also eine Kontrollmatrix von C. □

3.2.3.1. *Zyklische Codes, die von einem Idempotent erzeugt werden.*

DEFINITION 3.2.59. *Ein Element e eines kommutativen Ringes R mit 1 heißt* Idempotent, *falls $e^2 = e$ gilt. Dann gilt*

$$R = e \cdot R \oplus (1 - e) \cdot R,$$

denn $e \cdot x = (1 - e) \cdot y \implies e^2 \cdot x = e \cdot x = \left(e - e^2\right) \cdot y = 0.$

BEISPIEL 3.2.60. *Es ist z.B.* $3 \in \mathbb{Z}_6$ *ein Idempotent, denn* $3^2 = 9 \equiv 3 \pmod 6$. $1 - 3 = -2 \equiv 4 \pmod 6$, *und tatsächlich ist jede Restklasse modulo 6 eindeutig als Summe eines Vielfachen (in $\mathbb{Z}_6$) von 3 und von 4 darstellbar:* $0 = 0 \cdot 3 + 0 \cdot 4$, $1 = 1 \cdot 3 + 1 \cdot 4, 2 = 0 \cdot 3 + 2 \cdot 4, 3 = 1 \cdot 3 + 0 \cdot 4, 4 = 0 \cdot 3 + 1 \cdot 4$ *und* $5 = 1 \cdot 3 + 2 \cdot 4$.

Wird ein zyklischer Code C von einem Idempotent e erzeugt (also $C = (\!(e)\!)$), so ist $c \in C$ genau dann, wenn $e \cdot c = c$ gilt: $\Leftarrow$ ist klar, und aus $c = e \cdot g$ folgt $e \cdot c = e^2 \cdot g = e \cdot g = c$.

PROPOSITION 3.2.61. *Es sei* $\operatorname{ggT}(n, q) = 1$. *Dann wird jeder zyklische Code* $C \sqsubseteq \mathbb{F}_q[x] / (\!(x^n - 1)\!)$ *von genau einem Idempotent in* $\mathbb{F}_q[x] / (\!(x^n - 1)\!)$ *erzeugt.*

BEWEIS. Es ist

$$\operatorname{ggT}\left(x^n - 1, \mathrm{D}\left(x^n - 1\right)\right) = \operatorname{ggT}\left(x^n - 1, n \cdot x^{n-1}\right) = 1$$

(da $\operatorname{ggT}(n, q) = 1$, ist $n \neq 0$ in $\mathbb{F}_q$). Nach Lemma 2.1.11 hat $x^n - 1$ also keinen quadratischen Faktor: Erzeugerpolynom g und Kontrollpolynom h sind also teilerfremd, denn $x^n - 1 = g(x) \cdot h(x)$. Also existieren Polynome $a, b \in \mathbb{F}_q[x]$ mit

$$1 = a(x) \cdot g(x) + b(x) \cdot h(x).$$

Wir behaupten:

$$e(x) = a(x) \cdot g(x) = 1 - b(x) \cdot h(x)$$

ist ein Idempotent in $\mathbb{F}_q[x] / (\!(x^n - 1)\!)$. Denn wir rechnen einfach nach:

$$\begin{aligned} e^2 &= a \cdot g \cdot (1 - b \cdot h) \\ &= a \cdot g - a \cdot b \cdot (x^n - 1) \\ &\equiv a \cdot g = e \pmod{x^n - 1}. \end{aligned}$$

Weil jedes Codewort $c \in C$ ein Vielfaches von g ist, wirkt die Multiplikation mit $e = 1 - b \cdot h$ als Identität auf C:

$$c = g \cdot d \implies e \cdot c = (1 - b \cdot h) \cdot g \cdot d = 1 \cdot g \cdot d = c.$$

Insbesondere ist $e \cdot g = g$. Das heißt aber:

$$(\!(e)\!) = (\!(a \cdot g)\!) \sqsubseteq (\!(g)\!) = (\!(e \cdot g)\!) \sqsubseteq (\!(e)\!).$$

Sei e' ein weiteres Idempotent mit $C = (\!(e')\!)$. Dann ist aber $e' \cdot c = c$ *und* $e \cdot c = c$ für alle $c \in C$, also insbesondere

$$e = e' \cdot e = e \cdot e' = e'.$$

Damit ist auch die Eindeutigkeit von e gezeigt. □

BEISPIEL 3.2.62. *Sei* $C = ((g)) \sqsubseteq \mathbb{F}_3[x] / ((x^{11} - 1))$ *der zyklische Code mit Erzeugerpolynom*

$$g(x) = x^5 + x^4 - x^3 + x^2 - 1.$$

Dann ist C *der perfekte* $[11, 6, 5]_3$*–Golay–Code: Er wird von dem Idempotent* $e(x) = -x^{10} - x^8 - x^7 - x^6 - x^2$ *erzeugt.*
Denn die Faktorisierung von $x^{11} - 1$ *in irreduzible Faktoren über* $\mathbb{F}_3$ *lautet*

$$x^{11} - 1 = (x - 1)\left(x^5 + x^4 - x^3 + x^2 - 1\right)\left(x^5 - x^3 + x^2 - x - 1\right).$$

Beide Polynome fünften Grades erzeugen übrigens äquivalente $[11, 6, 5]_3$*–Codes. Es ist* $\operatorname{ggT}(11, 3) = 1$*. Das Kontrollpolynom zu*

$$g(x) = x^5 + x^4 - x^3 + x^2 - 1$$

ist also

$$h(x) = (x - 1)\left(x^5 - x^3 + x^2 - x - 1\right) = x^6 - x^5 - x^4 - x^3 + x^2 + 1.$$

Die Polynome g *und* h *sind teilerfremd, und wir finden* $a(x) = -x^6 - x^4 + x^3 - 1$ *und* $b(x) = x^5 - x^4 + x^2$ *mit*

$$a \cdot g + b \cdot h = 1$$

in $\mathbb{F}_3[x] / ((x^{11} - 1))$*. Damit ist* $e = a \cdot g = -x^{10} - x^8 - x^7 - x^6 - x^2$ *in* $\mathbb{F}_3[x] / ((x^{11} - 1))$*.*

BEISPIEL 3.2.63. *Der zyklische Code aus Beispiel 3.2.48 bzw. Beispiel 3.2.51 erfüllt nicht die Voraussetzung* $\operatorname{ggT}(n, q) = 1$*.*
In diesem Fall hat $x^3 - 1$ *nicht lauter verschiedene irreduzible Teiler:* $x^3 - 1 = (x + 2)^3$*; und es gibt kein Idempotent wie in Proposition 3.2.61, da* $g(x) = x + 2$ *und* $h(x) = x^2 + x + 1 = (x + 2)^2$ *nicht teilerfremd sind.*

3.2.3.2. *Zyklische Codes: "Abgeschlossen" unter Dualisierung.*

DEFINITION 3.2.64. *Sei* $f \in \mathbb{K}[x]$*,* $\deg f = n$*. Dann definieren wir das zu* f duale Polynom $f^\star$ *als*

$$f^\star(x) := x^n \cdot f\left(\frac{1}{x}\right).$$

Das heißt:

$$f(x) = \sum_{k=0}^{n} f_k \cdot x^k \iff f^\star(x) = \sum_{k=0}^{n} f_{n-k} \cdot x^k = \sum_{k=0}^{n} f_k \cdot x^{n-k}$$

PROPOSITION 3.2.65. *Sei* $g(x)$ *mit* $\deg g = (n - k)$ *das Erzeugerpolynom eines zyklischen Codes* $C \sqsubseteq \mathbb{F}_q[x] / ((x^n - 1))$*, und sei* $h(x)$ *das zugehörige Kontrollpolynom. Dann ist* $\dim C = k$*, und der duale Code* $C^\perp$ *ist ebenfalls ein zyklischer Code mit* $\dim C^\perp = n - k$*; sein Erzeugerpolynom* $g^\perp(x)$ *und sein Kontrollpolynom* $h^\perp(x)$ *sind*

$$g^\perp(x) = h(0)^{-1} \cdot h^\star(x),$$
$$h^\perp(x) = g(0)^{-1} \cdot g^\star(x).$$

Überdies ist $C^\perp$ äquivalent zu $((h))$, dem von h erzeugten zyklischen Code. Die Klasse der zyklischen Codes ist also abgeschlossen unter Dualisierung.

BEWEIS. Wir wissen:

$$H \text{ ist Kontrollmatrix von } C \iff H \text{ ist Erzeugermatrix von } C^\perp.$$

Aus Proposition 3.2.58 sehen wir aber: Die vom Kontrollpolynom h abgeleitete Kontrollmatrix H entspricht einer vom Polynom $h^\star$ abgeleiteten *Erzeugermatrix*; also ist $C^\perp = ((h^\star))$, und wenn wir h noch normieren, dann erhalten wir das Erzeugerpolynom von $C^\perp$:

$$h(0)^{-1} \cdot h^\star(x).$$

Analoges gilt für das Kontrollpolynom von $C^\perp$.
Die Polynome h und $h^\star$ erzeugen äquivalente Codes, denn die entsprechenden Erzeugermatrizen unterscheiden sich nur um eine Umordnung der Spalten. □

3.2.3.3. *Reformulierung mit dem algebraischen Abschluß.* Wir können diese Resultate auch durch die Nullstellenmengen von Erzeugerpolynom und Kontrollpolynom im *algebraischen Abschluss* von $\mathbb{F}_q$ formulieren; im folgenden verwenden wir die Abkürzung $R_n = \mathbb{F}_q[x]/((x^n - 1))$ und setzen $\operatorname{ggT}(n,q) = 1$ voraus:

PROPOSITION 3.2.66. *Es sei $C \sqsubseteq R_n$ ein zyklischer Code. Dann gibt es eine Menge $U(C)$ von n–ten Einheitswurzeln aus dem algebraischen Abschluß von $\mathbb{F}_q$ mit*

$$C = \{f(x) \in R_n \colon\ f(u) = 0 \text{ für alle } u \in U(C)\}.$$

BEWEIS. Das Erzeugerpolynom $g(x)$ von C besitzt als Teiler von $x^n - 1$ nur n–te Einheitswurzeln (aus dem algebraischen Abschluß von $\mathbb{F}_q$) als Nullstellen. Da alle Codewörter aus C Vielfache von $g(x)$ sind, folgt die Behauptung mit

$$U(C) = \left\{u \in \overline{\mathbb{F}}_q \colon\ g(u) = 0\right\}. \quad \square$$

KOROLLAR 3.2.67. *Sei $C \sqsubseteq R_n$ ein zyklischer $[n,k]$-Code, dessen erzeugendes Polynom g Nullstellenmenge*

$$U(C) = \{u_1, \dots u_{n-k}\}$$

habe. Für die Vandermonde–Matrix

$$L = \begin{pmatrix} 1 & u_1 & \cdots & u_1^{n-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & u_{n-k} & \cdots & u_{n-k}^{n-1} \end{pmatrix}$$

gilt dann

$$C = \left\{ \sum_{i=0}^{n-1} a_i x^i \in R_n \colon\ L \cdot (a_0, \dots, a_{n-1})^t = 0 \right\}.$$

BEWEIS. Das ist nur eine Umformulierung von Proposition 3.2.66. □

Es bezeichne $U_n = \left\{u \in \overline{\mathbb{F}}_q \colon\ u^n = 1\right\}$ die Menge aller n-ten Einheitswurzeln im algebraischen Abschluß $\overline{\mathbb{F}}_q$ von $\mathbb{F}_q$.

KOROLLAR 3.2.68. *Es sei $C \sqsubseteq R_n$ ein zyklischer Code über $\mathbb{F}_q$, seien $U(C)$ sowie $U\left(C^\perp\right)$ die zugehörigen Nullstellenmengen von C und $C^\perp$. Dann sind $U(C)^{-1}$ und $U\left(C^\perp\right)$ komplementär in U_n, d.h. es gilt*

$$U\left(C^\perp\right) = U_n \setminus \left\{u^{-1} \colon\ u \in U(C)\right\}.$$

BEWEIS. Nach Proposition 3.2.65 gilt für das Erzeugerpolynom $g^\perp(x)$ zu $C^\perp$

$$g^\perp\left(u^{-1}\right) = h(0)^{-1} h(u) u^{-k}.$$

Da das Kontrollpolynom $h(x)$ die Nullstellenmenge $U_n \setminus U(C)$ besitzt, folgt daraus die Behauptung. □

3.2.3.4. *Zyklische Hamming–Codes.* Wir wollen noch einmal auf die Hamming–Codes $\mathrm{Ham}[n, n-\ell]$ zurückkommen. Wegen

$$n = \frac{q^\ell - 1}{q-1} = q^{\ell-1} + \cdots + q + 1$$

gilt $\mathrm{ggT}(n,q) = 1$, daher haben zyklische Hamming–Codes gemäß Proposition 3.2.61 ein erzeugendes Idempotent. Zudem können wir die zyklischen Hamming-Codes wie folgt beschreiben. Laut Proposition 3.2.57 (unbewiesen) sind Hamming–Codes genau dann zu einem zyklischen Code äquivalent, wenn $\mathrm{ggT}(\ell, q-1) = 1$ gilt.

PROPOSITION 3.2.69. *Es seien $\ell \geq 2$ eine ganze Zahl, und q eine Primzahlpotenz mit $\mathrm{ggT}(\ell, q-1) = 1$. Es sei $n = \frac{q^\ell - 1}{q-1}$ und $u \in \mathbb{F}_{q^\ell}$ eine primitive n–te Einheitswurzel (wobei $\mathbb{F}_{q^\ell}$ ein geeigneter Erweiterungskörper von $\mathbb{F}_q$ ist, in dem $x^n - 1$ eine Nullstelle hat). Dann ist der zyklische Code*

$$C = \{f(x) \in R_n \colon\ f(u) = 0\}$$

äquivalent zu $\mathrm{Ham}[n, n-\ell]$.

BEWEIS. Aus $\mathrm{ggT}(\ell, q-1) = 1$ folgt auch $\mathrm{ggT}(n, q-1) = 1$ wegen

$$\begin{aligned} n &= q^{\ell-1} + \cdots + q + 1 \\ &= \ell + (q-1) \cdot \left(q^{\ell-2} + 2q^{\ell-3} + 3q^{\ell-4} + \cdots + (\ell-2)q + (\ell-1)\right), \end{aligned}$$

also $n \equiv l \pmod{q-1}$: Denn dann gibt es $i, j, k \in \mathbb{Z}$ sodaß

$$1 = i \cdot l + j \cdot (q-1) = i \cdot (n + k \cdot (q-1)) + j \cdot (q-1).$$

Wegen $\mathrm{ord}(u) = n$ gilt $u^m = 1 \implies n \mid m$, daher ist $u^{j(q-1)} \neq 1$ und $u^j \notin \mathbb{F}_q$ für $j = 1, \ldots, n-1$[8]. Sei H die Matrix, deren Spalten die Vektordarstellungen von $1, u, u^2, \ldots, u^{n-1}$ in $\mathbb{F}_q^\ell$ sind. Dann sind diese Spalten paarweise linear unabhängig über $\mathbb{F}_q$ (denn $u^j = \lambda \cdot u^k \implies u^{j-k} = \lambda \in \mathbb{F}_q$, ein Widerspruch), und somit ist H eine Kontrollmatrix eines Hamming–Codes, nämlich von $\mathrm{Ham}[n, n-\ell]$. Dieser Hamming–Code *ist* C, denn die *Polynomgleichung*

$\mathbb{F}_q^\ell \equiv \mathbb{F}_{q^\ell}$ als Vektorräume!

[8] Denn $n \nmid j \cdot (q-1)$ für $0 < j < n$, also kann u^j auch nicht in $\mathbb{F}_q^\star$ liegen; denn dann *wäre* $\left(u^j\right)^{q-1} = 1$.

$f(u) = 0$ bedeutet in $\mathbb{F}_q^\ell \equiv \mathbb{F}_{q^\ell}$ ja die *lineare Gleichung* $f_0 \cdot u^0 + f_1 u^1 + \cdots + f_{n-1} u^{n-1} = 0$. □

Für $q = 2$ ist die Bedingung ggT $(\ell, q-1) = 1$ natürlich immer erfüllt.

DEFINITION 3.2.70. *Ein normiertes Polynom $p(x) \in \mathbb{F}_q[x]$ heißt* primitiv, *wenn es eine Nullstelle α in $\mathbb{F}_{q^m}$ hat, die ein primitives Element ist, also mit*

$$\mathbb{F}_{q^m} = \left\{0, \alpha, \alpha^2, \ldots, \alpha^{q^m-2}, \alpha^{q^m-1} = 1\right\},$$

und wenn $p(x)$ das Polynom kleinsten Grades *ist, das α als Nullstelle hat.*

PROPOSITION 3.2.71. *Ist $p(x) \in \mathbb{F}_2[x]$ ein primitives Polynom vom Grad $\ell \geq 2$, dann ist der zyklische Code $C = ((p(x))) \sqsubseteq \mathbb{F}_2[x] / ((x^{2^\ell - 1} - 1))$ äquivalent zum binären $\left[2^\ell - 1, 2^\ell - \ell - 1\right]$–Hamming-Code.*

BEWEIS. Eine Nullstelle α des primitiven Polynoms $p(x)$ können wir mit der Äquivalenzklasse des Polynoms $x \in \mathbb{F}_2[x] \pmod{p(x)}$ identifizieren. Wie in Proposition 3.2.69 ist die Kontrollmatrix also durch $H = (1 \; x \; x^2 \; \ldots \; x^{2^\ell - 2})$ gegeben, wenn wir x^i als Spaltenvektor in $\mathbb{F}_2^\ell$ auffassen. Also gilt mit $q = 2$, $n = 2^\ell - 1$ und $C = \text{Ham}[n, n-\ell]$ die Kontrollgleichung

$$\begin{aligned} C &= \left\{(a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n \colon \; a_0 \cdot x^0 + a_1 \cdot x^1 + \cdots + a_{n-1} \cdot x^{n-1} = 0 \text{ in } \mathbb{F}_2^\ell\right\} \\ &= \{f(x) \in \mathbb{F}_2[x] / ((x^n - 1)) \colon \; p(x) \mid f(x)\} \\ &= ((p)) \sqsubseteq \mathbb{F}_2[x] / ((x^n - 1)). \end{aligned}$$

□

BEISPIEL 3.2.72. *Sei $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$: Dann ist der zyklische Code $C = ((p)) \sqsubseteq \mathbb{F}_2[x] / ((x^7 - 1))$ äquivalent zum $[7,4]_2$–Hamming-Code aus Beispiel 3.2.42. Er hat das Idempotent $e(x) = x^4 + x^2 + x$.*
Denn für $q = 2$, $\ell = 3$ und $n = 2^3 - 1 = 7$ ist das Polynom $x^7 - 1$ separabel *über $\mathbb{F}_2$, seine Faktorisierung ist*

$$x^7 - 1 = (x+1)\left(x^3 + x^2 + 1\right)\left(x^3 + x + 1\right).$$

Das Polynom $p(x) = x^3 + x + 1$ ist primitiv, und es gilt

$$\begin{aligned} &\mathbb{F}_2[x] / ((p(x))) = \\ &\quad \left\{0, x, x^2, x^3 = x+1, x^4 = x^2 + x, x^5 = x^2 + x + 1, x^6 = x^2 + 1, x^7 = 1\right\}. \end{aligned}$$

Wenn wir diese Polynome als Spaltenvektoren in $\mathbb{F}_2^3$ schreiben, erhalten wir die Kontrollmatrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Bis auf zyklische Permutation der letzten drei Spalten ist das genau die Kontrollmatrix des $[7,4]$-Hamming-Code aus Beispiel 3.2.42. Zu dem Erzeugerpolynom $g(x) = x^3 + x + 1$ gehört das Kontrollpolynom $h(x) = (x+1)x^3 + x^2 + 1 = x^4 + x^2 + x + 1$.

TABELLE 1. Tabelle primitiver Polynome f über $\mathbb{F}_2$

$\deg f$	$f(x)$
2	x^2+x+1
3	x^3+x+1
4	x^4+x+1
5	x^5+x^2+1
6	x^6+x+1
7	x^7+x^3+1
8	$x^8+x^4+x^3+x^2+1$
9	x^9+x^4+1
10	$x^{10}+x^3+1$

Wir haben $a(x)\cdot g(x)+b(x)\cdot h(x)=1$ *mit* $a(x)=x$ *und* $b(x)=1$, *also ist* $e(x)=a(x)\cdot g(x)=x^4+x^2+x \mod x^7-1$ *das Idempotent.*

BEMERKUNG 3.2.73. *Ein irreduzibles Polynom* $f(x)\in\mathbb{F}_2[x]$ *mit* $\deg f=\ell$ *ist genau dann primitiv, wenn die kleinste positive Zahl* n, *für die* $f(x)\mid x^n-1$ *gilt, durch* $n=2^\ell-1$ *gegeben ist.*

BEISPIEL 3.2.74. *Sei* $f(x)=x^4+x+1$: $\ell=\deg f=4$, *und* f *ist irreduzibel über* $\mathbb{F}_2$. *Es gilt* $2^\ell-1=15$ *und* $f(x)\mid x^{15}-1$ *in* $\mathbb{F}_2[x]$:

$$x^{15}-1=(x+1)\left(x^2+x+1\right)\left(x^4+x+1\right)\left(x^4+x^3+1\right)\left(x^4+x^3+x^2+x+1\right).$$

Man prüft leicht nach, daß $f(x)$ *kein* x^n-1 *mit* $n<15$ *teilt. Also ist* $f(x)=x^4+x+1$ *primitiv. Dagegen ist* $g(x)=x^4+x^3+x^2+x+1$ *zwar irreduzibel über* $\mathbb{F}_2$ *und teilt auch* $x^{15}-1$, *ist aber nicht primitiv wegen* $g(x)\mid x^5-1$. *(Tabelle 1 zeigt weitere Beispiele von primitiven Polynome über* $\mathbb{F}_2$.*)*

3.2.4. BCH– und Reed–Solomon–Codes. BCH–Codes haben ihren Namen von R.C. Bose, D.K. Ray–Chaudhuri und von A. Hocquenghem, die diese Codes 1960 [**1**] und 1959 [**7**] unabhängig voneinander entdeckt haben. Wir erinnern noch einmal an folgende Definition.

DEFINITION 3.2.75. *Sei* $q=p^n$ *für* $p\in\mathbb{P}$, $n\in\mathbb{N}$. *Ein Minimalpolynom eines Elementes* $\alpha\in\mathbb{F}_{q^\ell}$ *über* $\mathbb{F}_q$ *ist ein normiertes Polynom* $m(x)\in\mathbb{F}_q[x]$ *kleinsten Grades mit* $m(\alpha)=0$.

PROPOSITION 3.2.76. *Zu jedem* $\alpha\in\mathbb{F}_{q^\ell}$ *existiert ein eindeutig bestimmtes Minimalpolynom* $m_\alpha(x)$ *über* $\mathbb{F}_q$. *Es ist irreduzibel über* $\mathbb{F}_q$ *und teilt jedes andere Polynom* $f(x)\in\mathbb{F}_q[x]$ *mit* $f(\alpha)=0$, *insbesondere also* $x^{q^\ell-1}-1$.

BEWEIS. Siehe [**8**, Kapitel V, Theorem 1.6 (ii), Seite 234]. □

Natürlich ist $m_\alpha(t)=t-\alpha$ das Minimalpolynom von $\alpha\in\mathbb{F}_q$ über $\mathbb{F}_q$.

BEISPIEL 3.2.77. *Der Körper* $\mathbb{F}_9=\mathbb{F}_{3^2}$ *ist gegeben durch*

$$\mathbb{F}_3[x]/((x^2+1))=\{0,1,2,x,2x,x+1,2x+2,x+2,2x+1\}.$$

Die Minimalpolynome $m_\alpha(t)$ *sind:*

α	$m_\alpha(t)$
0	t
1	$t+2$
2	$t+1$
$x, 2x$	t^2+1
$x+1, 2x+1$	t^2+t+2
$x+2, 2x+2$	t^2+2t+2

Denn man sieht leicht, daß diese Polynome irreduzibel sind und α als Nullstelle haben. Zum Beispiel gilt für $m(t) = t^2+2t+2$ sowohl $m(x+2) = (x+2)^2+2(x+2)+2 = x^2+1 = 0$ als auch $m(2x+2) = x^2+1 = 0$ in $\mathbb{F}_9$.

PROPOSITION 3.2.78. *Es sei C ein zyklischer $[n,k]_q$–Code (gedeutet als Ideal $((g)) \sqsubseteq \mathbb{F}_q[x]/((x^n-1))$) mit Nullstellenmenge $U(C) = V(g)$. Es sei u eine primitive n–te Einheitswurzel, und es gebe natürliche Zahlen b, d mit $2 \leq d \leq n+1$, so daß die Elemente $u^b, u^{b+1}, \ldots, u^{b+d-2}$ in $U(C)$ enthalten sind. Dann ist $d(C) \geq d$.*

BEWEIS. Angenommen $d(C) < d$. Dann gibt es wegen

$$d(C) = \min\{\mathbf{w}(x) \colon\ 0 \neq x \in C\}$$

(siehe Proposition 3.2.21) ein Codewort (bzw. Polynom)

$$c(x) = \sum_{j=1}^{r} a_{k_j} x^{k_j} \text{ mit } a_{k_j} \neq 0 \text{ für alle } j, 1 \leq j \leq r.$$

in C mit Gewicht $\mathbf{w}(c) = r$, wobei $0 < r < d$; also $b+d-2 \geq b+r-1$.
Da nach Voraussetzung $\{u^b, \ldots, u^{b+r-1}\}$ in der Nullstellenmenge $U(C)$ von g enthalten ist und $g \mid c$ gilt, ist $(a_{k_1}, \ldots, a_{k_r})$ eine *nichttriviale* Lösung des homogenen linearen Gleichungssystems

$$\begin{aligned} y_1 \left(u^b\right)^{k_1} + \cdots + y_r \left(u^b\right)^{k_r} &= 0 \\ \vdots \qquad\qquad \vdots &\quad \vdots \\ y_1 \left(u^{b+r-1}\right)^{k_1} + \cdots + y_r \left(u^{b+r-1}\right)^{k_r} &= 0 \end{aligned}$$

über $\mathbb{F}_{q^n}$, also muß die Determinante von

$$L = \left(u^{(b+i)\cdot k_j}\right)_{(i,j)=(0,1)}^{(r-1,r)} = \begin{pmatrix} u^{b\cdot k_1} & \cdots & u^{b\cdot k_r} \\ \vdots & & \vdots \\ u^{(b+r-1)k_1} & \cdots & u^{(b+r-1)k_r} \end{pmatrix}$$

verschwinden. Das ist aber im wesentlichen eine *Vandermonde–Determinante*:

$$\begin{aligned} \det(L) &= \prod_{j=1}^{r} u^{b\cdot k_j} \cdot \det \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ (u^{k_1})^{r-1} & \cdots & (u^{k_r})^{r-1} \end{pmatrix} \\ &= \prod_{j=1}^{r} u^{b\cdot k_j} \cdot \prod_{j<i} \left(\underbrace{u^{k_i} - u^{k_j}}_{\neq 0}\right) \neq 0, \end{aligned}$$

ein Widerspruch. □

DEFINITION 3.2.79 (BCH–Code). *Es sei u ein Erzeuger der (zyklischen![9]) multiplikativen Gruppe $\mathbb{F}_{q^m}^\star$ (u ist also eine* primitive *n–te Einheitswurzel für $n = q^m - 1$), und sei*

$$U_{b,d} = \left\{u^b, u^{b+1}, \ldots, u^{b+d-2}\right\}$$

mit $2 \leq d \leq q^m = n+1$ und $b \geq 0$. Sei $m_i(x)$ das Minimalpolynom von u^i, und sei $g(x)$ das kleinste gemeinsame Vielfache der m_i, $b \leq i \leq b+d-2$:

$$g(x) = \mathrm{kgV}\left(m_b(x), m_{b+1}(x), \ldots, m_{b+d-2}(x)\right) \in \mathbb{F}_q[x].$$

Der zyklische Code

$$((g(x))) \sqsubseteq \mathbb{F}_q[x]/((x^{q^m-1}-1)),$$

der durch das Polynom $g(x)$ erzeugt wird, hat Länge $q^m - 1$: Er wird als primitiver BCH–Code *über $\mathbb{F}_q$ bezeichnet (wir sagen in der Folge einfach BCH–Code). Der Parameter d heißt* garantierte Minimaldistanz *des Codes (siehe Proposition 3.2.78). Ein (primitiver) BCH–Code C heißt* BCH–Code im eigentlichen Sinn, *falls $b = 1$ ist.*

BEMERKUNG 3.2.80. *Die Definition von BCH–Codes kann man allgemeiner fassen (es gibt auch* nicht *primitive BCH–Codes), aber das sprengt unseren Rahmen.*

PROPOSITION 3.2.81 (BCH–Schranke). *Ein (primitiver) BCH–Code C der Länge $n = q^m - 1$ mit Parameter $d \geq 2$ hat Dimension mindestens $n - m(d-1)$. Im Fall $q = 2$ und $b = 1$ gilt sogar*

$$\dim(C) \geq n - m\left\lfloor \frac{d}{2} \right\rfloor.$$

BEWEIS. Da $u^i \in \mathbb{F}_{q^m}$ und $\mathbb{F}_{q^m} \simeq \mathbb{F}_q^m$ (also: $\mathbb{F}_{q^m}$ erscheint als m–dimensionaler Vektorraum über $\mathbb{F}_q$), sind die $m+1$ Vektoren $1, u^i, u^{2\cdot i}, \ldots, u^{m\cdot i}$ *linear abhängig*, daher gibt es Koeffizienten $\lambda_i \in \mathbb{F}_q$, sodaß

$$\lambda_m \cdot u^{m\cdot i} + \cdots + \lambda_2 \cdot u^{2\cdot i} + \lambda_1 \cdot u^i + \lambda_0 = 0.$$

Das heißt aber: $\lambda_m \cdot x^m + \cdots + \lambda_2 \cdot x^2 + \lambda_1 \cdot x + \lambda_0$ ist ein Polynom in $\mathbb{F}_q[x]$ vom Grad m, das u^i als Nullstelle hat: Daher hat das *Minimalpolynom* $m_i(x)$ von u^i Grad $\leq m$, und $\deg g(x) \leq m(d-1)$ (denn $|U_{b,d}| = d-1$).
Im Spezialfall $q = 2$ und $b = 1$ gilt

$$m_i(x) = m_{2i}(x),$$

denn $m_i\left(u^{2i}\right) = \left(m_i\left(u^i\right)\right)^2 = 0$ (siehe Korollar A.3.65). Daher ist das Erzeugerpolynom $g(x)$ eines binären BCH–Codes C für $\left\{u^1, \ldots, u^{d-1}\right\} \subseteq U(C)$

$$g(x) = \mathrm{kgV}\left(m_1(x), m_3(x), \ldots, m_{2\left\lfloor \frac{d}{2} \right\rfloor - 1}\right);$$

g hat also höchstens Grad $m\lfloor d/2 \rfloor$.
Die Behauptungen folgen nun, weil ja ganz allgemein (siehe Proposition 3.2.52)

$$\dim(C) = n - \deg g$$

[9] Siehe Satz 3.1.9.

gilt. □

3.2.4.1. *Reed–Solomon–Codes.* Wir spezialisieren Definition 3.2.79 von BCH–Codes für $m = 1$:

DEFINITION 3.2.82. *Sei $n = q - 1$, sei u eine primitive n–te Einheitswurzel in $\mathbb{F}_q$ (also* $\operatorname{ord} u = n$*), und sei $b \geq 0$, $2 \leq d \leq n + 1 = q$. Ein BCH–Code der Länge $n = q - 1$ mit Erzeugerpolynom*

$$g(x) = \left(x - u^b\right)\left(x - u^{b+1}\right) \cdots \left(x - u^{b+d-2}\right)$$

heißt Reed–Solomon–Code *mit garantierter Minimaldistanz d:*

$$((g(x))) \sqsubseteq \mathbb{F}_q[x] / ((x^{q-1} - 1)).$$

Ein Reed-Solomon-Code ist ein *primitiver* BCH–Code, denn natürlich ist $(x - \alpha)$ Minimalpolynom für $\alpha \in \mathbb{F}_q$: Wir können ohne Einschränkung $b = 1$ und $g(x) = \prod_{i=1}^{d-1}(x - u^i)$ wählen; oder $b = 0$ und $g(x) = \prod_{i=0}^{d-2}(x - u^i)$.

DEFINITION 3.2.83. *Für lineare $[n, k, d]$–Codes C folgt aus der Singleton–Schranke (Proposition 3.2.16)*

$$\dim(C) = k \leq n - d + 1.$$

Ein linearer $[n, k, d]$–Code, der diese Schranke erreicht (also $k = n - d + 1$), heißt MDS–Code*: Die Abkürzung steht für* Maximum Distance Separable Code*.*

PROPOSITION 3.2.84. *Ein Reed–Solomon–Code C über $\mathbb{F}_q$* ist *ein MDS–Code.*

BEWEIS. Sei $\dim(C) = k$. Es gilt $k \leq n - d + 1$ wegen der Singleton-Schranke. Andererseits besagt die BCH–Schranke (Proposition 3.2.81 für $m = 1$) auch $k \geq n - d + 1$. □

Anders ausgedrückt: Wir haben eine Formel für die Größe $A_q(n, d)$ von Codes über q der Länge $n = q - 1$ und Minimaldistanz d gefunden:

KOROLLAR 3.2.85. *Sei q eine Primzahlpotenz, sei $n = q - 1$ und $d \leq n + 1 = q - 1$. Dann gilt $A_q(n, d) = q^{n-d+1}$.*

Die Klasse der MDS–Codes ist abgeschlossen unter Dualisierung:

PROPOSITION 3.2.86. *Sei C ein $[n, n - r, r + 1]$–MDS–Code. Dann ist der duale Code $C^\perp$ ein $[n, r, n - r + 1]$–MDS–Code.*

BEWEIS. Sei C ein $[n, n - r]$–MDS–Code über $\mathbb{F}_q$, dann ist $d = n - (n - r) + 1 = r + 1$.
Zu zeigen ist, daß der $[n, r]$–Code $C^\perp$ Minimaldistanz $d \geq n - r + 1$ hat (denn daraus folgt bereits $d = n - r + 1$ wegen der Singleton–Schranke). Es sei H eine Kontrollmatrix von C, also eine Erzeugermatrix von $C^\perp$. Ist $x \neq 0$ ein Codewort von $C^\perp$, dann gibt es $y \neq 0 \in \mathbb{F}_q^r$ mit $x = y^t \cdot H$. Angenommen, es wäre $\mathbf{w}(x) \leq n - r$: Dann gibt es eine $(r \times r)$–Untermatrix H' von H mit $y^t \cdot H' = 0$. Da aber je r Spalten von H linear unabhängig sind, ist $\det H' \neq 0$, und es folgt $y = 0$, ein Widerspruch.
Also ist $d(C^\perp) = \min\left\{\mathbf{w}(x) \colon\ 0 \neq x \in C^\perp\right\} \geq n - r + 1$. □

BEMERKUNG 3.2.87. *Ein Reed-Solomon-Code mit garantierter Minimaldistanz d hat die Kontrollmatrix (für $b = 1$ und $g(x) = \prod_{i=1}^{d-1}(x - u^i)$)*

$$H = \begin{pmatrix} 1 & u & \cdots & u^{q-2} \\ 1 & u^2 & \cdots & u^{2(q-2)} \\ \vdots & \vdots & \vdots & \\ 1 & u^{d-1} & \cdots & u^{(d-1)(q-2)} \end{pmatrix},$$

denn für $f = f_0 + f_1 \cdot x + f_{q-2} \cdot x^{q-2} \in \mathbb{F}_q[x] / \left(x^{q-1} - 1\right)$ gilt ja:

$$f \in (\!(g)\!) \iff f\left(u^i\right) = 0 \iff f_0 \cdot 1 + f_1 \cdot u^i + \cdots f_{q-2} \cdot u^{i\cdot(q-2)}.$$

Für $b = 0$ und $g(x) = \prod_{i=0}^{d-2}(x - u^i)$ streicht man die letzte Zeile von H, und fügt $(1, \ldots, 1)$ als erste Zeile hinzu.

BEISPIEL 3.2.88. *Sei $q = 2^3 = 8$, $n = q - 1 = 7$ und u ein primitives Element von $\mathbb{F}_8$ mit $u^3 = u + 1$. Dann erzeugt das Polynom*

$$g(x) = (x-1)(x-u)(x-u^2)(x-u^3)$$

einen $[7, 3, 5]_8$–Reed–Solomon–Code mit Minimaldistanz $d = 5$.
Denn das primitive Element $u \in \mathbb{F}_{2^3}$ ist Nullstelle des primitiven Polynoms $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Es gilt:

$$u^3 = u + 1, u^4 = u^2 + u, u^5 = u^2 + u + 1, u^6 = u^2 + 1 \text{ und } u^7 = 1,$$

siehe Beispiel 3.2.72. Das Generatorpolynom ist also

$$\begin{aligned} g(x) &= (x-1)(x-u)(x-u^2)(x-u^3) \\ &= x^4 + u^2x^3 + u^5x^2 + u^5x + u^6. \end{aligned}$$

Sei C der von $g(x)$ erzeugte zyklische Reed-Solomon-Code. Es gilt

$$\dim C = k = n - d + 1 = 3.$$

Die Erzeugermatrix von C ist

$$G = \begin{pmatrix} u^6 & u^5 & u^5 & u^2 & 1 & 0 & 0 \\ 0 & u^6 & u^5 & u^5 & u^2 & 1 & 0 \\ 0 & 0 & u^6 & u^5 & u^5 & u^2 & 1 \end{pmatrix}.$$

Es gibt $q^{n-d+1} = 8^3 = 512$ Codewörter. Die Kontrollmatrix ist

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & u & u^2 & u^3 & u^4 & u^5 & u^6 \\ 1 & u^2 & u^4 & u^6 & u^8 & u^{10} & u^{12} \\ 1 & u^3 & u^6 & u^9 & u^{12} & u^{15} & u^{18} \end{pmatrix}.$$

Das Kontrollpolynom lautet

$$\begin{aligned} h(x) &= (x^7 - 1)g(x)^{-1} \\ &= (x - u^4)(x - u^5)(x - u^6) \\ &= x^3 + u^2x^2 + x + u. \end{aligned}$$

BEMERKUNG 3.2.89. *Zur Fehlerkorrektur von Audio–CDs werden verkürzte Reed-Solomon-Codes über* $\mathbb{F}_{2^8} = \mathbb{F}_{256}$ *benutzt. Das primitive Polynom*

$$x^8 + x^4 + x^3 + x^2 + 1$$

liefert eine primitive n-te Einheitswurzel in $\mathbb{F}_{256}$ *mit* $n = q - 1 = 255$*, siehe Tabelle 1. Damit wird zunächst ein primitiver* $[255, 251, 5]_{256}$*–Reed–Solomon–Code der Länge* $n = 255$*, Dimension* $k = n - d + 1 = 251$ *und Minimaldistanz* $d = 5$ *konstruiert, aus dem (durch weitere Konstruktionen) der* Interleaved Reed–Solomon–Code *der Audio CDs entsteht.*

3.2.5. Quadratische–Reste–Codes (QR–Codes). Sei $p \in \mathbb{P}$,$p \neq 2$. Wir betrachten (vergleiche Definition A.2.6)

$$\mathcal{Q}_p := \left\{ i \in [p-1] : \ \left(\frac{i}{p}\right) = 1 \right\} \text{ (quadr. Reste modulo } p\text{)},$$
$$\mathcal{N}_p := \left\{ i \in [p-1] : \ \left(\frac{i}{p}\right) = -1 \right\} \text{ (quadr. Nichtreste modulo } p\text{)}.$$

Es gilt bekanntlich (Proposition A.2.7) $\left|\mathcal{Q}_p\right| = \left|\mathcal{N}_p\right| = \frac{p-1}{2}$.

Sei $r \in \mathbb{P}$ mit $r \neq p$ und $\left(\frac{r}{p}\right) = 1$. Betrachte den Körper $\mathbb{K} := \mathbb{F}_r$ sowie einen Erweiterungskörper $\mathbb{L} \sqsupseteq \mathbb{K}$, der eine p–te Einheitswurzel $\alpha \neq 1$ enthält[10].

BEISPIEL 3.2.90. *Für* $r = 2$ *und* $p = 7$ *enthält* $\mathbb{L} = \mathbb{F}_8 \sqsupseteq \mathbb{F}_2 = \mathbb{K}$ *eine 7–te Einheitswurzel; als* Zerfällungskörper *des Polynoms* $x^8 - x = x \cdot \left(x^7 - 1\right)$ *über* $\mathbb{F}_2$.

Definiere nun

$$q(x) := \prod_{i \in \mathcal{Q}_p} \left(x - \alpha^i\right) \in \mathbb{L}[x],$$
$$n(x) := \prod_{i \in \mathcal{N}_p} \left(x - \alpha^i\right) \in \mathbb{L}[x].$$

PROPOSITION 3.2.91. $q(x), n(x) \in \mathbb{K}[x]$.

BEWEIS. q und n sind sichtlich normierte separable Polynome in $\mathbb{L}[x]$; und $\mathbb{L}$ hat ebenso wie $\mathbb{K}$ die Charakteristik r. Wegen

$$\left(\frac{r \cdot i}{p}\right) = \left(\frac{r}{p}\right) \cdot \left(\frac{i}{p}\right) = \left(\frac{i}{p}\right)$$

ist

$$\mathcal{Q}_p = \left\{ r \cdot i : \ i \in \mathcal{Q}_p \right\},$$
$$\mathcal{N}_p = \left\{ r \cdot i : \ i \in \mathcal{N}_p \right\},$$

also permutiert die Frobenius–Abbildung $\mathrm{frob}_r : \mathbb{L} \to \mathbb{L}$

$$z \mapsto z^r$$

[10] Da $p \in \mathbb{P}$, ist das automatisch eine *primitive* Einheitswurzel.

die Nullstellen von q und n. Da die Koeffizienten von p bzw. q aber *elementarsymmetrische Funktionen* der Nullstellen von p bzw. q sind (vergleiche Definition A.3.83), werden diese Koeffizienten *auch* von frob_r *fixiert*:

$$\mathrm{frob}_r\left(\left[\!\left[x^k\right]\!\right] p\right) = \left[\!\left[x^k\right]\!\right] p \text{ für alle } k,$$

und ebenso für q. Das bedeutet aber, daß alle Koeffizienten von p und q Nullstellen des Polynomes

$$x^r - x \in \mathbb{L}[x]$$

sind: Dieses Polynom über $\mathbb{L}$ hat aber *genau* die Nullstellenmenge $\mathbb{K}$ (denn für jedes der r Elemente $z \in \mathbb{K}$ *gilt* $z^r = z$, und mehr als r Nullstellen kann das Polynom über dem Körper $\mathbb{L}$ nicht haben (siehe Lemma 2.1.9). □

DEFINITION 3.2.92. *Seien* $p \neq r \in \mathbb{P}$, $p \neq 2$ *und* $\left(\frac{r}{p}\right) = 1$. *Dann heißen die von den folgenden Polynomen erzeugten zyklischen Codes (also Ideale in* $\mathbb{F}_r[x]/((x^p - x))$ quadratische–Reste–Codes*:*

- $q(x)$ *erzeugt* Q,
- $n(x)$ *erzeugt* N,
- $(x-1)\,q(x)$ *erzeugt* $\overline{Q}$,
- $(x-1)\,n(x)$ *erzeugt* $\overline{N}$.

LEMMA 3.2.93. *Für die eben definierten quadratische–Reste–Codes gilt:*

$$\dim Q = \dim N = \frac{p+1}{2}, Q \sim N,$$
$$\dim \overline{Q} = \dim \overline{N} = \frac{p-1}{2}, \overline{Q} \sim \overline{N}.$$

BEWEIS. Gemäß Proposition 3.2.52 ist die Dimension des von q oder n bzw. von $(x-1)\,q$ oder $(x-1)\,n$ erzeugten Codes $p - \frac{p-1}{2} = \frac{p+1}{2}$ bzw. $p - \frac{p+1}{2} = \frac{p-1}{2}$.

Wir behaupten: Es gibt eine Permutation π, sodaß für die zugehörige Permutationsmatrix $P(\pi)$

$$Q \cdot P(\pi) = N \text{ bzw. } \overline{Q} \cdot P(\pi) = \overline{N}$$

gilt. Denn für $l \in \mathcal{N}_p \in \mathbb{F}_p^\star$ und irgendein $i \in \mathbb{Z}$ mit $p \nmid i$ gilt

$$\left(\frac{l \cdot i}{p}\right) = \left(\frac{l}{p}\right) \cdot \left(\frac{i}{p}\right) = -\left(\frac{i}{p}\right),$$

und die Abbildung

$$\pi : \mathbb{F}_p \to \mathbb{F}_p;\ i \mapsto l \cdot i \pmod{p}$$

ist also eine Permutation mit Fixpunkt 0, die $\mathcal{N}_p$ auf $\mathcal{Q}_p$ abbildet und umgekehrt. Sei $P(\pi)$ die zugehörige Permutationsmatrix, dann gilt wegen $c(x) \in$

$((g)) \iff V(g) \subset V(c)$:

$$\begin{aligned} c \in Q &\iff \sum_{i=0}^{p-1} c_i \cdot \left(\alpha^j\right)^i = 0 \text{ für alle } j \in \mathcal{Q}_p \\ &\iff \sum_{i=0}^{p-1} c_i \cdot \left(\alpha^{l \cdot j}\right)^{l^{-1} \cdot i} = 0 \text{ für alle } j \in \mathcal{Q}_p \\ &\iff \sum_{k=0}^{p-1} c_{\pi(k)} \cdot \left(\alpha^h\right)^k = 0 \text{ für alle } h \in \mathcal{N}_p \quad \leftarrow k = \pi^{-1}(i) = l^{-1} \cdot i \\ &\iff c \cdot P(\pi) = \left(c_{\pi(0)}, \ldots, c_{\pi(p-1)}\right) \in N. \end{aligned}$$

Ganz analog argumentiert man für $\overline{Q}$ und $\overline{N}$. □

3.2.5.1. *Konstruktion des ternären Golay–Codes als QR–Code.*

BEISPIEL 3.2.94 (Ternärer Golay–Code). *Sei* $p = 11$ *und* $r = 3$.
Es gilt $11 \mid 3^5 - 1 = 242$, *aber* $11 \nmid 3^4 - 1, 3^3 - 1, 3^2 - 1$: $\mathbb{F}_{3^k}$ *kann also keine* 11*–te Einheitswurzel enthalten für* $k < 5$; $\mathbb{F}_{3^5}$ *enthält aber eine: In* $\mathbb{F}_3$ *gilt die irreduzible Zerlegung*

$$x^{11} - 1 = (x-1) \cdot \left(x^5 + x^4 - x^3 + x^2 - 1\right) \cdot \left(x^5 - x^3 + x^2 - x - 1\right).$$

$q(x) = x^5 + x^4 - x^3 + x^2 - 1$ *erzeugt einen Quadratische–Reste–Code* Q *mit den Parametern* $[11, 6, d]$. *Die quadratischen Reste* $\mathcal{Q}_{11} = \{1, 3, 4, 5, 9\}$ *enthalten mit* $(1, 3, 5)$ *eine arithmetische Progression der Länge 3, also ist* $d \geq 4$, *vergleiche den Beweis von Proposition 3.2.78: Aus* $d < 4$ *würde folgen, daß es ein ein Codewort (bzw. Polynom)*

$$c(x) = c_{k_1} x^{k_1} + c_{k_2} x^{k_2} + c_{k_3} x^{k_3} \text{ mit } \left(c_{k_1}, c_{k_2}, c_{k_3}\right) \neq (0, 0, 0)$$

in Q *gibt mit Gewicht* $\mathbf{w}(c) \leq 3$. *Sei* α *die primitive* 11*–te Einheitswurzel, dann gilt nach Konstruktion*

$$c(\alpha) = c\left(\alpha^3\right) = c\left(\alpha^5\right) = 0.$$

Das hieße aber, $\left(c_{k_1}, c_{k_2}, c_{k_3}\right)$ *ist eine* nichttriviale *Lösung des homogenen Gleichungssystems*

$$\begin{aligned} x \cdot \left(\alpha^1\right)^{k_1} + y \cdot \left(\alpha^1\right)^{k_2} + z \cdot \left(\alpha^1\right)^{k_3} &= 0 \\ x \cdot \left(\alpha^3\right)^{k_1} + y \cdot \left(\alpha^3\right)^{k_2} + z \cdot \left(\alpha^3\right)^{k_3} &= 0 \\ x \cdot \left(\alpha^5\right)^{k_1} + y \cdot \left(\alpha^5\right)^{k_2} + z \cdot \left(\alpha^5\right)^{k_3} &= 0 \end{aligned}$$

über $\mathbb{F}_{3^5}$: *Das kann aber nicht sein, denn die Determinante der Koeffizientenmatrix ist*

$$\alpha^{k_1+k_2+k_3} \cdot \det \begin{pmatrix} 1 & 1 & 1 \\ \left(\alpha^{k_1}\right)^2 & \left(\alpha^{k_2}\right)^2 & \left(\alpha^{k_3}\right)^2 \\ \left(\alpha^{k_1}\right)^4 & \left(\alpha^{k_2}\right)^4 & \left(\alpha^{k_3}\right)^4 \end{pmatrix},$$

und das ist wieder eine Vandermonde–Determinante, *also* $\neq 0$. *Man kann aber sogar* $d \geq 5$ *zeigen, wie aus den folgenden Betrachtungen ersichtlich wird.*

Sei $\alpha \neq 1$ eine p–te Einheitswurzel in einem Oberkörper $\mathbb{L}$ von $\mathbb{F}_r$, mit $p \neq r \in \mathbb{P}$ und $\left(\frac{r}{p}\right) = 1$. Setze

$$\gamma := \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \alpha^i.$$

Dann gilt in $\mathbb{L}$:

$$\begin{aligned}
\gamma^r &= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^r \alpha^{i\cdot r} \quad \leftarrow \text{Freshman's dream für } \mathbb{F}_r \sqsubseteq \mathbb{L} \\
&= \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \alpha^{i\cdot r} \quad \leftarrow \text{für } r \text{ ungerade ist } (\pm 1)^r = \pm 1, \text{ und für } r = 2 \text{ ist } -1 = 1 \\
&= \sum_{i=1}^{p-1} \left(\frac{i\cdot r}{p}\right) \alpha^{i\cdot r} \quad \leftarrow \left(\tfrac{r}{p}\right) = 1 \\
&= \gamma. \quad \leftarrow i \mapsto r\cdot i \pmod p \text{ ist Permutation}
\end{aligned}$$

Außerdem gilt [**12**]: $\gamma^2 = \left(\frac{-1}{p}\right) \cdot p$. Denn

$$\gamma^2 = \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \left(\frac{i\cdot j}{p}\right) \alpha^{i+j}.$$

In dieser Doppelsumme gibt es $(p-1)$ Terme mit $i + j = p$: Für diese ist $\alpha^{i+j} = \alpha^p = 1$, und wegen $j = -i$ in $\mathbb{F}_p$ ist

$$\left(\frac{i\cdot j}{p}\right) = \left(\frac{i^2}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right).$$

Also ist

$$\gamma^2 = \left(\frac{-1}{p}\right)\cdot(p-1) + \sum_{i+j\neq p} \left(\frac{i\cdot j}{p}\right) \alpha^{i+j}.$$

Die Summanden mit $i = j$ liefern

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^2 \alpha^{2i} = \sum_{i=1}^{p-1} \alpha^{2i} = \sum_{i=1}^{p-1} \alpha^i = -1. \quad \leftarrow \text{denn } \textstyle\sum_{i=0}^{p-1} \alpha^i = 0$$

Dies ergibt

$$\gamma^2 = \left(\frac{-1}{p}\right)\cdot(p-1) - 1 + \sum_{k=1}^{p-1} \alpha^k \cdot \psi(k),$$

wobei

$$\psi(k) = \sum_{\substack{i=1 \\ i\neq k, 2i\neq k}}^{p-1} \left(\frac{i\cdot(k-i)}{p}\right). \quad \leftarrow \text{wenn } i+j>p, \text{ dann } j\to j-p\text{: } j=k-i$$

Betrachte die Menge der Zahlen, für die das Legendre–Symbol in der Summe $\psi(k)$ gebildet wird:

$$M_k := \left\{ t \in \mathbb{Z}_p : \ t = i \cdot (k-i) \text{ für } 1 \leq i \leq p-1, i \neq k, 2i \neq k \right\}.$$

Offensichtlich ist $|M_k| = \frac{1}{2}(p-3)$, und es ist

$$\psi(k) = 2 \cdot \sum_{t \in M_k} \left(\frac{t}{p} \right).$$

Für $t = i \cdot (k-i) \in M_k$ gilt

$$\frac{t}{i} + i = k \implies k^2 - 4t = \left(\frac{t+i^2}{i} \right)^2 - \frac{4 \cdot i^2 \cdot t}{i^2} = \left(\frac{i^2-t}{i} \right)^2.$$

Da $i^2 \neq t$, ist $k^2 - 4t \in \mathcal{Q}_p$; d.h., $-4t = r - k^2$ für ein $r \neq k^2$ in $\mathcal{Q}_p$. Anders gesagt:

$$M_k = \left\{ 4^{-1} \cdot \left(-r + k^2 \right) : \ r \in \mathcal{Q}_p, r \neq k^2 \right\}.$$

Da $4^{-1} = \left(2^{-1}\right)^2$ ein Quadrat ist, gilt

$$\left(\frac{4^{-1} \cdot t}{p} \right) = \left(\frac{t}{p} \right).$$

Die Summe $\psi(k)$ können wir also schreiben als

$$\psi(k) = 2 \cdot \sum_{\substack{r \in \mathcal{Q}_p \\ r \neq k^2}} \left(\frac{-r+k^2}{p} \right). \tag{3.9}$$

- Wenn $p = 4m-1$ (also $\left(\frac{-1}{p}\right) = -1$), dann ist $-r$ ein Nichtrest für alle $r \in \mathcal{Q}_p$, d.h., der Summationsbereich von (3.9) ist in diesem Fall

  $$\left\{ r + k^2 : \ r \in \mathcal{N}_p, r \neq -k^2 \right\}.$$

  Nach dem Satz von Perron A.2.11 enthält dieser Summationsbereich $(m-1)$ Reste und $(m-1)$ Nichtreste; es ist also $\psi(k) = 0$ und

  $$\gamma^2 = -(p-1) - 1 = -p.$$

- Wenn aber $p = 4m+1$ (also $\left(\frac{-1}{p}\right) = 1$), dann ist $-r$ ein Rest für alle $r \in \mathcal{Q}_p$, d.h., der Summationsbereich von (3.9) ist in diesem Fall

  $$\left\{ r + k^2 : \ r \in \mathcal{Q}_p, r \neq -k^2 \right\}.$$

  Nach dem Satz von Perron A.2.11 enthält dieser Summationsbereich $(m-1)$ Reste und m Nichtreste; es ist also $\psi(k) = -2$ und

  $$\gamma^2 = (p-1) - 1 - 2 \sum_{i=1}^{p-1} \alpha^k = p.$$

DEFINITION 3.2.95. *Die* Erweiterung $\widetilde{Q}$ *des Quadratische–Reste–Codes* Q *ist definiert durch*

$$\widetilde{Q} := \left\{ \left(c_0, \ldots, c_{p-1}, \frac{-\gamma}{p} \sum_{i=0}^{p-1} c_i \right) : \ \left(c_0, \ldots, c_{p-1} \right) \in Q \right\}.$$

BEMERKUNG 3.2.96. *Für* $p = 2$ *ist* $\gamma = p$*, also ergibt sich die "gewöhnliche" Erweiterung des Codes mit einer zusätzlichen "Prüfziffer".*

PROPOSITION 3.2.97. *Sei* $p \in \mathbb{P}$ *mit* $p \equiv -1 \pmod 4$*, und sei* Q *der Quadratische–Reste–Code der Länge* p *über* $\mathbb{F}_r$*. Dann gilt:*

(a) $Q^\perp = \overline{Q}$.
(b) $\widetilde{Q}^\perp = \widetilde{Q}$.

BEWEIS. Ad (a): Sei $q(x) = \prod_{i \in \mathcal{Q}_p} \left(x - \alpha^i \right)$ das erzeugende Polynome von Q. Dann ist $(x-1)\, n(x)$ das Kontrollpolynom von Q; sein Grad ist $\frac{p+1}{2}$.
Für das erzeugende Polynom von $Q^\perp$ gilt (siehe Proposition 3.2.65):

$$\begin{aligned}
q^\perp(x) &= -n(0)^{-1}\, x^{\frac{p+1}{2}} n\left(\frac{1}{x}\right) \cdot \left(\frac{1}{x} - 1\right) \\
&= -n(0)^{-1} \left(\prod_{j \in \mathcal{N}_p} \left(1 - \alpha^j \cdot x \right) \right) \cdot (1 - x) \\
&= \left(\prod_{j \in \mathcal{N}_p} \left(\alpha^{-j} - x \right) \right) \cdot (1 - x) \quad \leftarrow (-1)^{\frac{p-1}{2}} = -1 \Longrightarrow \textstyle\prod_{j \in \mathcal{N}_p} \alpha^{-j} = -n(0)^{-1} \\
&= \left(\prod_{i \in \mathcal{Q}_p} \left(\alpha^i - x \right) \right) \cdot (1 - x) \quad \leftarrow \left(\tfrac{-1}{p}\right) = -1 \text{ n.V.; siehe Korollar A.2.10} \\
&= \left(\prod_{i \in \mathcal{Q}_p} \left(x - \alpha^i \right) \right) \cdot (x - 1) \quad \leftarrow (-1)^{\frac{p-1}{2}} = -1 \\
&= q(x) \cdot (x-1)\,;
\end{aligned}$$

und das ist das erzeugende Polynom von $\overline{Q}$.
Ad (b): Sei $\overline{G}$ eine Erzeugermatrix von $\overline{Q}$ und betrachte die $\frac{p+1}{2} \times p$–Matrix

$$G := \begin{pmatrix} & \overline{G} & \\ 1 & 1 \ \ldots & 1 \end{pmatrix}$$

über $\mathbb{F}_r$.
Klarerweise gilt $\overline{Q} \sqsubseteq Q$; außerdem ist

$$\sum_{i=0}^{p-1} x^i = \frac{x^p - 1}{x - 1} = q(x) \cdot n(x).$$

Daher ist $(1, \ldots, 1) \in Q \setminus \overline{Q}$, denn $q(x) \mid \sum x^i$, aber $(x-1) \nmid \sum x^i$: Also ist G Erzeugermatrix von Q.

Betrachte weiters die $\frac{p+1}{2} \times (p+1)$–Matrix

$$\widetilde{G} := \begin{pmatrix} & \overline{G} & & 0 \\ 1 & 1 & \dots & 1 & -\gamma \end{pmatrix}$$

über $\mathbb{F}_r$.
Es ist $\langle c, (1, \dots, 1) \rangle = \sum_{i=0}^{p-1} c_i = 0$ für alle $c \in \overline{Q}$, denn $(x-1) \mid c(x)$ für alle $c \in \overline{Q}$, und das heißt $c(1) = 0$. Sei $z = (1, \dots, 1, -\gamma)$ die letzte Zeile in $\widetilde{G}$: Dann ist auch $z \in \widetilde{Q}$ wegen $-\gamma = \frac{-\gamma}{p} \sum_{i=0}^{p-1} 1$, also ist $\widetilde{G}$ eine Erzeugermatrix von $\widetilde{Q}$.
Nach Voraussetzung ist

$$p \equiv -1 \pmod 4 \implies \left(\frac{-1}{p}\right) = -1,$$

also ist

$$\langle z, z \rangle = p + \gamma^2 = p + \left(\frac{-1}{p}\right) p = p - p = 0.$$

Aus $\overline{Q} = Q^\perp$ folgt aber für alle $x \in \overline{Q}$:

- $\langle x, z_i \rangle = 0$ für die ersten Zeilen z_i in $\widetilde{G}$,
- $\langle x, z \rangle = 0$.

Insgesamt heißt das aber: $\widetilde{Q} \subseteq \widetilde{Q}^\perp$; wegen $\dim \widetilde{Q} = \frac{p+1}{2} = \dim \widetilde{Q}^\perp$ folgt die Behauptung. □

Nun zurück zu Beispiel 3.2.94: Betrachte für den dort beschriebenen $[11, 6, d]$–Code Q_{11} die Erweiterung $\widetilde{Q}$. Wegen $11 \equiv -1 \pmod 4$ ist also $\widetilde{Q} = \widetilde{Q}^\perp$. Also ist

$$0 = \langle c, c \rangle = \sum_{i=1}^{n} c_i^2 = \sum_{i=1}^{\mathbf{w}(c)} \mathbf{1} = \mathbf{w}(c) \cdot \mathbf{1} \text{ in } \mathbb{F}_3,$$

also ist $\mathbf{w}(c) \equiv 0 \pmod 3$. Nun ist aber $d\left(\widetilde{Q}_{11}^\perp\right) = d\left(\widetilde{Q}_{11}\right) \geq 4$, also muß $d\left(\widetilde{Q}_{11}\right) \geq 6$ gelten und wegen $d\left(\widetilde{Q}_{11}\right) - d(Q_{11}) \leq 1$ folgt $d(Q_{11}) \geq 5$. Die Kugelpackungsschranke Satz 3.2.17 besagt hier für $d \geq 2t+1$ allgemein

$$3^{11} \geq 3^6 \sum_{j=0}^{t} \binom{11}{j} 2^j \iff 3^5 \geq \sum_{j=0}^{t} \binom{11}{j} 2^j.$$

Für $t = 2$ ist aber speziell

$$\binom{11}{0} + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 4 = 1 + 22 + 220 = 243 = 3^5 :$$

Der Code ist also *perfekt*.

BEMERKUNG 3.2.98. *Ebenso ist auch der binäre Golay-Code ein Quadratischer–Reste–Code mit $r = 2$, $p = 23$.*

ANHANG A

Grundlagen

A.1. Allgemeines

DEFINITION A.1.1 (Partition). *Sei S eine Menge. Eine Familie von Teilmengen $S_i \subseteq S$*

$$\{S_i \colon\ i \in I\},$$

die mit Indices aus einer Menge I bezeichnet seien, heißt Partition *von S, wenn gilt:*

- $S = \bigcup_{i \in I} S_i$,
- $i \neq j \in I \implies S_i \cap S_j = \emptyset$,
- $S_i \neq \emptyset$ *für alle* $i \in I$.

Die ersten beiden Bedingungen bedeuten, daß S eine disjunkte Vereinigung *der Teilmengen S_i, $i \in I$, ist: Das kürzen wir ab mit*

$$S = \dot{\bigcup}_{i \in I} S_i.$$

Ein Repräsentantensystem *(oder eine* Transversale*) $\mathcal{R}$ einer Partition $\{S_i \colon\ i \in I\}$ von S ist eine Teilmenge von S, die aus jedem S_i* genau ein *Element (einen sogenannten* Repräsentanten *von S_i) enthält.*

DEFINITION A.1.2 (Relation, partielle Ordnung, Totalordnung, Wohlordnung). *Sei S eine Menge: Eine* Relation *R auf S ist (ganz abstrakt) eine Teilmenge des cartesischen Produkts, also*

$$R \subseteq S \times S.$$

Normalerweise beschreibt man aber R (etwas konkreter) durch ein "zweistelliges Symbol", z.B. "$\sim$", mit der Bedeutung

$$x \sim y :\iff (x, y) \in R : \text{ "}x \text{ steht in Relation } R \text{ zu } y\text{"}.$$

Eine Relation, die wir typischerweise mit dem Symbol $\preceq$ bezeichnen, heißt Halbordnung *oder* partielle Ordnung *auf S, wenn sie die folgenden drei Eigenschaften hat:*

Reflexivität: $s \preceq s$ *für alle* $s \in S$,
Transitivität: $s_1 \preceq s_2$ *und* $s_2 \preceq s_3 \implies s_1 \preceq s_3$ *für alle* $s_1, s_2, s_3 \in S$,
Antisymmetrie: $s_1 \preceq s_2$ *und* $s_2 \preceq s_1 \implies s_1 = s_2$.

Wenn $x \preceq y$, aber $x \neq y$, schreiben wir auch $x \prec y$.
Sei $T \subseteq S$: Ein Element $m \in T$ mit der Eigenschaft

$$(s \preceq m \implies s = m \text{ oder } s \notin T \text{ für alle } s \in S) \iff \nexists t \in T \colon\ t \prec m$$

heißt minimales Element *von T.*
Eine Halbordnung $\preceq$ heißt Totalordnung, *wenn für je zwei Elemente $s_1, s_2 \in S$ gilt*

$$s_1 \preceq s_2 \text{ oder } s_2 \preceq s_1$$

(d.h.: Je zwei Elemente sind vergleichbar).

Eine Totalordnung heißt Wohlordnung, *wenn jede Teilmenge $T \subseteq S$ ein minimales Element m hat: Als minimales Element in einer* Totalordnung *hat m die Eigenschaft*

$$m \preceq t \text{ für alle } t \in T.$$

(Wegen Antisymmetrie ist ein solches minimales Element immer eindeutig.)

BEISPIEL A.1.3. *Für $n \in \mathbb{N}$ ist die* Potenzmenge $2^{[n]}$ *(also die Familie aller Teilmengen von $[n]$) partiell geordnet durch die Mengeninklusion $\subseteq$; dies ist aber keine Totalordnung.*
Die Standardordnung $\leq$ ist auf $\mathbb{N}$ eine Wohlordnung, aber nicht auf $\mathbb{Z}$, denn es gibt z.B. kein minimales Element für ganz $\mathbb{Z}$.

DEFINITION A.1.4 (Produktordnung). *Sei S eine durch $\preceq$ halbgeordnete Menge. Dann ist das n–fache cartesische Produkt*

$$S^n := \{(s_1, \ldots, s_n) : \ s_1, \ldots, s_n \in S\}$$

eine halbgeordnete Menge mit der Produktordnung

$$(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n) :\Longleftrightarrow \ x_i \preceq y_i \text{ für alle } i \in [n]\,.$$

DEFINITION A.1.5 (Ordnungsideal). *Sei S eine durch $\preceq$ halbgeordnete Menge. Eine nicht–leere Teilmenge $T \subseteq S$ heißt* Ordnungsideal *in S, wenn*

$$\text{für alle } t \in T \text{ und } s \in S \text{ mit } t \preceq s \text{ gilt: } s \in T.$$

Sei $X \subseteq S$ eine Teilmenge von S, dann ist die Menge

$$\{s \in S : \ \exists x \in X \text{ sodaß } x \preceq s\}$$

ein Ordnungsideal: Wir nennen es das von X erzeugte Ordnungsideal.

A.2. Elementare Zahlentheorie

DEFINITION A.2.1 (Teilbarkeit in $\mathbb{Z}$). *Seien $d, n \in \mathbb{Z}$: Wir sagen "d teilt n" (und schreiben dafür $d \mid n$), wenn es eine Zahl $k \in \mathbb{Z}$ gibt sodaß $n = k \cdot d$. Wenn $d \mid n$ gilt, dann sagen wir auch: "d ist ein Teiler von n" bzw. "n ist ein Vielfaches von d".*
(Diese Definition von Teilbarkeit läßt sich ohne weiteres auch auf andere kommutative Ringe übertragen, z.B. auf Polynomringe, *vergleiche Definition A.3.46.)*
Wenn $d \mid n$, dann gilt natürlich auch $-d \mid n$: Wir können uns also auf die positiven *Teiler beschränken, was wir in der Folge auch tun.*
Jede Zahl $n \in \mathbb{Z}$ ist immer durch 1 *und durch sich selbst (also durch n) teilbar:*

$$n = 1 \cdot n,$$

die Teiler 1 *und n heißen die* trivialen Teiler *von n; wenn n noch weitere Teiler hat, so heißen diese* echte Teiler *von n.*
Ein $n \neq 0$ aus $\mathbb{Z}$ heißt

- irreduzibel, *wenn*

$$c = a \cdot b \implies a = \pm 1 \text{ oder } b = \pm 1,$$

- prim *oder* Primzahl, *wenn*

$$c \mid a \cdot b \implies c \mid a \text{ oder } c \mid b.$$

Die Menge aller Primzahlen bezeichnen wir mit $\mathbb{P}$.

Für alle $d \in \mathbb{Z}$ gilt $d \mid 0$, denn $0 = 0 \cdot d$: 0 ist Vielfaches *jeder* ganzen Zahl. Umgekehrt folgt aus $0 \mid n$ natürlich $n = k \cdot 0 = 0$: 0 ist das *einzige* Vielfache von 0. In $\mathbb{Z}$ sind die Begriffe "irreduzibel" und "prim" gleichbedeutend.

Für $p, q \in \mathbb{Z}$ können wir *Division mit Rest* durchführen, d.h., es gibt $t, r \in \mathbb{Z}$ mit $0 \leq |r| \leq |q|$, sodaß

$$p = q \cdot t + r. \tag{A.1}$$

Auf der Menge der natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$ ist Teilbarkeit eine Halbordnung, die mit der gewöhnlichen Ordnung auf $\mathbb{N}$ kompatibel ist:

$$d \mid n \implies d \leq n. \tag{A.2}$$

DEFINITION A.2.2. *Seien $a, b \in \mathbb{Z}$. Eine Zahl d, die sowohl a als auch b teilt, heißt ein* gemeinsamer Teiler *von a und b:*

$$d \mid a \text{ und } d \mid b.$$

Wir können uns, wie gesagt, auf positive *Teiler d beschränken. Wegen* (A.2) *hat die Menge aller gemeinsamen Teiler von a und b ein größtes Element, das wir als* größten gemeinsamen Teiler *bezeichnen und mit* $\operatorname{ggT}(a, b)$ *abkürzen.*

Der $\operatorname{ggT}(a, b)$ ist auch das maximale Element in der durch die Teilbarkeitsrelation halbgeordneten Menge der gemeinsamen Teiler von a und b, d.h.:

$$d \mid a \text{ und } d \mid b \implies d \mid \operatorname{ggT}(a, b).$$

Der $\operatorname{ggT}(a, b)$ läßt sich immer durch eine ganzzahlige Linearkombination von a und b darstellen, d.h.:

$$\text{es gibt } \lambda, \mu \in \mathbb{Z}\colon \quad \operatorname{ggT}(a, b) = \lambda \cdot a + \mu \cdot b.$$

Diese Darstellung ist nicht eindeutig; sie läßt sich aber ebenso wie der $\operatorname{ggT}(a, b)$ selbst durch den *Euklidischen Algorithmus* ganz einfach finden.

SATZ A.2.3 (Kleiner Satz von Fermat). *Sei $p \in \mathbb{P}$. Dann gilt für alle $a \in \mathbb{Z}$ mit $p \nmid a$:*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Für alle $a \in \mathbb{Z}$ gilt daher

$$a^p \equiv a \pmod{p}.$$

DEFINITION A.2.4 (Möbiusfunktion). *Die (klassische)* Möbiusfunktion $\mu : \mathbb{N} \to \mathbb{Z}$ *nimmt nur die Werte -1, 0 und 1 an:*

$$\mu(n) = \begin{cases} 0 & : \textit{wenn } n \textit{ durch eine quadratische Zahl teilbar ist,} \\ (-1)^l & : \textit{wenn } n \textit{ Produkt von } l \textit{ verschiedenen Primzahlen ist.} \end{cases}$$

SATZ A.2.5 (Möbiusinversion). *Seien $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ zwei Zahlenfolgen. Dann sind äquivalent:*

$$\forall n \in \mathbb{N}: \; a_n = \sum_{d \mid n} b_n, \tag{A.3}$$

$$\forall n \in \mathbb{N}: \; b_n = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) a_n. \tag{A.4}$$

DEFINITION A.2.6 (Quadratischer Rest, Legendre–Symbol, Jacobi–Symbol). *Seien $a, m \in \mathbb{Z}$ mit* ggT $(a, m) = 1$. *Die Zahl a heißt ein* quadratischer Rest *modulo m, wenn die Kongruenzengleichung*

$$x^2 \equiv a \pmod{m}$$

lösbar ist; andernfalls heißt a ein quadratischer Nichtrest.

Klarerweise kommt es nur auf die Restklasse *der Zahl a modulo m an: Quadratische Reste und Nichtreste erscheinen also natürlich als Teilmengen des* Restklassenrings $\mathbb{Z}_m \setminus \{0\}$. *Wir führen folgende Abkürzungen ein:*

$$\begin{aligned} \mathcal{Q}_m &:= \{a \in \mathbb{Z}_m : \ a \text{ ist quadratischer Rest}\}, \\ \mathcal{N}_m &:= \{a \in \mathbb{Z}_m : \ a \text{ ist quadratischer Nichtrest}\}, \\ \overline{\mathcal{Q}_m} &:= \mathcal{Q}_m \cup \{0\}. \end{aligned}$$

Die Menge *der quadratischen Reste modulo m*

Für $p \in \mathbb{P}$ ist das Legendre–Symbol $\left(\frac{a}{p}\right)$ *eine Kurzschreibweise mit folgender Bedeutung:*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{wenn } a \text{ quadratischer Rest modulo } p \text{ ist}, \\ -1 & \text{wenn } a \text{ quadratischer Nichtrest modulo } p \text{ ist}, \\ 0 & \text{wenn } a \text{ ein Vielfaches von } p \text{ ist}. \end{cases}$$

Sei die Primfaktorzerlegung von n gegeben durch

$$n = p_1^{\nu_1} \cdot p_2^{\nu_2} \cdots p_k^{\nu_k},$$

so definiert man das Jacobi–Symbol $\left(\frac{a}{n}\right)$ *(mit* derselben *Kurzschreibweise) als Produkt von Legendre–Symbolen:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\nu_1} \cdot \left(\frac{a}{p_2}\right)^{\nu_2} \cdots \left(\frac{a}{p_k}\right)^{\nu_k}.$$

PROPOSITION A.2.7 (Eulersches Kriterium). *Sei $p \in \mathbb{P}$, $p \neq 2$. Dann gilt für das Legendre–Symbol*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Insbesondere ist die Anzahl der quadratischen Reste modulo p gleich der Anzahl der quadratischen Nichtreste modulo p.

BEWEIS.

Für $a = 0 \pmod{p}$ ist $0 = \left(\frac{a}{p}\right) \equiv 0^{\frac{p-1}{2}} \pmod{p}$ natürlich richtig.

Nach dem kleinen Satz von Fermat (Satz A.2.3) gilt für jedes $a \neq 0$ in $\mathbb{F}_p$:

$$a^{p-1} = 1.$$

Daher ist $a^{\frac{p-1}{2}}$ eine Lösung der Gleichung $x^2 - 1 = 0$ in $\mathbb{F}_p$: Diese hat aber *nur* die beiden Lösungen ± 1 (gemäß Satz A.3.81), entsprechend der Faktorisierung $x^2 - 1 = (x+1)(x-1)$ (über $\mathbb{F}_2$ sind diese Lösungen nicht verschieden, da $1 \equiv -1 \pmod{2}$).

Wenn a quadratischer Rest ist, dann gibt es ein $x \in \mathbb{F}_p$ mit $x^2 = a$, und es ist $a^{\frac{p-1}{2}} = x^{p-1} = 1$ in $\mathbb{F}_p$.
Die multiplikative Gruppe $\mathbb{F}_p^\star$ ist *zyklisch* (Satz 3.1.9), enthält also ein erzeugendes Element b mit $\operatorname{ord} b = p - 1$: Für einen beliebigen quadratischen Rest a ist dann $a \cdot b$ ein quadratischer Nichtrest, denn

$$(a \cdot b)^{\frac{p-1}{2}} = b^{\frac{p-1}{2}} = -1 = \left(\frac{a \cdot b}{p}\right),$$

da $\operatorname{ord} b = p - 1 > \frac{p-1}{2}$.
Die Multiplikation mit dem Erzeuger b ist also eine bijektive Abbildung $\mathbb{F}_p^\star \to \mathbb{F}_p^\star$, die quadratische Reste auf quadratische Nichtreste abbildet, und umgekehrt: Daraus folgen alle Behauptungen. □

BEMERKUNG A.2.8. *Jede Menge M von $\frac{p-1}{2}$ Restklassen aus $\mathbb{Z}_p \setminus \{0\}$, die abgeschlossen ist in Bezug auf die Multiplikation, also*

$$\textit{Gruppenmultiplikation } \cdot\colon\ M \times M \to M,$$

stimmt mit der Menge der quadratischen Reste $\mathcal{Q}_p$ überein: Denn $\mathbb{F}_p^\star = \mathbb{Z}_p \setminus \{0\}$ ist zyklisch, und M bildet also die eindeutige Untergruppe vom Index 2, die zugleich die Menge der Reste ist.

KOROLLAR A.2.9. *Sei $p \neq 2$ Primzahl und $a, b \in \mathbb{Z}$ mit $p \nmid a$ und $p \nmid b$. Dann gilt:*

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Anders gesagt: Das Legendre–Symbol $\left(\frac{\div}{p}\right)$ ist ein Gruppenhomomorphismus $\mathbb{Z}_p^\star \to \{-1, 1\} \simeq \mathbb{Z}_2$, dessen Kern genau die quadratischen Reste sind.

BEWEIS. Der Beweis folgt sofort aus Proposition A.2.7:

$$\left(\frac{a \cdot b}{p}\right) \equiv (a \cdot b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p},$$

also $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$. □

KOROLLAR A.2.10 (Erster Ergänzungssatz).

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Wir formulieren und beweisen noch einen Satz von Oskar Perron [**13**].

SATZ A.2.11 (Perron). *Sei $p \in \mathbb{P}$, $p > 2$; und sei $a \neq 0 \in \mathbb{Z}_p$. Für eine beliebige Teilmenge $S \subseteq \mathbb{Z}_p$ bezeichnen wir mit $S + a$ die Menge $\{s + a\colon\ s \in S\} \subseteq \mathbb{Z}_p$. Dann gilt:*

- *Wenn $p = 4k - 1$ (also wenn $\left(\frac{-1}{p}\right) = -1$), dann gilt*

$$\left|\left(\overline{\mathcal{Q}_p} + a\right) \cap \overline{\mathcal{Q}_p}\right| = \left|\left(\overline{\mathcal{Q}_p} + a\right) \cap \mathcal{N}_p\right| = k$$

bzw. äquivalent

$$\left|\left(\mathcal{N}_p + a\right) \cap \overline{\mathcal{Q}_p}\right| = k \text{ und } \left|\left(\mathcal{N}_p + a\right) \cap \mathcal{N}_p\right| = k - 1.$$

- *Wenn $p = 4k + 1$ (also wenn $\left(\frac{-1}{p}\right) = 1$), dann müssen wir unterscheiden, ob a quadratischer Rest oder Nichtrest ist, und es gilt (unter Verwendung von* Iversons Notation*)*

$$\left|\left(\overline{\mathcal{Q}_p} + a\right) \cap \overline{\mathcal{Q}_p}\right| = k + [a \text{ ist quad. Rest}]$$
$$\left|\left(\overline{\mathcal{Q}_p} + a\right) \cap \mathcal{N}_p\right| = k + 1 - [a \text{ ist quad. Rest}]$$

bzw. äquivalent

$$\left|\left(\mathcal{N}_p + a\right) \cap \overline{\mathcal{Q}_p}\right| = k + 1 - [a \text{ ist quad. Rest}]$$
$$\left|\left(\mathcal{N}_p + a\right) \cap \mathcal{N}_p\right| = k - 1 + [a \text{ ist quad. Rest}]$$

BEWEIS. Die "äquivalenten" Aussagen ergeben sich jeweils aus der offensichtlichen Gleichung

$$\mathbb{Z}_p = \left(\overline{\mathcal{Q}_p} + a\right) \dot\cup \left(\mathcal{N}_p + a\right);$$

und wegen $\left|\mathcal{Q}_p\right| = \left|\mathcal{N}_p\right| = \frac{p-1}{2}$ genügt es also, die jeweils *erste* Aussage zu beweisen.

Sei also $r \in \overline{\mathcal{Q}_p}$: Dann gibt es also ein $s \in \mathbb{Z}_p$ mit $r = s^2$. Weiters sehen wir: $(r + a) \in \overline{\mathcal{Q}_p}$ gilt genau dann, wenn es auch auch ein $t \in \mathbb{Z}_p$ gibt ($t \neq \pm s$) mit $s^2 + a = t^2$, und

$$s^2 - t^2 = -a \iff s - t = -\frac{a}{s+t} \iff 2s = s + t - \frac{a}{s+t}.$$

Also: $s^2 + a$ ist quadratischer Rest genau dann, wenn es eine Zahl $u \neq 0 \in \mathbb{Z}_p$ gibt, für die

$$s = 2^{-1}\left(u - \frac{a}{u}\right)$$

gilt. Das heißt aber, $r + a$ ist genau dann *auch* quadratischer Rest, wenn der quadratische Rest r von der Form

$$r = 4^{-1}\left(u - \frac{a}{u}\right)^2$$

ist. Es ist also $\left|\left(\mathcal{N}_p + a\right) \cap \overline{\mathcal{Q}_p}\right|$ gleich der Anzahl der *inkongruenten* (in $\mathbb{Z}_p$ *verschiedenen*) Zahlen der Form

$$\left(u - \frac{a}{u}\right)^2.$$

Für *festes* u hat die Kongruenz

$$\left(x - \frac{a}{x}\right)^2 = \left(u - \frac{a}{u}\right)^2 \iff \left(x^2 - a\right)^2 - x^2\left(u - \frac{a}{u}\right)^2 = 0$$

als Gleichung vierten Grades höchstens 4 Lösungen, die man auch sofort angeben kann:

$$x = u,\ x = -u,\ x = \frac{a}{u},\ x = -\frac{a}{u}.$$

Da $u \neq 0$ und $p > 2$, ist $u \neq -u$; es könnte aber $u = \frac{a}{u}$ oder $u = -\frac{a}{u}$ gelten, und dann gibt es nur zwei verschiedene Lösungen der Kongruenz (sonst vier).

Sei nun $p = 4k - 1$. Dann ist $\left(\frac{-1}{p}\right) = -1$ und *genau eine* der zwei Zahlen $a, -a$ ist ein quadratischer Rest: Ist a quadratischer Rest, dann gibt es *ein* y mit $\pm y = \pm\frac{a}{y}$ und *kein* y mit $\pm y = \mp\frac{a}{y}$; und wenn a quadratischer Nichtrest ist, ist es genau umgekehrt. Betrachtet man also die Abbildung

$$\mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_p\colon\ x \mapsto \left(x - \frac{a}{x}\right)^2, \tag{A.5}$$

so ist das Urbild von $\left(y - \frac{a}{y}\right)^2$ genau $\{y, -y\}$; alle anderen Urbilder haben aber Kardinalität 4: Die Kardinalität des Bildes ist also

$$1 + \frac{(p-1)-2}{4} = 1 + \frac{4k-4}{4} = k.$$

Sei schließlich $p = 4k + 1$. Dann ist $\left(\frac{-1}{p}\right) = 1$, und a und $-a$ sind entweder beide quadratische Reste oder beide quadratische Nichtreste. Wenn a und $-a$ beide quadratische Nichtreste sind, gibt es kein x mit $x = -\frac{a}{x}$, und alle Urbilder der Abbildung (A.5) haben Kardinalität vier: Die Kardinalität des Bildes ist also

$$\frac{p-1}{4} = \frac{4k}{4} = k.$$

Wenn a und $-a$ beide quadratische Reste sind, dann gibt es *ein* y mit $\pm y = \pm\frac{a}{y}$ und *ein* z mit $\pm z = \mp\frac{a}{z}$: Die Urbilder von $\left(y - \frac{a}{y}\right)^2$ und von $\left(z - \frac{a}{z}\right)^2$ haben dann Kardinalität zwei, alle anderen Urbilder haben Kardinalität vier, und wir erhalten als Kardinalität des Bildes

$$2 + \frac{(p-1)-4}{4} = 2 + \frac{4k-4}{4} = k + 1.$$

Damit sind alle Behauptungen gezeigt. □

A.3. Algebra

DEFINITION A.3.1. *Sei S eine Menge, auf der eine* zweistellige Verknüpfung *gegeben ist, das ist eine Funktion*

$$f\colon\ S \times S \to S,$$

die meist mit einem Symbol wie "$+$" oder "$\cdot$" bezeichnet wird (aber auch mit $\times, \oplus, \otimes, \cdot$) in dem Sinne, daß nicht $f(s_1, s_2)$ geschrieben wird, sondern $s_0 + s_1$ oder $s_0 \cdot s_1$ (aber auch $s_0 \times s_1$, $s_0 \oplus s_1$, $s_0 \otimes s_1$ — je nachdem, welches Symbol für die Verknüpfung verwendet wird).

Sei also S eine Menge mit der zweistelligen Verknüpfung "$\cdot$", und sei $X \subseteq S$ eine Teilmenge von S und $s \in S$ ein Element in S. Dann bezeichnet

$$s \cdot X := \{s \cdot x\colon\ x \in X\}$$

bzw.

$$X \cdot s := \{x \cdot s\colon\ x \in X\}$$

Sei $Y \subseteq S$ eine weitere Teilmenge von S. Dann bezeichnet

$$X \cdot Y := \{x \cdot y\colon\ x \in X \text{ und } y \in Y\}\,.$$

BEISPIEL A.3.2. *Wenn wir die Menge $\mathbb{Z}$ der ganzen Zahlen mit der (gewöhnlichen) Multiplikation $\cdot$ als zweistelliger Verknüpfung betrachten, dann ist z.B. $2 \cdot \mathbb{Z}$ die Menge der geraden Zahlen.*

A.3.1. Gruppen.

DEFINITION A.3.3 (Gruppe, Untergruppe und Normalteiler).

DEFINITION A.3.4 (Halbgruppe, Gruppe). *Eine* Halbgruppe *ist ein Paar $(G, \odot)$, bestehend aus einer Menge G und einer zweistelligen Verknüpfung $\odot$ auf G mit folgender Eigenschaft:*

- *Für alle $a, b, c \in G$ gilt: $(a \odot b) \odot c = a \odot (b \odot c)$. (Assoziativität.)*

*Die (Halb–)*Gruppenoperation *$\odot$ bestimmt also eine Abbildung $G \times G \to G$ durch $(a, b) \mapsto a \odot b$.*
Eine Halbgruppe $(G, \odot)$ heißt Gruppe*, wenn darüber hinaus gilt:*

- *Es gibt ein* neutrales Element *$\mathbb{n} \in G$, sodaß für alle $a \in G$ gilt: $a \odot \mathbb{n} = \mathbb{n} \odot a = a$. (Existenz eines neutralen Elements.)*
- *Für alle $a \in G$ existiert ein* inverses Element *$a^{-1} \in G$ mit $a \odot a^{-1} = a^{-1} \odot a = \mathbb{n}$. (Existenz eines inversen Elements.)*

Die Anzahl der Elemente von G wird auch als die Ordnung *der Gruppe G bezeichnet und mit* ord G *abgekürzt: Eine Gruppe G mit* ord $G < \infty$ *heißt* endliche Gruppe*.*
Eine Gruppe $(G, \odot)$ heißt abelsch *oder* kommutativ*, wenn zusätzlich gilt:*

- *Für alle $a, b \in G$ gilt $a \odot b = b \odot a$. (Kommutativität.)*

Das Symbol $\odot$ für die Gruppenoperation ist natürlich nicht das einzig mögliche: Oft schreibt man auch "$\cdot$" oder "$\circ$" (*multiplikative Schreibweise*; dann verwendet man anstelle des Symbols "$\mathbb{n}$" auch **1**), aber auch "$+$" oder "$\oplus$" (*additive Schreibweise*; dann verwendet man anstelle des Symbols "$\mathbb{n}$" auch **0**).

BEISPIEL A.3.5. *Die Menge der $n \times n$–Matrizen über $\mathbb{R}$ oder über $\mathbb{Z}$ bilden eine Halbgruppe in bezug auf die Matrixmultiplikation. Die Menge der* invertierbaren *$n \times n$–Matrizen bildet eine Gruppe, die $\mathrm{GL}_n(\mathbb{R})$ bzw. $\mathrm{GL}_n(\mathbb{Z})$.*

DEFINITION A.3.6 (Untergruppe, Nebenklasse). *Eine nichtleere Teilmenge $U \subseteq G$ bildet eine* Untergruppe *$(U, \odot)$ von $(G, \odot)$, wenn gilt:*

- *$a, b \in U \implies a \odot b \in U$ (Abgeschlossenheit bezüglich $\odot$; also $U \odot U \subseteq U$.)*
- *$a \in U \implies a^{-1} \in U$ (Abgeschlossenheit bezüglich Inversenbildung.)*

Wir schreiben dann $U \sqsubseteq G$, und es gilt äquivalent das einfache Untergruppenkriterium*:*

$$U \sqsubseteq G :\Longleftrightarrow \left(a, b \in U \implies a \odot b^{-1} \in U\right). \tag{A.6}$$

Sei $H \sqsubseteq G$ eine Untergruppe von G, und sei $g \in G$. Die linke bzw. rechte Nebenklasse *$g \odot H$ bzw. $H \odot g$ ist*

$$g \odot H := \{g \odot n\colon\ n \in H\}\,,$$
$$H \odot g := \{n \odot g\colon\ n \in H\}\,.$$

PROPOSITION A.3.7. *Sei G eine* endliche *Gruppe, seien $P, Q \sqsubseteq G$ zwei Untergruppen von G. Dann gilt*

$$P \cap Q \sqsubseteq G \text{ und } |P \cdot Q| = \frac{|P| \cdot |Q|}{|P \cap Q|}.$$

BEWEIS. Die Abbildung

$$\varphi\colon\ P \times Q \to P \cdot Q,\ (p,q) \mapsto p \cdot q$$

ist surjektiv (definitionsgemäß), aber nicht notwendigerweise injektiv:

$$p \cdot q = p' \cdot q' \iff \left(p'\right)^{-1} \cdot p = q' \cdot q^{-1} =: x \in P \cap Q.$$

Das heißt aber: Das Urbild von $p \cdot q$ ist

$$\varphi^{-1}(p \cdot q) = \left\{ \left(p \cdot x^{-1}, x \cdot q \right) :\ x \in P \cap Q \right\},$$

für alle $(p,q) \in P \times Q$: Diese Urbilder haben alle dieselbe Mächtigkeit $|P \cap Q|$, also gibt es

$$|P \times Q| \,/\, |P \cap Q|$$

verschiedene Urbilder: Daraus folgt die Behauptung. □

PROPOSITION A.3.8. *Sei G eine Gruppe: Für eine beliebige Familie $\mathcal{U}$ von Untergruppen von G ist der Durchschnitt über alle $U \in \mathcal{U}$ wieder eine Untergruppe von G:*

$$\bigcap_{U \in \mathcal{U}} U \sqsubseteq G.$$

Sei $H \sqsubseteq G$ eine Untergruppe von G: Dann sind zwei Links–Nebenklassen $g \cdot H$, $h \cdot H$ genau dann gleich, wenn $g \cdot h^{-1} \in H$.
Zwei verschiedene *Nebenklassen von H sind stets* disjunkt, *also*

$$g, h \in G \implies g \cdot H = h \cdot H \text{ oder } g \cdot H \cap h \cdot H = \emptyset.$$

(Die analoge Aussage gilt für Rechts–Nebenklassen.)
Außerdem sind je zwei Links–Nebenklassen von H gleichmächtig; genauer gesagt: Die Abbildung

$$g \cdot H \to h \cdot H\colon\ x \mapsto h \cdot g^{-1} \cdot x$$

ist eine Bijektion. (Die analoge Aussage gilt für Rechts–Nebenklassen.)

BEWEIS. Die erste Behauptung ergibt sich sofort aus dem "Untergruppenkriterium" (A.6).
Die zweite Behauptung ist klar:

$$g \cdot H = h \cdot H \iff H = g^{-1} \cdot h \cdot H \iff g^{-1} \cdot h \in H.$$

Angenommen, es gibt ein $x \in g \cdot H \cap h \cdot H$: Dann ist also $x = g \cdot y = h \cdot y'$ für $y, y' \in H$; aber das bedeutet

$$h^{-1} \cdot g = y' \cdot y^{-1} \in H,$$

also nach dem vorigen $g \cdot H = h \cdot H$.

Daß schließlich die beschriebene Abbildung $g \cdot H \to h \cdot H$ bijektiv ist, ergibt sich einfach daraus, daß ihre Umkehrabbildung existiert — diese ist nämlich

$$h \cdot H \to g \cdot H\colon\ x \mapsto g \cdot h^{-1} \cdot x,$$

wie man sofort sieht. □

DEFINITION A.3.9 (Erzeugte Untergruppe, Ordnung eines Gruppenelements). *Sei G eine Gruppe, sei $X \subseteq G$ eine Teilmenge von G. Dann heißt der Durchschnitt über alle Untergruppen von G, die die Teilmenge X enthalten, die von X* erzeugte Untergruppe*: Wir bezeichnen sie mit*

$$\langle X \rangle := \bigcap_{X \subset U \sqsubseteq G} U.$$

Ist $X = \{g_1, \ldots, g_m\}$ endlich, dann schreiben wir statt $\langle \{g_1, \ldots, g_m\} \rangle$ kürzer

$$\langle g_1, \ldots, g_m \rangle.$$

Sei $g \in G$. Dann heißt die Ordnung der von $\{g\}$ erzeugten Untergruppe die Ordnung *von g; wir bezeichnen sie mit $\operatorname{ord}_G(g)$:*

$$\operatorname{ord}_G(g) := |\langle g \rangle|.$$

Ist $\operatorname{ord}_G(g)$ endlich, dann gilt

$$\operatorname{ord}_G(g) = \min\{n \in \mathbb{N}\colon\ g^n = \mathbb{n}_G\}.$$

Jede Gruppe G, die von einem einzigen Element erzeugt wird, also

$$G = \langle r \rangle,$$

heißt zyklische Gruppe*. Es ist leicht zu sehen, daß es bis auf Isomorphie genau eine zyklische Gruppe der Ordnung n gibt, für jedes $n \in \mathbb{N} \cup \{\infty\}$: Wir bezeichnen sie mit C_n. Offensichtlich gilt:*

$$C_n = \left\{e, r, r^2, \ldots, r^{n-1}\right\} \simeq \mathbb{Z}/n\mathbb{Z},$$
$$C_\infty = \left\{\ldots, r^{-i}, \ldots, r^{-1}, e, r, \ldots, r^i, \ldots\right\} \simeq \mathbb{Z}$$

PROPOSITION A.3.10. *Sei G eine Gruppe, sei $g \in G$ ein Element endlicher Ordnung. Dann gilt:*

$$g^n = \mathbb{n}_G \implies \operatorname{ord}_G(g) \mid n.$$

BEWEIS. Angenommen, $n = k \cdot \operatorname{ord}_G(g) + r$ mit $0 < r < \operatorname{ord}_G(g)$. Dann wäre

$$\mathbb{n}_G = g^n = \left(g^{\operatorname{ord}_G(g)}\right)^k \cdot g^r = g^r,$$

ein Widerspruch. □

DEFINITION A.3.11. *Wir bezeichnen die Familie der Nebenklassen einer Untergruppe $H \sqsubseteq G$ mit G/H: Aus Proposition A.3.8 ergibt sich, daß G/H eine eine* Mengenpartition *von G bildet, d.h.:*

$$G = \dot{\bigcup}_{n \in G/n} n.$$

Die Anzahl der verschiedenen Nebenklassen von H in G heißt der Index *der Untergruppe N in G und wird mit $(G : N) = |G/H|$ bezeichnet.*

Da laut Proposition A.3.8 alle Nebenklassen einer Untergruppe gleichmächtig sind, ergibt sich ohne weiteres:

SATZ A.3.12 (Satz von Lagrange). *Sei G eine endliche Gruppe und $H \sqsubseteq G$ eine Untergruppe von G. Dann ist die Ordnung von H ein Teiler der Ordnung von G, genauer gesagt:*

$$|G| = (G : H) \cdot |H| .$$

BEWEIS. Folgt sofort aus der ersten Aussage in Proposition A.3.15. □

PROPOSITION A.3.13. *Sei G eine Gruppe, sei $H \sqsubseteq G$ eine Untergruppe von G und sei $g \in G$. Dann ist*

$$g^{-1} \cdot H \cdot g \sqsubseteq G$$

ebenfalls eine Untergruppe von G.

BEWEIS. Zu zeigen ist:

$$a, b \in g^{-1} \cdot H \cdot g \implies a \cdot b^{-1} \in g^{-1} \cdot H \cdot g.$$

Das ist aber eine einfache Rechnung, denn die Voraussetzung bedeutet, daß es $a', b' \in H$ gibt mit $a = g^{-1} \cdot a' \cdot g$ und $b = g^{-1} \cdot b' \cdot g$, also ist

$$a \cdot b^{-1} = \left(g^{-1} \cdot a' \cdot g\right) \cdot \left(g^{-1} \cdot \left(b'\right)^{-1} \cdot g\right) = g^{-1} \cdot \left(a' \cdot \left(b'\right)^{-1}\right) \cdot g \in g^{-1} \cdot H \cdot g,$$

und daraus folgt sofort die Behauptung. □

DEFINITION A.3.14 (Normalteiler). *Sei $H \sqsubseteq G$ eine Untergruppe einer Gruppe G: Für $g \in G$ heißt die Untergruppe $g^{-1} \cdot H \cdot g$ (die mit g)* konjugierte Untergruppe *von H.*
Eine Untergruppe N von G heißt ein Normalteiler *oder eine* normale Untergruppe *von G, wenn eine der folgenden (äquivalenten) Bedingungen erfüllt ist:*

- *Für alle $g \in G$ gilt $g \cdot N \cdot g^{-1} = N$ (N ist invariant unter der* Konjugation *$g \cdot N \cdot g^{-1}$ mit g.)*
- *Für alle $g \in G$ gilt gilt $g \cdot N = N \cdot g$. (Linke und rechte Nebenklassen von N sind immer gleich.)*

Wir schreiben $N \lhd G$, wenn N eine normale Untergruppe von G ist.
In G sind die Untergruppen $\{\mathbb{n}_G\}$ und G (natürlich) immer normal: Eine Gruppe, die abgesehen von diesen trivialen Normalteiler *keine anderen Normalteiler hat, heißt* einfache Gruppe.

PROPOSITION A.3.15. *Sei G eine Gruppe und $H \sqsubseteq G$ eine Untergruppe von G.*
Wenn der Index von H gleich 2 ist, also $(G : H) = 2$ gilt, dann ist H ein Normalteiler von G.

BEWEIS. Für eine Untergruppe $H \sqsubseteq G$ vom Index 2 gibt es (abgesehen von H selbst) nur eine weitere Nebenklasse (egal ob Links– oder Rechtsnebenklasse): Als Menge ist das einfach $G \setminus H$. Insbesondere ist also für $g \notin H$

$$g \cdot H = G \setminus H = H \cdot g,$$

also ist H ein Normalteiler von G. □

PROPOSITION A.3.16. *Sei G eine Gruppe, und $Q \sqsubseteq G$ eine Untergruppe und $P \lhd G$ ein Normalteiler von G. Dann gilt*

$$P \cdot Q = Q \cdot P \sqsubseteq G. \tag{A.7}$$

Ist Q auch normal, dann gilt

$$P \cdot Q = Q \cdot P \lhd G.$$

BEWEIS. Wir zeigen zuerst $P \cdot Q = Q \cdot P$. Sei $p \cdot q$ in $P \cdot Q$: Weil P normal ist, gibt es ein $p' \in P$, sodaß $p \cdot q = q \cdot p' \in Q \cdot P$, also ist $P \cdot Q \subseteq Q \cdot P$. Völlig analog haben wir

$$q \cdot p = p'' \cdot q \text{ für ein } p'' \in P,$$

also auch $Q \cdot P \subseteq P \cdot Q$: Daraus folgt die Behauptung.

Nun zeigen wir, daß $P \cdot Q$ eine Untergruppe von G ist. Nach dem "Untergruppenkriterium" (A.6) genügt es zu zeigen: Für $p \cdot q$, $p' \cdot q'$ beliebig aus $P \cdot Q$ ist auch $(p' \cdot q') \cdot \left(q^{-1} \cdot p^{-1}\right) \in P \cdot Q$. Da P normal ist, ist

$$q^{-1} \cdot p^{-1} = p'' \cdot q^{-1} \text{ für ein } p'' \in P$$

und

$$q' \cdot p'' = p''' \cdot q' \text{ für ein } p''' \in P.$$

Also ist $(p' \cdot q') \cdot \left(q^{-1} \cdot p^{-1}\right) = p' \cdot p''' \cdot q' \cdot q^{-1} \in P \cdot Q$.

Ist Q auch normal, dann gilt für alle $p \cdot q \in P \cdot Q$ und $g \in G$

$$g \cdot (p \cdot q) \cdot g^{-1} = \left(g \cdot p \cdot g^{-1}\right) \cdot \left(g \cdot q \cdot g^{-1}\right) = p' \cdot q'$$

für gewisse $p' \in P, q' \in Q$: Also ist $P \cdot Q$ normal in G. □

Aus dem Satz von Lagrange Satz A.3.12 folgt sofort:

PROPOSITION A.3.17. *Jede Gruppe G von Primzahlordnung $p \in \mathbb{P}$ ist zyklisch.*

BEWEIS. Jedes Element $g \in G$ erzeugt eine Untergruppe $\langle g \rangle \sqsubseteq G$: Die Ordnung dieser Untergruppe (und damit die Ordnung von g) ist ein Teiler der Gruppenordnung p. □

DEFINITION A.3.18. *Sei G eine Gruppe und N ein Normalteiler in G. Dann induziert die Verknüpfung in G eine Verknüpfung auf der Menge der Nebenklassen von N durch*

$$\begin{aligned}(g \cdot N) \cdot (h \cdot N) &= g \cdot (N \cdot h) \cdot N \ \leftarrow \textit{Assoziativität} \\ &= g \cdot (h \cdot N) \cdot N \ \leftarrow \textit{N ist Normalteiler} \\ &= (g \cdot h) \cdot N \ \leftarrow \textit{Assoziativität und } N \cdot N = N\end{aligned}$$

die alle Eigenschaften einer Gruppenoperation erfüllen:

- *Assoziativität der Verknüpfung wird von G sozusagen "geerbt",*
- *Das neutrale Element in G/N ist N,*
- *Das inverse Element von $g \cdot N$ ist (natürlich) $g^{-1} \cdot N$.*

Die so gegebene Gruppe bezeichnen wir als Quotientengruppe *und schreiben G/N.*

BEMERKUNG A.3.19. *Man könnte auf die Idee kommen, auch für eine beliebige (nicht notwendigerweise normale) Untergruppe $H \sqsubseteq G$ eine Verknüpfung auf der Menge der Nebenklassen von H durch*

$$(g \cdot H) \cdot (k \cdot H) := (g \cdot k) \cdot H$$

zu definieren: Die Eigenschaften einer Gruppenoperation würden ja scheinbar ebenso "geerbt"! Aber wir müßten zeigen, daß diese Verknüpfung wohldefiniert *ist, also nicht von der Wahl der Repräsentanten g und k abhängt:*

$$g \cdot H = g' \cdot H \text{ und } k \cdot H = k' \cdot H \implies (g \cdot k) \cdot H = \left(g' \cdot k'\right) \cdot H.$$

Anders formuliert, es müßte gelten:

$$g^{-1} \cdot g' \in H \text{ und } k^{-1} \cdot k' \in H \implies (g \cdot k)^{-1} \cdot \left(g' \cdot k'\right) \in H.$$

Wir haben

$$\begin{aligned}(g \cdot k)^{-1} \cdot \left(g' \cdot k'\right) &= k^{-1} \cdot g^{-1} \cdot g' \cdot k' \\ &= k^{-1} \cdot h \cdot k' \text{ für ein } h \in H,\end{aligned}$$

aber jetzt müßten wir folgern können:

$$h \cdot k' = k' \cdot h' \text{ für ein } h' \in H,$$

und genau für diesen Schritt brauchen wir, daß H ein Normalteiler *ist.*

DEFINITION A.3.20 (Gruppenhomomorphismus). *Seien $(G, \cdot)$ und $(H, \odot)$ zwei Gruppen. Eine Funktion $\varphi : G \to H$ heißt* Gruppenhomomorphismus, *wenn für alle Elemente $g_1, g_2 \in G$ gilt:*

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \odot \varphi(g_2).$$

Ein injektiver *Homomorphismus heißt auch* Monomorphismus, *ein* surjektiver *Homomorphismus heißt auch* Epimorphismus.

Wenn der Gruppenhomomorphismus φ bijektiv ist, dann ist die Umkehrabbildung φ^{-1} auch ein Homomorphismus: φ heißt dann Gruppenisomorphismus.

DEFINITION A.3.21 (Automorphismengruppe). *Sei G eine Gruppe: Ein Gruppenisomorphismus $\varphi : G \to G$ heißt* Gruppenautomorphimus.

Die Familie aller Automorphismen einer Gruppe G hat (mit der Komposition von Funktionen) selbst die Struktur einer Gruppe (ihr neutrales Element ist id_G): Wir bezeichnen sie mit $\mathrm{Aut}(G)$.

DEFINITION A.3.22 (Kern eines Gruppenhomomorphismus). *Der* Kern $\ker \varphi \subset G$ *eines Gruppenhomomorphismus' $\varphi : G \to H$ ist das Urbild des neutralen Elementes $\mathbb{n}_H \in H$:* $\ker \varphi = \varphi^{-1}(\mathbb{n}_H)$.

PROPOSITION A.3.23 (Homomorphiesatz). *Seien G, H Gruppen, und sei $\varphi : G \to H$ ein Gruppenhomomorphismus.*

Dann ist $\ker \varphi$ *ein Normalteiler in G und φ ist genau dann injektiv, wenn* $\ker \varphi = \{\mathbb{n}_G\}$.

Von φ wird eine Abbildung

$$\overline{\varphi}\colon\ G/\ker \varphi \to \operatorname{img} \varphi \sqsubseteq H$$

induziert durch

$$g \cdot \ker \varphi \mapsto \varphi(g),$$

und diese Abbildung $\overline{\varphi}$ *ist ein* Gruppenisomorphismus*:*

$$G/\ker \varphi \simeq \operatorname{img} \varphi.$$

BEWEIS. Für jedes $x \in \ker \varphi$ und jedes $g \in G$ ist

$$\varphi\left(g^{-1} \cdot x \cdot g\right) = \varphi\left(g^{-1}\right) \cdot \varphi(x) \cdot \varphi(g) = (\varphi(g))^{-1} \cdot \mathbb{n}_H \cdot \varphi(g) = \mathbb{n}_H,$$

also ist auch $g^{-1} \cdot x \cdot g \in \ker \varphi$; d.h., $\ker \varphi$ ist ein Normalteiler.

Injektiv bedeutet $g \neq h \implies \varphi(g) \neq \varphi(h)$: Das ist äquivalent mit $g \cdot h^{-1} \neq \mathbb{n}_G \implies \varphi(g) \cdot (\varphi(h))^{-1} \neq \mathbb{n}_H$ bzw. (da φ ein Homomorphismus ist) mit $g \cdot h^{-1} \neq \mathbb{n}_G \implies \varphi\left(g \cdot h^{-1}\right) \neq \mathbb{n}_H$, und das ist wiederum äquivalent zu $\ker \varphi = \{\mathbb{n}_G\}$.

Für die Abbildung $\overline{\varphi}$ ist nur zu zeigen, daß sie *wohldefiniert* ist (die "Homomorphismus–Eigenschaft" erbt sie offensichtlich von φ, injektiv ist sie nach dem eben Gezeigten, und *jede* Abbildung ist surjektiv auf ihr Bild), daß also für zwei Elemente g, g' mit $g^{-1} \cdot g' = e \in \ker \varphi$ gilt $\varphi(g) = \varphi(g')$: Aber das ist klar, denn $\varphi(g') = \varphi(g \cdot e) = \varphi(g) \cdot \varphi(e) = \varphi(g)$. □

DEFINITION A.3.24 (Direktes Produkt). *Seien P und Q zwei Gruppen. Die "koordinatenweise" Gruppenoperation auf dem kartesischen Produkt $N \times Q$*

$$(p, q) \cdot (p', q') := (p \cdot p', q \cdot q')$$

erfüllt alle Eigenschaften einer Gruppenoperation; $P \times Q$ wird damit also zu einer Gruppe (mit neutralem Element $(\mathbb{n}_P, \mathbb{n}_Q)$): Sie heißt direktes Produkt *von P und Q.*

PROPOSITION A.3.25. *Sei G eine Gruppe, seien $P, Q \triangleleft G$ normale Untergruppen von G mit $P \cap Q = \{\mathbb{n}_G\}$. Dann gilt:*

(i) *$p \cdot q = q \cdot p$ für alle $p \in P$, $q \in Q$,*
(ii) *$P \cdot Q \simeq P \times Q$.*

BEWEIS. Daß $P \cdot Q \sqsubseteq G$ eine (normale) Untergruppe von G ist, folgt aus Proposition A.3.16, und daß $|P \cdot Q| = |P \times Q|$ gilt, folgt aus Proposition A.3.7.

Ad (i): Es ist für alle $(p, q) \in P \times Q$

$$p \cdot q \cdot p^{-1} \cdot q^{-1} \in P \cap Q = \{\mathbb{n}_G\},$$

denn $p \cdot q \cdot p^{-1} \in Q$ und $q \cdot p^{-1} \cdot q^{-1} \in P$: Daraus folgt die Behauptung.

Ad (ii): Die Abbildung

$$\varphi : P \times Q \to P \cdot Q,\ (p, q) \mapsto p \cdot q$$

ist *bijektiv* nach Proposition A.3.7. Aus (i) folgt, daß sie auch ein Homomorphismus ist:

$$\begin{aligned}\varphi\left((p,q)\cdot\left(p',q'\right)\right) &= \varphi\left(\left(p\cdot p',q\cdot q'\right)\right)\\ &= p\cdot p'\cdot q\cdot q'\\ &= (p\cdot q)\cdot\left(p'\cdot q'\right) \quad \leftarrow \text{nach (i)}\\ &= \varphi\left(p,q\right)\cdot\varphi\left(p',q'\right).\end{aligned}$$

Daraus folgt nun (ii). □

DEFINITION A.3.26 (Wirkung einer Gruppe). *Sei $G = (G,\cdot)$ eine Gruppe mit neutralem Element $\mathtt{n}_G$, und sei X eine Menge. Eine Abbildung*

$$G\times X\to X,$$

die wir wie folgt notieren

$$(g,x)\mapsto g\cdot x\in X,$$

nennt man eine Wirkung *(oder* Aktion *oder* Operation*) von G auf X, falls gilt:*

- *für alle $g,h\in G$ und alle $x\in X$ ist $g\cdot(h\cdot x)=(g\cdot h)\,x$,*
- *für das neutrale Element $\mathtt{n}\in G$ und alle $x\in X$ ist $\mathtt{n}\cdot x = x$.*

Eine Menge X, auf der eine Gruppe G operiert (oder agiert oder wirkt), heißt auch G–Menge.

DEFINITION A.3.27 (Semidirektes Produkt). *Seien P und Q zwei Gruppen. Sei θ ein Gruppenhomomorphismus*

$$\theta: Q\to \mathrm{Aut}\,(P).$$

Dann operiert Q auf P durch

$$q\cdot p = (\theta\,(q))\,(p),$$

wie man leicht sieht.
Damit kann man auf $P\times Q$ folgende zweistellige Verknüpfung definieren:

$$(p,q)\cdot\left(p',q'\right) := \left(p\cdot(\theta\,(q))\left(p'\right),q\cdot q'\right).$$

Diese Verknüpfung erfüllt alle Eigenschaften einer Gruppenoperation; z.B. ist ihr neutrales Element $\left(\mathtt{n}_P,\mathtt{n}_Q\right)$, und das inverse Element von (p,q) ist

$$(p,q)^{-1} = \left(\theta^{-1}\,(q)\left(p^{-1}\right),q^{-1}\right).$$

Wir nennen diese Gruppe semidirektes Produkt *von P und Q und bezeichnen sie mit $G = P\rtimes_\theta Q$. Für den trivialen Homomorphismus $Q\to\mathrm{Aut}\,(P)$, gegeben durch $\theta\,(q)=\mathrm{id}_P$ erhalten wir das direkte Produkt.*

DEFINITION A.3.28 (exakte Sequenz). *Eine Sequenz*

$$A'\xrightarrow{\phi}A\xrightarrow{\psi}A''$$

von Gruppen A', A, A'' und Homomorphismen ϕ, ψ heißt exakt *bei A, wenn*

$$\mathrm{img}\,\phi = \ker\psi.$$

Allgemeiner heißt eine Sequenz

$$A'\longrightarrow A_1\longrightarrow A_2\longrightarrow\cdots A_n\longrightarrow A''$$

exakt, wenn sie exakt bei $A_1, A_2 \dots A_n$ ist.
Eine exakte Sequenz der Form

$$\{\mathbb{n}\} \longrightarrow A' \xrightarrow{\phi} A \xrightarrow{\psi} A'' \longrightarrow \{\mathbb{n}\}$$

heißt kurze exakte Sequenz*: Das bedeutet, daß*

- $\phi : A' \to A$ *ein* Monomorphismus *ist,*
- $\psi : A \to A''$ *ein* Epimorphismus *ist,*
- $A' \simeq \operatorname{img}\phi = \ker\psi \triangleleft A$ *und* $A'' \simeq A/A'$.

Man sagt dann: A ist eine Erweiterung *von A' und A''.*

BEISPIEL A.3.29. *Sei $G = P \rtimes_\theta Q$ ein semidirektes Produkt. Dann ist*

$$\{\mathbb{n}\} \longrightarrow P \xrightarrow{\phi} G \xrightarrow{\psi} G/P \longrightarrow \{\mathbb{n}\}$$

eine kurze exakte Sequenz: ϕ ist einfach die Einbettung von $P \triangleleft G$ (daß P tatsächlich Normalteiler ist, zeigen wir gleich in Lemma A.3.32) in G und ψ die Quotientenabbildung. Also ist in diesem Fall G eine Erweiterung von P und G/P.

DEFINITION A.3.30 (Transversale und Schnitt). *Sei G eine Gruppe und $N \triangleleft G$ ein Normalteiler von G: Eine Auswahl von Repräsentanten aus jeder Nebenklassen von $g \cdot N \subseteq G$, also eine Menge*

$$\left\{x_g \in g \cdot N, x_h \in h \cdot N, \dots\right\},$$

heißt ein Repräsentantensystem *oder eine* Transversale *von G/N. Offensichtlich kann man eine Transversale auffassen als* injektive *Abbildung*

$$\tau\colon\ G/N \to G.$$

Wenn diese Abbildung τ ein Gruppenhomomorphismus *ist, dann nennt man τ einen* Schnitt *und sagt, daß die kurze exakte Sequenz*

$$\{\mathbb{n}\} \longrightarrow N \xrightarrow{\phi} G \xrightarrow{\psi} G/N \longrightarrow \{\mathbb{n}\}$$

zerfällt *bzw. daß G eine* zerfallende Erweiterung *von N und G/N ist. Es gilt dann $\psi \circ \tau = \mathrm{id}_{G/N}$, und die (genauer: ein isomorphes Bild der) Quotientengruppe G/N ist eine Untergruppe von G.*

BEISPIEL A.3.31. *Es gibt keineswegs immer einen Schnitt für eine kurze exakte Sequenz: Betrachte z.B.*

$$\{\mathbb{n}\} \longrightarrow 2\mathbb{Z} \xrightarrow{\phi} \mathbb{Z} \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z} \longrightarrow \{\mathbb{n}\}.$$

Natürlich gibt es keinen injektiven Gruppenhomomorphismus $\mathbb{Z}_2 \to (\mathbb{Z}, +)$.

LEMMA A.3.32 (Splitting Lemma). *Eine Gruppe G ist* genau dann *isomorph zum semidirekten Produkt zweier Gruppen N und H, also $G \simeq N \rtimes_\theta H$, wenn die kurze exakte Sequenz*

$$\{\mathbb{n}\} \longrightarrow N \xrightarrow{\phi} G \xrightarrow{\psi} H \longrightarrow \{\mathbb{n}\} \tag{A.8}$$

zerfällt, wenn es also einen Homomorphismus $\tau\colon\ H \to G$ gibt mit $\psi \circ \tau = \mathrm{id}_H$.

BEWEIS. Wenn $G \simeq N \rtimes_\theta H$, dann seien ϕ und τ die "natürlichen" Einbettungen der Untergruppen N und H in G:

$$\phi(n) := (n, \mathbb{m}_H) \text{ und } \tau(h) := (\mathbb{m}_N, h).$$

Klarerweise ist $\phi(\mathbb{m}_N) = \tau(\mathbb{m}_H) = (\mathbb{m}_N, \mathbb{m}_H) = \mathbb{m}_G$, und es ist

$$\begin{aligned}\phi(n \cdot n') &= (n \cdot n', \mathbb{m}_H) \\ &= \left(n \cdot \left(\underbrace{\theta(\mathbb{m}_H)}_{\mathrm{id}_N}\right)(n'), \mathbb{m}_H \cdot \mathbb{m}_H\right) \\ &= (n, \mathbb{m}_H) \cdot (n', \mathbb{m}_H) = \phi(n) \cdot \phi(n')\end{aligned}$$

und

$$\begin{aligned}\tau(h \cdot h') &= (\mathbb{m}_N, h \cdot h') \\ &= \left(\mathbb{m}_N \cdot \underbrace{(\theta(h))(\mathbb{m}_N)}_{\mathbb{m}_N}, h \cdot h'\right) \\ &= (\mathbb{m}_N, h) \cdot (\mathbb{m}_N, h') = \tau(h) \cdot \tau(h'),\end{aligned}$$

also sind ϕ und τ Homomorphismen.
Es ist $\phi(N) \lhd G$, denn für alle $(n, h) \in N \rtimes_\theta H \simeq G$ ist

$$\begin{aligned}(n,h) \cdot (n', \mathbb{m}_H) \cdot (n,h)^{-1} &= (n,h) \cdot (n', \mathbb{m}_H) \cdot \left(\theta^{-1}(h)\left(n^{-1}\right), h^{-1}\right) \\ &= (n,h) \cdot \left(n' \cdot \left(\underbrace{\theta(\mathbb{m}_H)}_{\mathrm{id}_N}\right)\left(\theta^{-1}(h)\left(n^{-1}\right)\right), \mathbb{m}_H \cdot h^{-1}\right) \\ &= \left(n \cdot (\theta(h))\left(n' \cdot \left(\theta^{-1}(h)\left(n^{-1}\right)\right)\right), h \cdot h^{-1}\right) \\ &= \left(n \cdot (\theta(h))(n') \cdot n^{-1}, \mathbb{m}_H\right) \in \phi(N).\end{aligned}$$

Schließlich ist definitionsgemäß die Rechtsnebenklasse

$$\phi(N) \cdot (n,h) = \left\{(n', \mathbb{m}_H) \cdot (n,h) : \ n' \in N\right\} = \left\{(n' \cdot n, h) : \ n' \in N\right\},$$

also ist die *Menge* der Rechtsnebenklassen

$$\{\phi(N) \times \{h\} : \ h \in H\},$$

und die Multiplikation von Rechtsnebenklassen entspricht offensichtlich der Multiplikation in H; d.h., die Abbildung

$$\phi(N) \times \{h\} \mapsto h$$

ist ein bijektiver Homomorphismus $G/N \to H$, also $G/N \simeq H$. Sei also ψ der Homomorphismus

$$G \to G/N \simeq H,$$

dann erfüllt die Einbettung $\tau\colon\ H \to N \rtimes_\theta H \simeq G$

$$h \mapsto (\mathbb{m}_N, h)$$

klarerweise $\psi \circ \tau = \mathrm{id}_H$: Das heißt, die Sequenz (A.8) ist *exakt* und *zerfällt*.
Wenn umgekehrt die Sequenz (A.8) zerfällt, dann existiert ein Schnitt τ, und wir betrachten die Abbildung θ, die durch

$$\theta(h)(n) = \phi^{-1}\left(\underbrace{\tau(h)\cdot\phi(n)\cdot\tau\left(h^{-1}\right)}_{\text{Konjugation von } \phi(N) \sqsubseteq G}\right)$$

gegeben ist. Die Abbildung $\theta(h)$ ist ein Automorphismus von N, denn sie entspricht der Konjugation des Normalteilers $N \simeq \phi(N) \lhd G$ mit dem Gruppenelement $\tau(h) \in G$: Also haben wir eine Abbildung $\theta\colon\ H \to \mathrm{Aut}(N)$ definiert. Diese Abbildung ist auch ein Homomorphismus, denn klarerweise ist $\theta(\mathbb{n}) = \mathrm{id}_N$ und

$$\begin{aligned}
\theta\left(h'\cdot h\right)(n) &= \phi^{-1}\left(\tau\left(h'\cdot h\right)\cdot\phi(n)\cdot\tau\left(h^{-1}\cdot h^{-1}\right)\right)\\
&= \phi^{-1}\left(\tau\left(h'\right)\cdot\tau(h)\cdot\phi(n)\cdot\tau\left(h^{-1}\right)\cdot\tau\left(h^{-1}\right)\right)\\
&= \phi^{-1}\left(\tau\left(h'\right)\cdot\phi\left(\phi^{-1}\left(\tau(h)\cdot\phi(n)\cdot\tau\left(h^{-1}\right)\right)\right)\cdot\tau\left(h^{-1}\right)\right)\\
&= \theta\left(h'\right)\left(\theta(h)(n)\right) = \left(\theta\left(h'\right)\circ\theta(h)\right)(n).
\end{aligned}$$

Und tatsächlich ist für den so gegebenen Homomorphismus θ

$$G \simeq N \rtimes_\theta H,$$

denn:
Erstens ist *jedes* Element $g \in G$ in genau einer Nebenklasse von $\phi(N)$ enthalten, läßt sich also *eindeutig* schreiben als

$$g = \phi(n)\cdot\tau(h) \text{ für ein } n \in N \text{ und ein } h \in H,$$

also ist die Abbildung $\mu\colon\ N \rtimes_\theta H \to G$, die durch

$$(n,h) \to \phi(n)\cdot\tau(h)$$

gegeben ist, *bijektiv*.
Zweitens ist definitionsgemäß

$$\begin{aligned}
(n,h)\cdot\left(n',n'\right) &= \left(n\cdot\left(\theta(h)\left(n'\right)\right),h\cdot h'\right)\\
&= \left(n\cdot\left(\phi^{-1}\left(\tau(h)\cdot\phi\left(n'\right)\cdot\tau\left(h^{-1}\right)\right)\right),h\cdot h'\right),
\end{aligned}$$

und dieses Produkt wird unter μ abgebildet auf

$$\begin{aligned}
&\phi\left(n\cdot\left(\phi^{-1}\left(\tau(h)\cdot\phi\left(n'\right)\cdot\tau\left(h^{-1}\right)\right)\right)\right)\cdot\tau\left(h\cdot h'\right)\\
&\quad= \phi(n)\cdot\phi\left(\left(\phi^{-1}\left(\tau(h)\cdot\phi\left(n'\right)\cdot\tau\left(h^{-1}\right)\right)\right)\right)\cdot\tau(h)\cdot\tau\left(h'\right)\\
&\quad= \phi(n)\cdot\tau(h)\cdot\phi\left(n'\right)\cdot\tau\left(h^{-1}\right)\cdot\tau(h)\cdot\tau\left(h'\right)\\
&\quad= \left(\phi(n)\cdot\tau(h)\right)\cdot\left(\phi\left(n'\right)\cdot\tau\left(h'\right)\right),
\end{aligned}$$

also ist μ ein Isomorphismus. □

BEISPIEL A.3.33. *Die beiden folgenden Erweiterungen zerfallen:*

$$1 \to T(n) \xrightarrow{\iota} \mathrm{Iso}(\mathbb{R}^n) \xrightarrow{\ell} O_n(\mathbb{R}) \to 1,$$
$$1 \to \mathrm{SL}_n(\mathbb{K}) \xrightarrow{\iota} \mathrm{GL}_n(\mathbb{K}) \xrightarrow{\det} \mathbb{K}^\star \to 1.$$

Die erste Sequenz zerfällt, weil die Isometriengruppe ein semidirektes Produkt ist; siehe die Überlegungen in der Folge von Definition 1.3.9.
Für die zweite Sequenz definiere man $\tau : \mathbb{K}^\star \to \mathrm{GL}_n(\mathbb{K})$ durch

$$a \mapsto \begin{pmatrix} 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ 0 & \dots & 0 & a \end{pmatrix}$$

Das ist ein Schnitt, denn

$$\tau(a \cdot b) = \tau(a) \cdot \tau(b) \text{ und } (\beta \circ \tau)(a) = \det \tau(a) = a.$$

A.3.2. Ringe.

DEFINITION A.3.34 (Ring, Nullteiler). *Ein* Ring *ist ein Tripel $(R, \oplus, \odot)$ bestehend aus einer Menge R und zwei zweistelligen Verknüpfungen $\oplus$ (Addition) und $\odot$ (Multiplikation) auf R mit folgenden Eigenschaften:*

- *$(R, \oplus)$ ist eine abelsche Gruppe,*
- *$(R, \odot)$ ist eine Halbgruppe (d.h., die Multiplikation ist* assoziativ*),*
- *für alle $a, b, c \in R$ gilt $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ und $(a \oplus b) \odot c = a \odot c \oplus c \odot c$ (*Distributivität*.)*

Das neutrale Element $\mathbb{n}$ von $(R, \oplus)$ heißt Nullelement *des Rings R; in der Regel wird dafür das Symbol $\mathbf{0}$ verwendet. (Der triviale Fall, daß R* nur *aus dem Nullelement besteht, wird als* Nullring *bezeichnet*[1]*.)*
Ein Ring R heißt kommutativ*, falls die Multiplikation kommutativ ist, also wenn für alle $a, b \in R$ gilt: $a \odot b = b \odot a$. Ein Ring muß keineswegs kommutativ sein: Wenn man das betonen möchte, spricht man von einem* nichtkommutativen *Ring. Wenn die Halbgruppe $(R, \odot)$ ein neutrales Element besitzt, heißt R ein* Ring mit Eins *oder ein* unitärer Ring*. Dieses neutrale Element heißt dann das* Einselement *des Rings; in der Regel wird dafür das Symbol $\mathbf{1}$ verwendet. In einem unitären Ring R ist die Menge der (multiplikativ) invertierbaren Elemente*

$$R^\star := \left\{ a \in R \colon \exists a^{-1} \in R \text{ mit } a \cdot a^{-1} = a^{-1} \cdot a = \mathbf{1} \right\}$$

nicht leer (denn $\mathbf{1} \in R^\star$): Diese invertierbaren Elemente heißen Einheiten *des Rings; mit der Multiplikation in R ist $R^\star$ eine Gruppe: Die* Einheitengruppe *von R.*

[1] Für unsere Zwecke ist der Nullring uninteressant: Er spielt nur für sehr abstrakte (kategorientheoretische) Betrachtungen eine Rolle. Alle Ringe, die wir hier betrachten, sind nicht–trivial.

Zwei Elemente $a, b \in R \setminus \mathbf{0}$ mit der Eigenschaft $a \odot b = \mathbf{0}$ heißen Nullteiler. *Ein Ring, der keine Nullteiler enthält, heißt* nullteilerfrei. *Ein kommutativer nullteilerfreier Ring mit Eins heißt* Integritätsbereich *oder* Integritätsring.

BEISPIEL A.3.35. *$\mathbb{Z}$ ist ein Integritätsbereich mit Einheitengruppe $\{1, -1\} \simeq \mathbb{Z}_2$.*

DEFINITION A.3.36 (Ideal). *Sei $R = (R, \oplus, \odot)$ ein Ring. Eine* nichtleere *Teilmenge $I \subseteq R$ heißt* Linksideal *bzw.* Rechtsideal, *wenn gilt:*

- *$I \sqsubseteq (R, \oplus)$ (I ist eine Untergruppe der additiven Gruppe)*
- *für jedes $r \in R$ ist $r \odot I \subseteq I$ (kurz: $RI \subseteq I$) bzw. $I \odot r \subseteq I$ (kurz: $IR \subseteq I$; I ist also abgeschlossen bezüglich Multiplikation mit R von links bzw. von rechts).*

Wenn I sowohl Links– als auch Rechtsideal ist, nennt man I einfach ein Ideal *und schreibt $I \sqsubseteq R$. (Die Unterscheidung zwischen Links– und Rechtsidealen ist in kommutativen Ringen natürlich überflüssig: In einem kommutativen Ring ist jedes Linksideal auch ein Rechtsideal und umgekehrt.) I heißt* echtes Ideal, *wenn $I \neq R$.*
Die Menge aller Ideale eines Rings ist halbgeordnet *durch Mengeninklusion:*

$$I_1 \leq I_2 :\Longleftrightarrow I_1 \subseteq I_2 \text{ (als Mengen).}$$

Klarerweise gibt es in dieser Halbordnung ein eindeutiges maximales Element — nämlich den ganzen Ring R. Wenn man diese Halbordnung aber auf die echten *Ideale* einschränkt, *dann kann es mehrere maximale Elemente geben: Ein* maximales Ideal *ist ein* echtes *Ideal I, das in keinem anderen* echten *Ideal* echt *enthalten ist, also*

$$I \subseteq I_1 \sqsubseteq R \implies I = I_1 \text{ oder } I_1 = R.$$

(Mit dem Lemma von Zorn *kann man für jedes echte Ideal I eines Rings mit Eins ein maximales Ideal I_{max} konstruieren, sodaß $I \subseteq I_{max}$: Abgesehen vom trivialen Nullring hat also jeder Ring mit Eins ein maximales Ideal.)*
Ein echtes *Ideal $P \sqsubseteq R$ heißt* prim *oder* Primideal, *wenn für alle Ideale $I, J \sqsubseteq R$ gilt:*

$$I \odot J \subseteq P \implies I \subseteq P \text{ oder } J \subseteq P.$$

In einem kommutativen *Ring (siehe etwa* [8, Theorem 2.15]*) ist diese Bedingung äquivalent mit*

$$x \odot y \in P \implies x \in P \text{ oder } y \in P \text{ für alle } x, y \in R. \tag{A.9}$$

KOROLLAR A.3.37. *Sei $\mathcal{I}$ eine* Familie *von Idealen in einem Ring R. Dann ist auch der Durchschnitt aller Elemente von $\mathcal{I}$ ein Ideal in R:*

$$\left(\bigcap_{I \in \mathcal{I}} I \right) \sqsubseteq R.$$

Ohne Beweis. □

DEFINITION A.3.38 (Homomorphismus, Kern). *Seien $(R, +, \cdot)$ und $(S, \oplus, \odot)$ zwei Ringe. Eine Funktion $g : R \to S$ heißt* Ringhomomorphismus, *wenn für alle Elemente $a, b \in R$ gilt:*

$$f(a + b) = f(a) \oplus f(b)$$
$$f(a \cdot b) = f(a) \odot f(b)$$

Der Kern *von f ist*

$$\ker f := \{r \in R\colon\ f(r) = \mathbf{0} \in S\}.$$

Ideale spielen bei Ringen eine ähnliche Rolle wie Normalteiler bei Gruppen:

SATZ A.3.39 (Faktorring). *Sei R ein Ring, sei I eine Ideal in R: $I \sqsubseteq R$. Dann ist I eine* normale *Untergruppe (der additiven abelschen Gruppe $(R,+)$), und die (additive) Quotientengruppe R/I ist ein Ring mit der Multiplikation*

$$(a+I)\cdot(b+I) := (a\cdot b + I).$$

BEWEIS. Wir müssen zeigen, daß diese Multiplikation *wohldefiniert* ist, daß also gilt

$$(a+I) = \left(a'+I\right) \text{ und } (b+I) = \left(b'+I\right) \implies (a\cdot b+I) = \left(a'\cdot b'+I\right).$$

Sei also $a' = a+i$ bzw. $b' = b+j$ für $i,j \in I$. Dann ist aber

$$a'\cdot b' - a\cdot b = i\cdot b + j\cdot a + i\cdot j \in I,$$

weil I ein Ideal ist, also ist tatsächlich

$$a'\cdot b' + I = a\cdot b + I.$$

Daß diese Multiplikation assoziativ und distributiv ist, ist leicht nachzurechnen: Die Faktorgruppe R/I ist also ein *Faktorring*. □

Die folgenden Aussagen sind leicht nachzurechnen:

SATZ A.3.40. *Sei $f : R \to S$ ein Homomorphismus von Ringen, dann ist der Kern von f ein Ideal in R:*

$$\ker f \sqsubseteq R.$$

Ist umgekehrt I ein Ideal in R, dann ist die Abbildung $\pi : R \to R/I$

$$r \mapsto r + I$$

ein Epimorphismus *von Ringen mit Kern* $\ker\pi = I$*: π heißt auch* kanonischer Epimorphismus *oder* Projektion.

Ohne Beweis. □

KOROLLAR A.3.41 (Erster Isomorphiesatz). *Sei $f : R \to S$ ein Homomorphismus von Ringen, dann induziert f einen* Isomorphismus

$$R/\ker f \simeq \operatorname{img} f.$$

Ohne Beweis. □

PROPOSITION A.3.42. *Sei R ein Ring mit Eins, sei $I \sqsubseteq R$ ein echtes Ideal. Dann gilt:*

$$R/I \text{ ist nullteilerfrei} \iff I \text{ ist Primideal.} \tag{A.10}$$

BEWEIS. "R/I nullteilerfrei" ist äquivalent mit

$$(x+I)\cdot(y+I) = 0+I \implies x+I = 0+I \text{ oder } y+I = 0+I.$$

Das ist wiederum äquivalent mit

$$x\cdot y \in I \implies x \in I \text{ oder } y \in I,$$

und das heißt: I ist ein Primideal. □

DEFINITION A.3.43 (Endlich erzeugte Ideale, Hauptideale, Hauptidealring, Hauptidealbereich). *Sei R ein Ring, sei $X \subseteq R$ und sei $\mathcal{I}$ die Familie aller Ideale in R, die X als Teilmenge enthalten. Dann nennen wir*

$$((X)) := \bigcap_{I \in \mathcal{I}}$$

das von X erzeugte *Ideal, und X heißt ein* Erzeugendensystem *oder eine* Basis *von $((X))$. Wenn X endlich ist, heißt $((X))$* endlich erzeugt*; wenn X einpunktig ist (also $X = \{x\}$), dann heißt $((x)) = ((\{x\}))$* Hauptideal*.*

Ein Ring R, in dem jedes Ideal ein Haupideal ist, heißt Hauptidealring*; wenn R überdies ein Integritätsbereich ist, heißt er* Hauptidealbereich*.*

KOROLLAR A.3.44. *Sei R ein kommutativer Ring R mit Eins, sei $A \subseteq R$. Dann ist das von A erzeugte Ideal*

$$((A)) = \left\{ \sum_{a \in A} r_a \cdot a \colon \; r_a \in R \text{ für alle } a, \text{ aber nur endlich viele } r_a \neq \mathbf{0} \right\}.$$

BEWEIS. Die angegebenen Menge *ist* ein Ideal in R, und jedes Ideal I mit $A \subseteq I$ muß *jedenfalls* alle Elemente dieser Menge enthalten. □

BEISPIEL A.3.45. *Der Ring $\mathbb{Z}$ ist ein Hauptidealbereich.*

A.3.2.1. *Teilbarkeit in kommutativen Ringen.* Ganz analog zur Teilbarkeit im Ring der ganzen Zahlen $\mathbb{Z}$ können wir definieren:

DEFINITION A.3.46 (Teilbarkeit). *Sei R ein kommutativer Ring, seien $a, b \in R$, $a \neq 0$. Wir sagen "a teilt b" bzw. "b ist ein* Vielfaches *von a" (und schreiben $a \mid b$), wenn gilt:*

$$\text{Es gibt ein } x \in R \colon \; a \cdot x = b.$$

Sei R ein kommutativer Ring mit Eins. Ein Element $c \in R$, $c \neq 0$ und $c \notin R^\star$, heißt

- irreduzibel*, wenn*
$$c = a \cdot b \implies a \in R^\star \text{ oder } b \in R^\star,$$
- prim*, wenn*
$$c \mid a \cdot b \implies c \mid a \text{ oder } c \mid b.$$

PROPOSITION A.3.47. *In einem Integritätsbereich ist jedes prime Element irreduzibel.*

BEWEIS. Sei p prim mit $p = a \cdot b$. Dann gilt o.B.d.A. $p \mid a$, d.h., es gibt ein x mit $a = x \cdot p$. Dann ist also $p = x \cdot p \cdot b$, also $p \cdot (\mathbf{1} - x \cdot b) = 0$. Da es keine Nullteiler gibt, muß $\mathbf{1} = x \cdot b$ gelten, d.h., b ist eine Einheit. □

SATZ A.3.48. *Sei R ein Integritätsbereich und $c \in R$, $c \neq 0$. Dann gilt:*

- *c ist prim $\iff$ $((c))$ ist Primideal.*
- *c ist irreduzibel $\iff$ $((c))$ ist maximales Ideal.*

BEWEIS. Wir verwende die Charakterisierung (A.9) für Primideale. Sei c prim: Für $a \cdot b \in (\!(c)\!)$ gilt $c \mid a \cdot b$, also folgt (o.B.d.A.) $c \mid a$, und das heißt $a \in (\!(c)\!)$. Sei umgekehrt $(\!(c)\!)$ ein Primideal: $c \mid a \cdot b \implies a \cdot b \in (\!(c)\!)$, das heißt (o.B.d.A.) $a \in (\!(c)\!)$, also $c \mid a$.
Sei c irreduzibel: Aus $(\!(c)\!) \subseteq (\!(d)\!)$ folgt $c = d \cdot x$, also ist $d \in R^\star$ (woraus $(\!(d)\!) = R$ folgt) oder $x \in R^\star$ (woraus $(\!(c)\!) = (\!(d)\!)$ folgt). Sei umgekehrt $(\!(c)\!)$ maximal, dann ist $c \neq 0$ und $c \notin R^\star$: Falls $c = a \cdot b$, dann gilt $(\!(c)\!) \subset (\!(a)\!)$, also $(\!(a)\!) = (\!(c)\!)$ (woraus $b \in R^\star$ folgt) oder $(\!(a)\!) = R$ (woraus $a \in R^\star$ folgt). □

DEFINITION A.3.49 (Faktorzerlegung, faktorieller Ring). *Sei R ein Integritätsbereich und $x \in R$. Eine Darstellung von x als Produkt irreduzibler Elemente*

$$x = p_1 \cdot p_2 \cdots p_n$$

heißt Faktorzerlegung *von x. Sie heißt* eindeutige Faktorzerlegung, *wenn für jede andere Faktorzerlegung $x = q_1 \cdot q_2 \cdots q_m$ $m = n$ gilt und es eine Permutation $\sigma \in \mathfrak{S}_n$ gibt, sodaß für alle $1 \leq i \leq n$ gilt:*

$$p_i = q_{\sigma_i} \cdot u_i \text{ für ein } u_i \in R^\star.$$

Ein Integritätsbereich, in dem jedes *Element $x \notin R^\star$, $x \neq 0$ eine eindeutige Faktorzerlegung hat, heißt* faktorieller Ring *oder* faktorieller Ring.

DEFINITION A.3.50 (Noetherscher Ring). *Ein Ring R heißt* Noetherscher Ring, *wenn* jede *aufsteigende Kette von Idealen in R*

$$I_1 \sqsubseteq I_2 \sqsubseteq \cdots R$$

irgendwann stationär *wird, also wenn für ein $k \in \mathbb{N}$ gilt:*

$$I_j = I_j \text{ für alle } j \geq k.$$

PROPOSITION A.3.51. *Ein Ring R ist noethersch genau dann, wenn jedes Ideal $I \in R$ endlich erzeugt ist.*

BEWEIS. ($\implies$): Sei $I \sqsubseteq R$ ein Ideal, und sei $\Sigma \neq \emptyset$ die Familie aller endlich erzeugten Ideale von R, die in I enthalten sind. Angenommen, Σ hätte kein maximales Element in bezug auf die Ordnung von Idealen durch Mengeninklusion: Dann könnte man eine unendlich lange aufsteigende Kette von Idealen konstruieren, im Widerspruch zur Voraussetzung. Sei also $S = (\!(s_1, \ldots, s_n)\!)$ ein maximales Element von Σ: Wäre $S \subset I$ eine *echte* Teilmenge, dann wäre für ein $x \in I \setminus S$ das Ideal $S' = (\!(s_1, \ldots, s_n; x)\!)$ endlich erzeugt mit $S \subset S'$, im Widerspruch dazu, daß S maximal in Σ. Also ist $I = S$ endlich erzeugt.
($\impliedby$): Sei $I_1 \sqsubseteq I_2 \cdots$ eine aufsteigende Kette von Idealen. Dann ist $S := \bigcup_j I_j$ ebenfalls ein Ideal (wie man leicht nachprüft) und nach Voraussetzung endlich erzeugt: $S = (\!(x_1, \ldots, x_n)\!)$. Sei k die kleinste Zahl sodaß $\{x_1, \ldots, x_n\} \in I_k$: Es ist $k < \infty$, und $I_j = I_k = S$ für alle $j \geq k$. □

KOROLLAR A.3.52. *Jeder Hauptidealbereich R ist nothersch: Sei*

$$(\!(a_1)\!) \subseteq (\!(a_2)\!) \subseteq \cdots$$

eine aufsteigene Kette von Idealen. Dann wird diese Kette irgendwann stationär, *d.h., es gibt ein $n \in \mathbb{N}$ sodaß*

$$(\!(a_j)\!) = (\!(a_n)\!) \text{ für alle } j \geq n.$$

BEWEIS. Siehe [**8**, Lemma 3.6]. □

SATZ A.3.53. *Jeder Hauptidealbereich ist ein faktorieller Ring .*

BEWEIS. Siehe [**8**, Theorem 3.7]. □

DEFINITION A.3.54 (Euklidischer Ring). *Sei R ein Ring: Eine* euklidische Norm *ist eine Funktion*

$$\mathbf{N} : R \setminus \{0\} \to \mathbb{N}_0.$$

Ein Integritätsbereich R heißt euklidischer Ring, *wenn es eine euklidische Norm* $\mathbf{N}$ *gibt, sodaß für alle $x \in R$ und alle $d \in R \setminus \{0\}$ Elemente $q, r \in R$ existieren mit*

$$x = q \cdot d + r, \text{ wobei } r = 0 \text{ oder } \mathbf{N}(r) < \mathbf{N}(d).$$

BEISPIEL A.3.55. *$\mathbb{Z}$ ist ein euklidischer Ring mit $N(z) := |z|$ (Division mit Rest).*

SATZ A.3.56. *Jeder euklidische Ring ist ein Hauptidealbereich.*

BEWEIS. Zu zeigen ist, daß jedes Ideal $I \sqsubseteq R$ ein Hauptideal ist: Für das Ideal $(\!(0)\!)$ ist das klar, sei also $I \neq (\!(0)\!)$. Dann gibt es ein $x \in I$ mit $\mathbf{N}(x) = \min\{\mathbf{N}(y) : \ y \in I\}$. Sei nun $y \in I$ beliebig, dann gibt es nach Voraussetzung Elemente $q, r \in R$ sodaß

$$y = q \cdot x + r \text{ mit } r = 0 \text{ oder } \mathbf{N}(r) < \mathbf{N}(d).$$

Es ist aber $r = y - q \cdot x \in I$, also $r = 0$ wegen Minimalität von x. Für jedes $y \in I$ gilt also $x \mid y$, also $I = (\!(x)\!)$. □

SATZ A.3.57 (Hilbertscher Basissatz). *Wenn R ein noetherscher Ring ist, dann ist auch $R[x]$ noethersch (mit Induktion ist dann also auch $R[x_1, \ldots, x_n]$ noethersch).*

BEWEIS. Sei I ein Ideal in $R[x]$: Gemäß Proposition A.3.51 wollen wir zeigen, daß es endlich erzeugt ist. Betrachte die Menge der führenden Koeffizienten von I:

$$J = \{\mathrm{lc}(p) : \ p \in I\}.$$

Es ist leicht nachzuprüfen, daß $J \sqsubseteq R$ ein Ideal ist: Nach Voraussetzung ist J endlich erzeugt, also

$$J = (\!(r_1, \ldots, r_n)\!).$$

Es existieren dann also n Polynome $p_1, \ldots, p_n \in I$ mit $\mathrm{lc}(p_i) = r_i$, also

$$p_i = r_i \cdot x^{k_i} + \cdots$$

Sei $k = \max\{k_1, \ldots, k_n\}$. Sei $q \in I$ ein Polynom mit $\deg q = m > k$, also

$$q = q_m \cdot x^m + \cdots,$$

dann können wir $q_m = \lambda_1 r_1 + \cdots + \lambda_n r_n$ schreiben und den Grad von q reduzieren: Denn sei

$$q' := \lambda_1 p_1 x^{m-r_1} + \cdots + \lambda_n p_n x^{m-r_n} \in (\!(p_1, \ldots, p_n)\!),$$

dann ist

$$q = (q - q') + q',$$

und durch Iteration sehen wir:

$$q = g + h$$

mit $\deg g \leq k$ und $h \in (\!(p_1, \ldots, p_n)\!)$. Sei I' die Menge aller Polynome vom GRD $\leq k$ (I' ist ein *Modul* über R). Dann ist aber Submodul $I \cap I'$ endlich erzeugt (als *Modul* über R!): $I \cap I' = \langle q_1, \ldots, q_l \rangle$, und $I = (\!(p_1, \ldots, p_n; q_1, \ldots, q_l)\!)$, also ist I endlich erzeugt. □

A.3.3. Körper.

DEFINITION A.3.58 (Schiefkörper, Körper). *Ein unitärer Ring $(R, \oplus, \odot)$ mit der zusätzlichen Eigenschaft, daß $(R \setminus \{\mathbf{0}\}, \odot)$ eine* Gruppe *ist, heißt ein* Schiefkörper *oder* Divisionsring. *Wenn diese* multiplikative Gruppe *zusätzlich* abelsch *(*kommutativ*) ist (also wenn R ein* kommutativer *Ring mit Eins ist), dann heißt R ein* Körper. *Für einen Körper verwenden wir meist die Symbole $\mathbb{K}$ oder $\mathbb{F}$ (Körper heißt auf Englisch* Field*), manchmal auch $\mathbb{L}$, und die (multiplikative) Einheitengruppe eines Körpers $\mathbb{K}$ bezeichnen wir mit $\mathbb{K}^\star = (\mathbb{K} \setminus \{\mathbf{0}\}, \odot)$*

BEISPIEL A.3.59. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p \simeq \mathbb{Z}_p$

LEMMA A.3.60. *Sei $p \in \mathbb{P}$, dann ist der Restklassenring $\mathbb{Z}_p$ ein Körper, den wir mit $\mathbb{F}_p$ bezeichnen*[2]*.*

BEWEIS. Der Ring $\mathbb{Z}_p$ ist ein Körper, wenn für jedes Element $n \neq 0$ ein multiplikatives Inverses existiert. Sei also $0 < n < p$, dann ist der $\mathrm{ggT}(n, p) = 1$ darstellbar als ganzzahlige Linearkombination[3]

$$1 = \lambda \cdot n + \mu \cdot p$$

für gewisse $\lambda, \mu \in \mathbb{Z}$. Das heißt aber $\lambda \cdot n \equiv 1 \pmod{p}$, also $\lambda = n^{-1}$ in $\mathbb{Z}_p$. □

DEFINITION A.3.61 (Charakteristik). *Sei R ein kommutativer Ring mit $\mathbf{1}$. Die Abbildung $h\colon\ R \to \mathbb{K}$, die durch*

$$n \mapsto n \cdot 1 := \begin{cases} \underbrace{1 + 1 + \cdots + 1}_{n\text{–mal}} & \text{für } n > 0 \\ 0 & \text{für } n = 0 \\ \underbrace{-1 - 1 - \cdots - 1}_{(-n)\text{–mal}} & \text{für } n < 0 \end{cases}$$

gegeben ist, ist ein Ringhomomorphismus*, wie man ganz leicht sieht: Jeder kommutative Ring mit $\mathbf{1}$ enthält also ein homomorphes Bild von $\mathbb{Z}$:* $\mathrm{img}\,(h) \subseteq R$.
Der Kern $\ker(h)$ *ist daher ein ein Ideal in $\mathbb{Z}$, und dafür gibt es zwei Möglichkeiten: Entweder gilt* $\ker(h) = \{0\}$*, dann sagt man "R hat die* Charakteristik 0*" und schreibt* $\mathrm{char}\, R = 0$*; oder* $\ker(h) = n \cdot \mathbb{Z}$ *für ein $n \in \mathbb{N}$, dann sagt man "R hat die* Charakteristik *n" und schreibt* $\mathrm{char}\, R = n$.

Es ist klar, daß die Charakteristik eines Ringes R *eindeutig* ist.

PROPOSITION A.3.62 (Primkörper). *Sei $\mathbb{K}$ ein Körper. Dann gibt es für* $\mathrm{char}\,\mathbb{K}$ *zwei Möglichkeiten: Entweder ist* $\mathrm{char}\,\mathbb{K} = p \in \mathbb{P}$ *und $\mathbb{K}$ enthält eine Kopie des Körpers $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, oder es ist* $\mathrm{char}\,\mathbb{K} = p \in \mathbb{P}$ *und der Homomorphismus h aus Definition A.3.61 läßt sich zu einem injektiven Homomorphismus $\mathbb{Q} \to \mathbb{K}$ fortsetzen, d.h., $\mathbb{K}$ enthält eine Kopie des Körpers $\mathbb{Q}$.*

[2] Die englische Bezeichnung für Körper ist "Field".

[3] Euklidischer Algorithmus.

BEWEIS. Wenn $\operatorname{char}\mathbb{K} = n \neq 0$ gilt, dann ist $h(n) = n \cdot \mathbf{1} = \mathbf{0}$ in $\mathbb{K}$ und n ist die *kleinste* natürliche Zahl mit dieser Eigenschaft. Angenommen, n wäre nicht prim, also $n = k \cdot m$: Dann folgte aber

$$\mathbf{0} = n \cdot \mathbf{1} = (k \cdot \mathbf{1}) \cdot (m \cdot \mathbf{1}) \text{ mit } (k \cdot \mathbf{1}) \neq \mathbf{0} \text{ und } (m \cdot \mathbf{1}) \neq \mathbf{0},$$

ein Widerspruch, da $\mathbb{K}$ keine Nullteiler hat.

Wenn $\operatorname{char}\mathbb{K} = 0$ gilt, dann ist der Homomorphismus h aus Definition A.3.61 definitionsgemäß *injektiv* und $\mathbf{0} \notin \operatorname{img} h$, also ist für jedes $n \in \mathbb{Z}$ das Bild $h(n)$ invertierbar in $\mathbb{K}$. Die Abbildung $\mathbb{Q} \to \mathbb{K}$

$$\frac{m}{n} \mapsto h(m) \cdot (h(n))^{-1} = (m \cdot 1)(n \cdot 1)^{-1}$$

ist ein injektiver Homomorphismus (wie man leicht sieht). □

DEFINITION A.3.63. *Die Körper $\mathbb{F}_p$, $p \in \mathbb{P}$ und $\mathbb{Q}$ heißen* Primkörper*: Nach Proposition A.3.62 enthält jeder Körper eine Kopie von genau einem Primkörper.*

LEMMA A.3.64. *Sei R ein kommutativer unitärer Ring der Charakteristik $p \in \mathbb{P}$, sei $n \in \mathbb{N}$ und seien $a, b \in R$. Dann gilt:*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

BEWEIS. Induktion nach n: Für $n = 1$ erhalten wir aus dem binomischen Lehrsatz, der ja für beliebige kommutative unitäre Ringe gültig ist,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Für den Binomialkoeffizienten gilt

$$\binom{p}{k} \cdot k! = p \cdot (p-1) \cdots (p-k+1),$$

und für $0 < k \leq p$ teilt p offensichtlich die rechte Seite. p teilt daher auch die linke Seite, und weil p eine Primzahl ist, muß $p \mid \binom{p}{k}$ oder $p \mid k \cdot (k-1) \cdots 2 \cdot 1$ gelten. Für $0 < k < p$ gilt also $p \mid \binom{p}{k}$, d.h.:

$$\binom{p}{k} \equiv 0 \pmod{p}$$

und der Induktionsanfang ist gezeigt. Für den Induktionsschritt $n \to n+1$ erhalten wir

$$(a+b)^{p^{n+1}} = \left((a+b)^{p^n}\right)^p = \left(a^{p^n} + b^{p^n}\right)^p = \left(a^{p^{n+1}} + b^{p^{n+1}}\right)$$

durch zweimalige Anwendung der Induktionsvoraussetzung. □

KOROLLAR A.3.65. *Über dem Körper $\mathbb{F}_2$ gilt für ein ein beliebiges Polynom $q(x)$*

$$q(x)^2 = q\left(x^2\right).$$

BEWEIS. Sei $q(x) = q_0 + q_1 \cdot x + \cdots + q_n \cdot x^n$, dann ist

$$q(x)^2 = \sum_{k=0}^{2n} x^k \left(\sum_{j=0}^{k} q_j \cdot q_{k-j} \right),$$

und die innere Summe ist

$$\left([k \equiv 0 \pmod 2] \cdot q_{k/2}^2 \right) + 2 \cdot \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} q_j \cdot q_{k-j}.$$

(Hier haben wir *Iversons Notation* verwendet: $[A] = 1$, wenn Aussage A wahr ist; 0 sonst.) Über $\mathbb{F}_2$ gilt also einfach

$$q(x)^2 = \sum_{k=0}^{n} q_k^2 \cdot x^{2k} = \sum_{k=0}^{n} q_k \cdot x^{2k} = q\left(x^2\right),$$

wie behauptet. □

PROPOSITION A.3.66. *Sei R ein kommutativer Ring mit Eins, sei $I \sqsubseteq R$ ein Ideal. Dann gilt:*

$$R/I \text{ ist ein Körper} \iff I \text{ ist ein maximales Ideal}.$$

BEWEIS. ($\Longrightarrow$) Wenn R/I ein Körper ist, dann ist $I \neq R$ und es gibt für alle Äquivalenzklassen $x + I \neq 0 + I$ eine Äquivalenzklasse $y + I$ mit

$$(x + I)(y + I) = 1 + I.$$

Das heißt: Für alle $x \in R \setminus I$ gibt es ein $y \in R$ sodaß

$$x \cdot y - 1 \in I,$$

und $y \notin I$, denn sonst wäre $-1 \in I \implies 1 \in I \implies I = R$.

Sei also $J \sqsubseteq R$ ein Ideal mit $I \subseteq J$, aber $I \neq J$. Dann gibt es also ein $x \in J \setminus I$ und ein $y \in R \setminus I$ mit $x \cdot y - 1 \in I \subset J$. Es ist aber $x \cdot y \in J$, weil $x \in J$, also ist $-1 \in J \implies 1 \in J \implies J = R$.

($\Longleftarrow$) Wenn $I \sqsubseteq R$ ein maximales Ideal ist, dann ist für jedes $x \in R \setminus I$ die Menge $J_x := I + (\!(x)\!)$ ein Ideal von R mit $I \subseteq J_x$, aber $I \neq J_x$: Daher ist $J_x = R$ und somit $1 \in J_x$, und das heißt

$$\mathbf{1} = i + r \cdot x$$

für geeignete Elemente $i \in I$ und $r \in R$. Also ist $(r + I)(x + I) = \mathbf{1} + I$ in R/I, d.h.: $x + I$ ist invertierbar. □

KOROLLAR A.3.67. *Sei R ein kommutativer Ring mit Eins. Dann ist* jedes *maximale Ideal in R prim.*

BEWEIS. Wenn $I \sqsubseteq R$ maximal ist, dann ist R/I ein Körper, also nullteilerfrei: Daher ist I prim. □

A.3.3.1. *Erweiterungskörper und Zerfällungskörper.*

DEFINITION A.3.68 (Körpererweiterung, Zerfällungskörper). *Sei* $\mathbb{L}$ *ein Körper, der einen Körper* $\mathbb{K}$ *als (echte) Teilmenge enthält: Dann heißt* $\mathbb{L}$ *ein (echter)* Oberkörper *oder ein* Erweiterungskörper *von* $\mathbb{K}$*, und* $\mathbb{K}$ *heißt umgekehrt ein (echter)* Unterkörper *von* $\mathbb{L}$*.*

Der Oberkörper L ist ein Vektorraum *über* $\mathbb{K}$ *(Vektoraddition ist Addition in* $\mathbb{L}$*, Skalarmultiplikation ist Multiplikation von Elementen aus* $\mathbb{L}$ *mit Skalaren aus* $\mathbb{K}$*). Die Dimension dieses Vektorraums wird* Grad der Erweiterung *genannt und mit* $[\mathbb{L}:\mathbb{K}]$ *bezeichnet.*

Sei $p \in \mathbb{K}[x]$ *ein nicht–konstantes Polynom. Eine Körpererweiterung* $\mathbb{L}$ *von* $\mathbb{K}$ *heißt* Zerfällungskörper *von p, wenn alle Nullstellen von p in* $\mathbb{L}$ *liegen (also: p zerfällt über* $\mathbb{L}$ *in Linearfaktoren) und* $\mathbb{L}$ *keinen Unterkörper enthält, der dieselbe Eigenschaft hat (d.h.,* $\mathbb{L}$ *ist der* kleinste *Körper, über dem p zerfällt). Man sagt auch:* $\mathbb{L}$ *entsteht durch* Adjunktion *aller* Wurzeln *(i.e., Nullstellen) von p an* $\mathbb{K}$*.*

Allgemeiner ist der Zerfällungskörper einer Menge $X \subseteq \mathbb{K}[x]$ *von Polynomen ein minimaler Oberkörper von* $\mathbb{K}$*, in dem* alle *Polynome aus X zerfallen. Ist speziell* $X = \mathbb{K}[x]$*, dann nennt man den entsprechenden Zerfällungskörper den* algebraischen Abschluß *von* $\mathbb{K}$ *und bezeichnet ihn mit* $\overline{\mathbb{K}}$*.*

PROPOSITION A.3.69. *Jedes nicht konstante Polynom* $p \in \mathbb{K}[x]$ *besitzt einen (bis auf Isomorphie) eindeutigen Zerfällungskörper.*

Jeder Körper $\mathbb{K}$ *besitzt einen (bis auf Isomorphie) eindeutigen algebraischen Abschluß* $\overline{\mathbb{K}}$*(dafür wird allerdings das* Zornsche Lemma *benötigt).*

Ohne Beweis. □

A.3.4. Polynome. In diesem Abschnitt über Polynome sei *R immer* ein *kommutativer* Ring mit *Eins*.

DEFINITION A.3.70. *Sei R ein kommutativer Ring mit Eins, sei* $n \in \mathbb{N}_0$ *und* $(c_0, \ldots, c_n) \in R^{n+1}$ *mit* $c_n \neq \mathbf{0}$*. Dann bezeichnen wir die formale Summe*

$$\sum_{k=0}^{n} c_k \cdot x^k = c_0 + c_1 \cdot x + c_2 \cdot x^2 + \cdots + c_{n-1} \cdot x^{n-1}$$

als ein Polynom *in der Variablen x und bezeichnen sie mit* $p = p(x)$ (typischerweise*, natürlich können wir Polynome auch mit andren Buchstaben bezeichnen; und natürlich können wir die Variable auch anders bezeichne, z.B. mit z statt mit x). Die Zahl n wird dabei der* Grad *des Polynoms (englisch:* degree*) genannt und mit* $\deg p$ *abgekürzt. Der Summand* $c_k \cdot x^k$ *in p heißt der k–te* Term *oder das k–te* Glied *im Polynom p, die Potenz* x^k *wird* Monom *(vom Grad k) genannt, und das Ringelement* c_k *heißt der k–te* Koeffizient *von p oder "der Koeffizient von* x^k *in p", was wir auch wie folgt schreiben:*

$$\left[\!\left[x^k\right]\!\right] p(x) := \begin{cases} c_k & \text{falls } 0 \leq k \leq \deg p, \\ \mathbf{0} & \text{sonst.} \end{cases}$$

Wenn in einem Polynom p der k–te Koeffizient $c_k = 0$ ist, dann sagt man auch: Der k–te Term in p verschwindet*: Normalerweise interessieren nur die* nichtverschwindenden *Terme von p, dementsprechend ist mit "Term" meist "nichtverschwindender Term" gemeint.*

Ebenso betrachten wir das Nullpolynom *$p(x) \equiv \mathbf{0}$ als ein Polynom: Dieses hat definitionsgemäß Grad $-\infty$, und es ist $[\![x^k]\!]\ p = 0$ für alle $k \in \mathbb{N}$. Offensichtlich liefert* deg *eine euklidische Norm auf $R[x]$ (siehe Definition A.3.54).*

Für einzelne Summanden des Polynoms p sind spezielle Bezeichnungen üblich: c_0 heißt absolutes Glied*, $c_1 \cdot x$ heißt* lineares Glied *und $c_2 \cdot x^2$ heißt* quadratisches Glied*. Ein Polynom, das nur aus einem absoluten Glied besteht, heißt* konstantes Polynom *$p(x) \equiv c$.*

Vom abstrakten Standpunkt aus können wir ein Polynom auch als die unendliche Folge *seiner Koeffizienten ansehen: $p \equiv \left([\![x^k]\!]\ p\right)_{k=0}^{\infty}$. Diese Folge hat dann natürlich die Eigenschaft, daß alle Glieder mit Index $k > \deg p$ gleich $\mathbf{0}$ sind: D.h., wir können ein Polynom p auch als* formal unendliche *Summe schreiben*

$$p(x) = \sum_{k=0}^{\infty} c_k \cdot x^k,$$

mit dem Verständnis, daß $c_k = \mathbf{0}$ für alle $k > \deg p$.

Wenn $(x) = \sum_{k=0}^{\infty} c_k$ ein Polynom vom Grad $\deg p = n$ ist, dann heißt $[\![x^n]\!]\ p$ (das ist also der "größte" Koeffizient $c_n \neq 0$; in dem Sinne, daß für alle $k > n$ $c_k = \mathbf{0}$ gilt) führender Koeffizient *oder* Leitkoeffizient *von p. Wenn der führende Koeffizient von p gleich $\mathbf{1}$ ist, nennt man p* normiert *oder* monisch*.*

Die Menge aller Polynome mit Koeffizienten aus R hat die Struktur eines kommutativen Rings mit Eins, wobei Addition und Multiplikation für zwei Polynome $p(x) = \sum_{k=0}^{n} c_k \cdot x^k$ und $q(x) \sum_{k=0}^{m} b_k \cdot x^k$ wie folgt gegeben sind:

$$(p+q)(x) := \sum_{k=0}^{\max(m,n)} (c_k + b_k) \cdot x^k,$$

$$(p \cdot q)(x) := \sum_{k=0}^{m+n} \left(\sum_{j=0}^{k} c_j \cdot b_{k-j} \right) \cdot x^k.$$

(Rein formal könnten wir hier als obere Summationsgrenzen auch ∞ setzen.) Daß mit diesen Rechenoperationen tatsächlich ein Ring gegeben ist, dessen Nullelement das Nullpolynom ist und dessen Einselement das Polynom $p(x) \equiv \mathbf{1}$ ist, rechnet man leicht nach: Wir bezeichnen diesen Ring mit $R[x]$. Offensichtlich können wir konstante Polynome mit Elementen aus $c \in R$ identifizieren[4]*, in diesem Sinne ist also $R \sqsubseteq R[x]$.*

Die Variable x ist dabei einfach ein Symbol, von dem wir annehmen, daß wir beliebige Potenzen $x^0 = \mathbf{1}, x^1 = x, x^2, \ldots$ bilden können. Aber wir können x auch durch ein konkretes r ersetzen, für das die Rechenoperationen (Multiplikation mit den Koeffizienten aus R und Summieren) sinnvoll sind, und erhalten so die Auswertung *$p(r)$ von*

[4] Für Freunde des Abstrakten: Diese Identifikation ist als Abbildung $R \to R[x]$ ($c \in R \mapsto c \in R[x]$) ein injektiver Ringhomomorphismus.

p in r. Insbesondere können wir ein $r \in R$ wählen: Die Abbildung $\mathrm{ev}_r : R[x] \to R$, *die durch*

$$\mathrm{ev}_r(p) := p(r)$$

gegeben ist, heißt Evaluationsabbildung *und ist ein Ringhomomorphismus (wie man leicht nachrechnet). Z.B. ist* $\mathrm{ev}_{\mathbf{0}}(p) = p(\mathbf{0}) = [\![x^0]\!]\, p(x)$.

BEMERKUNG A.3.71. *Zwei Polynome p, q in $R[x]$ sind* definitionsgemäß *genau dann gleich, wenn ihre Koeffizientenfolgen übereinstimmen:*

$$p = q \iff \left([\![x^k]\!]\, p\right)_{k\geq 0} = \left([\![x^k]\!]\, q\right)_{k\geq 0}.$$

Es gilt natürlich

$$p = q \implies \mathrm{ev}_r(p) = \mathrm{ev}_r(q) \text{ für alle } r \in R,$$

aber die Umkehrung ist im allgemeinen nicht richtig*: Zum Beispiel ist das Polynom $p(x) = x^2 - x$ über $R = \mathbb{F}_2$ nicht das Nullpolynom, aber $\mathrm{ev}_r(p) = 0$ für alle $r \in \mathbb{F}_2$.*

PROPOSITION A.3.72. *Sei R ein kommutativer Ring mit Eins, und seien f, g zwei Polynome in $R[x]$, beide nicht das Nullpolynom. Wenn der führende Koeffizient von f kein Nullteiler ist, dann gilt*

$$\deg(f \cdot g) = \deg f + \deg g.$$

BEWEIS. Die Behauptung folgt sofort aus der Definition der Multiplikation in $R[x]$. □

PROPOSITION A.3.73. *Sei R ein Integritätsbereich. Dann gilt für die Einheitengruppen:*

$$R[x]^\star = R^\star.$$

BEWEIS. Sei $f \in R[x]^\star$, dann gibt es $g = f^{-1} \in R[x]$ mit $f \cdot g \equiv \mathbf{1}$. Nach Proposition A.3.72 gilt also $\deg f + \deg g = \deg \mathbf{1} = 0$, also $\deg f = \deg g = 0$, d.h., $f \in R^\star$. Daher ist $R[x]^\star \subseteq R^\star$, und die umgekehrte Mengeninklusion ist sowieso klar. □

DEFINITION A.3.74. *Sei $p \in R[x]$. Ein Element $\alpha \in R$ heißt* Nullstelle *von p, wenn $\mathrm{ev}_\alpha(p) = p(\alpha) = \mathbf{0}$. Die Menge aller Nullstellen von p bezeichnen wir mit $V(p)$.*

LEMMA A.3.75 (Division mit Rest). *Seien $p, q \in R[x]$, und sei der führende Koeffizient von q eine Einheit in R. Dann gibt es Polynome $d, r \in R[x]$, mit denen sich p darstellen läßt als*

$$p(x) = q(x) \cdot d(x) + r(x), \text{ wobei } \deg r < \deg q.$$

Wenn $R = \mathbb{K}$ ein Körper ist, dann ist also $\mathbb{K}[x]$ ein euklidischer Ring.

BEWEIS. Sei m der Grad und q_m der führende Koeffizient von q, also $q_m = [\![x^m]\!]\, q(x)$: Nach Voraussetzung existiert $q_m^{-1} \in R$.

Die behaupteten Polynome d, r kann man algorithmisch wie folgt erhalten (*Divisionsalgorithmus*):

```
/* Starte mit d = Nullpolynom, r = p */
d ← 0
r ← p
/* In jedem Schritt gilt: p = q·d + r */
while (deg q ≤ deg r) do
  n ← deg r
  c ← q_m^{-1} · [[x^n]] r(x)
  d ← d + c · x^{n-m}
  r ← r − c · x^{n-m} · q(x) /* deg r wird vermindert! */
end while
/* Ende des Algorithmus: Rückgabe der Werte d,r */
return d, r
```

Da der Grad von r in jedem Durchlauf der Schleife vermindert wird, bricht der Algorithmus irgendwann (spätestens nach $\deg p - \deg q + 1$ Schritten) ab: Dann ist $\deg r = \deg p < \deg q$, und laut Konstruktion ist $p - d \cdot q = r$. □

LEMMA A.3.76. *Seien $d, n \in \mathbb{N}_0$. Dann gilt*

$$x^d - 1 \mid x^n - 1 \iff d \mid n.$$

(Die "linke" Teilbarkeitsrelation ist im Ring der Polynome $\mathbb{Z}[x]$ angesiedelt.)

BEWEIS. Falls $d = 0$, dann sind beide Teilbarkeitsrelationen nur für $n = 0$ möglich. Sei also $d \in \mathbb{N}$ und sei $n = k \cdot d + r$ mit $0 \leq r < d$ (Division mit Rest in $\mathbb{Z}$):

$$\frac{x^n - 1}{x^d - 1} = \frac{\left(x^d\right)^k x^r - 1}{x^d - 1} = x^r \frac{\left(x^d\right)^k - 1}{x^d - 1} + \frac{x^r - 1}{x^d - 1} =$$
$$x^r \left(1 + x^d + \left(x^d\right)^2 + \cdots + \left(x^d\right)^{k-1}\right) + \frac{x^r - 1}{x^d - 1}.$$

Wegen $r < d$ ergibt sich unmittelbar die Behauptung. □

KOROLLAR A.3.77. *Sei $p \in R[x]$. Dann gilt:*

$$\alpha \in V(p) \iff (x - \alpha) \mid p(x).$$

BEWEIS. ($\Longrightarrow$) Im Fall $p \equiv \mathbf{0}$ ist *jedes* $\alpha \in R$ Nullstelle von p, und *jedes* Polynom teilt das Nullpolynom.
Sei also $p \neq \mathbf{0}$ und α eine Nullstelle von p. Dann ist $\deg p > 0$ (denn $p \equiv c \in R$ hat natürlich *keine* Nullstelle, wenn $c \neq \mathbf{0} \in R$) und wir können p durch das Polynom $(x - \alpha)$ (vom Grad 1, mit führendem Koeffizienten $\mathbf{1} \in R^\star$) mit Rest dividieren:

$$p(x) = (x - \alpha) \cdot d(x) + r(x),$$

wobei $\deg r < \deg(x - \alpha) = 1$: Also $r = c$ für eine Konstante $c \in R$, und durch Auswertung bei α folgt $0 = p(\alpha) = 0 \cdot d(\alpha) + c$, also $c = 0$ und somit $(x - \alpha) \mid p(x)$.
($\Longleftarrow$) Die umgekehrte Richtung ist klar. □

DEFINITION A.3.78 (Vielfachheit einer Nullstelle). *Sei $p \in R[x]$. Die* Vielfachheit einer Nullstelle *α von p ist das größte $n \in \mathbb{N}_0$, für das $(x-\alpha)^n \mid p(x)$ gilt: Wir bezeichnen sie mit $\|\alpha\|_p$. Es ist $\|\alpha\|_p \leq \deg p$ für alle $\alpha \in R$ und $p = (x-\alpha)^{\|\alpha\|_p} \cdot q$ mit $q(\alpha) \neq 0$.*

BEMERKUNG A.3.79. *Achtung: Nicht alle "gewohnten Tatsachen" in bezug auf Polynome sind richtig! Sei $R = \mathbb{Z}/\mathbb{Z}_6$ und $p(x) = x^2 + 3x + 2 \in R[x]$. Dann ist $V(p) = \{1,2,4,5\}$, also $|V(p)| = 4 > 2 = \deg p$, und es ist*

$$p(x) \neq (x-1)(x-2)(x-4)(x-5),$$

sondern

$$p = (x-1)(x-2) = (x-4)(x-5).$$

LEMMA A.3.80. *Sei R ein* Integritätsbereich *(also nullteilerfrei), und seien $p, q \in R[x]$. Dann gilt:*

$$V(p \cdot q) = V(p) \cup V(q).$$

BEWEIS. Die Inklusion $V(p) \cup V(q) \subseteq V(p \cdot q)$ gilt natürlich immer.
Sei $\alpha \in V(p \cdot q)$: Dann ist $p(\alpha) \cdot q(\alpha) = 0$ in R, und weil R nullteilerfrei ist, muß $p(\alpha) = 0$ oder $q(\alpha) = 0$ gelten. Das heißt: $\alpha \in V(p)$ oder $\alpha \in V(q)$, also $\alpha \in V(p) \cup V(q)$. □

SATZ A.3.81. *Sei R ein* Integritätsbereich *und $p \in R[x]$, $p \neq \mathbf{0}$ mit Nullstellenmenge $V(p) = \{\alpha_1, \cdots, \alpha_k\}$. Dann gilt:*

$$p(x) = q(x)(x-\alpha_1)^{\|\alpha_1\|_p} \cdot (x-\alpha_2)^{\|\alpha_2\|_p} \cdots (x-\alpha_k)^{\|\alpha_k\|_p}, \tag{A.11}$$

wobei $q \in R[x]$ mit $V(q) = \emptyset$ und $\sum_{i=1}^{k} \|\alpha_i\|_p \leq \deg p$.

BEWEIS. Falls $V(p) = \emptyset$, ist die Aussage richtig für $q = p$ und $\sum_{\alpha \in \emptyset} \|\alpha\|_p = 0 \leq \deg p$.
Andernfalls führen wir Induktion nach $n := \deg p$ durch.
Für $n = 1$ sei $p(x) = a \cdot x + b$ mit $a \neq 0$. Für eine Nullstelle α von p gilt dann $-a \cdot \alpha = b$. Setze $q \equiv a$, dann gilt $p(x) = q \cdot (x-\alpha)$, und die Behauptung ist gezeigt.
Sei also $\deg p = n > 1$ und $\alpha \in V(p)$. Dann gilt

$$p = (x-\alpha)^{\|\alpha\|_p} \cdot q$$

mit $q(\alpha) \neq 0$, also $\alpha \notin V(q)$. Wegen $\|\alpha\|_p > 0$ ist $\deg q < n$, und nach Lemma A.3.80 ist

$$V(p) = \{\alpha\} \dot{\cup} V(q) = \{\alpha; \beta_1, \ldots, \beta_s\},$$

und nach Induktionsvoraussetzung ist

$$q = r \cdot (x-\beta_1)^{\|\beta_1\|_q} \cdots (x-\beta_s)^{\|\beta_s\|_q}$$

mit $V(r) = \emptyset$ und $\deg p = \|\alpha\|_p + \deg q$: Daraus folgt die Behauptung. □

Als Anwendung erhalten wir ein bekanntes Resultat der Zahlentheorie:

KOROLLAR A.3.82 (Satz von Wilson). *Sei $p \in \mathbb{P}$: Dann gilt*

$$(p-1)! \equiv -1 \pmod{p}. \tag{A.12}$$

BEWEIS. Denn das Polynom $p(x) = x^p - x \in \mathbb{F}_p[x]$ hat Nullstellenmenge $V(p) = \mathbb{F}_p$, also gilt

$$p(x) = q \cdot x(x-1)\cdots(x-(p-1))$$

nach Satz A.3.81, und ersichtlich ist $q \equiv 1$. Dann gilt aber auch

$$x^{p-1} - 1 = (x-1)\cdots(x-(p-1)),$$

und wenn wir hier bei $x = p$ (also bei $x = \mathbf{0} \in \mathbb{F}_p$) auswerten, folgt die Behauptung. □

DEFINITION A.3.83. *Sei $p \in R[x]$ ein Polynom vom Grad n, das in n verschiedene Linearfaktoren zerfällt, i.e.,*

$$p(x) = \prod_{\alpha \in V(p)} (x-\alpha) = (x-\alpha_1)\cdot(x-\alpha_2)\cdot(x-\alpha_n).$$

(D.h., $V(p) = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, und die α_i sind paarweise verschieden.)
Dann gilt (natürlich)

$$\left[\!\left[x^k\right]\!\right] p = (-1)^k \cdot \sum_{\substack{I \subseteq [n] \\ |I|=k}} \prod_{i \in I} \alpha_i.$$

wie sich das in einer Menge gehört;-)

Die hier auftretenden Summen von Produkten werden als elementarsymmetrische Funktionen *bezeichnet:*

$$\mathbf{e}_k(\alpha_1, \ldots, \alpha_n) := \sum_{\substack{I \subseteq [n] \\ |I|=k}} \prod_{i \in I} \alpha_i.$$

Die Funktionen $\mathbf{e}_k$ sind symmetrisch *in dem Sinn, daß sie* invariant *sind unter Permutationen der Variablen α_i, d.h., sei $\sigma \in \mathfrak{S}_n$ eine Permutation, dann gilt*

$$\mathbf{e}_k(\alpha_1, \ldots, \alpha_n) = \mathbf{e}_k\left(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}\right).$$

PROPOSITION A.3.84. *Sei R ein Ring und $f = a_0 + a_1 \cdot x + \cdots + a_{n-1}x^{n-1} + x^n \in R[x]$ ein monisches Polynom vom Grad $n > 0$. Dann ist $R \cap (\!(f)\!) = (\!(0)\!)$. Die Elemente $\overline{g} := g + (\!(f)\!)$ im Quotientenring $R[x]/(\!(f)\!)$ haben eine* eindeutige *Darstellung*

$$\overline{g} = b_0 + b_1\overline{x} + \cdots + b_{n-1}\overline{x}^{n-1} \text{ für } b_0, \ldots, b_n \in R.$$

In $R[x]/(\!(f)\!)$ gilt:

$$\overline{x}^n = -a_{n-1}\overline{x}^{n-1} - \cdots - a_1\overline{x} - a_0.$$

BEWEIS. Sei $r \in R \cap (\!(f)\!)$, dann ist also $r = q \cdot f$ für ein $q \in R[x]$: Wenn $q \neq 0$, dann wäre $0 = \deg r = \deg q + \deg f > n$, ein Widerspruch.
Sei $\overline{g} \in R[x]/(\!(f)\!)$: Sei $g = q \cdot f + r$ (Division mit Rest) mit $r = 0$ oder $\deg r < n = \deg f$, also ist $\overline{g} = \overline{r}$ und die behauptete Darstellung von $\overline{g}$ ist gefunden. Sie ist eindeutig, denn gäbe es eine weitere Darstellung $\overline{g} = \overline{r'}$ mit $\deg r' < \deg f = n$, dann gälte ja $r - r' = q \cdot f$, und bei Betrachtung der Grade der linken und rechten Seite folgt $q = 0$, also $r = r'$.
Wegen

$$\overline{f} = \overline{a_0 + a_1 \cdot x + \cdots + a_{n-1}x^{n-1} + x^n} = a_0 + a_1 \cdot \overline{x} + \cdots + a_{n-1}\overline{x}^{n-1} + \overline{x}^n$$

folgt sofort die letzte Behauptung. □

A.4. Lineare Algebra

DEFINITION A.4.1 (Vektorraum). *Sei* $\mathbb{K}$ *ein Körper und* V *eine abelsche Gruppe, deren Nullelement wir mit* $\mathbf{0}_V$ *bezeichnen. Wenn es eine Abbildung* $\mathbb{K} \times V \to V$ *gibt, die wir* $(\alpha, v) \mapsto \alpha \cdot v$ *notieren, für die*

- $\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$ *für alle* $\alpha, \beta \in \mathbb{K}$ *und alle* $v \in V$,
- $\mathbf{1} \cdot v = v$ *für das Einselement* $\mathbf{1} \in \mathbb{K}$ *und alle* $v \in V$,
- *für alle* $\alpha \in \mathbb{K}$, $u, v \in V$ *gilt* $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$,
- *für alle* $\alpha, \beta \in \mathbb{K}$, $v \in V$ *gilt* $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$,

gilt, dann heißt V *ein* Vektorraum *über* $\mathbb{K}$. *Es gilt dann auch*

- $\mathbf{0} \cdot v = \mathbf{0}_V$ *für das Nullelement* $\mathbf{0} \in \mathbb{K}$ *und alle* $v \in V$
- $(-\alpha) \cdot v = -(\alpha \cdot v)$ *für alle* $\alpha \in \mathbb{K}$ *und alle* $v \in V$,

wie man leicht sieht.
Die Elemente von V *heißen* Vektoren, *die von* $\mathbb{K}$ Skalare, *und die Abbildung* $\mathbb{K} \times V \to V$ *wird als* Skalarmultiplikation *bezeichnet. Das Nullelement von* V *wird als* Nullvektor *bezeichnet.*

In diesem Skriptum wird die n–dimensionale Einheitsmatrix als E_n bezeichnet:

$$E_n := \left([i = j]\right)_{(i,j)=(1,1)}^{(n,n)} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

PROPOSITION A.4.2 (Polarisierungsformel). *Sei* V *ein Vektorraum über einem Körper* $\mathbb{K}$ *mit* $\operatorname{char}(\mathbb{K}) \neq 2$ *und sei* $\beta : V \times V \to K$ *eine symmetrische Bilinearform mit zugehöriger quadratischer Form* $q(v) = \beta(v, v)$.
Dann gilt

$$\beta(v, w) = \frac{1}{2}\left(q(v + w) - q(v) - q(w)\right) \tag{A.13}$$

$$= \frac{1}{4}\left(q(v + w) - q(v - w)\right). \tag{A.14}$$

(D.h., β *kann aus* q *rekonstruiert werden.)*

BEWEIS. Aus Bilinearität und Symmetrie von β folgt

$$\beta(v + w, v + w) = \beta(v, v) + 2\beta(v, w) + \beta(w, w),$$

also

$$2\beta(v, w) = q(v + w) - q(v) - q(w). \tag{A.15}$$

Da $0 \neq 2$ in $\mathbb{K}$, folgt die erste Polarisierungsformel (A.13).
Ersetzt man in (A.15) w durch $-w$, so ergibt sich

$$-2\beta(v, w) = q(v - w) - q(v) - q(w), \tag{A.16}$$

und Subtraktion der Gleichungen (A.15) und (A.16) ergibt die zweite Polarisierungsformel (A.14). (Denn natürlich: $\operatorname{char}(\mathbb{K}) \neq 2 \implies 2 \times 2 = 4 \neq 0$ in $\mathbb{K}$.) □

SATZ A.4.3 (Rangsatz). *Seien V und W Vektorräume, und sei $f\colon\ V \to W$ eine lineare Abbildung. Dann gilt:*

$$\dim V = \dim \ker f + \dim \operatorname{img} f.$$

SATZ A.4.4 (Cayley–Hamilton). *Sei V ein n–dimensionaler Vektorraum über einem Körper $\mathbb{K}$, sei $A : V \to V$ ein linearer Operator und $P_A \in \mathbb{K}[t]$*

$$P_A := \det(A - t \cdot E_n)$$

sein charakteristisches Polynom. Dann gilt

$$P_A(A) = 0. \tag{A.17}$$

Literaturverzeichnis

[1] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3(1):68–79, 1960.

[2] D. Burde. Algebra im Überblick. Skriptum zur Vorlesung, 2010.

[3] E. Fedorov. Simmetrija na ploskosti (Symmetrie in der Ebene). *Zapiski Imperatorskogo Sant-Petersburgskogo Mineralogicheskogo Obshchestva*, 28(245–291), 1891.

[4] M. Fulmek and C. Krattenthaler. Kombinatorik. Vorlesungsskriptum.

[5] M. Fulmek and C. Krattenthaler. Diskrete Mathematik. Vorlesungsskriptum, 2013.

[6] B. Grünbaum. What symmetry groups are present in the Alhambra? *Notices of the AMS*, 53(6):670–673, June/July 2006.

[7] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, September 1959.

[8] T. W. Hungerford. *Algebra*. Springer Verlag, 1974.

[9] K. Lamotke. Die Symmetriegruppen der ebenen Ornamente. *Math. Semesterber.*, 52:153–174, 2005.

[10] G. Mackiw. Finite groups of 2×2 integer matrices. *Math. Magazine*, 69(5):356–361, 1996.

[11] F.J. MacWilliams. *Combinatorial Problems of Elementary Group Theory*. PhD thesis, Harvard University, 1961.

[12] F.J. MacWilliams and N. J. A. Sloane. *The theory of error correcting codes*. North-Holland mathematical library. North-Holland Pub. Co. New York, Amsterdam, New York, 1977.

[13] O. Perron. Bemerkungen über die Verteilung der quadratischen Reste. *Math. Zeitschrift*, 56(2):122–130, 1952.

[14] R.C. Singleton. Maximum distance q–nary codes. *IEEE Trans. Inf. Theory*, 10(2):116–118, 1964.

[15] L. Summerer. Algebra im Überblick. Vorlesungsmitschrift, 2011.

Index

Verzeichnis von Symbolen und Abkürzungen

$|z|$**:** Absolutbetrag der komplexen Zahl z. 25

$\dot{\bigcup}$**:** disjunkte Vereinigung. 111

$\mathbb{C}$**:** Körper der komplexen Zahlen. 1
$\lceil x \rceil$**:** Nächstgrößere ganze Zahl an x. 68
$\mathrm{cnt}_G\,(x)$**:** Zentralisator. 3
char**:** Charakteristik eines Körpers. 33
char**:** Charakteristik eines Körpers. 135
$\overline{z}$**:** Konjugierte der komplexen Zahl z. 28

D**:** Formale (gliedweise) Ableitung. 33
$\dot{\cup}$**:** disjunkte Vereinigung. 116

e: Elementarsymmetrische Funktion. 29
N: euklidische Norm auf einem Ring R: $\mathbf{N} : R \to \mathbb{N}$. 143
φ**:** Eulersche Phi–Funktion: $\varphi(n)$ ist die Anzahl der primen Restklassen modulo n. 53

$\mathbb{F}$**:** Bezeichnung für einen Körper allgemein (englisch: field). 9
$\mathbb{K}\,(\alpha)$**:** Körpererweiterung eines Körpers $\mathbb{K}$ mit einem Element α. 69
$\mathrm{fxp}_G\,(S)$**:** Menge der Punkte in S, die von der Wirkung von G fixiert werden. 3
$\lfloor x \rfloor$**:** Nächstkleinere ganze Zahl an x. 61
frob_p**:** Frobenius–Abbildung $\mathbb{K} \to \mathbb{K} : \; z \mapsto z^p$, wobei $\mathbb{K}$ ein Körper der Charakteristik $p \in \mathbb{P}$ ist. 28

$(G : U)$**:** Index der Untergruppe U in G. 1

$\mathbb{H}$**:** Schiefkörper der Quaternionen. 32

img**:** Bildbereich einer Funktion f: Menge der Funktionswerte. 66
E**:** Einheitsmatrix. 25
$[A]$**:** Iversons Notation: 1, wenn Aussage A wahr ist; 0 sonst. 47

$\mathbb{K}$**:** Bezeichnung für einen Körper allgemein. 1
$\mathrm{kgV}\,(n_1, \ldots, n_k)$**:** Kleinstes gemeinsames Vielfaches der Zahlen $n_1, \ldots, n_k$. 10

$\mathbb{L}$**:** Bezeichnung für einen Körper allgemein. 103
$\prec_{grlex}$**:** Graduierte lexikographische Monomordnung. 40
$\prec_{grulex}$**:** Graduierte umgekehrt lexikographische Monomordnung. 40

$\prec_{lex}$: Lexikographische Monomordnung. 34
$\prec_{ulex}$: Umgekehrt lexikographische Monomordnung. 40

M: Matrizenalgebra. 14
M: Matrizenalgebra. 26
mdeg: Multigrad. 41

$\mathbb{N}$: Menge der natürlichen Zahlen $\{1, 2, 3, \dots\}$. 2
$\mathbb{N}_0$: Menge der nichtnegativen ganzen Zahlen $\{0, 1, 2, \dots\}$. 9
$\mathbf{w}(x)$: Anzahl der Stellen ungleich Null. 86
$\mathbf{w}(x)$: Anzahl der Stellen ungleich Null. 76
$\subseteq$: Normalteiler: $H \subseteq G$ normale Untergruppe, wenn $ghg^{-1} \in H$ für alle $h \in H, g \in G$. 7
$[n]$: Menge der ersten n natürlichen Zahlen: $\{1, 2, \dots, n\}$. 2
$f \to_F 0$: Polynom $f \in (\!(F)\!)$ ist durch eine "Polynomialkombination" darstellbar, bei der keine Kürzung führender Terme auftritt. 41
$f \to_F 0$: Polynom $f \in (\!(F)\!)$ ist durch eine "Polynomialkombination" darstellbar, bei der keine Kürzung führender Terme auftritt. 51
$V(p)$: Nullstellenmenge (Verschwindungsmenge; daher "V") von p. 34

$G \cdot x$: Orbit (oder Bahn) von Element $x \in X$ unter der Gruppenwirkung von G auf X. 6
ord: Ordnung (einer Gruppe oder eines Elements einer Gruppe). 33
$\mathrm{ord}_G(x)$: Ordnung des Elements x in G. 96

$\mathbb{P}$: Menge der Primzahlen $\{2, 3, 5, 7, 11, \dots\}$. 3
$R[z]$: Ring der Polynome in der Variablen z mit Koeffizienten im Ring R. 33
$\mathbb{C}[[z]]$: Ring der formalen Potenzreihen über $\mathbb{C}$ in der Variablen z. 35

$\mathbb{Q}$: Körper der rationalen Zahlen. 29
$\mathcal{Q}_m$: Menge der quadratischen Reste modulo m. 114

$\mathbb{R}$: Körper der reellen Zahlen. 5
$\mathbb{R}^+$: Menge der nichtnegativen reellen Zahlen. 13

$\mathrm{SL}_n(R)$: Spezielle Lineare Gruppe: $n \times n$–Matrizen mit Eintragungen aus R und Determinante 1. 1
$\mathrm{SL}_n(R)$: Spezielle Lineare Gruppe: $n \times n$–Matrizen mit Eintragungen aus R und Determinante 1. 1
$\overline{AB}$: Strecke, die Punkte A und B verbindet. 23

$|$: Teilbarkeitsrelation: $k|n \iff \exists d \in \mathbb{Z}\ n = k \cdot d$. 4
trace: Spur eines Operators. 13

$\|\alpha\|_q$: Vielfachheit einer Nullstelle α des Polynoms q. 35
$\|\alpha\|_q$: Vielfachheit einer Nullstelle α des Polynoms q. 35

$\mathbb{Z}$: Ring der ganzen Zahlen $\{\dots, -2, -2, -1, 0, 1, 2, \dots\}$. 4