Modul Überblicke über Teilgebiete
der Mathemathik (UEB)

– Vorlesungsskript –

Algebra im Überblick

Dietrich Burde

2011

Inhaltsverzeichnis

1 Einleitung

Die Vorlesung *Algebra im Überblick* ist Bestandteil des Bachelor-Studiengangs in Mathematik der Universität Wien und gehört zum Modul *Überblicke über Teilgebiete der Mathematik*. In den Zielen dazu heißt es, die Studierenden sollen zentrale Resultate der Algebra kennenlernen, oft auch ohne detaillierte Beweise. Für Studierende, die nach dem Bachelorstudium in das Berufsleben einsteigen wollen, liefert dieses Modul eine Verbreiterung des allgemeinmathematischen Wissens.
Einige Themen über Gruppen, Ringe und Körper werden vorher im Modul *Elementare Algebra* angeboten. Wir stellen drei ausgewählte Themenbereiche vor, von denen das erste mit Gruppentheorie assoziiert ist, das zweite mit Ringtheorie, und das dritte mit Körpertheorie. Alle drei Themen sind auch Beispiele für die Anwendungen der Algebra.

2 Algebra und Symmetrie

In diesem Abschnitt wollen wir Symmetriegruppen von Ornamenten und Kristallen behandeln, und eine kleine Einführung ist das Gebiet der kristallographischen Gruppen geben. Die Klassifikation kristallographischer Gruppen ist durchaus wichtig in den Anwendungen, sei es für die Festkörperphysik, bei der Beschreibung von inkommensurabel modulierten Strukturen, Quasikristallen und magnetischen Strukturen, oder für Anwendungen innerhalb der Kristallographie.

2.1 Gruppenoperationen

Die Definition einer Gruppenoperation, oder einer Gruppenwirkung ist wie folgt.

Definition 2.1. Sei G eine Gruppe und X eine Menge. Eine Abbildung

$$\begin{aligned} G \times X &\mapsto X, \\ (g, x) &\mapsto gx \end{aligned}$$

nennt man eine *Operation von G auf X*, falls gilt

(1) $g(hx) = (gh)x$ für alle $g, h \in G$ und alle $x \in X$,

(2) $ex = x$ für das neutrale Element $e \in G$ und alle $x \in X$.

Eine Menge X mit einer Operation einer Gruppe G auf X heißt auch *G-Menge*. Wir wollen uns einige Beispiele anschauen.

1. Die Gruppe $GL_n(K)$ der invertierbaren $n \times n$ Matrizen über einem Körper K operiert auf dem K^n durch Matrixmultiplikation $(A, x) \mapsto Ax$.

2. Jede Gruppe G operiert auf jeder Menge X durch die triviale Operation, d.h. durch $gx = x$ für alle $g \in G$ und alle $x \in X$.

3. Die symmetrische Gruppe $\mathcal{S}_n$ operiert durch Permutationen auf der Ziffernmenge $X = \{1, 2, \ldots, n\}$.

4. Jede Gruppe G operiert auf sich selbst durch Konjugation: mit $X = G$ ist die Operation durch $(g, x) \mapsto gxg^{-1}$ gegeben.

5. Die Gruppe $SL_2(\mathbb{C})$ 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 Möbiustransformationen

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

Dabei gilt $A \cdot \infty = a/c$ und $A \cdot (-d/c) = \infty$. Die Einheitsmatrix E operiert durch $Ez = \frac{1z+0}{0z+1} = z$. 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, daß gilt

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

Es bezeichne $Sym(X)$ die Menge aller Bijektionen $X \to X$. Sie bildet eine Gruppe unter Komposition. Für jedes $g \in G$ sei $L(g)\colon x \to gx$ die Linksmultiplikation mit g. Offenbar ist $L(g)$ eine Bijektion von X, mit inverser Abbildung $L(g^{-1})$.

Satz 2.1.1. *Sei G eine Gruppe, die auf einer Menge X operiert. Dann ist die Abbildung $L\colon G \to Sym(X)$, $g \mapsto L(g)$ ein Gruppenhomomorphismus. Ist umgekehrt ein Gruppenhomomorphismus $\theta\colon G \to Sym(X)$ gegeben, so operiert die Gruppe G auf X durch $(g, x) \mapsto \theta(g)x$.*

Beweis. Die beiden Bedingungen einer Gruppenoperation bedeuten $L(e) = \mathrm{id}$ und $L(g) \cdot (L(h) \cdot x) = L(gh) \cdot x$ für alle $g, h \in G$ und $x \in X$. Das besagt genau, daß L ein Gruppenhomomorphismus ist. Dabei ist $L(g) \in Sym(X)$ für $g \in G$. Die zweite Aussage folgt analog. □

Der Satz ist manchmal hilfreich. So nennt man eine Operation von G auf X auch *treu*, falls der Homomorphismus $L\colon G \to Sym(X)$ injektiv ist; mit anderen Worten, wenn $gx = x$ für alle $x \in X$ schon $g = e$ impliziert. Zum Beispiel operiert jede Untergruppe der $\mathcal{S}_n$ treu auf $X = \{1, 2, \ldots, n\}$.

Definition 2.2. Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ heißt die Menge

$$Gx = \{gx \mid g \in G\} \subseteq X$$

die *Bahn* von x, oder der *Orbit* von x.

Manchmal sagt man auch G-Bahn von x. Eine Operation heißt *transitiv*, falls es ein $x \in X$ gibt mit $X = Gx$. In diesem Fall nennt man X einen *homogenen Raum* für G. Zum Beispiel operiert die symmetrische Gruppe $\mathcal{S}_n$ transitiv auf $X = \{1, 2, \ldots, n\}$.
Wenn G auf X operiert, so nennt man eine Teilmenge $S \subseteq X$ auch *G-invariant*, falls $gx \in S$ gilt für alle $g \in G$ und alle $x \in S$. Dann induziert die Operation von G auf X auch eine Operation von G auf S. Die Bahn Gx von X ist die kleinste G-invariante Teilmenge von X, die x enthält.
Für $x, y \in X$ schreiben wir $x \sim y$, falls es ein $g \in G$ gibt mit $y = gx$. Das definiert

offensichtlich eine Äquivalenzrelation:

1. Die Relation is reflexiv, da $x = ex$ gilt.

2. Die Relation ist symmetrisch, da aus $x \sim y$ folgt $y = gx$, und somit $x = g^{-1}y$, also $y \sim x$.

3. Die Relation ist transitiv, weil $y = gx$ und $z = hy$ zusammen offenbar $z = h(gx) = (hg)x$ implizieren.

Die Äquivalenzklassen dieser Relation sind nichts anderes als die G-Bahnen. Sie bilden eine Partition von X.

Beispiel 2.1.2. *Für eine Gruppe G, die auf sich selbst operiert durch Konjugation, sind die G-Bahnen genau die Konjugationsklassen.*

Für $x \in X = G$ ist die Konjugationsklasse von x die Menge

$$\{gxg^{-1} \mid g \in G\}.$$

Beispiel 2.1.3. *Sei $G = D_\infty$ die Untergruppe von $\mathrm{Sym}(\mathbb{R})$, die von allen Translationen $T(x) = x + 1$ und allen Spiegelungen $S(x) = -x$ erzeugt wird. Sie heißt die unendliche Diedergruppe. Sie operiert auf $X = \mathbb{R}$. Die G-Bahnen der Elemente $x = 1, \frac{1}{2}, \frac{1}{3}$ sind gegeben durch*

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

Definition 2.3. Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ heißt die Menge

$$G_x = \{g \in G \mid gx = x\} \subseteq G$$

der *Stabilisator* von x, oder die Isotropiegruppe von x.

In der Tat ist G_x eine Untergruppe von G, aber nicht unbedingt ein Normalteiler. Vielmehr haben wir folgendes Resultat.

Lemma 2.1.4. *Für $g \in G$ und $x \in X$ gilt*

$$gG_xg^{-1} = G_{gx}.$$

Beweis. Es sei $h \in G_x$, also $hx = x$. Dann folgt $(ghg^{-1})gx = ghx = gx$, also $ghg^{-1} \in G_{gx}$. Das bedeutet $gG_xg^{-1} \subseteq G_{gx}$. Gilt umgekehrt $h(gx) = gx$, so folgt

$$(g^{-1}hg)x = g^{-1}(h(gx)) = g^{-1}gx = x.$$

Das bedeutet $g^{-1}hg \in G_x$, oder $h \in gG_xg^{-1}$. □

Beispiel 2.1.5. *Falls G durch Konjugation auf sich selbst operiert, so ist der Stabilisator von x die Gruppe*

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Sie heißt Zentralisator *von x in G.*

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

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{g \in G \mid gx = xg \; \forall \, x \in G\}.$$

Für eine Teilmenge $S \subseteq X$ definieren wir den Stabilisator von S als

$$\mathrm{Stab}(S) = \{g \in G \mid gS = S\}.$$

Offenbar ist $\mathrm{Stab}(S)$ eine Untergruppe von G, und $\mathrm{Stab}(x) = G_x$ für ein Element $x \in X$. Wie in Lemma 2.1.4 zeigt man, daß $\mathrm{Stab}(gS) = g\,\mathrm{Stab}(S)g^{-1}$.

Beispiel 2.1.6. *Für die Operation der unendlichen Diedergruppe D_∞ auf $\mathbb{R}$ sind die Satbilisatoren von $x = 1, \frac{1}{2}, \frac{1}{3}$ gegeben durch*

$$G_1 = \{\mathrm{id}, T^2S\},$$
$$G_{\frac{1}{2}} = \{\mathrm{id}, TS\},$$
$$G_{\frac{1}{3}} = \{\mathrm{id}\}.$$

Beweis. Die Gruppenelemente sind von der Form T^nS oder T^n für $n \in \mathbb{Z}$, wegen $S^2 = \mathrm{id}$ und $ST = T^{-1}S$. Für $x = \frac{1}{3}$ hat die Gleichung $W(x) = x$ nur die Lösung $W = \mathrm{id}$. Falls $W = T^n$ so impliziert $T^n(\frac{1}{3}) = \frac{1}{3}$ natürlich $n = 0$. Für $W = T^nS$ ergibt die Gleichung

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

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

Beispiel 2.1.7. *Es operiere G auf sich selbst durch Konjugation. Sei H eine Untergruppe von G. Der Stabilisator von H heißt dann der* Normalisator $N_G(H)$ *von H in G:*

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Satz 2.1.8. *Operiert eine Gruppe G auf einer Menge X, so ist die Abbildung*

$$G/G_x \to Gx, gG_x \mapsto gx$$

eine Bijektion. Es gilt $|Gx| = (G : G_x)$.

Korollar 2.1.9. *Die Anzahl der Konjugierten gHg^{-1} einer Untergruppe H von G ist gleich $(G : N_G(H))$.*

Wenn X eine endliche Menge ist, dann ist X eine disjunkte Vereiningung von endlich vielen Bahnen O_i, also

$$X = \bigcup_{i=1}^{m} O_i.$$

Das bedeutet dann

$$|X| = \sum_{i=1}^{m} |O_i| = \sum_{i=1}^{m} (G : G_{x_i})$$

für $x_i \in O_i$. Wenn G auf $X = G$ durch Konjugation operiert, erhält man dadurch die sogenannte Klassengleichung.

Theorem 2.1.10 (Klassengleichung)**.** *Es bezeichne $\mathcal{C}$ ein Vertretersystem von Elementen für die Konjugationsklassen von G. Dann gilt*

$$|G| = \sum_{x \in \mathcal{C}} (G : C_G(x)).$$

Die Klassengleichung hat viele Folgerungen für die Gruppentheorie. Wir wollen an einige ausgewählte Resultate erinnern.

Theorem 2.1.11 (Cauchy)**.** *Sei p eine Primzahl, die die Gruppenordnung $|G|$ teilt. Dann enthält G ein Element der Ordnung p.*

Korollar 2.1.12. *Sei G eine Gruppe der Ordnung $2p$ für eine Primzahl $p > 2$. Dann ist G zyklisch oder eine Diedergruppe.*

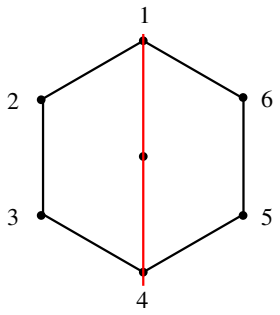
Eine Gruppe G heißt *zyklisch*, falls sie von einem Element $r \in G$ erzeugt wird. Man schreibt dann auch $G = \langle r \rangle$. Wenn r endliche Ordnung hat, also wenn $r^n = e$ für ein $n \in \mathbb{N}$ gilt, so ist $G = \{e, r, r^2, \ldots, r^{n-1}\}$. Es ist leicht zu sehen, daß es bis auf Isomorphie genau eine zyklische Gruppe der Ordnung n gibt, für jedes $n \leq \infty$. Man hat

$$C_n = \{e, r, r^2, \ldots, r^{n-1}\} \approx \mathbb{Z}/n\mathbb{Z},$$
$$C_\infty = \{\ldots, r^{-i}, \ldots, r^{-1}, e, r, \ldots, r^i, \ldots\} \approx \mathbb{Z}$$

Der Satz von Lagrange impliziert folgendes Resultat:

Satz 2.1.13. *Jede Gruppe von Primzahlordnung p ist zyklisch.*

Geometrisch gesehen kann man sich C_n als die Gruppe der Drehungen eines regulären Polygons mit n Seiten vorstellen.



Die Diedergruppe D_n für $n \geq 3$ ist die Symmetriegruppe eines regulären n-Ecks. Nummeriert man die Ecken des Polygons gegen den Uhrzeigersinn mit $1, 2, \ldots, n$, so bezeichne r die Drehung um $2\pi/n$, und s die Spiegelung an der Geraden durch 1 und den Mittelpunkt des Polygons. In Formeln,

$$\begin{aligned} r(i) &= i + 1 \mod n, \\ s(i) &= n + 2 - i \mod n. \end{aligned}$$

Man rechnet leicht nach, daß $(srs)(i) = i + n - 1 = r^{n-1}(i)$ gilt. Man hat außerdem $r^n = e$ und $s^2 = e$. Die Gruppe D_n wird also präsentiert durch

$$D_n = \langle r, s \mid r^n = s^2 = e, sr = r^{n-1}s \rangle.$$

Man hat $D_n = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots, r^{n-1}s\}$. Die geometrische Definition zeigt, daß alle Elemente hier verschieden sind, d.h., $|D_n| = 2n$. Des weiteren ist $D_n = \langle r \rangle \rtimes_\theta \langle s \rangle = C_n \rtimes_\theta C_2$ ein semidirektes Produkt der zyklischen Gruppen C_n und C_2, mit $\theta(s)(r^i) = r^{-i}$. Wir bemerken noch, daß man für $n \leq 2$ die Diedergruppen wie folgt definiert:

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

Beweis. Wir wollen nun das Korollar 2.1.12 beweisen. Sei G eine Gruppe der Ordnung $2p$ mit $p > 2$. Der Satz von Cauchy zeigt, daß es ein Element s der Ordnung 2, und ein Element r der Ordnung p in G geben muß, da 2 und p ein Teiler von $|G|$ sind. Dann ist $C_p = \langle r \rangle$ ein Normalteiler in G wegen $(G : C_p) = 2$. Natürlich ist $s \notin C_p$, weshalb $G = C_p \cup C_p s$ ist. Das bedeutet $G = \{1, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}$. Da C_p ein Normalteiler ist, gilt $srs^{-1} = r^i$ für ein $i \in \mathbb{Z}$. Wegen $s^2 = e$ ist

$$r = s^2 r s^{-2} = s(srs^{-1})s^{-1} = r^{i^2}.$$

Das bedeutet $i^2 \equiv 1 \mod p$, oder $i^2 = 1$ im Körper $\mathbb{Z}/p\mathbb{Z}$. Diese quadratische Gleichung hat genau zwei Lösungen $i = \pm 1$, also $i \equiv 1 \mod p$ oder $i \equiv -1 \mod p$. Im ersten Fall ist die Gruppe G kommutativ, d.h. $G = \langle r, s \mid r^p = s^2 = e, rs = sr \rangle \approx C_{2p}$. Im zweiten Fall hat man $srs^{-1} = r^{-1}$, also $G \approx D_p$. □

Beispiel 2.1.14. *Jede Gruppe der Ordnung* 6 *ist entweder isomorph zu* C_6*, oder zu* $\mathcal{S}_3$*.*

Das folgt aus Korollar 2.1.12 mit $p = 3$. Eine Gruppe der Ordnung $2p = 6$ ist demnach entweder zyklisch, oder isomorph zu D_3. Die Gruppe D_3 ist erzeugt von den beiden Permutationen $s = (23)$ und $r = (123)$, nach Definition von r und s. Damit ist aber klar, daß $D_3 = \mathcal{S}_3$ gilt.

Eine Gruppe G der Ordnung p^n heißt p-Gruppe. Die Klassengleichung impliziert auch folgenden Satz.

Satz 2.1.15. *Jede nicht-triviale* p*-Gruppe hat ein nicht-triviales Zentrum.*

Korollar 2.1.16. *Jede Gruppe der Ordnung p^2 ist kommutativ, und damit isomorph zu $C_p \times C_p$ oder C_{p^2}.*

Beweis. Sei G eine Gruppe der Ordnung p^2 mit Zentrum Z. Dann ist $|Z|$ ein Teiler von p^2, der wegen Satz 2.1.15 von 1 verschieden ist. Somit hat G/Z die Ordnung p oder 1. In beiden Fällen folgt, daß G/Z eine zyklische Gruppe ist. Es gibt also ein $x \in G$ mit $G/Z = \langle xZ \rangle$. Für zwei beliebige Elemente $g = x^r z_1$ und $h = x^s z_2$, mit $z_i \in Z$ folgt dann

$$gh = x^r z_1 x^s z_2 = x^{r+s} z_1 z_2 = x^s z_2 x^r z_1 = hg.$$

Also ist G kommutativ. □

2.2 Isometriegruppen des Euklidischen Raumes

Definition 2.4. Ein Euklidischer Vektorraum ist ein Paar (E, σ), bestehend aus einem endlich-dimensionalen $\mathbb{R}$-Vektorraum E und einer positiv definiten Bilinearform $\sigma\colon E \times E \to \mathbb{R}$.

Für $x \in E$ setzen wir $|x| = \sqrt{\sigma(x,x)}$ und $d(x,y) = |x-y|$. Das definiert eine Metrik $d\colon E \times E \to \mathbb{R}$. Wir können den Vektorraum E nach Wahl einer orthonormalen Basis mit dem Koordinatenraum $\mathbb{R}^n$ identifizieren. Dann ist $\sigma(x,x) = \langle x, x\rangle$ das übliche Skalarprodukt, und $d(x,y) = \|x-y\|$ die übliche Euklidische Metrik.

Definition 2.5. Eine Abbildung $f\colon E \to E$ heißt *Isometrie*, oder *Bewegung*, falls

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

für alle $x, y \in E$ gilt.

Eine Isometrie erhält also den Abstand zwischen zwei Punkten. Sie ist offensichtlich injektiv. Wir werden auch sehen, daß jede Isometrie zugleich auch surjektiv ist. Somit ist jede Isometrie bijektiv, und ihre Umkehrabbildung ist wieder eine Isometrie. Die Isometrien eines Euklidischen Vektorraums bilden eine Gruppe unter Komposition. Sie wird mit $Iso(E)$ bezeichnet.

Beispiel 2.2.1. *Eine* Translation *von E ist eine Abbildung $T\colon E \to E$ der Form*

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

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

Eine lineare Abbildung $f\colon \mathbb{R}^n \to \mathbb{R}^n$ heißt *orthogonal*, falls

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

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

$$x^t B^t B y = x^t y$$

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

Beispiel 2.2.2. *Eine orthogonale lineare Abbildung $f\colon E \to E$ ist eine Isometrie.*

In der Tat, es gilt

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

Lemma 2.2.3. *Es sei $f\colon E \to E$ eine Isometrie, die den Ursprung fixiert, d.h., mit $f(0) = 0$. Dann ist f eine orthogonale lineare Abbildung.*

Beweis. Mit der sogenannten Polarisierungsformel folgt

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

für alle $x, y \in E$. Also erhält f das innere Produkt. Es bleibt zu zeigen, daß f eine lineare Abbildung ist. Sei $e_1, \ldots, e_n$ die Standardbasis des $\mathbb{R}^n$. Da f das innere Produkt erhält, ist auch $f(e_1), \ldots, f(e_n)$ eine ONB. Für jedes $x \in E$ gilt jetzt

$$\begin{aligned} x &= \sum_{k=1}^{n} \langle x, e_k\rangle e_k, \\ f(x) &= \sum_{k=1}^{n} \langle f(x), f(e_k)\rangle f(e_k) \\ &= \sum_{k=1}^{n} \langle x, e_k\rangle f(e_k). \end{aligned}$$

Also folgt $f(\sum_{k=1}^n x_k e_k) = \sum_{k=1}^n x_k f(x_k)$ und f ist linear. □

Wir sehen nun, daß Euklidische Isometrien affine Abbildungen sind.

Satz 2.2.4. *Sei $f\colon E \to E$ eine Isometrie von E. Identifizieren wir E mit dem Standardraum $\mathbb{R}^n$, so gibt es eine orthogonale Matrix $A \in O_n(\mathbb{R})$ und einen Vektor $v \in \mathbb{R}^n$ mit*

$$f(x) = Ax + v$$

für alle $x \in E = \mathbb{R}^n$.

Beweis. Sei $f\colon E \to E$ eine Isometrie und $v = f(0)$. Dann ist

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

eine Isometrie mit $g(0) = 0$. Also ist g nach Lemma 2.2.3 eine orthogonale lineare Abbildung, und $f(x) = g(x) + v$. □

Nun ist es leicht zu sehen, daß $\mathrm{I}so(E)$ eine Gruppe unter Komposition ist. Seien f, g gegeben durch $f(x) = Ax + v$ und $g(x) = Bx + w$, mit $A, B \in O_n(\mathbb{R})$ und $v, w \in \mathbb{R}^n$. Dann gilt

$$\begin{aligned}(f \circ g)(x) &= A(Bx + w) + v \\ &= ABx + (Aw + v)\end{aligned}$$

$$f^{-1}(x) = A^{-1}x - A^{-1}v.$$

Wir können damit Isometrien von E durch $(n+1) \times (n+1)$-Matrizen beschreiben.

$$\mathrm{I}so(E) = \left\{ \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \mid A \in O_n(\mathbb{R}), v \in \mathbb{R}^n \right\}$$

Jedes $x \in E$ entspricht einem Punkt $\binom{x}{1}$ in der Hyperebene

$$\{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{R}^{n+1} \mid x_{n+1} = 1\}$$

im $\mathbb{R}^{n+1}$. Die Gruppe $\mathrm{I}so(E)$ operiert auf dem Raum $E = \mathbb{R}^n$ durch

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

Wir können nun die Struktur der Matrixgruppe $\mathrm{I}so(E)$ studieren. Die Multiplikation ist gegeben durch

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} AB & Aw + v \\ 0 & 1 \end{pmatrix}.$$

Das Inverse ist dann

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

Die Translationen bilden einen Normalteiler in $\mathrm{I}so(E)$, gegeben durch

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

In der Tat ist

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} E_n & w \\ 0 & 1 \end{pmatrix} \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} E_n & Aw \\ 0 & 1 \end{pmatrix}$$

Es ist nun leicht zu sehen, daß I$so(E)$ ein semidirektes Produkt von $O_n(\mathbb{R})$ und $T(n)$ ist:

$$\mathrm{I}so(E) = T(n) \rtimes O_n(\mathbb{R}).$$

Sind N und Q zwei Gruppen, so können wir eine Gruppenstruktur auf dem kartesischen Produkt $N \times Q$ definieren durch punktweise Multiplikation:

$$(n, q) \cdot (n', q') = (nn', qq')$$

für alle $n, n' \in N$ und $q, q' \in Q$. Diese Gruppe heißt das *direkte Produkt* von N und Q und wird mit $G = N \times Q$ bezeichnet. Nun kann Q durch einen Gruppenhomomorphismus $\theta\colon Q \to \mathrm{A}ut(N)$ auf N operieren, via

$$q \cdot n = \theta(q)(n).$$

Damit kann man $N \times Q$ wie folgt mit einer Gruppenstruktur versehen:

$$(n, q) \cdot (n', q') = (n\theta(q)(n'), qq').$$

Diese Gruppe nennen wir das *semidirekte Produkt* von N und Q, und schreiben $G = N \rtimes_\theta Q$. Für den trivialen Homomorphismus $Q \to \mathrm{A}ut(N)$, gegeben durch $\theta(q)(n) = n$, erhalten wir das direkte Produkt zurück. Die Gruppe N ist ein Normalteiler von G, und $Q \approx G/N$ ist der Quotient. Für $N = T(n)$, $Q = O_n(\mathbb{R})$ und die natürliche Inklusion $\theta\colon O_n(\mathbb{R}) \to \mathrm{A}ut(T(n))$ erhalten wir $G = \mathrm{I}so(E) = T(n) \rtimes_\theta O_n(\mathbb{R})$.
Wir können das semidirekte Produkt auch noch etwas abstrakter beschreiben.

Definition 2.6. Eine Sequenz von Gruppen und Gruppenhomomorphismen

$$1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$$

heißt *exakt*, falls α injektiv, β surjektiv ist, und $\alpha(N) = \ker(\beta)$ gilt.

Damit ist $\alpha(N) \approx N$ ein Normalteiler von G, den wir oft mit N identifizieren. Weiterhin ist $Q \approx G/\alpha(N)$ der Quotient. Man sagt auch, daß G dann eine *Erweiterung* von Q durch N ist. Offenbar liefert ein semidirektes Produkt $N \rtimes_\theta Q$ eine Erweiterung von Q durch N, nämlich

$$1 \to N \to N \rtimes_\theta Q \to Q \to 1.$$

Diese kurze exakte Sequenz hat dann allerdings eine besondere Eigenschaft: sie *zerfällt*.

Definition 2.7. Sei $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ eine Gruppenerweiterung. Bezeichne mit $\tau : Q \cong G/\alpha(N) \to G$ die Abbildung, die jeder Restklasse $x \in G/\alpha(N)$ einen Vertreter $\tau(x) \in G$ zuordnet. Eine solche Funktion $\tau : Q \to G$ heißt *Transversale*.

Nach Definition gilt $\beta(\tau(x)) = x$, i.e.,

$$\beta\tau = \mathrm{id}_{|Q} \tag{2.1}$$

Im allgemeinen muß eine Transversale kein Gruppenhomomorphismus sein. Genau diese Eigenschaft ist aber wichtig:

Definition 2.8. Eine Erweiterung $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} Q \to 1$ heißt *zerfallend*, falls es eine Transverale $\tau : Q \to G$ gibt, die ein Gruppenhomomorphismus ist. In diesem Fall heißt τ ein Schnitt.

Satz 2.2.5. *Eine Gruppe G ist ein semidirektes Produkt $N \rtimes_\theta Q$ genau dann, wenn G eine zerfallende Erweiterung von Q durch N ist.*

Beispiel 2.2.6. *Die beiden folgenden Erweiterungen zerfallen:*

$$1 \to T(n) \xrightarrow{\iota} \mathrm{I}so(\mathbb{R}^n) \xrightarrow{\ell} O_n(\mathbb{R}) \to 1,$$
$$1 \to SL_n(k) \xrightarrow{\iota} GL_n(k) \xrightarrow{det} k^\times \to 1.$$

Die erste Sequenz zerfällt wie folgt. Wir schreiben (A, v) für die Matrix $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$. Dann ist $\ell(A, v) = A$, und man kann $\tau(A) = (A, 0)$ wählen.
Für die zweite Sequenz definiere man $\tau : k^\times \to GL_n(k)$ 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 wegen $\tau(ab) = \tau(a)\tau(b)$ und $(\beta \circ \tau)(a) = \det \tau(a) = a$.

Die Gruppe $\mathrm{I}so(E)$ operiert, wie gesagt, auf dem $\mathbb{R}^n$. Wir benutzen diese Tatsache, um *diskrete* Untergruppen von $\mathrm{I}so(E)$ zu definieren.

Definition 2.9. Eine Untergruppe $\Gamma \subseteq \mathrm{I}so(E)$ heißt *diskret*, falls ihre Bahnen $\Gamma x \subseteq \mathbb{R}^n$ unter der Operation diskrete Mengen im $\mathbb{R}^n$ sind.

Eine Menge ist diskret im $\mathbb{R}^n$, falls sie keinen Häufungspunkt hat. Das bedeutet, für $x \neq y$ mit $y = \gamma x$, $\gamma \in \Gamma$ gibt es ein $c > 0$, so daß der Abstand zwischen x und y mindestens c ist: $d(x, y) \geq c > 0$.

Beispiel 2.2.7. *Die Untergruppe $\Gamma \subseteq \mathrm{I}so(\mathbb{R}^2)$, die einen Kreis S^1 in sich überführt ist nicht diskret. Sei enthält Drehungen um einen beliebigen Winkel, und Spiegelungen an einem beliebigen Durchmesser.*

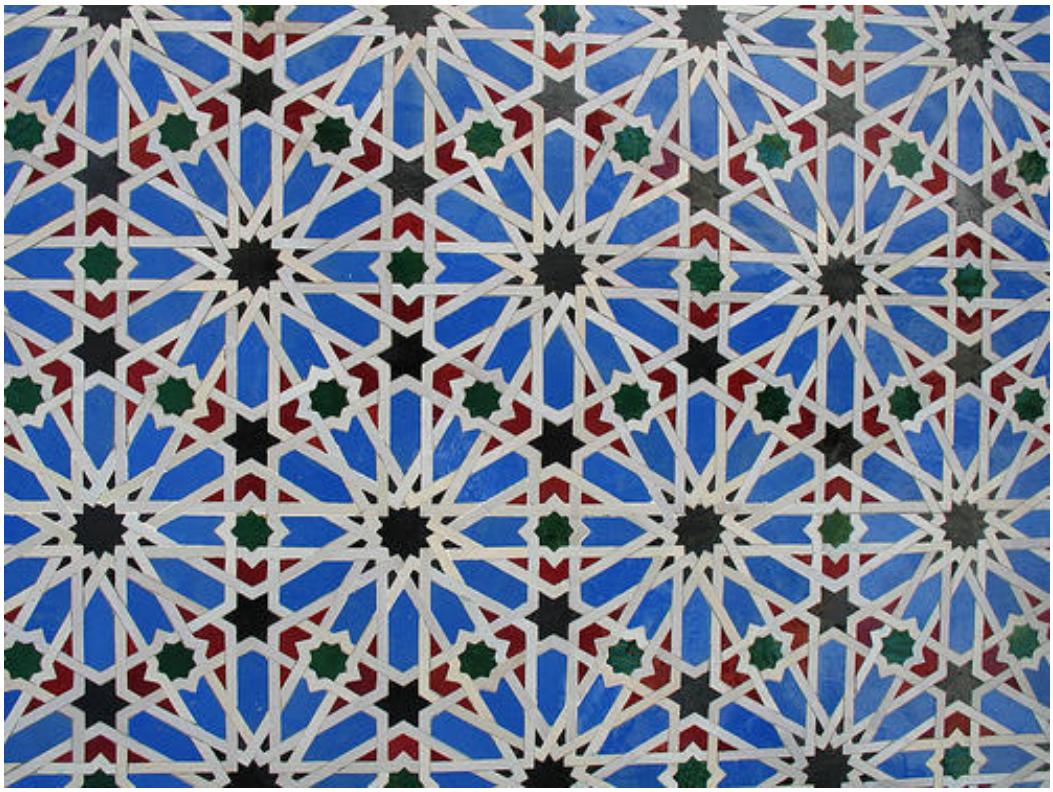
In der Tat, diese Gruppe ist $\Gamma = O_2(\mathbb{R})$.

Beispiel 2.2.8. *Die Untergruppe $\Gamma \subseteq \mathrm{I}so(\mathbb{R}^2)$, die von zwei Translationen $t_1(x) = x + \binom{1}{0}$ und $t_2(x) = x + \binom{0}{1}$ erzeugt wird ist diskret.*

Es handelt sich um die Gruppe $\Gamma = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$.

2.3 Symmetriegruppen von Ornamenten

Bei einem Ornament wird ein Motiv auf einem ebenen Flächenstück derart regelmäßig gestaltet, daß seine Fortsetzung ins Unendliche suggeriert wird. Es breitet sich sozusagen regelmäßig wiederholend über die ganze Ebene aus. Das entstehende Muster ist sehr symmetrisch in dem Sinne, daß man es auf vielerlei Weise drehen, verschieben oder spiegeln kann, ohne das Muster zu verändern. Eine solche Operation der Ebene, die das Muster unverändert läßt, nennt man eine *Symmetrie* des Musters. Solche Symmetrien bilden eine Gruppe.



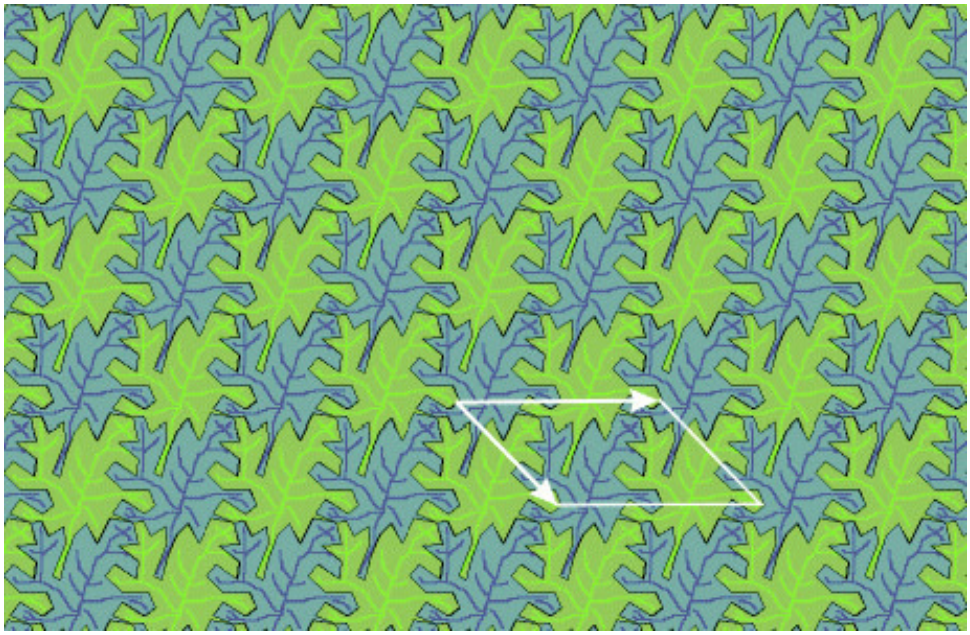
Im allgemeinen ist eine Symmetrie einer Menge M in einem Euklidischen Raum wie folgt definiert.

Definition 2.10. Sei M eine nicht-leere Teilmenge von E. Eine Isometrie $s\colon E \to E$ heißt eine *Symmetrie* von M, falls $s(M) = M$ gilt.

Die Menge aller Symmetrien von M bildet eine Untergruppe von $\mathrm{I}so(E)$, die mit $\mathrm{S}ym(M)$ bezeichnet wird.
Wir wollen uns hier nun den Symmetriegruppen von Ornamenten in der Ebene widmen. Darunter versteht man eine ganz spezielle Klasse von Gruppen.

Definition 2.11. Eine Untergruppe $\Gamma \subseteq \mathrm{I}so(\mathbb{R}^2)$ heißt *Ornamentgruppe*, falls sie diskret ist, und zwei Translationen mit linear unabhängigen Richtungen enthält.

Unter einem *Ornament* versteht man dann ein Muster $M \subset \mathbb{R}^2$, deren Symmetriegruppe $Sym(M)$ eine Ornamentgruppe ist.
Wir wollen uns folgendes Ornament anschauen, und seine Symmetriegruppe bestimmen.



Die einzigen Isometrien der Ebene, die das Ornament M in sich überführen, sind Translationen in die gezeigten Richtungen. In Bezug auf diese Basis des $\mathbb{R}^2$ wird $Sym(M)$ also erzeugt von den beiden Translationen

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

und es gilt $AB = BA$. Damit besteht die Gruppe $Sym(M)$ also aus den Matrizen , mit $n, m \in \mathbb{Z}$,

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

wobei $n, m \in \mathbb{Z}$. Es gilt also $Sym(M) \approx \mathbb{Z}^2$. Man vergleiche mit Beispiel 2.2.8.
Es stellt sich nun heraus, daß man alle Ornamentgruppen klassifizieren kann. Bis auf Isomorphie gibt es genau 17 Ornamentgruppen, und für jede dieser Gruppen kann man ein Ornament aus der Kunst finden, das genau diese Symmetriegruppe hat. Einen ersten Beweis dieser Klassifikation hat Fedorov 1891 erbracht.

Theorem 2.3.1 (Fedorov 1891)**.** *Es gibt genau* 17 *verschiedene Ornamentgruppen Gruppen in der Ebene.*

Fedorov hatte zuerst Symmetriegruppen von Kristallen im 3-dimensionalen Raum betrachtet, und danach erst die einfacheren 2-dimensionalen Entsprechungen der Kristalle, nämlich die Ornamente, untersucht. Dazu kommen wir noch. Zunächst aber wollen wir noch etwas zu den Beweismethoden des Satzes in Dimension 2 sagen. Die waren zuerst vor allen Dingen geometrischer Natur. Isometrien der Ebene sind entweder Drehungen, Spiegelungen oder Gleitspiegelungen. Endliche Isometriegruppen der Ebene kann man dann wie folgt beschreiben.

Satz 2.3.2. *Eine endliche Untergruppe Γ von $\mathrm{I}so(\mathbb{R}^2)$ ist entweder eine zyklische Gruppe C_n, die aus Drehungen um die Winkel $2\pi k/n$ für $k = 0, 1, 2, \ldots, n-1$ um einen Punkt P besteht, oder aber eine Diedergruppe D_n, die aus solchen Drehungen und zusätzlich aus n Spiegelungen an Geraden durch P besteht.*

Hat man nun eine Ornamentgruppe $\Gamma \subseteq \mathrm{I}so(\mathbb{R}^2)$, so bilden die Translationen in Γ einen Normalteiler $N = T(2) \cap \Gamma \approx \mathbb{Z}^2$, so daß der Quotient $\Gamma/\mathbb{Z}^2$ eine endliche Untergruppe von $\mathrm{I}so(\mathbb{R}^2)$ ist, die sogenannte *Punktgruppe*. Man kann nun obigen Satz anwenden und das folgende Resultat zeigen.

Korollar 2.3.3. *Die Punktgruppen einer Ornamentgruppe Γ ist 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.*

Tatsächlich kann eine Drehung in einer Punktgruppe nur die Ordnung $1, 2, 3, 4, 6$ haben. Das nennt man manchmal die *kristallographische Restriktion*. Sei $A \in O_2(\mathbb{R})$ eine solche Drehung. Dann ist $\det(A) = \pm 1$. Falls $\det(A) = -1$, so gilt $A^2 = E$, und A hat Ordnung 2. Andernfalls ist $\det(A) = 1$, und

$$A^2 - \mathrm{t}r(A)A + E = 0$$

nach Cayley-Hamilton. Nach Multiplikation mit A^{-1} folgt

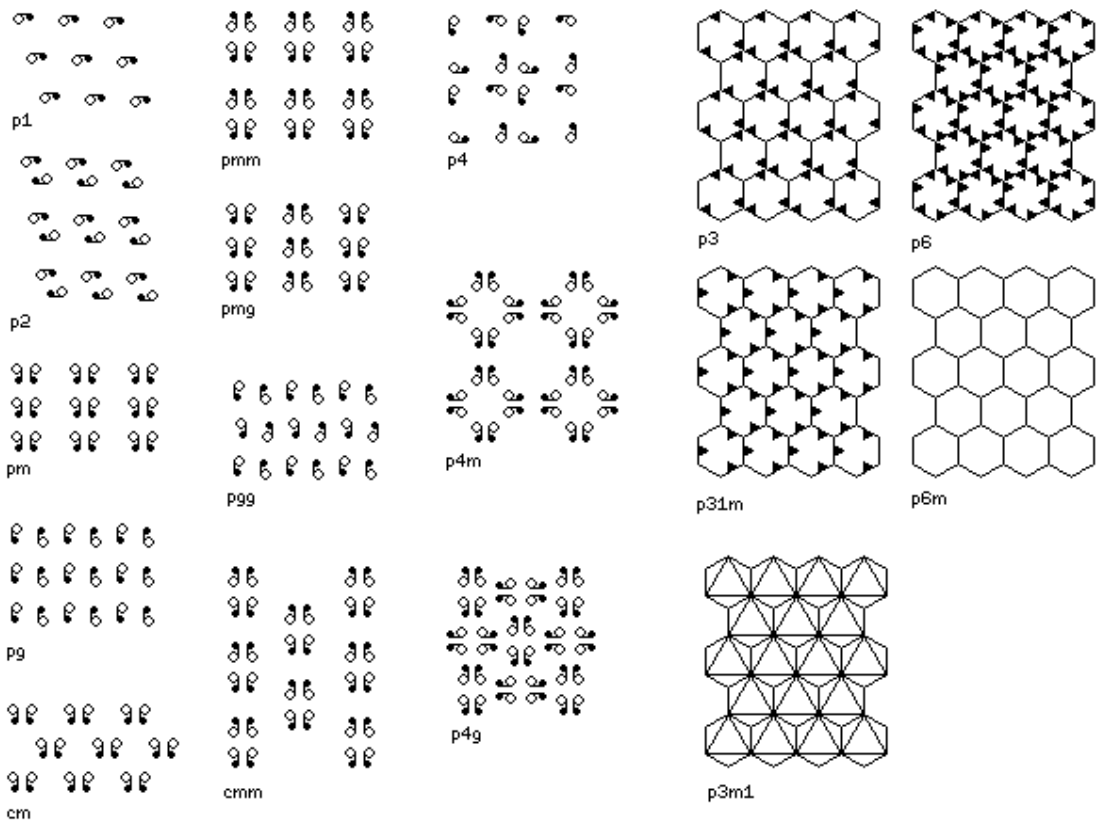
$$A + A^{-1} = \mathrm{t}r(A)E.$$

Für $v \in N$ folgt $Av \in N$ und $A^{-1}v \in N$ wegen $(A, w) \circ (E, v) \circ (A, w)^{-1} = (E, Av)$. Deshalb ist $(A + A^{-1})v = \mathrm{t}r(A)v \in N$. Wählt man nun v so, daß es kein Vielfaches eines anderen Vektors aus N ist, so folgt $\mathrm{t}r(A) \in \mathbb{Z}$. Da aber $A \in SO_2(\mathbb{R})$ ist, und

$$SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} \right\},$$

folgt $\mathrm{t}r(A) = 2\cos(\varphi)$. Deshalb ist $|\mathrm{t}r(A)| \leq 2$, und somit $\mathrm{t}r(A) = -2, -1, 0, 1, 2$. Das bedeutet für den Drehwinkel die Möglichkeiten $\varphi = \pi, \frac{2\pi}{3}, \frac{\pi}{2}, \frac{\pi}{3}, 0$, und A hat die Ordnung $2, 3, 4, 6, 1$.

Nun kann man Theorem 2.3.1 mit Hilfe dieses Korollars beweisen. Das ist aber immer noch relativ mühsam. Einen ausführlichen geometrischen Beweis findet man in [3]. Eine mögliche Darstellung der 17 Ornamente sieht wie folgt aus:



Die Klassifikation der Ornamentgruppen kann auch mit *algebraischen Methoden* erreicht werden. Damit wird dann auch eine Klassifikation solcher Gruppen in höheren Dimensionen $n \geq 3$ möglich - in diesem Fall spricht man von *kristallographischen Gruppen*. Die algebraischen Methoden gestatten einen algorithmischen Zugang, mit dem man dann, im Prinzip, alle kristallographischen Gruppen berechnen kann. Ein wichtiger Satz von Bieberbach besagt, daß es in jeder Dimension nur endlich viele solche Gruppen geben kann.
Mit Hilfe von umfangreichen Computerrechnungen liegt heute die Klassifikation bis einschließlich Dimension 6 vor. Die Anzahl der kristallographischen Gruppen steigt exponentiell an. In Dimension 3 hat man 219 verschiedene kristallographische Gruppen, in Dimension 6 schon 28927922. Die Resultate sind auch wichtig für die Anwendungen in der Kristallographie und Festkörperphysik.

Wir wollen einige dieser algebraischen Überlegungen skizzieren. Sei $\Gamma \subseteq Iso(\mathbb{R}^2)$ also eine Ornamentgruppe. Die folgende Argumentation ist übrigens nicht nur für die Ebene, sondern für $E = \mathbb{R}^n$ gültig. Wie schon gesagt besitzt Γ dann einen Translationsnormalteiler $N \approx \mathbb{Z}^2$, mit endlichem Quotienten $F = \Gamma/\mathbb{Z}^2$. Anders gesagt, man hat eine kurze exakte Sequenz von Gruppen

$$1 \to \mathbb{Z}^2 \xrightarrow{\iota} \Gamma \to F \to 1,$$

wobei $\iota(\mathbb{Z}^2)$ eine maximal abelsche Untergruppe von Γ ist. Die endliche Gruppe F operiert durch Konjugation auf dem Translationsgitter $N \approx \mathbb{Z}^2$. Damit wird F zu einer

endlichen Untergruppe von

$$\mathrm{A}ut(\mathbb{Z}^2) = GL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}.$$

Genauer gesagt, erhält man eine Konjugationsklasse von F in $GL_2(\mathbb{Z})$. Nun gibt es aber immer nur endlich viele solcher Konjugationsklassen:

Satz 2.3.4 (C. Jordan, 1880)**.** *Die Gruppe $GL_n(\mathbb{Z})$ hat nur endlich viele Konjugationsklassen endlicher Untergruppen.*

Diese Konjugationsklassen heißen *arithmetische Ornamentklassen*. Hat man diese Konjugationsklassen bestimmt, so muß man gemäß der obigen exakten Sequenz alle möglichen Erweiterungen bis auf Isomorphie finden, und erhält so alle Ornamentgruppen. Es gibt wiederum nur endlich viele solche Erweiterungen.

Die Konjugationsklassen endlicher Untergruppen von $GL_2(\mathbb{Z})$ lassen sich aber relativ elementar bestimmen. Es gibt genau 13 endliche Untergruppen von $GL_2(\mathbb{Z})$, die jeweils nicht zueinander konjugiert sind in $GL_2(\mathbb{Z})$. Es seien

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

Es gilt $V^2 = -E$, also $V^4 = E$, und $U^3 = E$, $W^6 = E$. Die Ordungen von U, V und W sind in der Tat 3, 4 und 6.

Satz 2.3.5. *Es gibt genau* 13 *arithmetische Ornamentklassen, also* 13 *endliche, nichtkonjugierte Untergruppen von $GL_2(\mathbb{Z})$. Sie sind wie folgt gegeben:*

$$\begin{aligned}
&C_1 \approx \langle E \rangle, \qquad C_2 \approx \langle -E \rangle, \qquad C_3 \approx \langle U \rangle, \\
&C_4 \approx \langle V \rangle, \qquad C_6 \approx \langle W \rangle, \qquad D_1 \approx \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle, \\
&D_1 \approx \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, \quad D_2 \approx \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, -E \right\rangle, \quad D_2 \approx \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, -E \right\rangle, \\
&D_3 \approx \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, U \right\rangle, \quad D_3 \approx \left\langle \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, U \right\rangle, \quad D_4 \approx \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, V \right\rangle, \\
&D_6 \approx \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, W \right\rangle.
\end{aligned}$$

Beweis. Wir geben eine Beweisskizze. Sei A ein Element von $GL_2(\mathbb{Z})$ von endlicher Ordnung. Das bedeutet, $A^m = E$ für ein $m \geq 1$. Die Eigenwerte von A sind also m-te Einheitswurzeln.

1. *Behauptung:* A ist diagonalisierbar.

Angenommen, das ist nicht der Fall. Dann hat A zwei gleiche Eigenwerte, und seine Jordanform über $\mathbb{C}$ ist

$$J = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, \quad \lambda^2 = \pm 1,$$

da $\det(A) = \det(J) = \lambda^2 = \pm 1$. Offensichtlich hat wegen $\lambda \neq 0$ die Matrix J unendliche Ordnung, und damit auch A, weil A und J konjugiert sind. Das ist ein Widerspruch zu $A^m = E$. Es gibt also doch ein $S \in GL_2(\mathbb{C})$ mit

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

Angenommen es gilt $A^2 = E$. Dann folgt

$$\begin{pmatrix} \lambda^2 & 0 \\ 0 & \mu^2 \end{pmatrix} = (SAS^{-1})^2 = SA^2S^{-1} = SES^{-1} = E.$$

Das bedeutet $\lambda^2 = \mu^2 = 1$, also $\lambda, \mu = \pm 1$. Somit ist A eine der folgenden vier Matrizen:

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

Dabei hat E Ordnung 1, und die anderen Matrizen Ordnung 2. Die einzige Matrix aus $SL_2(\mathbb{Z})$ der Ordnung 2 ist $-E$.

2. *Behauptung:* Es gelte $A^m = E$ mit $m \geq 3$. Dann folgt $A \in SL_2(\mathbb{Z})$.

Da die Eigenwerte λ, μ beide m-te Einheitswurzeln sind, gilt $|\lambda| = |\mu| = 1$, und einer der beiden kann nicht reell sein, wegen $m \geq 3$. Nur für $m \leq 2$ sind alle m-ten Einheitswurzeln reell. Sagen wir also, daß $\lambda \notin \mathbb{R}$. Nun gilt aber $tr(A) = \lambda + \mu \in \mathbb{Z}$. Insbesondere muß $\lambda + \mu$ reell sein. Es folgt $\mu = \overline{\lambda}$. Das impliziert $\det(A) = \lambda\mu = \lambda\overline{\lambda} = |\lambda|^2 = 1$.

3. *Behauptung:* Es gelte $A^m = E$ in $GL_2(\mathbb{Z})$. Dann folgt $m = 1, 2, 3, 4, 6$.

Für $m \geq 3$ ist $A \in SL_2(\mathbb{Z})$ und

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

ganzzahlig, mit $|tr(A)| \leq 2$. Die Gleichungen $2\cos(2\pi/m) = -2, -1, 0, 1, 2$ ergeben dann $m = 2, 3, 4, 6, 1$. Alle Fälle treten auch wirklich auf. Die obengenannten Matrizen $A \in GL_2(\mathbb{Z})$ haben Ordnung $m = 1$ und $m = 2$, und es gilt ja $U^3 = V^4 = W^6 = E$ für die im Satz genannten Matrizen.

4. *Behauptung:* Jede endliche Untergruppe $G \subseteq SL_2(\mathbb{Z})$ hat die Ordnung $1, 2, 3, 4, 6$ und ist in $GL_2(\mathbb{Z})$ zu einer der 5 zyklischen Gruppen $\langle E \rangle$, $\langle -E \rangle$, $\langle U \rangle$, $\langle V \rangle$ oder $\langle W \rangle$ konjugiert.

Man beachte, daß wir bisher nur die möglichen Ordnungen von Gruppenelementen kennen. Wir können G in eine Gruppe $SL_2(\mathbb{F}_p)$ über einem endlichen Körpern $\mathbb{F}_p$ einbetten. Die Projektion $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induziert einen Gruppenhomomorphismus $SL_2(\mathbb{Z}) \to SL_2(\mathbb{F}_p)$, und damit einen Gruppenhomomorphismus

$$\pi_p \colon G \to SL_2(\mathbb{F}_p).$$

Dieser ist für $p = 3$ injektiv: sei $A \in \ker(\pi_3)$, also $A \equiv E \bmod 3$. Angenommen A ist nicht-trivial. Dann folgt $ord(A) \geq 3$, da die einzige Matrix der Ordnung 2 in $SL_2(\mathbb{Z})$ ja $-E$ ist, die nicht im Kern von π_3 liegt. Die Eigenwerte von A sind also nicht reell und somit komplex konjugierte Einheitswurzeln λ und $\overline{\lambda}$. Wegen $A \equiv E \bmod 3$ folgt $tr(A) \equiv 2 \bmod 3$. Wegen

$$|tr(A)| = |\lambda + \overline{\lambda}| < |\lambda| + |\overline{\lambda}| = 2$$

und $A \neq E$ muß $tr(A) = -1$ gelten. Damit gibt es ganze Zahlen a, b, c mit

$$A = \begin{pmatrix} a & b \\ c & -(1+a) \end{pmatrix}$$

mit $b \equiv c \equiv 0 \bmod 3$, also mit $bc \equiv 0 \bmod 9$. Wegen

$$1 = \det(A) = -(a^2 + a + bc)$$

folgt also $a^2 + a + 1 \equiv 0 \bmod 9$. Das ist ein Widerspruch, und somit ist π_3 injektiv, d.h., G ist isomorph zu einer Untergruppe von $SL_2(\mathbb{F}_3)$. Wegen $|SL_2(\mathbb{F}_3)| = 24$ und nach Lagrange ist $|G|$ also ein Teiler von 24, d.h. $|G| = 1, 2, 3, 4, 6, 12, 24$.

Fakt 1: Die echten Untergruppen von $SL_2(\mathbb{F}_3)$ sind genau C_2, C_3, C_4, C_6 und die Quaternionengruppe Q_8.

Einen Beweis findet man in [5]. Die Quaternionengruppe Q_8 ist abstrakt definiert als

$$Q_8 = \langle a, b \mid a^4 = e, a^2 = b^2, bab^{-1} = a^3 \rangle.$$

Sie wird durch $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $a = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$ in $SL_2(\mathbb{F}_3)$ realisiert. Es gilt $a^2 = -E$ und $b^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \equiv -E \bmod 3$, also $ord(a) = ord(b) = 4$ in $SL_2(\mathbb{F}_3)$.

Fakt 2: Die Quaternionengruppe kann nicht als Untergruppe von $SL_2(\mathbb{Z})$ realisiert werden. Insbesondere ist $SL_2(\mathbb{F}_3)$ selbst keine Untergruppe von $SL_2(\mathbb{Z})$.

Angenommen es gäbe eine Untergruppe $G \leq SL_2(\mathbb{Z})$, die isomorph zu Q_8 wäre. Sei $\pi_2 \colon G \to SL_2(\mathbb{F}_2)$ der Gruppenhomomorphismus, der durch Reduktion modulo 2 gegeben ist. Dann ist $G/\ker(\pi_2) \leq SL_2(\mathbb{F}_2)$, und nach Lagrange $\frac{|G|}{|\ker(\pi_2)|}$ ein Teiler von $|SL_2(\mathbb{F}_2)| = 6$. Wegen $|G| = 8$ bedeutet das aber $|\ker(\pi_2)| = 4$ oder $|\ker(\pi_2)| = 8$. Somit liegt ein Element A der Ordnung 4 im Kern von π_2. Die Eigenwerte von A sind dann vierte Einheitswurzeln, die nicht reell sind, also $\lambda = i$ und $\overline{\lambda} = -i$. Insbesondere gilt $tr(A) = 0$. Es gibt also ganze Zahlen a, b, c mit

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix},$$

wobei a ungerade, und b, c gerade sind. Damit gilt $bc \equiv 0 \bmod 4$ und $1 = \det(A) = -(a^2 + bc)$ impliziert $a^2 \equiv -1 \bmod 4$, was ein Widerspruch bedeutet.

Somit kann G auch nicht zu $SL_2(\mathbb{F}_3)$ selbst isomorph sein, denn ansonsten hätte G eine zu Q_8 isomorphe Untergruppe. Es bleiben also nur die in Fakt 1 angegebenen Möglichkeiten.

5. *Behauptung:* Die endlichen Untergruppen $G \subseteq GL_2(\mathbb{Z})$ sind diejenigen unter 4., und D_1, D_2, D_3, D_4, D_6. Daraus erhält man noch genau weitere 8 Konjugationsklassen.

Sei G also eine endliche Untergruppe in $GL_2(\mathbb{Z})$. Dann ist $H = G \cap SL_2(\mathbb{Z})$ eine der Gruppen C_1, C_2, C_3, C_4, C_6 wegen 4.. Für $G \neq H$ ist $(G : H) = 2$, und damit H Normalteiler in $G = H \cup Hx$. Hier ist $x \in G \setminus H$. Alle Elemente in Hx haben nun Ordnung 2, weil sie Matrizen endlicher Ordnung in $GL_2(\mathbb{Z})$ sind mit Determinante -1; und diese haben *alle* Ordnung 2. Ist y nun ein Erzeuger der zyklischen Gruppe H, so hat also yx die Ordnung 2, d.h., es gilt also $(yx)(yx) = 1$ und $xyx^{-1} = y^{-1}$. Daraus folgt, daß G isomorph ist zu einer der Gruppen D_1, D_2, D_3, D_4, D_6. □

Bemerkung 2.3.6. Die Quaternionengruppe Q_8 verdankt ihren Namen auch der Tatsache, daß sie auch 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, nämlich durch die Multiplikation, die durch

$$i^2 = -1 = j^2,\ ij = k = -ji.$$

bestimmt wird. Des weiteren haben wir gesehen, daß man die Gruppe Q_8 nicht als Untergruppe von $GL_2(\mathbb{Z})$ realisieren kann. Man kann sie aber sehr wohl als Untergruppe von $GL_2(\mathbb{C})$ realisieren:

$$\begin{array}{l} e = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right),\ a = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right),\ a^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right),\ a^3 = \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right), \\ b = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right),\ ab = \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right),\ a^2b = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right),\ a^3b = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right). \end{array}$$

Bemerkung 2.3.7. Ist G eine endliche Untergruppe von $GL_2(\mathbb{Q})$, so ist G isomorph zu einer der folgenden 9 Gruppen:

$$C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6.$$

Aus Satz 2.3.7 kann man nun die Klassifikation der 17 Ornamentgruppen gewinnen. Sei F eine der 13 arithmetischen Ornamentklassen. Die Ornamentgruppen Γ entstehen daraus durch Erweiterungen.

$$1 \to \mathbb{Z}^2 \xrightarrow{\iota} \Gamma \to F \to 1,$$

Dazu kann man die Kohomologiegruppen $H^2(F, \mathbb{Z}^2) \approx H^1(F, \mathbb{R}^2/\mathbb{Z}^2)$ berechnen. Diese endlichen Gruppen liefern dann zusammen mit den arithmetischen Klassen alle Ornamentgruppen.
Ist die Kohomologiegruppe $H^1(F, \mathbb{R}^2/\mathbb{Z}^2)$ trivial, dann erhält man zu F auch nur eine Gruppe Γ. Das passiert in allen Fällen bis auf drei Ausnahmen: für die Klassen $F = D_1, D_2, D_4$. Dort erhält man zu D_1 dann 2 Gruppen, zu D_2 dann 3 Gruppen, und zu D_4 auch 2 Gruppen. Also zusätzlich jeweils 1, 2 und 1 Gruppe. Das sind insgesamt dann $13 + 1 + 2 + 1 = 17$ Gruppen.

2.4 Kristallographische Gruppen

Die allgemeine Definition einer kristallographischen Gruppe ist wie folgt. Wir identifizieren den n-dimensionalen Euklidischen Raum E mit dem $\mathbb{R}^n$.

Definition 2.12. Eine Untergruppe Γ von $\mathrm{Iso}(E)$ heißt *kristallographische Gruppe*, falls Γ diskret ist und $\mathbb{R}^n/\Gamma$ kompakt ist.

Tatsächlich ist das eine Verallgemeinerung von Ornamentgruppen, wie das Resultat von Bieberbach zeigt.

Satz 2.4.1 (Bieberbach 1, 1910)**.** *Sei $\Gamma \leq \mathrm{Iso}(E)$ eine kristallographische Gruppe. Dann enthält Γ die Translationsgruppe $\mathbb{Z}^n$ als abelschen Normalteiler, und der Quotient $\Gamma/\mathbb{Z}^n$ ist eine endliche Gruppe.*

Der Quotient $F = \Gamma/\mathbb{Z}^n$ heißt *Punktgruppe*. Hilbert hatte 1900 gefragt, ob es in jeder Dimension nur endlich viele solcher Gruppen gibt. Dieses Problem wurde von Bieberbach gelöst.

Satz 2.4.2 (Bieberbach 2, 1910)**.** *In jeder Dimension enthält $\mathrm{Iso}(E)$ nur endlich viele verschiedene kristallographische Gruppen.*

Beweis. Der 1. Satz von Bieberbach liefert eine kurze, exakte Sequenz von Gruppen

$$1 \to \mathbb{Z}^n \xrightarrow{\iota} \Gamma \to F \to 1.$$

Die endliche Punktgruppe $F = \Gamma/\mathbb{Z}^n$ operiert treu durch Konjugation, also durch innere Automorphismen, auf dem Gitter $\mathbb{Z}^n$. Dadurch erhält man eine Einbettung von F bis auf Konjugation in die Automorphismengruppe von $\mathbb{Z}^n$, also in die Gruppe

$$GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}.$$

Es gibt aber nur endlich viele Konjugationsklassen von F in $GL_n(\mathbb{Z})$. Das besagt der Satz von Jordan, 2.3.4. Daraus ergeben sich alle kristallographischen Gruppen durch Erweiterungen. Daß man dort wieder nur endlich viele Möglichkeiten hat, liegt an der Tatsache, daß die Kohomologiegruppe $H^2(F, \mathbb{Z}^n) \approx H^1(F, \mathbb{R}^n/\mathbb{Z}^n)$ endlich ist. In der Tat, die Gruppe H^2 links ist diskret, und H^1 rechts ist kompakt. □

Sei $N(F)$ der Normalisator von F in $GL_n(\mathbb{Z})$. Der letzte Schritt in der Klassifikation der kristallographischen Gruppen beruht auf folgendem Satz.

Satz 2.4.3. *Es gibt eine bijektive Korrepsondenz zwischen den kristallographischen Gruppen in den arithmetischen Kristallklassen und den Bahnen unter der Operation der Gruppe $N(F)$ auf der Kohomologiegruppe $H^1(F, \mathbb{R}^n/\mathbb{Z}^n)$.*

Darauf aufbauend gibt es einen Algorithmus von Zassenhaus, um alle kristallographischen Gruppen zu klassifizieren.
Die Klassifikation in Dimension 3 wurde unabhängig voneinander schon 1885 von Fedorov, Schönflies und Barlow erbracht, allerdings mehr mit geometrischen Methoden. Es gibt 219 Gruppen. Jede von ihnen kann als Symmetriegruppe eines echten Kristalls verwirklicht werden.

Satz 2.4.4 (Schoenflies, Barlow, Fedorov 1885)**.** *Es gibt genau* 219 *verschiedene kristallographische Gruppen im drei-dimensionalen Raum.*

Beweis. Zuerst bestimmt man die arithmetischen Kristallklassen, d.h. die Konjugationsklassen endlicher Untergruppen in $GL_3(\mathbb{Z})$. Davon gibt es genau 73. Es gibt mehrere Wege, das einzusehen. Man kann zunächst bemerken, daß aus $A^m = E$ in $GL_3(\mathbb{Z})$ wieder folgt $m = 1, 2, 3, 4, 6$. Damit hat eine endliche Untergruppe $G \subseteq GL_3(\mathbb{Z})$ höchstens Ordnung $2^4 \cdot 3 = 48$, und $H = G \cap SL_3(\mathbb{Z})$ höchstens Ordnung 24. Die endlichen Untergruppen in $SL_3(\mathbb{Z})$ sind bis auf Isomorphie $C_1, C_2, C_3, C_4, C_6,\ D_4, D_6, D_8, D_{12}$ und A_4, S_4.
Danach berechnet man die Bahnen der Normalisatoren $N(F)$ auf den Gruppen $H^1(F, \mathbb{R}^3/\mathbb{Z}^3)$. Dann erhält man genau 219 verschiedene Gruppen. □

Mit Hilfe des Zassenhaus-Algorithmus sind bisher alle kristallographischen Gruppen in den Dimensionen $1 \leq n \leq 6$ klassifiziert worden. Die folgende Tabelle gibt ihre Anzahl s_n wieder, wobei a_n die Anzahl der arithemtischen Klassen 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

Eine explizite Formel für s_n ist bisher nicht bekannt. Für die Asymptotik wird $s_n \sim 2^{n^2}$ vermutet.

3 Algebra und Gleichungen

Algebra ist im ursprünglichen Sinn die Lehre der Auflösung von Gleichungen. Damit beschäftigten sich bereits Mathematiker früherer Kulturen, etwa im Zusammenhang mit Problemen der Landvermessung. Es gibt Keilschrifttafeln aus dem 2. Jahrtausend, auf denen bereits lineare Gleichungssysteme mit mehreren Unbekannten gelöst werden. Auch polynomiale Gleichungen werden behandelt.
Die Naturwissenschaften und die Technik stellen heutzutage allerhöchste Anforderungen an die Mathematik hinsichtlich der Auflösung von Gleichungssystemen. Die numerische Mathematik befasst sich dabei mit dem Auffinden von Näherungslösungen. Der Verzicht auf Exaktheit wirft allerdings auch Probleme auf. Den exakten Lösungen, und dem Studium von qualitativen Aspekten der Lösungsmengen widmet sich eine mathematische Disziplin, die *algebraische Geometrie* heißt. Wir können hier nicht genauer auf diese Theorie eingehen. Vielmehr geben wir einen Einstieg in die Frage nach den Lösungen polynomialer Gleichungssysteme. Ein zentraler Begriff dabei ist eine *Gröbnerbasis*.

3.1 Polynomiale Gleichungssysteme

Hat man ein System von linearen Gleichungen, so kann man das Eliminationsverfahren von Gauß anwenden, um es auf Dreiecksform zu bringen. Aus dieser Dreiecksgestalt liest man dann die Lösung unmittelbar ab. Wir betrachten folgendes Beispiel über einem Körper K:

$$\begin{aligned} 2x - y - z &= 0, \\ x + 2y - 2z - 1 &= 0, \\ x - y + 2z - 2 &= 0. \end{aligned}$$

Sei zuerst $char(K) \neq 11$. Nach Anwendung des Gauß -Algorithmus erhalten wir folgendes äquivalente System (d.h., mit der gleichen Lösungsmenge) von Gleichungen.

$$\begin{aligned} x + 2y - 2z - 1 &= 0, \\ y - 5z + 4 &= 0, \\ z - 1 &= 0. \end{aligned}$$

Das bedeutet $(x, y, z) = (1, 1, 1)$. Wegen

$$\det \begin{pmatrix} 2 & -1 & -1 \\ 1 & 2 & -2 \\ 1 & -1 & 2 \end{pmatrix} = 11$$

haben wir alle Lösungen bestimmt, außer für den Fall, daß die Charakteristik von K gleich 11 ist. In diesem Fall hat das homogene System die Lösungen $(\lambda, 9\lambda, 4\lambda)$, für $\lambda \in K$. Alle Lösungen sind dann gegeben durch $(1,1,1) + \lambda(1,9,4)$.
Normalerweise wollen wir $K = \mathbb{C}, \mathbb{R}$ oder $\mathbb{Q}$ annehmen.
Für polynomiale Gleichungssysteme kann man dieses Verfahren in adaptierter Form auch machen. Wir betrachten das folgende Beispiel:

$$\begin{aligned} x^2 + y^2 + z^2 - 6 &= 0, \\ x^3 + y^3 + z^3 - xyz + 4 &= 0, \\ xy + xz + yz + 3 &= 0. \end{aligned}$$

Dazu berechnen wir eine sogenannte Gröbnerbasis. Sie liefert das folgende äquivalente System von Gleichungen

$$\begin{aligned} 49x + 49y + 12z^5 - 16z^4 - 18z^3 + 72z^2 - 37z + 36 &= 0, \\ 49y^2 + 12yz^5 - 16yz^4 - 18yz^3 + 72yz^2 - 37yz + 36y - 16z^5 & \\ +54z^4 + 24z^3 - 145z^2 + 180z - 195 &= 0, \\ (z+2)^2(z-1)^4 &= 0. \end{aligned}$$

Die dritte Gleichung bestimmt z, nämlich $z = 1$ oder $z = -2$. Daraus gewinnt man dann die Lösungen für y aus der zweiten Gleichung, und dann für x aus der ersten Gleichung. Sei also zuerst $z = 1$. Dann folgt

$$(y+2)(y-1) = 0, \quad x + y + 1 = 0.$$

Somit erhält man die Lösungen $(x,y,z) = (-2,1,1), (1,-2,1)$. Beginnt man mit $z = -2$, so folgt $x + y - 2 = 0$ und $(y-1)^2 = 0$, also $(x,y,z) = (1,1,-2)$. Insgesamt gibt es also genau drei Lösungen,

$$S = \{(1,1,-2), (1,-2,1), (-2,1,1)\}.$$

Hat man ein System von polynomialen Gleichungen gegeben, so kann man zuerst die Frage betrachten, ob es überhaupt irgendeine Lösung gibt, ob es nur endlich viele Lösungen gibt, oder sogar unendlich viele. Wir haben gerade ein System mit nur endlich vielen Lösungen betrachtet. Wenn wir es nur ein wenig variieren, hat es *gar keine* Lösung mehr:

$$\begin{aligned} x^2 + y^2 + z^2 - 6 &= 0, \\ x^3 + y^3 + z^3 - 3xyz + 4 &= 0, \\ xy + xz + yz + 3 &= 0. \end{aligned}$$

Das kann man wiederum mit Hilfe einer Gröbnerbasis sehen. Und schließlich ist die Anzahl der Lösungen über $\mathbb{C}$ des folgenden Systems unendlich:

$$\begin{aligned} z^3y - 2xy + z &= 0, \\ 3xz + y^4x - 2x^2 &= 0, \\ y^3z - 2xz &= 0. \end{aligned}$$

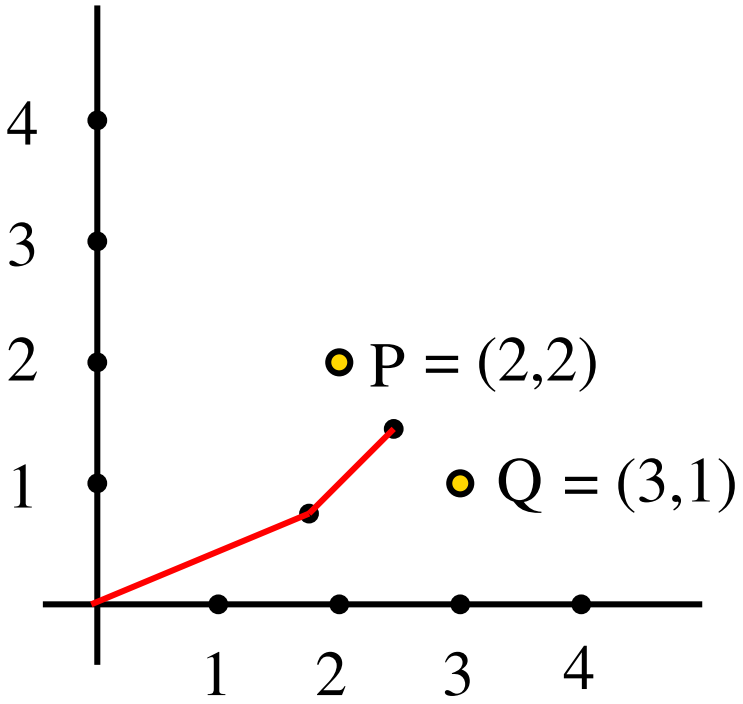
Es ist natürlich nicht schwer zu sehen, daß alle $(x, y, z) = (0, y, 0)$ Lösungen sind. Sieht man allerdings von diesen irgendwie trivialen Lösungen ab, gibt es nur noch 10 weitere. In der Tat, aus einer Gröbnerbasis erhält man dann die Relation

$$3z^{10} - 3z^7 + 30z^5 - 128z^3 + 256z - 1 = 0,$$

und sowohl x als auch y lassen sich dann durch Polynome in z ausdrücken, und sind damit für gegebenes z bestimmt.

Bemerkung 3.1.1. Jedes nicht-konstante Polynom $f(z)$ hat über $\mathbb{C}$ mindestens eine Nullstelle. Das besagt der Fundamentalsatz der Algebra. Es hat dann genau so viele Nullstellen, wie sein Grad $n \geq 1$ angibt. Allerdings sind Auflösungen durch Radikale nur bis $n \leq 4$ möglich. Für $n = 5$ gibt es schon Beispiele, die nicht mehr durch Radikale gelöst werden können: man betrachte etwa $f(z) = z^5 - 16z + 2$. Dieses Polynom 5-ten Grades ist irreduzibel über $\mathbb{Q}$ und hat genau drei reelle und zwei komplexe Nullstellen. Damit ist nach einem Satz seine Galoisgruppe die volle symmetrische Gruppe S_5, die nicht auflösbar ist. Deshalb kann es nicht durch Radikale gelöst werden.

Polynomiale Gleichungssysteme tauchen 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. Beispiele solcher Anwendungsbereiche sind u.a. die System- und Kontrolltheorie zur Steuerung von Prozessen; Gleichgewichtsreaktionen in der Kinematik; die Stabilitätsanalyse bei der Entwicklung von elektrischen Schaltungen; Bewegungsabläufe bei der Robotersteuerung, und statistische Modelle in der algebraischen Statistik. Zudem gibt es weitere Bereiche in der Kryptographie und der Kodierungstheorie.
Wir wollen ein bescheidenes Beispiel geben, in bezug auf geometrische Beschreibungen von Robotern. Angenommen wir haben folgenden Roboterarm (siehe Zeichnung).



Er besteht aus zwei Stangen der Länge 2 und 1 in der Ebene $\mathbb{R}^2$. Der Arm ist bei $O = (0, 0)$ verankert. Bezeichnen wir die zwei weiteren Punkte des Armes mit (x, y) und (z, w), so ist der Zustand des Armes vollständig durch die Koordinaten $(x, y, z, w) \in \mathbb{R}^4$ beschrieben. Es können natürlich nur bestimmte Tupel als Zustand auftreten. Sie werden durch die folgenden Gleichungen beschrieben:

$$\begin{aligned} x^2 + y^2 - 4 &= 0, \\ (x - z)^2 + (y - w)^2 - 1 &= 0. \end{aligned}$$

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, bei vorgegebenen (z, w).

1. *Beispiel:* $P = (2, 2)$. Wir wollen also die reellen Lösungen des Systems

$$\begin{aligned} x^2 + y^2 - 4 &= 0, \\ (x - 2)^2 + (y - 2)^2 - 1 &= 0 \end{aligned}$$

bestimmen. Wiederum ist eine Gröbnerbasis sehr nützlich. Sie liefert das folgende äquivalente Gleichungssystem

$$\begin{aligned} 4x - 4y - 11 &= 0, \\ 32y^2 - 88y + 57 &= 0. \end{aligned}$$

Damit erkennt man leicht, daß es genau zwei reelle Lösungen gibt:

$$(x, y) = \left(\frac{11 + \sqrt{7}}{8}, \frac{11 - \sqrt{7}}{8} \right), \quad (x, y) = \left(\frac{11 - \sqrt{7}}{8}, \frac{11 + \sqrt{7}}{8} \right).$$

Die Symmetrie der Lösungen ist natürlich geometrisch sofort ersichtlich.

2. *Beispiel:* $Q = (3, 1)$. Nun lautet das System

$$\begin{aligned} x^2 + y^2 - 4 &= 0, \\ (x-3)^2 + (y-1)^2 - 1 &= 0. \end{aligned}$$

Die Bestimmung einer Gröbnerbasis liefert das folgende äquivalente Gleichungssystem

$$\begin{aligned} 6x + 2y - 13 &= 0, \\ 40y^2 - 52y + 25 &= 0. \end{aligned}$$

Damit erhält man zwei nicht-reelle, komplex-konjugierte Lösungen

$$(x, y) = \left(\frac{39 + 3i}{20}, \frac{13 - 9i}{20}\right), \quad (x, y) = \left(\frac{39 - 3i}{20}, \frac{13 + 9i}{20}\right).$$

Der Roboterarm kann den Punkt $Q = (3, 1)$ also nicht erreichen. Das ist wiederum geometrisch vollkommen klar, da der ausgestreckte Arm ja Länge 3 hat, und der Punkt Q außerhalb des Kreises um $(0, 0)$ mit Radius 3 liegt. Man kann sich aber kompliziertere Situationen im 3-dimensionalen Raum vorstellen, wo man die Situation keineswegs geometrisch sofort versteht.

3.2 Polynomringe in mehreren Variablen

Sei R ein kommutativer Ring mit 1. Der Polynomring $R[x]$ in einer Variablen besteht aus den Polynomen

$$f = \sum_{i=0}^{n} a_i x^i$$

mit Koeffizienten a_i aus R. Ist f nicht das Nullpolynom, so heißt die größte Zahl n, für den $a_n \neq 0$ gilt, der *Grad von* f. Wir schreiben $n = \deg(f)$. Die Menge $R[x]$ wird durch die übliche Addition und Multiplikation ebenfalls zu einem kommutativen Ring mit 1:

$$\begin{aligned} \left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) &= \sum_{i=0}^{n} (a_i + b_i) x^i, \\ \left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{j=0}^{m} b_j x^j\right) &= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) x^k. \end{aligned}$$

Bei der Addition kann man durch Hinzufügen von Termen mit Null-Koeffizienten annehmen, daß beide Summen von 0 bis n laufen.
Ein Element $x \in R, x \neq 0$ heißt *Nullteiler*, wenn es 0 teilt, d.h., wenn es ein $y \in R$ gibt mit $xy = 0$.

Definition 3.1. Ein kommutativer Ring R mit 1 heißt *Integritätsring*, falls er keine Nullteiler hat.

Zum Beispiel ist $R = \mathbb{Z}$ ein Integritätsring, oder auch jeder Körper $R = K$. Andererseits ist etwa $R = \mathbb{Z}/6\mathbb{Z}$ kein Integritätsring, da $\overline{2} \cdot \overline{3} = \overline{0}$, aber beide Faktoren von Null verschieden sind. Polynomringe $R = K[x]$ über einem Körper sind ebenfalls Integritätsringe, wie folgender Satz zeigt.

Satz 3.2.1. *Der Polynomring $R[x]$ ist genau dann ein Integritätsring, wenn R ein Integritätsring ist.*

Für jedes $x \in R$ ist die Menge $(x) = xR = \{xy \mid y \in R\}$ ein Ideal. Solche Ideale heißen *Hauptideale*.

Definition 3.2. Sei R ein kommutativer Ring mit 1. Dann heißt R *Hauptidealring* (HIR), falls jedes Ideal ein Hauptideal ist.

Zum Beispiel ist $R = \mathbb{Z}$ ein HIR, weil jedes Ideal in $\mathbb{Z}$ von der Form $m\mathbb{Z}$ ist. Andererseits kann man etwa zeigen, daß der Unterring

$$\mathbb{Z}[\sqrt{-5}] = \{x + \sqrt{-5}y \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$$

von $\mathbb{C}$ kein HIR ist. Der Polynomring $\mathbb{Z}[x]$ ist ebenfalls kein HIR, wie folgender Satz zeigt.

Satz 3.2.2. *Der Polynomring $R[x]$ ist genau dann ein HIR, wenn R ein Körper ist.*

Eine stärkere Eigenschaft als HIR ist die folgende.

Definition 3.3. Ein Integritätsring R zusammen mit einer Abbildung $d\colon\ R \setminus 0 \to \mathbb{N}$ heißt *Euklidischer Ring*, falls für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit $a = qb + r$, so daß entweder $r = 0$ gilt, oder $d(r) < d(b)$.

Satz 3.2.3. *Jeder Euklidische Ring R ist ein HIR.*

Beweis. Sei $I \neq 0$ ein Ideal in R. Dann hat die Menge $\{d(b) \mid b \in I \setminus 0\}$ nicht-negativer ganzer Zahlen ein minimales Element $d(a)$ mit $a \neq 0$, d.h., es gilt $d(a) \leq d(b)$ für alle $b \in I \setminus 0$. Nach Annahme existieren für jedes $b \in I$ Elemente $q, r \in R$ mit $b = qa + r$, so daß $r = 0$ oder $d(r) < d(a)$. Der zweite Fall ist aber unmöglich, weil $r = b - qa \in I$, und $d(a)$ minimal war. Also folgt $r = 0$ und $b = qa \in (a)$. Damit erhält man $(a) \subset I \subset (a)$, und somit $I = (a)$. □

Der Ring $R = \mathbb{Z}$, zusammen mit der Abbildung $d(n) = |n|$ ist ein Euklidischer Ring. Man hat eine Division mit Rest, die zu gegebenen $a, b \in \mathbb{Z}$, $b \neq 0$ die Elemente q, r liefern mit $a = qb + r$, so daß entweder $r = 0$ oder $|r| < |b|$ gilt. Damit kann man unter

anderem den ggT von zwei Zahlen ausrechnen. Betrachten wir das Beispiel $a = 903$ und $b = 700$:

$$\begin{aligned} 903 &= 1 \cdot 700 + 203, \\ 700 &= 3 \cdot 203 + 91, \\ 203 &= 2 \cdot 91 + 21, \\ 91 &= 4 \cdot 21 + 7, \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

Es gilt also $ggT(903, 700) = 7$. Den dazugehörigen Algorithmus nennt man den *Euklidischen Algorithmus*. Damit ist $\mathbb{Z}$ auch ein HIR. Der Ring $R = \mathbb{Z}[\sqrt{-2}]$ ist ein Euklidischer Ring, und somit auch ein HIR. Hingegen ist $R = \mathbb{Z}[\sqrt{-5}]$ kein Euklidischer Ring, und auch kein HIR. Interessanterweise gibt es Ringe von diesem Typ, die zwar nicht Euklidisch sind, aber doch HIR. Ein bekanntes Beispiel ist der Ring $\mathbb{Z}[(1 + \sqrt{-19})/2]$.
Der Polynomring $R = K[x]$ über einem Körper ist Euklidisch mit $d(f) = \deg(f)$. Man erhält die Elemente q, r durch Polynomdivision. Damit kann man dann auch einen ggT von zwei Polynomen ausrechnen. Betrachten wir zum Beispiel $R = \mathbb{Q}[x]$ und die beiden Polynome $f(x) = x^3 - \frac{7}{3}x^2 + \frac{5}{3}x - \frac{1}{3}$, $g(x) = x^2 - \frac{5}{6}x + \frac{1}{6}$. Mit 12 multipliziert schreiben sie sich als $12x^3 - 28x^2 + 20x - 4$ und $12x^2 - 10x + 2$ in $\mathbb{Z}[x]$.

$$\begin{aligned} x^3 - \frac{7}{3}x^2 + \frac{5}{3}x - \frac{1}{3} &= \left(x - \frac{3}{2}\right)\left(x^2 - \frac{5}{6}x + \frac{1}{6}\right) + \frac{1}{4}\left(x - \frac{1}{3}\right), \\ x^2 - \frac{5}{6}x + \frac{1}{6} &= \left(x - \frac{1}{2}\right)\left(x - \frac{1}{3}\right) + 0. \end{aligned}$$

Daher ist $ggT(f, g) = (x - \frac{1}{3})$.

Kommen wir nun zu Polynomringen in mehreren Variablen. Wir können dabei von dem Polynomring $R_1 = R[x]$ ausgehen, und den Polynomring $R_2 = R_1[y] = R[x, y]$ betrachten. Seine Elemente lassen sich eindeutig in der Form

$$f = \sum_{i,j \geq 0} a_{i,j} x^i y^j$$

schreiben, mit $a_{i,j} \in R$, fast alle gleich Null. Wir können induktiv so fortfahren, also mit $R_3 = R_2[z] = R[x, y, z]$ und so weiter. Dann erhalten wir den Polynomring $R[x_1, \ldots, x_n]$ in n Variablen. Allerdings sind diese Polynomringe für $n \geq 2$ nun komplizierter als der Polynomring in einer Variablen. Der bedeutsamste Unterschied für uns ist, daß der Ring $K[x_1, \ldots, x_n]$ nicht mehr Euklidisch ist, und auch kein HIR mehr.

Im folgenden wollen wir also einen Polynomring $S = K[x_1, \ldots, x_n]$ über einem Körper K fixieren. Wir interessieren uns für die Ideale in S. Nach Definition ist ein Ideal $I \subseteq S$ eine Teilmenge von S mit

$$\begin{aligned} 0 &\in I, \\ f, g \in I &\Rightarrow f + g \in I, \\ f \in I, h \in S &\Rightarrow hf, fh \in I. \end{aligned}$$

Wir bezeichnen das Ideal, das von Polynomen $f_1, \ldots, f_s \in S$ erzeugt wird mit

$$(f_1, \ldots, f_s) = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_i \in S, i = 1, \ldots, s \right\}.$$

Nach dem Hilbertschen Basissatz ist jedes Ideal $I \subseteq S$ endlich erzeugt, und daher von dieser Form. Die Nullstellenmenge eines Ideals I ist gegeben durch

$$V(I) = \{x \in K^n \mid f(x) = 0 \; \forall \, f \in I\}.$$

Wegen $I = (f_1, \ldots, f_s)$ ist $x = (x_1, \ldots, x_n) \in V(I)$ gleichwertig mit einem System polynomialer Gleichungen

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0, \\ \vdots \qquad &= \vdots, \\ f_1(x_1, \ldots, x_n) &= 0. \end{aligned}$$

In diesem Kapitel wollen wir ja etwas zur Lösung solcher Gleichungssysteme sagen. Wie schon erwähnt, sollen Gröbnerbasen eine tragende Rolle dafür spielen. Sie helfen aber auch bei anderen Fragen. Sei I ein Ideal in S. Wir befassen uns mit folgenden algorithmischen Problemen bezüglich I:

(1) Gilt $V(I) \neq \emptyset$? Ist $I = S$?

(2) Polynomiale Gleichungen: man bestimme die Punkte in $V(I)$.

(3) Idealzugehörigkeitsproblem: sei $f \in S$ ein gegebenes Polynom. Gilt dann $f \in I$?

Das erste und letzte Problem wird durch die Berechnung einer Gröbnerbasis gelöst. Wie wir schon gesehen haben, hilft eine Gröbnerbasis auch sehr bei der Lösung polynomialer Gleichungssysteme, obwohl man vielleicht noch mehr tun muß, um alle Lösungen zu finden.
Falls $S = K[x]$ gilt, also $n = 1$, sind alle diese Fragen einfach zu beantworten. In der Tat, ein Ideal $I \subset K[x]$ ist dann von der Form $I = (g)$, und $f \in I = (g)$ gilt genau dann, wenn der Euklidische Algorithmus $f = qg + r$ liefert, mit $r = 0$. Damit kann das Idealzugehörigkeitsproblem durch den Euklidischen Algorithmus entschieden werden. Schon für $n = 2$ geht das so nicht mehr. Der Ring $K[x, y]$ ist nicht Euklidisch. Betrachten wir ein Beispiel. Seien $g = xy + 1$ und $h = y^2 - 1$ Polynome in $K[x, y]$. Sei

$$I = (g, h) = \{f_1(xy + 1) + f_2(y^2 - 1) \mid f_1, f_2 \in K[x, y]\}.$$

Wir wollen wissen, ob das Polynom $f = xy^2 - x$ in I liegt oder nicht. Wir haben die Darstellung $f = y \cdot g + 0 \cdot h + r$ mit $r(x) = -(x + y) \neq 0$. Wenn die Division mit Rest eindeutig wäre, könnten wir $f \notin I$ schließen. Das ist aber falsch. Es gilt $f \in I$, da wir auch $f = 0 \cdot g + x \cdot h + 0$ schreiben können.

Unser Ziel ist es nun, eine geeignete Basis für I zu finden, so daß man eine Division mit Rest hat, die die richtige Antwort zu dem Idealzugehörigkeitsproblem liefert. Tatsächlich existiert so eine Basis, nämlich eine Gröbnerbasis. Um sie einzuführen, brauchen wir Monomordnungen, Monomideale, und die multivariate Division.

3.3 Monomordnungen

Sei $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ ein n-Tupel nicht-negativer ganzer Zahlen. Wir schreiben

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

für ein Monom in $S = K[x_1, \ldots, x_n]$. Wir möchten die Monome, die als Terme in einem Polynom auftauchen, eindeutig ordnen, sei es in aufsteigender oder absteigender Reihenfolge.

Definition 3.4. Eine Relation $\leq$ heißt *partielle Ordnung* auf einer Menge S, falls sie folgende Axiome erfüllt:

(1) Reflexivität: $a \leq a$ für alle $a \in S$.

(2) Antisymmetrie: $a \leq b$ und $b \leq a$ implizieren $a = b$ für alle $a, b \in S$.

(3) Transitivität: $a \leq b$ und $b \leq c$ implizieren $a \leq c$ für alle $a, b, c \in S$.

A Partialordnung auf S heißt *Totalordnung*, falls $a \leq b$ oder $b \leq a$ gilt für je zwei Elemente $a, b \in S$. Diese Eigenschaft impliziert die Reflexivität.

Beispiel 3.3.1. *Die Menge $2^{\mathbb{N}}$ aller Teilmengen von $\mathbb{N}$ ist eine partielle geordnete Menge bezüglich der Inklusion $\subseteq$, aber keine Totalordnung.*

Für Polynomringe sind auch die folgenden Ordnungen relevant:

Definition 3.5. Eine *Wohlordnung* auf einer Menge S ist eine Totalordnung auf S mit der Eigenschaft, daß jede nicht-leere Teilmenge von S ein kleinstes Eelment bezüglich dieser Ordnung hat.

Beispiel 3.3.2. *Die Standardordnung $\leq$ auf $\mathbb{N}$ ist eine Wohlordnung. Auf $\mathbb{Z}$ hingegen ist sie keine Wohlordnung, da zum Beispiel die Teilmenge der negativen ganzen Zahlen kein kleinstes Element enthält.*

Definition 3.6. Eine *Monomordnung* auf $S = K[x_1, \ldots, x_n]$ ist eine Relation $\prec$ auf $\mathbb{N}^n$, so daß gilt:

(1) $\prec$ ist eine Wohlordnung auf $\mathbb{N}^n$.

(2) $\alpha \prec \beta$ impliziert $(\alpha + \gamma) \prec (\beta + \gamma)$ für alle $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Es gilt das folgende Resultat, siehe [2].

Lemma 3.3.3. *Eine Totalordnung $\prec$ auf $\mathbb{N}^n$ ist genau dann eine Wohlordnung wenn jede echt absteigende Sequenz in $\mathbb{N}^n$*

$$\alpha(1) \succ \alpha(2) \succ \alpha(3) \succ \cdots$$

schließlich endet.

Definition 3.7 (Lexikographische Ordnung)**.** Sei $\alpha = (\alpha_1, \ldots, \alpha_n)$ und $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$. Wir definieren $\alpha \prec_{lex} \beta$, falls der erste von Null verschiedene Eintrag von links gesehen in der Vektordifferenz $\alpha - \beta \in \mathbb{Z}^n$ negativ ist.

Beispiel 3.3.4. *Sei $n = 3$, $S = K[x, y, z]$ und*

$$\begin{aligned} \alpha &= (0, 4, 0) \leftrightarrow y^4 \\ \beta &= (1, 1, 2) \leftrightarrow xyz^2 \\ \gamma &= (1, 2, 1) \leftrightarrow xy^2z \\ \delta &= (3, 0, 0) \leftrightarrow x^3 \end{aligned}$$

Dann gilt $\alpha \prec_{lex} \beta \prec_{lex} \gamma \prec_{lex} \delta$.

Definition 3.8 (Graduierte lexikographische Ordnung)**.** Seien $\alpha = (\alpha_1, \ldots, \alpha_n)$ und $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$. Sei $|\alpha| = \sum_{i=1}^n \alpha_i$. Wir definieren $\alpha \prec_{grlex} \beta$, falls gilt

$$|\alpha| < |\beta|, \text{ oder } |\alpha| = |\beta| \text{ and } \alpha \prec_{lex} \beta.$$

Mit anderen Worten, *grlex* ordnet die Monome zuerst nach Totalgrad, und entscheidet dann im "tie-break" mit der lexikographischen Ordnung. Für obiges Beispiel von $\alpha, \beta, \gamma, \delta$ erhalten wir

$$\delta \prec_{grlex} \alpha \prec_{grlex} \beta \prec_{grlex} \gamma.$$

In der Tat, die Entscheidung $\alpha \prec_{grlex} \beta \prec_{grlex} \gamma$ fällt durch tie-break. Wir haben $|\alpha| = |\beta| = |\gamma| = 4$.

Definition 3.9 (Graduierte reverslexikographische Ordnung)**.** Seien $\alpha = (\alpha_1, \ldots, \alpha_n)$ und $\beta = (\beta_1, \ldots, \beta_n)$ in $\mathbb{N}^n$. Wir definieren $\alpha \prec_{grevlex} \beta$, falls $|\alpha| < |\beta|$, oder falls $|\alpha| = |\beta|$ und der erste von Null verschiedene Eintrag von rechts in $\alpha - \beta \in \mathbb{Z}^n$ positiv ist.

Für unser Standardbeispiel haben wir

$$\delta \prec_{grevlex} \beta \prec_{grevlex} \gamma \prec_{grevlex} \alpha.$$

Wir haben $\beta \prec_{grevlex} \gamma$, weil $\beta - \gamma = (0, -1, 1)$ ist. Man beachte, daß *grevlex* nicht durch Umordnung der Variablen aus *grlex* entsteht, wie der Name vielleicht vermuten lässt.

Satz 3.3.5. *Die Ordnungen* `lex`*,* `grlex` *und* `grevlex` *sind Monomordnungen auf $\mathbb{N}^n$.*

Für $n = 1$ sind diese Monomordnungen übrigens identisch. Sobald wir eine Monomordnung $\prec$ auf $\mathbb{N}^n$ fixiert haben, können wir die Monome eines Polynoms $f \in S$ eindeutig in bezug auf $\prec$ anordnen.

Beispiel 3.3.6. *Man betrachte das Polynom $f = 4xyz^2 + 4x^3 - 5y^4 + 7xy^2z$ in $\mathbb{Q}[x, y, z]$.*

Bezüglich *lex* würden wir die Terme von f wie folgt absteigend ordnen

$$f = 4x^3 + 7xy^2z + 4xyz^2 - 5y^4,$$

während wir für *grlex*

$$f = 7xy^2z + 4xyz^2 - 5y^4 + 4x^3$$

hätten, und für *grevlex* schließlich

$$f = -5y^4 + 7xy^2z + 4xyz^2 + 4x^3.$$

Bemerkung 3.3.7. Es gibt eine weitere Ordnung *alex*, definiert durch

$$\alpha \prec_{alex} \beta \Leftrightarrow \beta \prec_{lex} \alpha.$$

Das ist aber keine Monomordnung auf $\mathbb{N}^n$, weil es keine Wohlordnung ist: betrachte die Teilmenge $\mathbb{N} \times \{0\} \subset \mathbb{N}^2$. Dann wird die echt absteigende Folge in $\mathbb{N}^2$

$$(0,0) \succ_{alex} (1,0) \succ_{alex} (2,0) \succ_{alex} \cdots$$

nicht enden.

Definition 3.10. Sei $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$ ein von Null verschiedenes Polynom in S und $\prec$ eine Monomordnung.

(1) Der *Multigrad* von f ist $\mathrm{m}deg(f) = \max_\prec\{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\}$.

(2) Der *Leitkoeffizient* von f ist $\mathrm{l}c(f) = c_{\mathrm{m}deg(f)}$.

(3) Das *führende Monom* von f ist $\mathrm{l}m(f) = x^{\mathrm{m}deg(f)}$.

(4) Der *führende Term* von f ist $\mathrm{l}t(f) = \mathrm{l}c(f) \cdot \mathrm{l}m(f)$.

Beispiel 3.3.8. *Betrachten wir wieder das Polynom*

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

Die folgende Tabelle zeigt die definierten Begriffe für f.

Ordnung	$\prec_{lex}$	$\prec_{grlex}$	$\prec_{grevlex}$
$\mathrm{m}deg(f)$	$(3,0,0)$	$(1,2,1)$	$(0,4,0)$
$\mathrm{l}c(f)$	4	7	-5
$\mathrm{l}m(f)$	x^3	xy^2z	y^4
$\mathrm{l}t(f)$	$4x^3$	$7xy^2z$	$-5y^4$

Für das Nullpolynom kann man $\mathrm{m}deg(0) = -\infty \in \overline{\mathbb{N}^n}$ definieren. Man hat folgendes Resultat.

Lemma 3.3.9. *Sei $\prec$ eine Monomordnung auf $\mathbb{N}^n$ und $f, g \in S$. Dann gilt:*

(1) $\mathrm{m}deg(fg) = \mathrm{m}deg(f) + \mathrm{m}deg(g)$.

(2) $\mathrm{m}deg(f+g) \prec \max_\prec\{\mathrm{m}deg(f), \mathrm{m}deg(g)\}$.

(3) Gilt $\mathrm{m}deg(f) \neq \mathrm{m}deg(g)$*, so folgt sogar*

$$\mathrm{m}deg(f+g) = \max_\prec\{\mathrm{m}deg(f), \mathrm{m}deg(g)\}.$$

3.4 Multivariate Division

Wir wollen einen Divisionsalgorithmus für Polynome in mehreren Variablen vorstellen. Unser Ziel ist es, ein Polynom $f \in S$ durch Polynome $f_1, \ldots, f_s \in S$ zu teilen, i.e., f in der Form

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

auszudrücken. Der Algorithmus geht wie folgt:

Input: Polynome $f, f_1, \ldots, f_s \in S$, ungleich Null, und eine Monomordnung $\prec$ auf $\mathbb{N}^n$.

Output: Polynome $q_1, \ldots, q_s, r \in S$ mit $f = q_1 f_1 \cdots + q_s f_s + r$, so daß kein Monom in r durch einen der führenden Terme $\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s)$ teilbar ist.

1. $r \leftarrow 0$, $p \leftarrow f$.
   for $i = 1, \ldots, s$ do $q_i \leftarrow 0$.
2. while $p \neq 0$ do
   if $\mathrm{lt}(f_i) \mid \mathrm{lt}(p)$ for some $1 \leq i \leq s$, then choose some such i,

$$q_i \leftarrow q_i + \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)}, \quad p \leftarrow p - \frac{\mathrm{lt}(p)}{\mathrm{lt}(f_i)} f_i$$

   else $r \leftarrow r + \mathrm{lt}(p)$, $p \leftarrow p - \mathrm{lt}(p)$.
3. return $q_1, \ldots, q_s, r$.

Man beachte aber, daß das Resultat dieses Algorithmus noch nicht eindeutig ist - wir haben noch die Wahl eines möglichen Index i wo $\mathrm{lt}(f_i)$ den führenden Term $\mathrm{lt}(p)$ teilt. Wir können aber Eindeutigkeit herstellen, indem wir immer den *kleinsten Index* i wählen.

Beispiel 3.4.1. *Sei $S = K[x, y]$, versehen mit der lexikographischen Ordnung $\prec$, und $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$. Dann liefert der Algorithmus $q_1 = x + y$, $q_2 = 1$ und $r = x + y + 1$, also*

$$f = (x + y)(xy - 1) + (y^2 - 1) + (x + y + 1).$$

Man beachte, daß $x^2y \succ xy^2 \succ y^2$, und $\mathrm{lt}(f_1) = xy$, $\mathrm{lt}(f_2) = y^2$ gilt. Dann sind die Schritte im Algorithmus wie folgt:

1. $r = 0$, $p = x^2y + xy^2 + y^2$, $q_1 = q_2 = 0$.
2. $\mathrm{lt}(f_1) \mid \mathrm{lt}(p)$, d.h., für $i = 1$. Dann folgt

$$q_1 = 0 + \frac{x^2y}{xy} = x,$$
$$p = (x^2y + xy^2 + y^2) - \frac{x^2y}{xy}(xy - 1) = xy^2 + x + y^2.$$

Dann ist $\mathrm{lt}(f_1) \mid \mathrm{lt}(p)$, aber auch $\mathrm{lt}(f_2) \mid \mathrm{lt}(p)$. Also haben wir zwei Möglichkeiten, entweder $i = 1$ oder $i = 2$. Wenn wir $i = 1$ nehmen, folgt

$$q_1 = x + \frac{xy^2}{xy} = x + y,$$
$$p = (xy^2 + x + y^2) - \frac{xy^2}{xy}(xy - 1) = x + y^2 + y.$$

Nun gibt es keinen Index i mit $\mathrm{lt}(f_i) \mid \mathrm{lt}(p)$. Der Algorithmus liefert dann

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

es folgt $\mathrm{lt}(f_2) \mid \mathrm{lt}(p) = y^2$, so daß

$$q_2 = 0 + \frac{y^2}{y^2} = 1,$$
$$p = (y^2 + y) - \frac{y^2}{y^2}(y^2 - 1) = y + 1.$$

Hier gilt $\mathrm{lt}(f_i) \nmid \mathrm{lt}(p)$ für alle i, so daß

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

Wiederum ist $\mathrm{lt}(f_i) \nmid \mathrm{lt}(p)$ für alle i, so daß

$$r = x + y + 1,$$
$$p = 0,$$

und der Algorithmus terminiert. Der Output ist $q_1 = x + y$, $q_2 = 1$ and $r = x + y + 1$.

Bemerkung 3.4.2. Hätten wir oben die andere Wahl $i = 2$ getroffen, so hätten wir $q_1 = x$, $q_2 = x + 1$ and $r = 2x + 1$, und

$$f = x(xy - 1) + (x + 1)(y^2 - 1) + (2x + 1).$$

erhalten.

Definition 3.11. Das Polynom r, daß 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

$$r = f \mod (f_1, \ldots, f_s).$$

Eine natürliche Frage ist nun, ob dieser Divisionsalgorithmus das Idealzugehörigkeitsproblem löst. In jedem Fall wissen wir, wenn wir $r = 0$ nach Division erhalten, daß $f = q_1 f_1 + \ldots + q_s f_s$ gilt, und daher f tatsächlich zu dem Ideal $I = (f_1, \ldots, f_s)$ gehört. Also ist die Bedingung $r = 0$ eine *notwendige Bedingung* für Idealzugehörigkeit. Leider ist sie keine hinreichende Bedingung, wie das folgende Beispiel zeigt (das wir schon aus Abschnitt 3.2 kennen).

Beispiel 3.4.3. *Sei $f = xy^2 - x$ und $f_1 = xy + 1$, $f_2 = y^2 - 1$ in $K[x, y]$. Dann ist f im Ideal $I = (f_1, f_2)$ enthalten, aber $r = f \mod (f_1, f_2) = -(x + y) \neq 0$.*

In der Tat, das Resultat der multivariaten Division ist

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

aber wegen $f = 0 \cdot f_1 + x \cdot f_2 + 0$ ist $f \in (f_1, f_2)$.

Wir können diese Situation aber reparieren, indem wir ein "gutes" Erzeugendensystem für das Ideal $I = (f_1, \ldots, f_s)$ finden, so daß die Bedingung $r = 0$ tatsächlich äquivalent zur Idealzugehörigkeit ist. Natürlich ist es a priori überhaupt nicht klar, ob es eine solche "gute" Menge gibt. Wir werden aber sehen, daß eine *Gröbnerbasis* genau eine solche gute Menge ist.

3.5 Monomideale und Dicksons Lemma

Monomideale in S stellen sich als sehr wichtig für uns heraus.

Definition 3.12. Ein Ideal $I \subseteq S$ heißt *Monomideal*, falls es eine Teilmenge $A \subseteq \mathbb{N}^n$ gibt mit $I = \langle x^A \rangle = \langle \{x^\alpha \mid \alpha \in A\} \rangle$.

Mit anderen Worten, I ist durch Monome mit Exponenten von A erzeugt. Man betrachte zum Beispiel $A = \{(4, 2), (3, 4), (2, 5)\} \subset \mathbb{N}^2$. Dann ist $I = (x^4y^2, x^3y^4, x^2y^5) \subset K[x, y]$ das zu A assoziierte Monomideal.

Beispiel 3.5.1. *Sei $n = 2$ und $S = K[x, y]$. Dann ist $I = (x^2 - y, x^2 + y)$ ein Monomideal, $I = (x + y, y^2 - 1)$ hingegen nicht (siehe 3.5.6).*

In der Tat, $I = (x^2 - y, x^2 + y) = (x^2, y)$.

Lemma 3.5.2. *Sei $I = \langle x^A \rangle$ ein Monomideal von S und $\beta \in \mathbb{N}^n$. Dann gilt $x^\beta \in I$ genau dann, wenn es ein $\alpha \in A$ gibt mit $x^\alpha \mid x^\beta$.*

Bemerkung 3.5.3. Man beachte, daß $x^\alpha \mid x^\beta$ genau dann gilt, wenn $x^\beta = x^\alpha x^\gamma$ für ein $\gamma \in \mathbb{N}^n$. Das ist äquivalent zu $\beta = \alpha + \gamma$. Mit anderen Worten, die Exponenten aller Monome, die durch x^α teilbar sind, sind gegeben durch die Menge $\alpha + \mathbb{N}^n = \{\alpha + \gamma \mid \gamma \in \mathbb{N}^n\}$.

Man betrachte zum Beispiel das Monomideal $I = (y^3, xy^2, x^3y)$ in $K[x, y]$. Die Exponenten der Monome in I bilden die Menge

$$\left((0,3) + \mathbb{N}^2\right) \cup \left((1,2) + \mathbb{N}^2\right) \cup \left((3,1) + \mathbb{N}^2\right).$$

Man kann sie sich in der Ebene als die Gitterpunkte vorstellen, die über und rechts von den drei angegebenen Punkten liegen.

Lemma 3.5.4. *Sei I ein Monomideal und $f \in S$. Dann sind die folgenden Aussagen äquivalent.*

(1) Es gilt $f \in I$.

(2) Jeder Term von f liegt in I.

(3) f ist eine K-lineare Kombination von Monomen in I.

Beweis. Die Implikationen (2) $\Rightarrow$ (3) $\Rightarrow$ (1) sind klar und gelten für jedes Ideal von S. Die Folgerung (1) $\Rightarrow$ (2) hingegen ist nicht immer wahr. Hier braucht man, daß I ein Monomideal ist. □

Bemerkung 3.5.5. In der Tat, I ist genau dann ein Monomideal wenn für alle $f \in I$ jeder Term von f schon in I liegt.

Beispiel 3.5.6. *Sei $I = (x + y, y^2 - 1)$ wie oben, in $K[x, y]$. Dann ist $x + y \in I$, aber $x \notin I$, $y \notin I$. Also ist I kein Monomideal.*

Wegen (3) ist jedes Monomideal eindeutig durch seine Monome bestimmt. Wir erhalten also folgendes Korollar.

Korollar 3.5.7. *Zwei Monomideale stimmen genau dann überein, wenn sie die gleichen Monome enthalten.*

Theorem 3.5.8 (Dicksons Lemma)**.** *Jedes Monomideal $I = \langle x^A \rangle$ wird von endlich vielen Monomen erzeugt, d.h., für alle $A \subseteq \mathbb{N}^n$ gibt es eine endliche Teilmenge $B \subseteq A$ mit $I = \langle x^A \rangle = \langle x^B \rangle$.*

Es gibt einen konstruktiven Beweis, der nicht den Hilbertschen Basissatz verwendet. Wir verweisen auf [2].

Beispiel 3.5.9. *Sei $A = \{(\alpha_1, \alpha_2) \in \mathbb{N}^2 \mid 6\alpha_2 = \alpha_1^2 - 7\alpha_1 + 18\}$ und $I = \langle x^A \rangle$. Dann ist die Teilmenge B der minimalen Elemente von A gegeben durch*

$$B = \{(0,3), (1,2), (3,1)\}.$$

Also folgt $I = \langle x^A \rangle = \langle y^3, xy^2, x^3y \rangle$.
Man beachte, dass A eine unendliche Menge ist, und $\alpha_2 \geq 1$ gilt, da $\alpha_1^2 - 7\alpha_1 + 18 = 0$ keine ganzzahligen Lösungen hat, wegen negativer Diskriminante.

3.6 Gröbnerbasen

Angenommen, wir haben eine Monomordnung auf $\mathbb{N}^n$ fixiert. Dann hat jedes $f \in S$ einen eindeutigen führenden Term $\mathrm{lt}(f)$. Für jede Teilmenge $P \subseteq S = K[x_1, \ldots, x_n]$ definieren wir die Menge ihrer führenden Terme wie folgt.

Definition 3.13. Für $P \subseteq S$ setzen wir $\mathrm{lt}(P) = \{\mathrm{lt}(f) \mid f \in P\}$. Es bezeichne $\langle \mathrm{lt}(P) \rangle$ das Ideal, das von den Elementen aus $\mathrm{lt}(P)$ erzeugt wird.

Wegen Dicksons Lemma existiert für jedes Ideal I von S eine endliche Menge $P \subseteq I$ mit $\langle \mathrm{lt}(P) \rangle \subseteq \langle \mathrm{lt}(I) \rangle$: in der Tat, sei $P = \{f_1, \ldots, f_s\}$ und $I = \langle f_1, \ldots, f_s \rangle = (f_1, \ldots, f_s)$. Dann gilt

$$\langle \mathrm{lt}(P) \rangle = \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle \subseteq \langle \mathrm{lt}(I) \rangle.$$

Hier gilt allerdings im allgemeinen keine Gleichheit, denn $\langle \mathrm{lt}(I) \rangle$ kann echt größer sein als $\langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle$, obwohl $I = \langle f_1, \ldots, f_s \rangle$. Hier ist ein Beispiel.

Beispiel 3.6.1. *Sei $I = \langle f_1, f_2 \rangle$ gegeben durch $f_1 = x^3 - 2xy$ und $f_2 = x^2y + x - 2y^2$ in $K[x, y]$, zusammen mit der Ordnung* grlex. *Dann ist $x^2 \in \langle \mathrm{lt}(I) \rangle$, aber $x^2 \notin \langle \mathrm{lt}(f_1), \mathrm{lt}(f_2) \rangle = \langle x^3, x^2y \rangle$.*

In der Tat gilt

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

Aber x^2 ist nicht teilbar durch $\mathrm{lt}(f_1) = x^3$ oder $\mathrm{lt}(f_2) = x^2y$, so daß $x^2 \notin \langle x^3, x^2y \rangle$ wegen Lemma 3.5.2. Andererseits haben wir aber folgendes Resultat:

Lemma 3.6.2. *Sei $I \subseteq S$ ein Ideal und $P \subseteq I$ eine endliche Menge mit $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(P) \rangle$, Dann folgt $\langle P \rangle = I$.*

Beweis. Sei $P = \{f_1, \ldots, f_s\}$ und $f \in I$. Dann liefert der multivariate Divisionsalgorithmus

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

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. Da aber $r = f - q_1 f_1 - \cdots - q_s f_s \in I$ gilt, folgt

$$\mathrm{lt}(r) \in \mathrm{lt}(I) \subseteq \langle \mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_s) \rangle.$$

Das widerspricht der Teilbarkeit wegen Lemma 3.5.2, und wir erhalten $r = 0$ und $f \in \langle f_1, \ldots, f_s \rangle = \langle P \rangle$. □

Tatsächlich ist $\langle \mathrm{lt}(I) \rangle$ ein Monomideal, und wir können Dicksons Lemma anwenden.

Satz 3.6.3. *Sei $I \subseteq S$ ein Ideal. Dann ist $\langle \mathrm{lt}(I) \rangle$ ein Monomideal, und es gibt $g_1, \ldots, g_s \in I$ mit $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$.*

Beweis. Die führenden Monome $lm(g)$ der Elemente $g \in I$ ungleich Null erzeugen das Monomideal $\langle lm(g) \mid g \in I, g \neq 0\rangle$. Da $lm(g)$ und $lt(g)$ sich nur durch eine von Null verschiedene Konstante unterscheiden, ist dieses Ideal gleich $\langle lt(g) \mid g \in I, g \neq 0\rangle = \langle lt(I)\rangle$. Da $\langle lt(I)\rangle$ von den Monomen $lm(g)$ erzeugt wird, für $g \in I, g \neq 0$, besagt das Lemma von Dickson, daß endlich viele davon schon das Ideal erzeugen, d.h.,

$$\langle lt(I)\rangle = \langle lm(g_1), \ldots, lm(g_s)\rangle = \langle lt(g_1), \ldots, lt(g_s)\rangle.$$

□

Damit erhält man folgenden bekannten Satz.

Theorem 3.6.4 (Hilberts Basissatz)**.** *Jedes Ideal $I \subseteq S$ ist endlich erzeugt: es gibt eine endliche Menge $P \subseteq I$ mit $\langle P\rangle = I$ und $\langle lt(P)\rangle = \langle lt(I)\rangle$.*

Das Nullideal ist ein gewisser Sonderfall, es wird durch $f = 0$ erzeugt. Die endliche Menge $P = \{g_1, \ldots, g_s\}$ heißt auch *Basis* von I, da es I als Ideal erzeugt, wegen Lemma 3.6.2. Sie hat die schöne Eigenschaft, daß $\langle lt(I)\rangle = \langle lt(g_1), \ldots, lt(g_s)\rangle$ gilt. Wie wir in Beispiel 3.6.1 gesehen haben, haben nicht alle Basen diese Eigenschaft. Deshalb bekommen diese speziellen Basen einen besonderen Namen.

Definition 3.14. Sei $I \subseteq S$ eine Ideal und fixiere eine Monomordnung auf $\mathbb{N}^n$. Eine endliche Teilmenge $G \subseteq I$ heißt **Gröbnerbasis** für I, falls $\langle lt(G)\rangle = \langle lt(I)\rangle$ gilt.

Korollar 3.6.5. *Man fixiere eine Monomordnung auf $\mathbb{N}^n$. Dann hat jedes Ideal $I \subseteq S$ eine Gröbnerbasis.*

Wir setzen Beispiel 3.6.1 fort:

Beispiel 3.6.6. *Sei $I = \langle f_1, f_2\rangle$, mit $f_1 = x^3 - 2xy$ und $f_2 = x^2y + x - 2y^2$ in $K[x, y]$, mit der Ordnung grlex. Dann ist $G = \{f_1, f_2\}$* `keine` *Gröbnerbasis. Eine mögliche Gröbnerbasis ist etwa*

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

Wir haben schon gesehen, daß $\langle lt(G)\rangle = \langle lt(f_1), lt(f_2)\rangle \neq \langle lt(I)\rangle$ gilt, wegen

$$x^2 \in \langle lt(I)\rangle \setminus \langle lt(f_1), lt(f_2)\rangle.$$

Also ist $G = \{f_1, f_2\}$ keine Gröbnerbasis. Wir werden noch sehen, wie man eine Gröbnerbasis berechnen kann.

Beispiel 3.6.7. *Sei $I = \langle g_1, g_2\rangle$ in $K[x, y, z]$ mit der Ordnung* `lex`*, wobei $g_1 = x + z$ und $g_2 = y - z$. Dann ist $G = \{g_1, g_2\}$ eine Gröbnerbasis von I.*

In diesem Fall können wir direkt die Definition überprüfen. Wir müssen zeigen, daß

$$\langle lt(I)\rangle \subseteq \langle lt(G)\rangle = \langle lt(g_1), lt(g_2)\rangle = \langle x, y\rangle$$

gilt, d.h., daß der führende Term eines jeden Polynoms $f \in I \setminus 0$ in $\langle x, y \rangle$ liegt. Wegen Lemma 3.5.2 ist das gleichwertig 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 nur in z sein. 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 $t \in K$, wegen $g_i(-t, t, t) = 0$. Insbesondere verschwindet f auf allen Punkten $(-t, t, t) \in V(I)$, d.h., $f(t) = 0$ für alle $t \in K$. Das bedeutet $f = 0$, also einen Widerspruch.

Bemerkung 3.6.8. Gröbnerbasen wurden 1965 durch Bruno Buchberger eingeführt. Er benannte sie nach seinem Lehrer Wolfgang Gröbner (1899-1980).

Die multivariate Division liefert auch folgendes Resultat.

Satz 3.6.9. *Sei $I \subseteq S$ ein Ideal, $f \in S$ und $G = \{g_1, \ldots, g_s\}$ eine Gröbnerbasis von I. Dann existiert ein eindeutiges $r \in S$, so daß $f - r \in I$ und kein Term von r durch irgendein $\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)$ teilbar ist.*

Korollar 3.6.10. *Der Rest r bei der multivariaten Division von f durch G hängt nicht von der Reihenfolge der Elemente aus G ab. Wir schreiben*

$$r = f \mod G.$$

Diese Eigenschaft einer Gröbnerbasis löst das Idealzugehörigkeitsproblem:

Korollar 3.6.11. *Sei $I \subseteq S$ ein Ideal und $G = \{g_1, \ldots, g_s\}$ eine Gröbnerbasis von I. Für jedes Polynom $f \in S$ gilt nun $f \in I$ genau dann, wenn $r = f \mod G$ Null ist:*

$$f \in I \Leftrightarrow r = 0.$$

Beweis. Aus $r = 0$ folgt natürlich $f \in I$. Ist umgekehrt $f \in I$, dann erfüllt $f = f + 0$ die Bedingungen aus Satz 3.6.9. Also ist $r = 0$ der eindeutige Rest von f bei Division durch G. □

Bemerkung 3.6.12. Man kann leicht zeigen, daß eine Menge

$$G = \{g_1, \ldots, g_s\}$$

genau dann eine Gröbnerbasis für I ist, wenn für alle $f \in S$ gilt

$$f \in I \Leftrightarrow f \mod G = 0.$$

In der Tat, diese Eigenschaft ist äquivalent zu $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle$.

Wir wissen jetzt, daß jedes Ideal $I \subseteq S$ eine Gröbnerbasis hat. Es fehlt uns aber noch ein Algorithmus, um eine solche Basis zu berechnen. Das wird der *Buchberger Algorithmus* leisten, den wir im nächsten Abschnitt vorstellen.

Nehmen wir igendein Erzeugendensystem $\{f_1, \ldots, f_s\}$ von I. Dann liegt die Obstruktion

für diese Menge, eine Gröbnerbasis zu sein darin, daß Polynomialkombinationen der f_i auftreten könnten, deren führende Terme nicht in dem von den $\mathrm{lt}(f_i)$ erzeugten Ideal liegen. Zum Beispiel könnten sich die führenden Terme in einer geeigneten Kombination $\lambda x^\alpha f_i - \mu x^\beta f_j$ wegheben, so daß nur kleinere Terme blieben, und der neue führende Term eben nicht mehr durch irgendein $\mathrm{lt}(f_i)$ teilbar wäre. Andererseits ist $\lambda x^\alpha f_i - \mu x^\beta f_j \in I$, so daß sein führender Term in $\langle \mathrm{lt}(I) \rangle$ liegt. Dann ist aber $\{f_1, \ldots, f_s\}$ keine Gröbnerbasis.

Beispiel 3.6.13. *Sei $I = \langle f_1, f_2 \rangle$ wie in Beispiel* 3.6.1*, d.h.,*

$$\begin{aligned} f_1 &= x^3 - 2xy, \\ f_2 &= x^2 y + x - 2y^2. \end{aligned}$$

Eine geeignete Kombination ist $-yf_1 + xf_2 = x^2$, wo $\mathrm{lt}(x^2) = x^2$ weder durch $\mathrm{lt}(f_1)$ noch durch $\mathrm{lt}(f_2)$ teilbar ist.

Um dieses Kürzungsphänomen zu studieren, werden folgende Polynome eingeführt.

Definition 3.15. Seien $f, g \in S$ von Null verschiedenen Polynome mit

$$\begin{aligned} \alpha &= (\alpha_1, \ldots, \alpha_n) = \mathrm{m}deg(f), \\ \beta &= (\beta_1, \ldots, \beta_n) = \mathrm{m}deg(g), \\ \gamma &= (\max\{\alpha_1, \beta_1\}, \ldots, \max\{\alpha_n, \beta_n\}). \end{aligned}$$

Dann heißt x^γ das *kgV* von $\mathrm{l}m(f)$ and $\mathrm{l}m(g)$. Das *S-Polynom* von f und g ist definiert durch

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

Ein S-Polynom ist so angelegt, daß es ein Wegheben von führenden Termen produziert. Es gilt $S(f,g) = -S(g,f)$ und $S(f,g) \in \langle f, g \rangle$.

Beispiel 3.6.14. *Seien $f_1, f_2 \in K[x,y]$ wie oben, mit der Ordnung* `grlex`*. Dann ist $S(f_1, f_2) = -x^2$.*

Wir haben $\alpha = \mathrm{m}deg(f_1) = (3,0)$, $\beta = \mathrm{m}deg(f_2) = (2,1)$, also $\gamma = (3,1)$, und das kgV von x^3 und x^2y ist $x^\gamma = x^3y$. Also folgt

$$S(f_1, f_2) = \frac{x^3y}{x^3} \cdot f_1 - \frac{x^3y}{x^2y} \cdot f_2 = yf_1 - xf_2 = -x^2.$$

Beispiel 3.6.15. *Seien $f, g \in K[x,y]$ gegeben, mit der Ordnung* `grlex`*, durch*

$$\begin{aligned} f &= x^3y^2 - x^2y^3 + x, \\ g &= 3x^4y + y^2. \end{aligned}$$

Dann ist $S(f,g) = -x^3y^3 + x^2 - \frac{1}{3}y^3$.

Es gilt $\gamma = (4, 2)$ und

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

Bemerkung 3.6.16. Man kann zeigen, daß alles Wegkürzen, das auftreten kann, durch S-Polynome beschrieben werden kann.

Wir haben das folgende Kriterium von Buchberger, wann eine Idealbasis für $I \subseteq S$ eine Gröbnerbasis ist.

Theorem 3.6.17. *Eine endliche Menge $G = \{g_1, \ldots, g_s\}$ von Polynomen in S ist genau dann eine Gröbnerbasis für das Ideal $I = \langle G \rangle$, falls*

$$S(g_i, g_j) \mod G = 0 \quad \textit{für alle } 1 \leq i < j \leq s.$$

Beispiel 3.6.18. *Man fixiere die Ordnung* `lex` *auf $K[x, y, z]$ mit $y \succ z \succ x$. Seien $g_1 = y - x^2$, $g_2 = z - x^3$ in $K[x, y, z]$. Dann ist $G = \{g_1, g_2\}$ eine Gröbnerbasis für $I = \langle g_1, g_2 \rangle$.*

Es gilt m$deg(g_1) = (1, 0, 0)$, m$deg(g_2) = (0, 1, 0)$, so daß das kgV gleich $x^\gamma = yz$ ist, mit $\gamma = (1, 1, 0)$. Dann folgt mit multivariater Division

$$\begin{aligned} S(g_1, g_2) &= \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) \\ &= -zx^2 + yx^3 \\ &= x^3 \cdot g_1 - x^2 \cdot g_2 + 0. \end{aligned}$$

Das bedeutet $S(g_1, g_2) \mod G = 0$, so daß G nach Theorem 3.6.17 eine Gröbnerbasis ist.

Bemerkung 3.6.19. Das Ergebnis hängt von der Ordnung ab. In der Tat, G ist keine Gröbnerbasis für I bezüglich der Ordnung *lex* mit $x \succ y \succ z$.

3.7 Buchbergers Algorithmus

Wir stellen nun Buchbergers Algorthmus vor, für die Berechnung einer Gröbnerbasis. Er basiert auf dem Kriterium aus Theorem 3.6.17. Wir starten mit einem Erzeugendensystem $\{f_1, \ldots, f_s\}$ für das Ideal I, und fügen dann jedes S-Polynom hinzu, daß das Kriterium noch nicht erfüllt. Da der Ring $S = K[x_1, \ldots, x_n]$ Noethersch ist, wird dieses Verfahren nach endlich vielen Schritten terminieren. Das Resultat ist dann eine Gröbnerbasis für I. Sie muß allerdings (noch) nicht minimal oder eindeutig sein.

Input: Von Null verschiedene Polynome $f_1, \ldots, f_s \in S$, und eine Monomordnung $\prec$ auf $\mathbb{N}^n$.

Output: Eine Gröbnerbasis $G = \{g_1, \ldots g_t\}$ für das Ideal $I = \langle f_1, \ldots, f_s \rangle$ bezüglich $\prec$, mit $f_i \in G$ für alle $1 \leq i \leq s$.

1. $G \leftarrow \{f_1, \ldots, f_s\}$.
2. repeat
3. $H \leftarrow \emptyset$
   order the elements of G as $g_1, \ldots, g_t$.
   for $1 \leq i < j \leq t$ do
4. $r \leftarrow S(g_i, g_j) \mod (g_1, \ldots, g_t)$
   if $r \neq 0$ then $H \leftarrow H \cup \{r\}$.
5. if $H = \emptyset$ then return G
   else $G \leftarrow G \cup H$.

Beispiel 3.7.1. *Sei* $\{f_1, f_2\} = \{x^3 - 2xy, x^2y - 2y^2 + x\}$ *in* $K[x, y]$ *mit der Ordnung* `grlex` *und* $y \prec x$. *Dann erhalten wir die folgende Gröbnerbasis für das Ideal* $I = \langle f_1, f_2 \rangle$*:*

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

Wie wir schon gesehen haben, gilt $S(f_1, f_2) = -x^2$ und

$$S(f_1, f_2) = 0 \cdot f_1 + 0 \cdot f_2 + (-x^2).$$

Also ist $r = S(f_1, f_2) \mod (f_1, f_2) \neq 0$ und wir setzen $H = \{-x^2\} = \{f_3\}$ und $G = \{f_1, f_2, f_3\}$. Nach Konstruktion gilt dann

$$S(f_1, f_2) \mod (f_1, f_2, f_3) = 0,$$

aber leider auch $S(f_1, f_3) \mod (f_1, f_2, f_3) = -2xy \neq 0$:

$$\begin{aligned} S(f_1, f_3) &= \frac{x^3}{x^3} f_1 - \frac{x^3}{-x^2} f_3 \\ &= -2xy \end{aligned}$$

Weiterhin ist

$$\begin{aligned} S(f_2, f_3) &= \frac{x^2y}{x^2y} f_2 - \frac{x^2y}{-x^2} f_3 \\ &= -2y^2 + x, \end{aligned}$$

und

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

Deshalb setzen wir $f_4 = -2xy$, $f_5 = -2y^2 + x$ und $G = \{f_1, f_2, f_3, f_4, f_5\}$. Dann ist das Kriterium schließlich erfüllt:

$$S(f_i, f_j) \mod (f_1, \ldots, f_5) = 0 \quad \text{für alle } 1 \leq i < j \leq 5.$$

Es gilt folgender Satz.

Satz 3.7.2. *Buchbergers Algorithmus liefert eine Gröbnerbasis für I nach endlich vielen Schritten.*

Beweis. Die im Algorithmus konstruierten Mengen $G_1 \subseteq G_2 \subseteq \cdots \subseteq I$ induzieren eine aufsteigende Kette von Idealen

$$\langle \mathrm{lt}(G_1) \rangle \subseteq \langle \mathrm{lt}(G_2) \subseteq \cdots$$

Da der Ring S Noethersch ist, muß diese Kette stationär werden, d.h. es gibt ein $r \geq 1$

$$\langle \mathrm{lt}(G_n) \rangle = \langle \mathrm{lt}(G_r) \rangle$$

für alle $n \geq r$. Dann kann man zeigen, daß G_r eine Gröbnerbasis ist. □

Bemerkung 3.7.3. Die Berechnung einer Gröbnerbasis und das Idealzugehörigkeitsproblem sind im Sinne der Komplexitätstheorie ein inhärent schwieriges Problem. Mit anderen Worten, alle bekannten Algorithmen haben (im ungünstigsten Fall) eine doppeltexponentielle Laufzeit. Damit sind sie noch einmal erheblich schwieriger als die sogenannten NP-vollständigen Probleme.
Vom praktischen Standpunkt aus kann der Buchberger-Algorithmus auf verschiedene Arten beschleunigt werden, unter anderem dadurch, dass die Berechnungung überflüssiger S-Polynome vermieden wird. Trotzdem kann die Berechnung einer Gröbnerbasis in der Praxis ganz schnell unmöglich werden.

Wir wollen noch die Minimalität und Eindeutigkeit von Gröbnerbasen behandeln.

Lemma 3.7.4. *Sei G eine Gröbnerbasis für das Ideal $I \subseteq S$. Sei $p \in G$ ein Polynom mit $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\}) \rangle$. Dann ist $G \setminus \{p\}$ ebenfalls eine Gröbnerbasis für I.*

Beweis. Nach Annahme gilt $\langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$. Also gilt

$$\langle \mathrm{lt}(G \setminus \{p\}) \rangle = \langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle,$$

falls $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\}) \rangle$. Also ist $G \setminus \{p\}$ eine Gröbnerbasis für I. □

Indem wir alle Leitkoeffizienten auf 1 normieren, und alle Polynome p mit $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\})\rangle$ aus G entfernen, produzieren wir eine *minimale* Gröbnerbasis.

Definition 3.16. Eine Gröbnerbasis für ein Ideal $I \subseteq S$ heißt *minimal*, falls

(1) $\mathrm{lc}(p) = 1$ für alle $p \in G$.

(2) Es gilt $\mathrm{lt}(p) \notin \langle \mathrm{lt}(G \setminus \{p\})\rangle$ für alle $p \in G$.

Beispiel 3.7.5. *Sei* $I = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$ *in* $K[x,y]$ *mit der Ordnung* `grlex` *und* $y \prec x$. *Dann ist die Gröbnerbasis*

$$G = \{f_1, \ldots, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}$$

nicht minimal. Hingegen ist die folgende Gröbnerbasis $G' \subset G$ *minimal:*

$$G' = \{g_3, g_4, g_5\} = \{x^2, xy, y^2 - \frac{1}{2}x\}.$$

In der Tat, zuerst werden die Leitkoeffizienten auf 1 normiert, d.h.,

$$G = \{g_1, \ldots, g_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, x^2, xy, y^2 - \frac{1}{2}x\}.$$

Dann wenden wir Lemma 3.7.4 an. Für $p = g_1$ gilt $\mathrm{lt}(p) = x^3$ und $\mathrm{lt}(p) \in \langle \mathrm{lt}(G \setminus \{p\})\rangle = \langle \mathrm{lt}(g_2), \ldots, \mathrm{lt}(g_5)\rangle$, wegen $x\,\mathrm{lt}(g_3) = x^3 = \mathrm{lt}(p)$. Deshalb ist $\{g_2, \ldots, g_5\}$ wieder eine Gröbnerbasis.
Für $p = g_2$ gilt $\mathrm{lt}(p) = x^2y = x\,\mathrm{lt}(g_4)$, und $G' = \{g_3, g_4, g_5\}$ ist wieder eine Gröbnerbasis von I. Sie ist nun minimal, da es nicht mehr möglich ist, daß ein $\mathrm{lt}(g_i)$ noch ein anderes $\mathrm{lt}(g_j)$ teilt.

Bemerkung 3.7.6. Eine minimale Gröbnerbasis muß noch nicht eindeutig sein - ein gegebenes Ideal kann sogar unendlich viele minimale Gröbnerbasen haben. Man bestrachte zum Beispiel das Ideal aus Beispiel 3.7.5. Für jedes $\lambda \in K$ ist

$$G' = \{g_3 + \lambda g_4, g_4, g_5\} = \{x^2 + \lambda xy, xy, y^2 - \frac{1}{2}x\}$$

eine minimale Gröbnerbasis von I.

Um die Eindeutigkeit zu erreichen, müssen wir den Begriff einer minimalen Gröbnerbasis noch verschärfen:

Definition 3.17. Eine Gröbnerbasis G für ein Ideal $I \subseteq S$ heißt *reduziert*, falls

(1) $\mathrm{lc}(p) = 1$ für alle $p \in G$.

(2) Für alle $p \in G$ liegt kein Monom von p in $\langle \mathrm{lt}(G \setminus \{p\})\rangle$.

Man beachte, daß eine reduzierte Gröbnerbasis auch minimal ist. Im obigen Beispiel sieht man bei dem Polynom $p = x^2 + \lambda xy$, daß das Monom λxy in $\langle \mathrm{lt}(G \setminus \{p\})\rangle$ liegt für alle $\lambda \neq 0$. Daher ist die einzige minimale Gröbnerbasis, die reduziert ist, diejenige mit $\lambda = 0$.

Im allgemeinen hat man folgendes Resultat, siehe [2].

Satz 3.7.7. *Sei $I \subseteq S$ ein von Null verschiedenes Ideal. Man fixiere eine Monomordnung. Dann besitzt I eine eindeutige reduzierte Gröbnerbasis.*

Falls $I = S$, so ist $G = \{1\}$ eine reduzierte Gröbnerbasis für I.

Nun sind wir schließlich in der Lage, die folgenden Probleme algorithmisch zu lösen:

1. *Das Idealgleichheitsproblem*: wann erzeugen zwei Mengen von Polynomen das gleiche Ideal ?

Seien $I = \langle f_1, \ldots, f_s\rangle$ und $J = \langle g_1, \ldots, g_t\rangle$ gegeben. Fixiere eine Monomordnung und berechne eine reduzierte Gröbnerbasis G_I für I, und G_J für J. Dann gilt $I = J$ genau dann, wenn $G_I = G_J$.

Übung 3.7.8. *Gegeben seien die beiden folgenden Ideale in $K[x, y]$,*

$$I = \langle x^2 + y - 1, xy - x\rangle,$$
$$J = \langle x^2 + y^2 - 1, xy - 1, x^3 + x - y\rangle.$$

Gilt $I = J$? Hinweis: $G_J = \{1\}$, also $J = K[x, y]$.

2. *Das Idealzugehörigkeitsproblem*: Gegeben sei ein Ideal

$$I = \langle f_1, \ldots, f_s\rangle.$$

Ist das Polynom $f \in S$ in I enthalten, oder nicht ?

Dazu sei G eine Gröbnerbasis von I. Sie muß nicht unbedingt reduziert sein. Es gilt dann $f \in I$ genau dann, wenn $f \mod G = 0$.

Beispiel 3.7.9. *Sei $I = \langle xz - y^2, x^3 - z^2\rangle$ in $K[x, y, z]$, mit der Ordnung* `grlex`*, und*

$$f = -4x^2y^2z^2 + y^6 + 3z^5,$$
$$g = xy - 5z^2 + x.$$

Dann gilt $f \in I$, aber $g \notin I$.

Das sieht man so: eine Gröbnerbasis von I ist gegeben durch

$$G = \{f_1, \ldots, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

Der Divisionsalgorithmus liefert

$$f = 0 \cdot f_1 + 0 \cdot f_2 + (-4z^2) \cdot f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

Das zeigt $f \in I$. Andererseits gilt $g \mod G = g \neq 0$, so daß $g \notin I$ folgt. Hier ist $\mathrm{lt}(g) = xy$ nicht in $\langle \mathrm{lt}(G) \rangle = \langle xz, x^3, x^2y^2, xy^4, y^6 \rangle$ enthalten.

3. *Das Problem der Lösung polynomialer Gleichungssysteme*: gegeben eine endliche Menge von Polynomen $\{f_1, \ldots, f_s\}$ aus S. Wir wollen das Gleichungssystem

$$f_i = 0, \quad i = 1, \ldots, s$$

lösen. Für $I = \langle f_1, \ldots, f_s \rangle$ wollen wir also alle Punkte von $V(I)$ bestimmen. Dazu können wir jede Basis von I benutzen, insbesondere also eine reduzierte Gröbnerbasis.

Beispiel 3.7.10. *Man betrachte das System $f_1 = f_2 = f_3 = 0$ in $\mathbb{C}[x, y, z]$ mit*

$$\begin{aligned} f_1 &= x^2 + y + z - 1, \\ f_2 &= x + y^2 + z - 1, \\ f_3 &= x + y + z^2 - 1. \end{aligned}$$

Dann gibt es genau fünf Lösungen für (x, y, z), nämlich

$$\begin{aligned} (x, y, z) &= (1, 0, 0), \\ &= (0, 1, 0), \\ &= (0, 0, 1), \\ &= (\sqrt{2} - 1, \sqrt{2} - 1, \sqrt{2} - 1), \\ &= (-\sqrt{2} - 1, -\sqrt{2} - 1, -\sqrt{2} - 1). \end{aligned}$$

In der Tat, eine reduzierte Gröbnerbasis bezüglich der Ordnung *lex* mit $x \succ y \succ z$ ist gegeben durch:

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2 \\ &= z^2(z - 1)^2(z^2 + 2z - 1). \end{aligned}$$

Die Lösungsmenge des Systems $g_j = 0$ ist die gleiche wie die für $f_i = 0$. Aus $g_4 = 0$ folgt $z \in \{0, 1, -1 \pm \sqrt{2}\}$. Wie wir schon in Abschnitt 3.1 vorgeführt haben, setzen wir die Werte für z einzeln ein, und bestimmen dann y und x aus den anderen Gleichungen. Für $z = 0$ zum Beispiel liefert das $y = 0, x = 1$ oder $y = 1, x = 0$. Setzen wir übrigens $x = y = z$ in den ursprünglichen Gleichungen, so reduzieren sich alle Gleichungen zu $z^2 + 2z - 1 = 0$, deren Lösungen $z = \pm\sqrt{2} - 1$ sind.

4 Algebra und Codierung

Codierungstheorie beschäftigt sich mit dem Problem, wie man Nachrichten über einen störungsanfälligen Kanal, zum Beispiel über Internet, Satellit, Schall oder ein Speichermedium, so übertragen kann, daß die ursprünglich gesendete Nachricht aus der gestörten Nachricht rekonstruiert werden kann. Um das zu erreichen, muß man die eigentliche Nachricht mit einer zusätzlichen Information senden. Diese wird manchmal als Redundanz bezeichnet, weil sie nur zur Fehlererkennung oder Fehlerkorrektur dient, und nicht zur eigentlichen Nachricht gehört.

Wir können das Prinzip an einem einfachen Beispiel verdeutlichen, dem sogenannten ISBN-Code. ISBN steht für *International Standard Book Number*, und ist ein 10-stelliger Zahlencode $x_{10}x_9 \cdots x_2x_1$, der jedes Buch international erkennbar macht. Dabei sind $x_i \in \{0, 1, 2, \ldots, 9\}$ für $2 \leq i \leq 10$ und $x_1 \in \{0, \ldots, 9, X\}$. Die ersten 9 Ziffern kennzeichnen das Erscheinungsland, den Verlag, und den Buchtitel. Die letzte Ziffer aber, die Prüfziffer, ist genau die Zusatzinformation, oder Redundanz. Die Prüfziffer x_1 wird nun so gewählt, daß gilt

$$S = \sum_{k=1}^{10} kx_k = 1x_1 + 2x_2 + \cdots 10x_{10} \equiv 0 \mod 11$$

ist. Betrachten wir zum Beispiel die ISBN-Nummer

`3-540-20521-7`

Die letzte Ziffer, nämlich 7, ist eine Prüfziffer, da

$$10 \cdot 3 + 9 \cdot 5 + 8 \cdot 4 + 7 \cdot 0 + 6 \cdot 2 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 2 + 2 \cdot 1 + 1 \cdot 7 = 154$$

tatsächlich durch 11 teilbar ist. Die Redundanz bei dieser Codierung ist recht gering, und die zwei häufigsten Übertragunsfehler beim Lesen oder Abtippen werden erkannt:

(1) Genau eine Ziffer ist falsch.

(2) Genau zwei Ziffern sind vertauscht.

Zu (1): angenommen, anstatt der Ziffer x_i wird die Ziffer $y_i \neq x_i$ übermittelt. Dann gilt $(y_i - x_i) \not\equiv 0 \mod 11$ wegen $1 \leq |y_i - x_i| \leq 9$. Deshalb gilt für die gewichtete Summe

$$\begin{aligned} S = iy_i + \sum_{k=1, k\neq i}^{10} kx_k &= i(y_i - x_i) + \sum_{k=1}^{10} kx_k \\ &\equiv i(y_i - x_i) \not\equiv 0 \mod 11. \end{aligned}$$

Hätten wir also zum Beispiel die ISBN-Nummer

8-540-20521-7

erhalten, so wüßten wir wegen $S = 204$ sofort, daß die Zahl fehlerhaft ist, denn 204 ist nicht durch 11 teilbar.

Zu (2): Angenommen, die Ziffern x_i und x_j mit $x_i \neq x_j$ werden vertauscht. Dann ist $(j-i)(x_i - x_j) \not\equiv 0 \mod 11$ wegen $1 \leq |j-i| \leq 9$. Deshalb gilt für die gewichtete Summe

$$\begin{aligned} S &= ix_j + jx_i + \sum_{k=1,k\neq i,j}^{10} kx_k = (j-i)(x_i - x_j) + \sum_{k=1}^{10} kx_k \\ &\equiv (j-i)(x_i - x_j) \not\equiv 0 \mod 11. \end{aligned}$$

Die ISBN-Zahl

3-450-20521-7

wird also wegen $S = 153 \not\equiv 0 \mod 11$ sofort als falsch entlarvt.

Wir überlassen es dem Leser, jede Menge anderer Übertragungsfehler zu finden, die durch die Prüfsumme unentdeckt bleiben. Die falsche ISBN-Nummer

3-503-20521-7

wird durch $S = 143 \equiv 0 \mod 11$ nicht entlarvt.

Wir wollen noch ein Beispiel geben, wo das Hinzufügen der Zusatzinformation, das Codieren, nicht nur Fehler entdeckt, sondern in gewissen Situationen auch korrigieren kann. Das Modell der Datenübertragung ist im allgemeinen von der folgenden Form:

$$\boxed{\text{Sender}} \to \boxed{\text{Codierer}} \to \boxed{\text{Kanal}} \to \boxed{\text{Dekodierer}} \to \boxed{\text{Empfänger}}$$

Angenommen, wir wollen 2-Bit Nachrichten senden, also 00, 10, 01 und 11. Der Codierer wiederholt die Nachricht einfach dreimal, d.h.,

$$\begin{aligned} 00 &\to 000000, \\ 10 &\to 101010, \\ 01 &\to 010101, \\ 11 &\to 111111. \end{aligned}$$

Sagen wir, über den Kanal haben wir das Codeword 101011 empfangen. Wir sehen sofort, daß mindestens 1 Fehler passiert ist. Wir vereinbaren, daß der Dekodierer dasjenige Codeword (aus der Liste der 4 Codewörter oben) auswählt, wo zum empfangenen Codeword die wenigsten Bit geändert werden müssen. In unserem Fall ist das 101010. Passiert im Kanal höchstens ein Fehler, d.h., wird höchstens ein Bit im Codeword gestört, so wird richtig dekodiert, wie man leicht überprüft. Somit kann der Fehler sogar korrigiert werden.

Wir möchten noch bemerken, daß man Nachrichten manchmal vor unerlaubten aktiven oder auch passiven Zugriff seitens Dritter schützen muß - etwa beim Homebanking oder Pay-TV. Hiermit beschäftigt sich die *Kryptographie*, und nicht die Codierungstheorie.

4.1 Grundlagen

In der Codierungstheorie geht es um die fehlerfreie Übertragung von Daten. Der Sender codiert eine Nachricht m in ein Codewort c und sendet auch c. Der Kanal produziert eine Fehler e, so daß der Empfänger das Signal $y = c + e$ erhält. Er decodiert y. Dabei sollte er mit hoher Wahrscheinlichkeit sagen können, ob ein Fehler aufgetreten ist und diesen, falls nötig, auch korrigieren können.

Definition 4.1. Ein *Code der Länge n* über dem Alphabet $F_q := \{\lambda_1, \ldots, \lambda_q\}$ ist eine Menge C von n-Tupeln aus F_q.

Solche Codes heißen auch Blockcodes: jedes Wort hat dieselbe Länge.
Oft wird $F = \{0, 1, \ldots, q-1\}$ gesetzt, und i mit $i + q\mathbb{Z}$ in $Z/q\mathbb{Z}$ identifiziert. Das hat den Vorteil, daß $F = \mathbb{Z}/q\mathbb{Z}$ die Struktur einer abelschen bzw. zyklischen Gruppe trägt. Ist $q = p^k$ eine Primzahlpotenz, so können wir F auch mit dem endlichen Körper $\mathbb{F}_q$ identifizieren. Dann sagt man auch, C ist ein *Code über q*. Für $q = 2$ spricht man von einem *binären Code*, für $q = 3$ von einem *ternären Code*.

Beispiel 4.1.1. *Ein Code C mit M Wörtern der Länge n kann als $(M \times n)$-Matrix geschrieben werden, deren Zeilen die Codewörter sind. Zum Beispiel ist*

$$C = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

ein binärer Code 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:

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Er ist 1-fehlererkennend. Wird genau 1 Bit falsch übertragen, so ist die Parität nicht mehr gerade, sondern ungerade.

Nehmen wir nun an, daß unsere Codes C Teilmengen eines Vektorraums V sind, z.B. von $V = \mathbb{F}_q^n$. Dann können wir eine Abstandsfunktion in V zum Entdecken und Korrigieren von Fehlern verwenden. R.W. Hamming hat eine solche Funktion im Jahr 1950 eingeführt.

Definition 4.2. Sei C ein Code in $V = \mathbb{F}_q^n$. Für zwei Vektoren $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_n)$ aus V ist der *Hamming-Abstand* $d(x, y)$ definiert als die Anzahl der Indizes i mit $x_i \neq y_i$.

Der Hamming-Abstand ist translationsinvariant, d.h., es gilt

$$d(x+z, y+z) = d(x, y)$$

für alle $x, y \in V$. Man hat $0 \leq d(x, y) \leq n$ für alle $x, y \in V$. Weiterhin gilt:

Lemma 4.1.2. *Der Hamming-Abstand definiert eine Metrik auf $V = \mathbb{F}_q^n$, d.h., es gilt*

(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. Es ist nur die Dreiecksungleichung nachzuweisen. Nach Definition ist $d(x, y)$ die kleinste Anzahl von Koordinatenänderungen, die man braucht, um x in y überzuführen. Diese Zahl ist aber kleiner oder gleich der kleinsten Anzahl von Änderungen, die wir brauchen, um zuerst x in z, und dann z in y zu überführen. □

Bemerkung 4.1.3. Über $\mathbb{F}_2$ ist der Hamming-Abstand das Quadrat des Euklidischen Abstandes. Es gilt dann nämlich

$$d(x, y) = \sum_{i=1}^{n} (x_i - y_i)^2 = \langle x, y \rangle^2$$

für alle $x, y \in \mathbb{F}_2^n$.

Definition 4.3. Sei C ein Code in $V = \mathbb{F}_q^n$. Die *Minimaldistanz* von C ist definiert als

$$d(C) = \min\{d(x, y) \mid x, y \in C, x \neq y\}.$$

Das *Gewicht* von $x \in V$ ist definiert als die Anzahl der Koordinaten in $x = (x_1, \ldots, x_n)$ mit $x_i \neq 0$. Es wird mit $w(x)$ bezeichnet.

Beispiel 4.1.4. *Der binäre Code C_1 aus Beispiel* 4.1.1 *hat die Minimaldistanz $d(C_1) = 2$.*

Die Zeilenvektoren von C_1 sind $x_1 = (0, 0, 0)$, $x_2 = (0, 1, 1)$, $x_3 = (1, 0, 1)$ und $x_4 = (1, 1, 0)$ aus $\mathbb{F}_2^3$. Offenbar gilt $d(x_i, x_j) = 2$ für alle $i \neq j$. Zudem ist $w(x_i) = 2$ für $i \geq 2$.

Satz 4.1.5. *Es sei C ein Code in V. Dann gilt:*

(1) Ist $d(C) \geq t + 1$, dann deckt C bis zu t Fehler in einem Wort auf. Der Dekodierer von C entdeckt also bis zu $d(C) - 1$ Fehler.

(2) Ist $d(C) \geq 2t + 1$, dann korrigiert C bis zu t Fehler in einem Wort. Der Decodierer kann also bis zu $\lfloor \frac{d(C)-1}{2} \rfloor$ Fehler über das nächstgelegene Codewort korrigieren.

Beweis. Es seien x der gesendete, und y der empfangene Vektor mit höchstens t Fehlern. Zu Punkt (1) nehmen wir nun $d(C) \geq t+1$ an. Damit müssen sich entweder x und y in mindestens $t+1$ Einträgen unterscheiden, oder es gilt $y = x$. Erstere Möglichkeit haben wir aber ausgeschlossen, da es höchstens t Fehler geben soll. Also folgt $y = x$. Somit werden $\leq t$ Fehler aufgedeckt.
Zu (2): wegen $d(x, y) \leq t$ gilt $d(y, z) \geq t+1$ für jedes andere Codewort $z \in C$ mit $z \neq x$. Denn sonst wäre

$$d(x, z) \leq d(x, y) + d(y, z) \leq t + t = 2t,$$

im Widerspruch zu $d(C) \geq 2t + 1$. □

Beispiel 4.1.6. *Der Code C_1 aus Beispiel* 4.1.1 *deckt bis zu einem Fehler auf, wegen $d(C_1) = 2 \geq t + 1$. Er korrigiert keinen Fehler.*
Der Repetitions-Code in $\mathbb{F}_2^6$

$$C = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

aus 4.1 *erfüllt $d(C) = 3$ und kann daher einen Fehler korrigieren.*

Es ist folgende Abkürzung gebräuchlich.

Definition 4.4. Ein (n, M, d)-*Code* über q ist ein Code C der Länge n in $V = \mathbb{F}_q^n$ mit M Wörtern und Minimaldistanz $d = d(C)$. Es bezeichne $A_q(n, d)$ die größte Zahl M, für die ein (n, M, d)-Code über q existiert.

Ein guter (n, M, d)-Code sollte eine kleine Länge n haben, für eine schnelle Übertragung, eine große Minimaldistanz d, für eine gute Fehlererkennung bzw. Fehlerkorrektur, und ein möglichst großes M. Die Zahl $A_q(n, d)$ spezifiziert das größt-mögliche M.

Satz 4.1.7. *Es gilt $A_q(n, 1) = q^n$ und $A_q(n, n) = q$.*

Beweis. Ist $d = 1$ für einen Code $C \subseteq \mathbb{F}_q^n$, so kann man $C = \mathbb{F}_q^n$ wählen. Das ist sicherlich maximal und C hat dann q^n Worte.
Ist C ein (n, M, n)-Code über q, so unterscheiden sich je zwei Codewörter in allen Koordinaten. Da der erste Eintrag nur q verschiedene Werte haben kann, folgt schon einmal $A_q(n, n) \leq q$. Der Repetitions-Code der Länge n über q, mit Worten $(i, i, \ldots, i)$ für $0 \leq i \leq q-1$ ist aber ein Code mit Minimaldistanz n und q Wörtern. Daher gilt $A_q(n, n) = q$. □

Die folgende Tatsache wurde von R.C. Singleton im Jahr 1964 entdeckt.

Satz 4.1.8 (Singleton-Schranke)**.** *Es gilt $A_q(n, d) \leq q^{n-d+1}$.*

Beweis. Es sei C ein (n, M, d)-Code über q. Löschen wir die letzten $d-1$ Stellen aller Codewörter, dann sind die resultierenden Vektoren der Länge $n - d + 1$ paarweise verschieden. Das bedeutet $M \leq q^{n-d+1}$. □

Für gegebene $u \in \mathbb{F}_q^n$ und $r \in \mathbb{N}$ ist die *Kugel vom Radius r um u* die Menge

$$K_r(u) = \{v \in \mathbb{F}_q^n \mid d(u,v) \leq r\}.$$

Wir können eine Formel für $|K_r(u)|$ angeben:

Lemma 4.1.9. *Eine Kugel vom Radius r in $\mathbb{F}_q^n$ mit $0 \leq r \leq n$ enthält genau*

$$\sum_{i=0}^{r} \binom{n}{i}(q-1)^i = 1 + n(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{r}(q-1)^r$$

Vektoren aus $\mathbb{F}_q^n$.

Beweis. Für gegebenes $u \in \mathbb{F}_q^n$ zählen wir die Vektoren mit Abstand i von u für $i = 0, 1, \ldots, r$. Das sind genau $\binom{n}{i}(q-1)^i$ viele Vektoren für jedes i. Durch Aufsummieren folgt die Behauptung. □

Satz 4.1.10 (Kugelpackungsschranke)**.** *Für $1 \leq d \leq n$ gilt*

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i}.$$

Beweis. Sei C ein (n, M, d)-Code mit $d = d(C) = 2t + 1$. Also sind die Kugeln $K_t(c)$ um Codewörter c disjunkt. Anders ausgedrückt, die Kugeln $K_{\lfloor (d-1)/2 \rfloor}(c)$ mit $c \in C$ sind paarweise disjunkt, und es gilt

$$\bigcup_{c \in C} K_{\lfloor \frac{d-1}{2} \rfloor}(c) \subseteq \mathbb{F}_q^n.$$

Daher folgt

$$\sum_{c \in C} |K_{\lfloor \frac{d-1}{2} \rfloor}(c)| \leq q^n.$$

Mit Lemma 4.1.9 folgt die Behauptung. □

Definition 4.5. Ein (n, M, d)-Code über q mit ungerader Minimaldistanz $d = 2t + 1$, $t \in \mathbb{N}$ heißt *perfekter Code*, wenn für die Schranke in Satz 4.1.10 Gleichheit gilt, d.h., wenn

$$A_q(n,d) = \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i}.$$

Man beachte, daß die rechte Seite dazu *ganzzahlig* sein muß. Für den Code $C = \mathbb{F}_q^n$, also mit $d = 1$, gilt $A_q(n,1) = q^n$ nach Satz 4.1.7. Er ist also ein perfekter Code. Eine große Familie von perfekten Codes sind die *Hamming-Codes*, die linear sind. Wir behandeln sie im Abschnitt 4.4.

Man kann auch eine untere Schranke für $A_q(n,d)$ angeben, in der Art wie die Kugelpackungsschranke als obere Schranke.

Satz 4.1.11 (Gilbert-Varshamov-Schranke). *Für $1 \leq d \leq n$ gilt*

$$A_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}.$$

Der einfache Beweis sei dem Leser überlassen.

Übung 4.1.12. *Man schätze $A_2(13,5)$ ab. Ist das genaue Ergebnis auch bekannt ?*

Ergebnis: Wir haben $q = 2$, $n = 13$, $d = 5$ und $V = \mathbb{F}_2^{13}$. Die obengenannten Schranken liefern dann:

Gilbert-Varshamov: $A_2(13,5) \geq 8$.
Kugelpackung: $A_2(13,5) \leq 89$.
Singleton: $A_2(13,5) \leq 512$. Eine Literatursuche ergibt, daß $A_2(13,5) = A_2(14,6) = 64$ ist.

4.2 Lineare Codes

Allgemeine Codes $C \subseteq \mathbb{F}_q^n$ sind meist schwierig zu codieren und zu decodieren. Das wird viel besser, wenn man eine zusätzliche Vektorraumstruktur voraussetzt.

Definition 4.6. Ein *linearer Code* C der Länge n über $\mathbb{F}_q$ ist ein Untervektorraum von $\mathbb{F}_q^n$.

Ist $k \leq n$ die Dimension des linearen Codes C über $\mathbb{F}_q$, so ist C ein (n, q^k, d)-Code. Es ist dann üblich, $[n,k,d]_q$ oder nur $[n,k,d]$ für (n,q^k,d) zu schreiben.
Eine $(k \times n)$-Matrix über $\mathbb{F}_q$, deren Zeilen eine Basis des Untervektorraums $U = C$ bilden, heißt dann *Erzeugermatrix* des linearen Codes $[n,k,d]$, oder kurz $[n,k]$.

Beispiel 4.2.1. *Der binäre Code*

$$C_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

aus Beispiel 4.1.1 *und* 4.1.4 *ist ein linearer $[n,k,d] = [3,2,2]$-Code mit Erzeugermatrix*

$$G = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

In der Tat, die Zeilen von C_1 sind linear abhängig über $\mathbb{F}_3$. Sie spannen einen Untervektorraum von $\mathbb{F}_2^3$ der Dimension 2 auf. Es gilt $d(C_1) = 2$.

Beispiel 4.2.2. *Der triviale Code $C = \mathbb{F}_q^n$ ist ein linearer $[n,n,1]$-Code.*

Satz 4.2.3. *Für einen linearen Code $C \leq \mathbb{F}_q^n$ gilt:*

(1) Der Hamming-Abstand zweier Codewörter x, y aus C ist identisch mit dem Gewicht, ihrer Differenz, d.h. es gilt $d(x, y) = w(x - y)$.

(2) Die Minimaldistanz von C entspricht dem minimalen Gewicht nicht-verschwindender Codewörter aus C, d.h. es gilt

$$d(C) = \min\{w(x) \mid 0 \neq x \in C\}.$$

Beweis. Da C linear ist, sind mit x und y auch stets $x-y$ in C, und auch der Nullvektor 0. Die Aussagen folgen dann aus der Tatsache, daß

$$d(x, y) = d(x - y, 0) = w(x - y)$$

für alle $x, y \in C$ gilt, da d translationsinvariant ist. □

Zur Bestimmung der Minimaldistanz eines linearen Codes braucht man also nur $M-1$ Vergleiche, bei M Wörtern in C. Im Gegensatz dazu benötigt man im allgemeinen

$$\binom{M}{2} = \frac{M(M-1)}{2}$$

Vergleiche. Bei einem linearen Code muß man zudem nicht alle Wörter auflisten. Es genügt ja eine Basis. Es gibt zahlreiche weitere Vorteile von linearen Codes, etwa bezüglich Codierung und Decodierung. Als Nachteil kann man anführen, daß es nicht so viele lineare Codes gibt, und q eine Primzahlpotenz sein muß. Allerdings kann man aber oft Codes, wo dies nicht der Fall ist, von solchen mit $q = p^n$ ableiten. Das gilt etwa für den erwähnten ISBN-Code. Man kann ihn aus dem Code

$$D = \{(x_1, \ldots, x_{10}) \in \mathbb{F}_{11}^{10} \mid \sum_{i=1}^{10} i x_i \equiv 0 \mod 11\} \subseteq \mathbb{F}_{11}^{10}$$

ableiten. Dazu löscht man alle Wörter von D, die eine Ziffer 10 in einer der ersten 9 Koordinaten haben, und ersetzt dann die Wörter $(x_1, \ldots, x_9, 10)$ mit $x_i \leq 9$ von D durch, sagen wir, $(x_1, \ldots, x_9, X)$.

Beispiel 4.2.4. *Es sei C der ternäre lineare Code mit Erzeugermatrix*

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Er ist ein $[5, 3, 2]_3$-Code, d.h. mit $n = 5$, $k = 3$, $d = 2$ und $q = 3$.

Wir wollen $d = d(C) = 2$ zeigen mit Satz 4.2.3. Nach Definition ist

$$C = \left\{ \begin{pmatrix} c_3, & c_2, & c_2 + c_3, & c_1, & c_1 + c_3 \end{pmatrix} \mid c_i \in \mathbb{F}_3 \right\} \subset \mathbb{F}_3^5.$$

Daher ist

$$w(c) = d(c,0) = c_3^2 + c_2^2 + (c_2+c_3)^2 + c_1^2 + (c_1+c_3)^2 \mod 3$$

mindestens 2 für alle $c \in C$, wobei $c_i = 0,1,2$. Das Minimum wird auch angenommen, zum Beispiel für $c_1 = 1$, $c_2 = 0$ und $c_3 = 0$. Also ist

$$d(C) = \min\{w(x) \mid 0 \neq x \in C\} = 2.$$

Definition 4.7. Sei $[n,k,d]$ ein linearer Code in $\mathbb{F}_q^n$. Eine Erzeugermatrix G von C heißt *reduziert*, falls G die Gestalt

$$G = (E_k \mid P) = \left(\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & P \\ 0 & & 1 & \end{array}\right)$$

mit $P \in M_{k,n-k}(\mathbb{F}_q)$ hat. Zwei Codes C, C' aus $\mathbb{F}_q^n$ heißen *äquivalent*, wenn es eine Permutation $\sigma \in \mathcal{S}_n$ 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 $\sigma \in \mathcal{S}_n$ eine *Symmetrie* von C. Die Menge aller Symmetrien von C bildet eine Gruppe, die mit $Sym(C)$ oder $Aut(C)$ bezeichnet wird.

Satz 4.2.5. *Zu jedem linearen Code C in $\mathbb{F}_q^n$ gibt es einen äquivalenten linearen Code mit reduzierter Erzeugermatrix.*

Beweis. Es seien C ein linearer $[n,k]_q$-Code und G eine Erzeugermatrix von C. Dann gibt es eine Permutationsmatrix $Q \in GL_n(\mathbb{F}_q)$, so daß die ersten k Spalten von $G' := GQ$ linear unabhängig sind. Also hat G' die Gestalt $(J' \mid P')$ mit $J' \in GL_k(\mathbb{F}_q)$. Unter der Basistransformation $(J')^{-1}$ besitzt der Code $C' := \mathbb{F}_q^k \cdot G'$ eine reduzierte Erzeugermatrix und ist wegen $C \cdot Q = C'$ äquivalent zu C. □

Beispiel 4.2.6. *Es sei $C \leq \mathbb{F}_2^4$ ein linearer $[4,3]_2$-Code, gegeben durch*

$$C = \{(x_1,x_2,x_3,x_4) \in \mathbb{F}_2^4 \mid \sum_{i=1}^{4} x_i = 0\}.$$

Dann besitzt C die reduzierte Erzeugermatrix

$$G = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right).$$

Der Code heißt auch *parity check code*, weil die Parität gerade ist, siehe Beispiel 4.1.1. Im allgemeinen ist der parity check code ein linearer $[n, n-1, 2]_q$-Code der Länge n, gegeben durch

$$C = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} x_i = 0\}.$$

Die Erzeugermatrix ist dann $G = (E_{n-1} \mid (-1, \ldots, -1)^t)$.

Man kann die Erzeugermatrix G eines linearen Codes auch als lineare Abbildung $\mathbb{F}_q^k \hookrightarrow \mathbb{F}_q^n$ auffassen. Diese Abbildung ist injektiv und dient als Codierer von C. Zur Decodierung verwendet man sogenannte *Kontrollmatrizen*.

Definition 4.8. Sei $C \leq \mathbb{F}_q^n$ ein linearer Code. Dann heißt

$$C^\perp := \{y \in \mathbb{F}_q^n \mid \langle x, y\rangle = 0 \text{ für alle } x \in C\}$$

der zu C *duale Code*. Eine Erzeugermatrix H von $C^\perp$ heißt *Kontrollmatrix* zu C. Im Falle $C = C^\perp$ nennen wir C *selbstdual*.

Satz 4.2.7. *Es sei $C \leq \mathbb{F}_q^n$ ein linearer $[n, k]_q$-Code. Dann gilt*

(1) Der zu C duale Code $C^\perp$ ist ein linearer $[n, n-k]_q$-Code.

(2) Die Dualisierung wirkt involutiv, d.h. $(C^\perp)^\perp = C$.

(3) Jede Kontrollmatrix H zu C liefert die Kontrollgleichung

$$C = \{x \in \mathbb{F}_q^n \mid Hx^t = 0\}.$$

Beweis. Es gilt $\dim(C) + \dim(C^\perp) = \dim(\mathbb{F}_q^n) = n$ nach dem Dimensionssatz für Vektorräume. Also ist $\dim(C^\perp) = n - k$ und $C^\perp$ ist ein linearer $[n, n-k]_q$-Code. Ebenso ist $\dim(C^\perp) + \dim(C^\perp)^\perp = n$. Es folgt $\dim(C) = \dim(C^\perp)^\perp = k$ und wegen $C \leq (C^\perp)^\perp$ die Gleichheit. Ist G die Erzeugermatrix von C, so gilt $x \in C^\perp$ genau dann, wenn $Gx^t = 0$ ist. Eine Kontrollmatrix H von C ist dann eine $(n-k) \times n$-Matrix mit $GH^t = 0$. Es folgt $C = \{x \in \mathbb{F}_q^n \mid Hx^t = 0\}$. □

Beispiel 4.2.8. *Sei $C \leq \mathbb{F}_2^4$ der lineare $[4, 2]_2$-Code mit Erzeugermatrix*

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Dann ist $C^\perp$ ein linearer $[4, 2]_2$-Code mit Erzeugermatrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Diese Matrix ist eine Kontrollmatrix zu C.

Es gilt $x = (x_1, x_2, x_3, x_4) \in C^\perp$ genau dann wenn $Gx^t = 0$, also $x_2 + x_3 + x_4 = 0$ und $x_1 + x_3 = 0$ gilt. Deshalb ist

$$C^\perp = \{(x_1, x_2, x_1, x_1 + x_2 \mid x_i \in \mathbb{F}_2\}$$

Hierbei beachte man, daß $-1 = 1$ wegen $q = 2$ ist. Die Matrix H ist offenbar eine Erzeugermatrix für $C^\perp$. Sie erfüllt die Gleichung

$$GH^t = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Es gilt die Kontrollgleichung

$$C = \{x \in \mathbb{F}_q^n \mid Hx^t = 0\} = \{(x_1, x_2, x_1 + x_2, x_2) \mid x_i \in \mathbb{F}_2\}.$$

Beispiel 4.2.9. *Der n-fache Repetitions-Code*

$$C = \{x \in \mathbb{F}_q^n \mid x_1 = \cdots = x_n\}$$

ist dual zum allgemeinen parity check code der Länge n.

C ist ein linearer $[n, 1]_q$-Code. Seine Erzeugermatrix ist $G_1 = (1, \ldots, 1)$. Daher ist

$$\begin{aligned} C^\perp &= \{x \in \mathbb{F}_q^n \mid Gx^t = 0\} \\ &= \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} x_i = 0\}. \end{aligned}$$

Das ist der parity check code. Die Kontrollmatrix zu C ist, wie schon oben erwähnt, die $n \times (n-1)$-Matrix

$$H_1 = (E_{n-1} \mid (-1, \ldots, -1)^t) = \left(\begin{array}{ccc|c} 1 & & 0 & -1 \\ & \ddots & & \vdots \\ 0 & & 1 & -1 \end{array}\right)$$

Die Kontrollmatrix hilft bei der Bestimmung der Minimaldistanz.

Satz 4.2.10. *Sei $C \leq \mathbb{F}_q^n$ ein linearer $[n, k]_q$-Code mit Kontrollmatrix H. Dann gilt*

$$\begin{aligned} d(C) &= \min\{\ell \geq 1 \mid \text{ es gibt } \ell \text{ linear abhängige Spalten in } H\} \\ &= \max\{\ell \geq 1 \mid \text{ je } \ell - 1 \text{ Spalten von } H \text{ sind linear unabhängig}\}. \end{aligned}$$

Wendet man das auf den Repetitions-Code C an, so folgt $d = n$. Er ist also ein $[n, 1, n]_q$-Code. Das folgt natürlich auch direkt aus $w(x) = n$ für alle $x \neq 0$ und $d(C) = \min\{w(x) \mid 0 \neq x \in C\}$. Der parity check code ist ein $[n, n-1, 2]_q$-Code.

Beispiel 4.2.11. *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*.*

Wir können $H = G$ wählen. Es ist $GG^t = 0$, und C ist selbstdual. Jeweils drei Spalten der Kontrollmatrix $H = G$ sind linear unabhängig. Deshalb ist nach obigem Satz $d(C) \geq 4$. Alle Zeilenvektoren von G, bis auf den ersten, haben aber Gewicht 4, weswegen das Minimum 4 angenommen wird. Also ist $d(C) = 4$.

Definition 4.9. Es sei $C \leq \mathbb{F}_q^n$ ein linearer Code. Die Anzahl aller Codewörter vom Gewicht r sei mit

$$w_r(C) := \#\{x \in C \mid w(x) = r\}$$

bezeichnet. Das homogene Polynom

$$W_C(X, Y) = \sum_{r=0}^{n} w_r(C) X^{n-r} Y^r \in \mathbb{Z}[X, Y]$$

heißt *Gewichtspolynom* von C. Die *erzeugende Funktion* von C ist durch

$$W_C(X) := W_C(X, 1) = \sum_{t=0}^{n} w_{n-t}(C) X^t \in \mathbb{Z}[X]$$

definiert.

Beispiel 4.2.12. *Es sei* $C \leq \mathbb{F}_2^7$ *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

$$W_C(X, Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7,$$
$$W_C(X) = 1 + 7X^3 + 7X^4 + X^7.$$

Es ist $n = 7$, $k = 4$ und $q = 2$. Weiterhin folgt $d = 3$ aus Satz 4.2.10. Wir können alle Worte in C nach ihrem Gewicht auflisten.

Gewicht 0 : 0000000,
Gewicht 3 : 1101000, 1010100, 0110010, 0001110, 0011001, 0100101, 1000011,
Gewicht 4 : 0111100, 1011010, 1100110, 1110001, 1001101, 0101011, 0010111,
Gewicht 7 : 1111111.

Damit ist $w_0(C) = w_7(C) = 1$, $w_3(C) = w_4(C) = 7$ und $W_i(C) = 0$ für alle anderen i. Wir erhalten obige Polynome. Zudem ist der Code *perfekt* im Sinne von 4.5. Denn C besitzt genau $q^k = 16$ Wörter, und die maximale Schranke, die Kugelpackungsschranke aus Satz 4.1.10, wird angenommen:

$$A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i} = \frac{2^7}{1+7} = 16.$$

Die Gewichtspolynome zu einem linearem Code C und seinem dualen Code $C^\perp$ erfüllen eine interessante Funktionalgleichung.

Satz 4.2.13 (MacWilliams Identität 1962)**.** *Es sei C ein linearer $[n,k]_q$-Code und $C^\perp$ sein dualer $[n,n-k]_q$-Code. Dann gilt*

$$W_{C^\perp}(X,Y) = \frac{1}{q^k} W_C(X + (q-1)Y, X - Y).$$

4.3 Endliche Körper

Zu den algebraischen Grundlagen der Codierungstheorie zählen unter anderem auch Körper, und zwar insbesondere endliche Körper. Wir stellen das wichtigste kurz zusammen.

Definition 4.10. Ein *Körper* K ist ein kommutativer Ring mit 1, bei dem alle Elemente bis auf das Nullelement Einheiten sind.

Wir erinnern daran, daß $x \neq 0$ eine Einheit ist, falls es ein $y \in K$ gibt mit $xy = 1$. Wir schreiben dann $y = x^{-1}$. Mit anderen Worten, $(K^\times, \cdot)$ ist eine multiplikative Gruppe. Wir nennen K einen *endlichen Körper*, falls K nur endlich viele Elemente hat.

Körper sind Integritätsringe, d.h., aus $xy = 0$ folgt entweder $x = 0$ oder $y = 0$. Umgekehrt sind Integritätsringe im allgemeinen keine Körper. Man betrachte den Ring $\mathbb{Z}$ der ganzen Zahlen.

Beispiel 4.3.1. *Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann ein Körper wenn m eine Primzahl ist.*

Ist $m \geq 1$ keine Primzahl, so findet man ganze Zahlen $1 < r, n < m$ mit $rn = m$. Dann gilt $\overline{rn} = \overline{m} = \overline{0}$, aber $\overline{r}, \overline{n} \neq \overline{0}$ in $\mathbb{Z}/m\mathbb{Z}$. Also ist $\mathbb{Z}/m\mathbb{Z}$ kein Integritätsring, und somit auch kein Körper.
Ist umgekehrt $m = p$ eine Primzahl und $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ ungleich Null, so ist a teilerfremd zu p und es existiert ein $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ mit $\overline{b}\overline{a} = \overline{1}$ in $\mathbb{Z}/p\mathbb{Z}$, wegen des Euklidischen Algorithmus. Damit sind alle Elemente ungleich Null Einheiten, und $\mathbb{Z}/p\mathbb{Z}$ ein Körper.

Übung 4.3.2. *Man bestimme das Inverse von $\overline{5}$ in $\mathbb{Z}/13\mathbb{Z}$.*

Der Euklidische Algorithmus liefert

$$\begin{aligned} 13 &= 5 \cdot 2 + 3, \\ 5 &= 3 \cdot 1 + 2, \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$

und dann

$$\begin{aligned} 1 &= 3 \cdot 2 - 5, \\ &= (13 - 5 \cdot 2) \cdot 2 - 5, \\ &= 13 \cdot 2 - 5 \cdot 5. \end{aligned}$$

In $\mathbb{Z}/13\mathbb{Z}$ liest sich das als $\overline{1} = \overline{0} + \overline{-5} \cdot \overline{5}$. Also ist $\overline{-5} = \overline{8}$ das Inverse zu $\overline{5}$.

Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist also ein Körper, falls er ein Integritätsring ist. Das ist kein Zufall.

Satz 4.3.3. *Ein endlicher Intergritätsring ist ein Körper.*

Beweis. In einem Integritätsring ist die Linksmultiplikation $L\colon R \to R$, $L(x) = ax$ mit $a \neq 0$ eine injektive lineare Abbildung. In der Tat, $L(x) = L(y)$ bedeutet $a(x - y) = 0$ und deshalb $x - y$, wegen $a \neq 0$. Da R endlich ist, muß L auch surjektiv sein. Das folgt aus dem Schubfachprinzip. Demnach existiert zu jedem $a \neq 0$ ein x mit $1 = L(x) = ax$. □

Sei K ein Körper. Man betrachte die Abbildung $\varphi\colon \mathbb{Z} \to K$, die durch

$$n \mapsto n \cdot 1 = 1 + 1 + \cdots + 1$$

gegeben ist. Das ist ein Ringhomomorphismus, und daher ist $\ker(\varphi)$ ein Ideal von $\mathbb{Z}$.

1. Fall: Es gilt $\ker(\varphi) = 0$, also $n \cdot 1 = 0 \Rightarrow n = 0$ in $\mathbb{Z}$. Für $n \neq 0$ ist $\varphi(n)$ dann ein invertierbares Element in K, und φ läßt sich zu einem Homomorphismus $\mathbb{Q} \hookrightarrow K$ fortsetzen, der durch

$$\frac{m}{n} \to (m \cdot 1)(n \cdot 1)^{-1}$$

gegeben ist. Somit enthält K eine Kopie des Körpers $\mathbb{Q}$. Wir sagen dann, K hat die *Charakteristik Null*.

2. Fall: Es gilt $\ker(\varphi) \neq 0$. Es gibt also ein $n \neq 0$ mit $(n \cdot 1) = 0$. Das kleinste solche n muß eine Primzahl sein, ansonsten hätte K Nullteiler. Also induziert φ einen Isomorphismus von $\mathbb{Z}/p\mathbb{Z}$ auf den Unterring

$$\{m \cdot 1 \mid m \in \mathbb{Z}\} \subseteq K.$$

In diesem Fall enthält K also eine Kopie des Körpers $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, und wir sagen dann, K hat die *Charakteristik* $p > 0$.

Wir nennen die Körper $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \ldots$, und den Körper $\mathbb{Q}$ auch *Primkörper*. Jeder Körper enthält eine Kopie von genau einem dieser Primkörper.

Satz 4.3.4. *Die Anzahl der Elemente eines endlichen Körpers K ist eine Primzahlpotenz, d.h., $|K| = p^n$.*

Beweis. Da K endlich ist, enthält K einen Primkörper $\mathbb{F}_p$. Als Vektorräume betrachtet heißt das, K ist ein endlich-dimensionaler Vektorraum über $\mathbb{F}_p$, sagen wir mit Basis $(e_1, \ldots, e_n)$. Somit hat $K = \{\sum_{i=1}^{n} \lambda_i e_i \mid \lambda_i \in \mathbb{F}_p\}$ genau p^n Elemente. □

Zu einem Körper K betrachten wir den Polynomring $K[x]$. Ein Polynom $f(x)$ vom Grad $n \geq 1$ heißt *reduzibel über* K, wenn es Polynome $g(x)$ und $h(x)$ in $K[x]$ vom Grad kleiner als n gibt mit $f(x) = g(x)h(x)$. Andernfalls heißt $f(x)$ *irreduzibel über* K.

Lemma 4.3.5. *Der Quotientenring $K[x]/(f(x))$ ist genau dann ein Körper, wenn $f(x)$ irreduzibel ist.*

Beweis. Die Restklassen modulo $f(x)$ sind repräsentiert durch Polynome

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}, \quad a_i \in K.$$

Der Beweis verläuft nun ebenso, wie der für $\mathbb{Z}/m\mathbb{Z}$, wenn m eine Primzahl ist. □

Wenn $K = \mathbb{F}_p$ ist und $f(x)$ ein normiertes Polynom vom Grad n, so hat der Körper $\mathbb{F}_p[x]/(f(x))$ genau p^n Elemente.

Beispiel 4.3.6. *Sei $K = \mathbb{F}_2$ und $f(x) = x^3 + x + 1$. Dann ist $f(x)$ irreduzibel, und*

$$\mathbb{F}_2[x]/(x^3 + x + 1) = \{a_0 + a_1 x + a_2 x^2 \mid a_i \in \mathbb{F}_2\}$$

ist ein Körper mit 8 Elementen.

Wir werden sehen, daß *jeder* endliche Körper K isomorph ist zu einem Körper der Form $\mathbb{F}_p[x]/(f(x))$. Es gibt aber auch noch andere Darstellungen. Einen Körper mit 9 Elementen erhält man zum Beispiel nicht nur durch

$$\mathbb{F}_3[x]/(x^2 + 1),$$

sondern auch durch $\mathbb{Z}[i]/(3)$. Wir benötigen folgendes Resultat.

Lemma 4.3.7. *Für jeden endlichen Körper K ist die Gruppe $K^\times$ zyklisch.*

Beispiel 4.3.8. *Für $K = \mathbb{F}_3[x]/(x^2 + 1)$ ist $K^\times$ isomorph zu C_8.*

Wir können auch einen Erzeuger angeben, wobei wir die Restklasse $\overline{x}$ wieder mit x bezeichnen. Die Potenzen von x in K sind wie folgt:

$$1, x, x^2 = -1 = 2, x^3 = 2x, x^4 = (2x)^2 = -2 = 1.$$

Also hat x die Ordnung 4 und kann kein Erzeuger von $K^\times$ sein. Besser ist es, $x + 1$ zu betrachten:

$$\begin{aligned}
(x+1)^1 &= x + 1, \quad (x+1)^2 = 2x, \\
(x+1)^3 &= 2x + 1, \quad (x+1)^4 = 2, \\
(x+1)^5 &= 2x + 2, \quad (x+1)^6 = x, \\
(x+1)^7 &= x + 2, \quad (x+1)^8 = 1.
\end{aligned}$$

Satz 4.3.9. *Jeder endliche Körper K ist isomorph zu $\mathbb{F}_p[x]/(f(x))$ für eine Primzahl p und ein normiertes, irreduzibles Polynom $f(x)$ in $\mathbb{F}_p[x]$.*

Beweis. Sei K ein endlicher Körper. Wegen Satz 4.3.4 hat K also p^n Elemente für eine Primzahl p und ein $n \geq 1$. Wir haben eine Körpereinbettung $\mathbb{F}_p \hookrightarrow K$. Die Gruppe $K^\times$ ist zyklisch nach Lemma 4.3.7. Sei α ein Erzeuger. Dann erhalten wir einen Ringhomomorphismus $\varphi\colon \mathbb{F}_p[x] \to K$ durch Evaluierung von Polynomen bei α, also durch $\varphi(f(x)) = f(\alpha)$. Da jedes Element entweder Null oder α^k ist, muß φ surjektiv sein: es gilt $\varphi(0) = 0$ und $\alpha^k = \varphi(x^k)$ für alle $k \geq 0$. Der Homomorphiesatz für Ringe liefert dann

$$\mathbb{F}_p[x]/\ker(\varphi) \approx K.$$

Hierbei ist ist $\ker(\varphi)$ ein Hauptideal, das von der Form $(f(x))$ ist, für ein normiertes, irreduzibles Polynom $f(x)$ in $\mathbb{F}_p[x]$, siehe Lemma 4.3.5. □

Der Satz sagt nicht, ob es überhaupt zu jeder Primzahlpotenz einen endlichen Körper gibt. Er sagt nur, daß wenn ein Körper mit p^n Elementen existiert, dann ist er isomorph zu einem Körper $\mathbb{F}_p[x]/(f(x))$.

Satz 4.3.10. *Zu jeder Primzahlpotenz $q = p^n$ gibt es bis auf Isomorphie genau einen endlichen Körper $\mathbb{F}_q$.*

Beweis. Um die Existenz zu zeigen, sei K der Zerfällunskörper des Polynoms $g(x) = x^q - x$ über $\mathbb{F}_p$. Das bedeutet, $g(x)$ zerfällt in K in Linearfaktoren

$$x^q - x = (x - a_1) \cdots (x - a_q)$$

mit $a_q \in \mathbb{F}_p$. Es folgt aus der Körpertheorie, daß so ein Körper existiert. In K betrachten wir nun die Menge

$$S = \{a \in K \mid a^q = a\}.$$

Sie hat genau q Elemente, weil $x^q - x$ keine doppelten Nullstellen hat wegen $(x^q - x)' = qx^{q-1} - 1 = -1 \neq 0$. Nun ist S ein Unterkörper von K, wegen

$$\begin{aligned}(a - b)^q &= a^q - b^q = a - b,\\ (ab^{-1})^q &= a^q(b^q)^{-1} = ab^{-1}\end{aligned}$$

für $a, b \in S$. Für die erste Gleichung haben wir benutzt, daß alle inneren Binomialkoeffizienten in $(a - b)^q$ durch p teilbar sind, und $p \equiv 0 \mod p$ ist. Der kleine Fermat impliziert $a^p = a$ und $a^q = a$. Somit ist $S = K$ unser gesuchter Körper mit q Elementen. Die Eindeutigkeit folgt aus der Eindeutigkeit von Zerfällungskörpern. □

4.4 Perfekte Codes

Wir können die Definition eines perfektes Codes auch wie folgt formulieren:

Definition 4.11. Ein Code $C \subseteq \mathbb{F}_q^n$ mit ungerader Minimaldistanz $d(C) = 2t(C) + 1$ heißt *perfekt*, falls es zu jedem Element $y \in \mathbb{F}_q^n$ genau ein Codewort $x \in C$ mit Abstand $d(x, y) \leq t(C)$ gibt.

Die Kugeln mit Radius $t(C) = (d(C) - 1)/2$ partitionieren also C. Der Code ist, falls er existiert, genau dann perfekt, wenn n und q die folgende kombinatorische Bedingung erfüllen:

$$A_q(n, d) = |C| = \frac{q^n}{\sum_{i=0}^{t(C)} \binom{n}{i}(q-1)^i}.$$

Ist C ein linearer $[n, k, d]_q$-Code, so ist $|C| = q^k$, und die Bedingung wird zu

$$q^{n-k} = \sum_{i=0}^{t(C)} \binom{n}{i}(q-1)^i. \tag{4.1}$$

Beispiel 4.4.1. *Für ein ungerades $n \geq 1$ ist der binäre n-fache Repetitions-Code perfekt.*

In der Tat, dieser Code ist ein linearer $[n, 1, n]_2$-Code, mit $k = 1$, $q = 2$ und $t = t(C) = (n-1)/2$. Siehe auch Beispiel 4.2.9 und Satz 4.1.7. Die Bedingung 4.1 ist erfüllt, denn es gilt

$$2^{n-1} = \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i}$$

Ebenso ist der triviale Code $C = \mathbb{F}_q^n$, oder der triviale Code $C = \{0\}$ perfekt. Man nennt auch den n-fachen Repetitions-Code *trivial*, wenn man von perfekten linearen Codes spricht.

Die Erfüllung der Bedingung 4.1 bedeutet nicht, daß es einen linearen Code $[n, k, d]_q$ mit diesen Parametern überhaupt geben muß.

Beispiel 4.4.2. *Für $n = 90$, $k = 78$, $d = 5$ und $q = 2$ ist die Bedingung* 4.1 *erfüllt. Es gibt aber keinen linearen $[90, 78, 5]_2$-Code.*

Wir haben $n - k = 12$ und $\binom{90}{2} = 4005$. Somit gilt

$$2^{12} = 4096 = \sum_{i=0}^{2} \binom{90}{i},$$

und die Bedingung 4.1 ist erfüllt. Andererseits gibt es aber folgendes Argument. Hat C den Fehlerkorrekturparameter t mit $d = 2t + 1$, so ist das *Lloyd Polynom* definiert als

$$L_t(n, x) := \sum_{j=0}^{t} (-1)^j \binom{x-1}{j}\binom{n-x}{t-j}(q-1)^{t-j}.$$

Hierbei benutzt man die Konvention $\binom{x}{j} := x(x-1)\cdots(x-j+1)/j!$ für $x \in \mathbb{R}$. Das Polynom hat t verschiedene reelle Nullstellen. Nun gilt folgendes Resultat.

Theorem 4.4.3 (Lloyd 1957, Lenstra 1972). *Sei C ein perfekter Code der Länge n mit Fehlerkorrekturparameter t. Dann hat das Polynom $L_t(n,x)$ genau t verschiedene ganzzahlige Nullstellen aus $\{1,2,\ldots,n\}$.*

In unserem Beispiel ist $t = q = 2$, und das Llody Polynom ist

$$L_2(90,x) = \sum_{j=0}^{2}(-1)^j\binom{x-1}{j}\binom{90-x}{2-j} = 2x^2 - 182x + 4096.$$

Offensichtlich hat es keine ganzzahlige Nullstelle.

Die folgende Klassifikation zeigt, daß es nur sehr wenige perfekte, lineare Codes gibt.

Theorem 4.4.4 (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.

Wir können leicht überprüfen, daß die Parameter in (1), (2), (3) die Bedingung 4.1 erfüllen. Für (1) gilt $t(C) = 1$, $k = n - \ell$, und daher

$$\sum_{i=0}^{1}\binom{n}{i}(q-1)^i = 1 + n(q-1) = q^\ell = q^{n-k}.$$

Für $[n,k,d] = [23,12,7]$ und $q = 2$, $t(C) = 3$ gilt

$$\sum_{i=0}^{3}\binom{23}{i} = 1 + 23 + 253 + 1771 = 2048 = 2^{23-12}.$$

Für $[n,k,d] = [11,6,5]$ und $q = 3$, $t(C) = 2$ gilt

$$\sum_{i=0}^{2}\binom{11}{i}2^i = 1 + 2\cdot 11 + 4\cdot 22 = 1 + 22 + 220 = 3^{11-6}.$$

Zudem ist die notwendige Bedingung aus Theorem 4.4.3 erfüllt. Für den $[23,12,7]_2$-Golay-Code etwa gilt, mit $q = 2$, $t = 3$, $n = 23$,

$$\begin{aligned} L_3(23,x) &= \sum_{j=0}^{3}(-1)^j\binom{x-1}{j}\binom{23-x}{3-j} \\ &= \frac{-4x^3 + 144x^2 - 1664x + 6144}{3} \\ &= -\frac{4}{3}(x-8)(x-12)(x-16). \end{aligned}$$

Die Nullstellen $x = 8, 12, 16$ sind ganzzahlig, und aus $\{1, \ldots, 23\}$.

Wir wollen nun auf die genannten Codes eingehen. Hamming-Codes sind wie folgt definiert:

Definition 4.12. 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 dann mit $\mathrm{H}am[n, n-\ell]_q$.

Satz 4.4.5. *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 $[n, n-\ell, 3]_q$-Code mit Fehlerkorrekturparameter $t(C) = 1$ und Minimaldistanz $d(C) = 3$.*

Beweis. Man wähle aus allen 1-dimensionalen Unterräumen in $\mathbb{F}_q^\ell$ jeweils einen nichtverschwindenden Vektor als Spaltenvektor einer Matrix H. Dann besteht H aus $n = \frac{q^\ell - 1}{q-1} = q^{\ell-1} + \cdots + q + 1$ Spalten und ist somit als Element von $\mathbb{F}_q^{\ell \times n}$ eine Kontrollmatrix eines linearen $[n, n-\ell]_q$-Codes C. Da zwei verschiedene 1-dimensionale Unterräume in $\mathbb{F}_q^\ell$ einen 2-dimensionalen Unterraum aufspannen, sind die Spalten von H paarweise linear unabhängig. Deswegen ist C ein Hamming-Code. Er erfüllt die Bedingung 4.1, ist also perfekt. Aus Satz 4.2.10 folgt $d(C) = 3$. □

Ein wichtiges Beispiel ist der lineare $[7, 4, 3]_2$-Code aus Beispiel 4.2.12.

Beispiel 4.4.6. *Der lineare Code aus Beispiel* 4.2.12 *ist ein Hamming-Code mit Kontrollmatrix*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Dabei ist $q = 2$, $\ell = 3$ und $n = \frac{q^\ell - 1}{q-1} = \frac{2^3 - 1}{2-1} = 7$.
Die folgende Tabelle gibt einige Beispiele für die Parameter $[n, n-\ell]_q$ von Hamming-Codes.

	$q = 2$	$q = 3$	$q = 4$	$q = 5$
$\ell = 2$	$[3, 1]_2$	$[4, 2]_3$	$[5, 3]_4$	$[6, 4]_5$
$\ell = 3$	$[7, 4]_2$	$[13, 10]_3$	$[21, 18]_4$	$[31, 28]_5$
$\ell = 4$	$[15, 11]_2$	$[40, 36]_3$	$[85, 81]_4$	$[156, 152]_5$
$\ell = 5$	$[31, 26]_2$	$[121, 116]_3$	$[341, 336]_4$	$[781, 776]_5$
$\ell = 6$	$[63, 57]_2$	$[364, 358]_3$	$[1365, 1359]_4$	$[3906, 3900]_5$
$\ell = 7$	$[127, 120]_2$	$[1093, 1086]_3$	$[5461, 5454]_4$	$[19531, 19524]_5$
$\ell = 8$	$[255, 247]_2$	$[3280, 3272]_3$	$[21845, 21837]_4$	$[488281, 488273]_5$

Nachdem die Hamming-Codes bekannt waren, wurde nach weiteren perfekten Codes gesucht, die einen höheren Fehlerkorrekturparameter $t(C)$ haben sollten. Golay bemerkte die kombinatorischen Identitäten $\sum_{i=0}^{3} \binom{23}{i} = 2^{23-12}$ und $\sum_{i=0}^{2} \binom{11}{i} 2^i = 3^{11-6}$. Im Jahr 1949 fand er dazu tatsächlich je einen perfekten, linearen Code, nämlich C_{23} und C_{11}.

Beispiel 4.4.7. *Der ternäre Golay-Code C_{11} ist durch die Erzeugermatrix*

$$G = \left(\begin{array}{cccccc|ccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

definiert. Es gilt $d(C_{11}) = 5$, und $t(C_{11}) = 2$. Er ist ein perfekter, linearer $[11, 6, 5]_3$-Code.

Der Golay-Code C_{11} ist auch äquivalent zu einem *zyklischen* Code, der durch das Erzeugerpolynom

$$g(x) = x^5 + x^4 - x^3 + x^2 - 1$$

definiert werden kann. Die Symmetriegruppe von C_{11} ist die sogenannte *Mathieugruppe* M_{11} der Ordnung $8 \cdot 9 \cdot 10 \cdot 11 = 7920$. Sie ist eine der 26 einfachen, sporadischen Gruppen, und zwar die *kleinste*. Sie wird erzeugt von den Permutationen

$$\sigma = (2, 10)(4, 11)(5, 7)(8, 9), \quad \tau = (1, 4, 3, 8)(2, 5, 6, 9)$$

in $\mathcal{S}_{11}$.

Bemerkung 4.4.8. Die größte einfache, sporadische Gruppe ist das *Monster*. Sie hat die Ordnung

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 =$$
$$808017424794512875886459904961710757005754368000000000.$$

Beispiel 4.4.9. *Der binäre Golay-Code C_{23} ist durch die Erzeugermatrix $G = (E_{12} \mid P)$ 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 $t(C_{11}) = 3$. Er ist ein perfekter, linearer $[23, 12, 7]_2$-Code.

Man beachte, daß die 11 Zeilen sich zyklisch nach links verschieben. Die zwöfte Zeile ist $(1, \ldots, 1)$. Es gibt viele Möglichkeiten, diesen Code zu definieren. Eine Möglichkeit ist es, den $[7, 4, 3]_2$-Hamming-Code C aus Beispiel 4.2.12 zu einem selbstdualen $[8, 4]_2$-Code C_1 durch ein Paritätsbit zu erweitern, und einen dazu äquivalenten $[8, 4]_2$-Code C_2 zu definieren. Damit erhält man den selbstdualen $[24, 12, 8]_2$-Golay-Code durch

$$C_{24} = \{(x + z, y + z, x + y + z \mid x, y \in C_1, z \in C_2\}.$$

Durch Streichen des letzten Symbols erhält man daraus den perfekten, linearen $[23, 12, 7]_3$-Golay-Code. Eine weitere Möglichkeit besteht darin, C_{23} als zyklischen Code durch das Polynom

$$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$

zu erzeugen. Die Symmetriegruppe von C_{23} ist die Mathieugruppe M_{23} der Ordnung 10200960. Sie ist eine weitere der 26 einfachen, sporadischen Gruppen.

Satz 4.4.10. *Der ternäre $[11, 6, 5]_3$-Golay-Code besitzt die erzeugende Funktion*

$$W_C(X) = 24 + 110X^2 + 330X^3 + 132X^5 + 132X^6 + X^{11}.$$

Der binäre $[23, 12, 7]_2$-Golay-Code besitzt die erzeugende Funktion

$$W_C(X) = 1 + 253X^7 + 506X^8 + 1288X^{11} + 1288X^{12} + 506X^{15} + 253X^{16} + X^{23}.$$

4.5 Zyklische Codes

Definition 4.13. Ein linearer Code $C \leq \mathbb{F}_q^n$ der Länge n heißt *zyklisch*, falls

$$(x_1, \ldots, x_n) \in C \Leftrightarrow (x_n, x_1, \ldots, x_{n-1}) \in C$$

gilt.

Die *Symmetriegruppe* $Sym(C)$ eines Codes C ist definiert als die Menge der Permutationen π, die C fixieren: also mit $\pi(c) \in C$ für alle $c \in C$. Die Symmetriegruppe eines zyklischen Codes umfasst also nach Definition die zyklische Gruppe C_n.

Beispiel 4.5.1. *Der ternäre Code mit Erzeugermatrix* $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}$ *ist zyklisch.*

Beispiel 4.5.2. *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.

In der Tat, $C' = \{(0,0,0,0),(1,0,1,0),(0,1,0,1),(1,1,1,1)\}$ ist ein zyklischer Code. Natürlich gibt es auch lineare Codes, nicht nicht zyklisch sind, bzw. nicht äquivalent zu einem zylischen Code sind. Wir werden noch sehen, daß etwa $Ham[4,2]_3$ so ein Beispiel ist.

Man betrachte folgenden Vektorraumisomorphismus

$$\rho\colon \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n-1), \quad (a_0,\ldots,a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i x^i$$

zwischen $\mathbb{F}_q^n$ und $\mathbb{F}_q[x]/(x^n-1)$. Er liefert ein Kriterium für die Zyklizität eines linearen Codes.

Lemma 4.5.3. *Es gelten folgende Aussagen.*

(1) Ein linearer Code $C \leq \mathbb{F}_q^n$ ist genau dann zyklisch, falls sein Bild $\rho(C)$ in $\mathbb{F}_q[x]/(x^n-1)$ ein Ideal ist.

(2) Jedes Ideal in dem Ring $\mathbb{F}_q[x]/(x^n-1)$ ist ein Hauptideal und wird von einem Teiler des Polynoms x^n-1 erzeugt.

Beweis. Zu (1): Es gilt wegen $x^n \equiv 1 \mod x^n-1$

$$\begin{aligned} x \cdot \sum_{i=0}^{n-1} a_i x^i &= a_0 x + a_1 x^2 + a_2 x^3 + \cdots + a_{n-1} x^n \\ &\equiv a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} \mod x^n - 1. \end{aligned}$$

Also wird das zyklische Rotieren um eine Koordinate durch Multiplikation mit x beschrieben. Ein linearer Code C ist also genau dann zyklisch, wenn $x\rho(C) \leq \rho(C)$ gilt. Das ist aber genau dann der Fall, wenn $\rho(C)$ ein Ideal in $\mathbb{F}_q[x]/(x^n-1)$ ist.

Zu (2): Sei $\pi\colon \mathbb{F}_q[x] \to \mathbb{F}_q[x]/(x^n-1)$ der kanonische Ring -Epimorphismus. Für ein Ideal I in $\mathbb{F}_q[x]/(x^n-1)$ ist dann $\pi^{-1}(I)$ 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. Wegen $\pi(x^n-1) = 0$ gilt dann

$$(x^n-1) \subseteq \pi^{-1}(I) = (g(x)).$$

Also ist $g(x)$ ein Teiler von x^n-1 in $\mathbb{F}_q[x]$. □

Wir betrachten ab jetzt einen zyklischen Code C immer als Ideal in $\mathbb{F}_q[x]/(x^n-1)$.

Definition 4.14. Es sei $C \trianglelefteq \mathbb{F}_q[x]/(x^n-1)$ ein zyklischer Code und $g(x)$ das eindeutige, normierte Polynom mit $C = (g(x))$. Dann heißt $g(x)$ das *Erzeugerpolynom*, und $h(x) = (x^n-1)g(x)^{-1}$ das *Kontrollpolynom* von C.

Beispiel 4.5.4. *Der zyklische Code aus Beispiel* 4.5.1 *hat das Erzeugerpolynom* $x+2$ *und das Kontrollpolynom* $h(x) = x^2+x+1$.

In $\mathbb{F}_3[x]/(x^3-1)$ gilt

$$\begin{aligned} I = (1+2x^2, x+2x^2) = \{&0, x+2, 2x+1, 2x^2+1, x^2+2,\\ &x^2+2x, 2x^2+x, x^2+x+1, 2x^2+2x+2\}\\ = \{&(a_2x^2+a_1x+a_0)(x+2)\}. \end{aligned}$$

Also wird I von $g(x) = x+2$ erzeugt. Es besteht aus den Polynomen, deren Koeffizientensumme gleich Null ist in $\mathbb{F}_3$. Wegen $(x+2)(x^2+x+1) = (x+2)^3 = x^3-1$ über $\mathbb{F}_3$ ist x^2+x+1 das Kontrollpolynom.

Lemma 4.5.5 (Kontrollgleichung)**.** *Für einen zyklischen Code $C \trianglelefteq \mathbb{F}_q[x]/\,(x^n-1)$ mit Kontrollpolynom $h(x)$ gilt*

$$C = \{f(x) \in \mathbb{F}_q[x]/(x^n-1) \mid f(x)h(x) = 0\}.$$

Beweis. Jedes Polynom $f(x) \in C$ ist ein Vielfaches von $g(x)$, erfüllt also $f(x) = a(x)g(x)$ für ein geeignetes Polynom $a(x)$. Wegen $g(x)h(x) = x^n - 1 = 0$ in $\mathbb{F}_q[x]/(x^n-1)$ erfüllt $f(x)$ daher die Kontrollgleichung $f(x)h(x) = 0$. Umgekehrt gilt für jedes $f(x)$ mit $f(x)h(x) = 0$ die Teilerbedingung $g(x) \mid f(x)$. Somit ist $f(x) \in C$. □

Beispiel 4.5.6. *Die Kontrollgleichung für den zyklischen Code $C = (x+2) \trianglelefteq \mathbb{F}_3[x]/(x^3-1)$ lautet*

$$\begin{aligned} f(x)h(x) &= (a_2x^2+a_1x+a_0)(x^2+x+1)\\ &\equiv (a_0+a_1+a_2)(x^2+x+1)\\ &\equiv 0 \mod x^3-1. \end{aligned}$$

Also ist

$$C = \{(a_2x^2+a_1x+a_0 \in \mathbb{F}_3[x]/(x^3-1) \mid a_0+a_1+a_2 = 0 \text{ in } \mathbb{F}_3\}.$$

Das sind genau die 9 Polynome, die wir im Beispiel 4.5.4 angegeben haben.

Angenommen, n und q sind teilerfremd. Dann ist das Polynom $x^n-1 \in \mathbb{F}_q[x]$ separabel. Sei $x^n-1 = f_1(x)f_2(x)\cdots f_r(x)$ seine Faktorisierung in irreduzible Faktoren. Das Polynom x^n-1 hat dann $\binom{r}{1} + \cdots \binom{r}{r} = 2^r$ normierte Teiler, und diese erzeugen insgesamt 2^r zyklische Codes in $\mathbb{F}_q^n$, die aber nicht unbedingt inäquivalent sein müssen.

Beispiel 4.5.7. *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

$$x^4-1 = (x+2)(x+1)(x^2+1)$$

Daraus ergeben sich die 6 nichttrivialen Teiler

$$x+2, x+1, x^2+1, (x+2)(x+1), (x+2)(x^2+1), (x+1)(x^2+1),$$

Das Polynom 1 erzeugt ganz $\mathbb{F}_3^4$, das Polynom x^4-1 den 0-Code.

Korollar 4.5.8. *Der Hamming-Code* $\mathrm{Ham}[4,2]_3$ *ist nicht äquivalent zu einem zyklischen Code.*

Beweis. Der Hamming-Code $\mathrm{Ham}[4,2]_3$ hat Minimaldistanz $d = 3$ wie alle Hamming-Codes. Er hat die Dimension $k = n - \ell = \frac{3^2-1}{3-1} - 2 = 2$. Gemäß obiger Liste aller ternären zyklischen Codes der Länge 4 kommen also höchstens die beiden Codes der Dimension 2 in Frage. Diese sind von x^2+1 bzw. von x^2+2 erzeugt. Im Fall $g(x) = x^2+1$ ist das Kontrollpolynom $h(x) = x^2+2$, und Erzeugermatrix bzw. Kontrollmatrix 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 nach Satz 4.2.10, also ungleich 3. Für den Code C mit $g(x) = x^2+2$ gilt $h(x) = x^2+1$, und ebenso $d(C) = 2$. □

In der Tat, man kann folgendes Resultat zeigen, siehe auch Satz 4.5.17:

Satz 4.5.9. *Ein Hamming-Code* $\mathrm{Ham}[n, n-\ell]_q$ *ist genau dann zu einem zyklischen Code äquivalent, wenn* $gcd(\ell, q-1) = 1$ *gilt.*

Als nächstes wollen wir auf das Idempotent eines zyklischen Codes eingehen. Ein Element e eines kommutativen Ringes R heißt *Idempotent*, falls $e^2 = e$ gilt. Dann gilt $R = eR \oplus (1-e)R$. Wird ein zyklischer Code von einem Idempotent erzeugt, so ist der Zugehörigkeitstest für ein empfangenes Wort y sehr einfach. Es gehört genau dann zum Code, wenn $ey = y$ gilt.

Satz 4.5.10. *Es sei* $gcd(n,q) = 1$. *Dann wird jeder zyklische Code* $C \trianglelefteq \mathbb{F}_q[x]/\,(x^n-1)$ *von genau einem Idempotent in* $\mathbb{F}_q[x]/\,(x^n-1)$ *erzeugt.*

Beweis. Wegen $gcd(n,q) = 1$ ist $x^n - 1$ separabel, d.h., alle Nullstellen in einem algebraischen Abschluß sind verschieden. Erzeugerpolynom und Kontrollpolynom erfüllen $g(x)h(x) = x^n - 1$ und sind deshalb teilerfremd. Also existieren Polynome $a(x), b(x) \in \mathbb{F}_q[x]$ mit

$$1 = a(x)g(x) + b(x)h(x).$$

Damit können wir unser Idempotent definieren als

$$e(x) = a(x)g(x) = 1 - b(x)h(x).$$

Wir rechnen nach, daß

$$\begin{aligned} e(x)^2 &= a(x)g(x)(1 - b(x)h(x)) \\ &= a(x)g(x) - a(x)b(x)(x^n-1) \\ &\equiv a(x)g(x) \mod x^n - 1 \\ &= e(x) \end{aligned}$$

gilt. Weil jedes Codewort $c(x) \in C$ ja ein Vielfaches von $g(x)$ ist, wirkt $e(x) = 1 - b(x)h(x)$ als Identität auf C. Das zeigt

$$(\mathbb{F}_q[x]/(x^n-1)) \cdot e(x) \leq C = C \cdot e(x) \leq (\mathbb{F}_q[x]/(x^n-1)) \cdot e(x).$$

Um die Eindeutigkeit von $e(x)$ zu zeigen, nehmen wir an, $\overline{e}(x) \in C$ sei ein weiteres Idempotent mit $C = (\mathbb{F}_q[x]/(x^n-1)) \cdot \overline{e}(x)$. Wir haben $\overline{e}(x)c(x) = c(x)$ für alle Wörter $c(x) \in C$, also auch

$$\overline{e}(x) = \overline{e}(x)e(x) = e(x).$$

□

Beispiel 4.5.11. *Sei $C = (g(x)) \trianglelefteq \mathbb{F}_3[x]/(x^{11}-1)$ 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.

Die Faktorisierung von $x^{11} - 1$ in irreduzible Faktoren über $\mathbb{F}_3$ lautet

$$x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1).$$

Beide Polynome fünften Grades erzeugen übrigens äquivalente $[11, 6, 5]_3$-Codes. Wir haben $(n, q) = (11, 3) = 1$. Das Kontrollpolynom zu $g(x)$ ist also

$$h(x) = (x-1)(x^5 - x^3 + x^2 - x - 1) = x^6 - x^5 - x^4 - x^3 + x^2 + 1.$$

Die Polynome $g(x)$ und $h(x)$ sind teilerfremd, und wir finden $a(x), b(x)$ mit

$$a(x)g(x) + b(x)h(x) = 1$$

in $\mathbb{F}_3[x]/(x^{11}-1)$, zum Beispiel mit $a(x) = -x^6 - x^4 + x^3 - 1$ und $b(x) = x^5 - x^4 + x^2$. Damit ist $e(x) = a(x)g(x) = -x^{10} - x^8 - x^7 - x^6 - x^2$ in $\mathbb{F}_3[x]/(x^{11}-1)$. Man prüft leicht nach, daß auch tatsächlich $e(x)^2 = e(x)$ in $\mathbb{F}_3[x]/(x^{11}-1)$ gilt.

Beispiel 4.5.12. *Der zyklische Code aus Beispiel* 4.5.1 *und* 4.5.4 *erfüllt nicht die Voraussetzung $gcd(n, q) = 1$.*

In diesem Fall ist $x^3 - 1$ nicht separabel über $\mathbb{F}_3$, denn $x^3 - 1 = (x+2)^3$. Es gibt dann auch kein solches Idempotent, da $g(x) = x + 2$ und $h(x) = x^2 + x + 1 = (x+2)^2$ nicht teilerfremd sind.

Die Klasse der zyklischen Codes ist abgeschlossen unter Dualisierung.

Satz 4.5.13. *Sei $g(x)$ das Erzeugerpolynom eines zyklischen Codes $C \trianglelefteq \mathbb{F}_q[x]/(x^n-1)$ vom Grad $n-k$, und $h(x)$ das zugehörige Kontrollpolynom. Dann ist* $\dim(C) = k$, *und $C^\perp$ ebenfalls ein zyklischer Code, der Dimension $n-k$, mit Erzeugerpolynom und Kontrollpolynom*

$$g^\perp(x) = h(0)^{-1}h(x^{-1})x^k,$$
$$h^\perp(x) = g(0)^{-1}g(x^{-1})x^{n-k}.$$

Wir benutzen im folgenden die Abkürzung $R_n = \mathbb{F}_q[x]/(x^n - 1)$ und setzen $gcd(n, q) = 1$ voraus.

Satz 4.5.14. *Es sei $C \trianglelefteq R_n$ ein zyklischer Code. Dann gibt es eine Menge $U(C)$ von n-ten Einheitswurzeln aus $\overline{\mathbb{F}}_q$ mit*

$$C = \{f(x) \in R_n \mid f(u) = 0 \text{ für alle } u \in U(C)\}.$$

Beweis. Das Erzeugerpolynom $g(x)$ von C besitzt als Teiler von $x^n - 1$ nur n-te Einheitswurzeln aus dem algebraischen Abschluss $\overline{\mathbb{F}}_q$ von $\mathbb{F}_q$ als Nullstellen. Da alle Codewörter aus C Vielfache von $g(x)$ sind, folgt die Behauptung mit

$$U(C) = \{u \in \overline{\mathbb{F}}_q \mid g(u) = 0\}.$$

□

Korollar 4.5.15. *Sei $C \trianglelefteq R_n$ ein zyklischer $[n, k, d]_q$-Code mit Nullstellenmenge $U(C) = \{u_1, \ldots u_{n-k}\}$. Mit*

$$L = \begin{pmatrix} 1 & u_1 & \cdots & u_1^{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & u_{n-k} & \cdots & u_{n-k}^{n-1} \end{pmatrix}$$

gilt dann

$$C = \left\{ \sum_{i=0}^{n-1} a_i x^i \in R_n \mid L \cdot (a_0, \ldots, a_{n-1})^t = 0 \right\}.$$

Es bezeichne $U_n = \{u \in \overline{\mathbb{F}}_q \mid u^n = 1\}$ die Menge aller n-ten Einheitswurzeln in $\overline{\mathbb{F}}_q$.

Korollar 4.5.16. *Es sei C ein zyklische Code über $\mathbb{F}_q$ und $U(C)$ sowie $U(C^\perp)$ die zugehörigen Nullstellenmengen von C und $C^\perp$. Dann sind $U(C)^{-1}$ und $U(C^\perp)$ komplementär in U_n, d.h. es gilt*

$$U(C^\perp) = U_n \setminus \{u^{-1} \mid u \in U(C)\}.$$

Beweis. Nach Satz 4.5.13 gilt für das Erzeugerpolynom $g^\perp(x)$ zu $C^\perp$

$$g^\perp(u^{-1}) = h(0)^{-1} h(u) u^{-k}.$$

Da das Kontrollpolynom $h(x)$ die Nullstellenmenge $U_n \setminus U(C)$ besitzt, folgt daraus die Behauptung. □

Wir wollen noch einmal auf die Hamming-Codes $Ham[n, n - \ell, 3]_q$ zurückkommen. Wegen

$$n = \frac{q^\ell - 1}{q - 1} = q^{\ell-1} + \cdots + q + 1$$

gilt $gcd(n, q) = 1$. Daher haben Hamming-Codes ein erzeugendes Idempotent. Zudem können wir die zyklischen Hamming-Codes wie folgt beschreiben. Wie wir aus Satz 4.5.9 wissen, sind Hamming-Codes genau dann zu einem zyklischen Code äquivalent, wenn $gcd(\ell, q - 1) = 1$ gilt.

Satz 4.5.17. *Es seien $\ell \geq 2$ eine ganze Zahl, und q eine Primzahlpotenz mit $gcd(\ell, q-1) = 1$. Weiterhin seien $u \in \mathbb{F}_{q^\ell}$ eine primitive n-te Einheitswurzel und $n = \frac{q^\ell - 1}{q-1}$. Dann ist der zyklische Code*

$$C = \{f(x) \in R_n \mid f(u) = 0\}$$

äquivalent zu $\mathrm{Ham}[n, n-\ell, 3]_q$.

Beweis. Aus $gcd(\ell, q-1) = 1$ folgt auch $gcd(n, q-1) = 1$ wegen

$$\begin{aligned} n &= q^{\ell-1} + \cdots + q + 1 \\ &= \ell + (q-1)(q^{\ell-2} + 2q^{\ell-3} + 3q^{\ell-4} + \cdots + (\ell-2)q + \ell - 1). \end{aligned}$$

Das bedeutet $u^{j(q-1)} \neq 1$ und $u^j \notin \mathbb{F}_q$ für $j = 1, \ldots, n-1$. 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 die Spalten linear unabhängig über $\mathbb{F}_q$, und somit ist H eine Kontrollmatrix eines Hamming-Codes, nämlich von $\mathrm{Ham}[n, n-\ell, 3]_q$. □

Für $q = 2$ und $n = 2^\ell - 1$ kann man den Satz ohne Einschränkung anwenden. Ein normiertes Polynom $p(x) \in \mathbb{F}_q[x]$ heißt *primitiv*, falls es eine Nullstelle α in $\mathbb{F}_{q^m}$ hat, die ein primitives Eelement ist, also mit $\mathbb{F}_{q^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q^m-2}\}$, und außerdem $p(x)$ das Polynom mit dem kleinsten Grad ist, das α als Nullstelle hat.

Satz 4.5.18. *Ist $p(x) \in \mathbb{F}_2[x]$ ein primitives Polynom vom Grad $\ell \geq 2$, dann ist der zyklische Code $C = (p(x)) \trianglelefteq \mathbb{F}_2[x]/(x^{2^\ell - 1} - 1)$ äquivalent zum $[2^\ell - 1, 2^\ell - \ell - 1]_2$-Hamming-Code.*

Beweis. Ist α eine Nullstelle des primitiven Polynoms $p(x)$, so können wir α^i mit x^i mod $p(x)$ identifizieren, $i = 0, 1, \ldots, 2^\ell - 2$. Wie in Satz 4.5.17 ist die Kontrollmatrix 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 $n = 2^\ell - 1$ und $C = \mathrm{Ham}[n, n-\ell]_2$

$$\begin{aligned} C &= \{(a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n \mid a_0 + a_1 x + \cdots +, a_{n-1}x^{n-1} = 0 \text{ in } \mathbb{F}_2^\ell\} \\ &= \{f(x) \in \mathbb{F}_2[x]/(x^n - 1) \mid p(x) \text{ teilt } f(x)\} \\ &= (p(x)). \end{aligned}$$

□

Beispiel 4.5.19. *Mit $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ ist der zyklische Code $C = (p(x)) \trianglelefteq \mathbb{F}_2[x]/(x^7 - 1)$ äquivalent zum $[7, 4]_2$-Hamming-Code aus Beispiel* 4.4.6. *Er hat das Idempotent $e(x) = x^4 + x^2 + x$.*

Für $q = 2$, $\ell = 3$ und $n = 2^3 - 1 = 7$ ist das Polynom $x^7 - 1$ separabel über $\mathbb{F}_2$, mit Faktorisierung

$$x^7 - 1 = (x+1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

Das Polynom $p(x) = x^3 + x + 1$ ist primitiv, und es gilt

$$\begin{aligned} \mathbb{F}_2[x]/(p(x)) = \{&0, x, x^2, x^3 = x + 1, x^4 = x^2 + x, \\ &x^5 = x^2 + x + 1, x^6 = x^2 + 1, x^7 = 1\}. \end{aligned}$$

Als Spaltenvektoren im $\mathbb{F}_2^3$ geschrieben bedeutet das

$$1 = \begin{pmatrix}1\\0\\0\end{pmatrix},\ x = \begin{pmatrix}0\\1\\0\end{pmatrix},\ x^2 = \begin{pmatrix}0\\0\\1\end{pmatrix},\ x^3 = \begin{pmatrix}1\\1\\0\end{pmatrix},\ x^4 = \begin{pmatrix}0\\1\\1\end{pmatrix},$$

$$x^5 = \begin{pmatrix}1\\1\\1\end{pmatrix},\ x^6 = \begin{pmatrix}1\\0\\1\end{pmatrix}.$$

Die Kontrollmatrix lautet also

$$H = \begin{pmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{pmatrix}.$$

Bis auf zyklische Permutation der letzten drei Spalten ist sie also genau die Kontrollmatrix des $[7,4]_2$-Hamming-Code aus Beispiel 4.4.6. Zu dem Erzeugerpolynom $g(x) = x^3+x+1$ gehört das Kontrollpolynom $h(x) = (x+1)(x^3+x^2+1) = x^4+x^2+x+1$. Wir haben $a(x)g(x)+b(x)h(x) = 1$ mit $a(x) = x$ und $b(x) = 1$. Somit ist $e(x) = a(x)g(x) = x^4+x^2+x \mod x^7-1$ das Idempotent.

Bemerkung 4.5.20. Ein irreduzibles Polynom $f(x) \in \mathbb{F}_2[x]$ mit $\deg(f) = \ell$ ist genau dann primitiv, falls die kleinste positive Zahl n mit $f(x) \mid x^n - 1$ durch $n = 2^\ell - 1$ gegeben ist.

Betrachten wir zum Beispiel $f(x) = x^4+x+1$. Es hat Grad $\ell = 4$ und ist irreduzibel über $\mathbb{F}_2$. Es gilt $2^\ell - 1 = 15$ und $f(x) \mid x^{15}-1$ in $\mathbb{F}_2[x]$. In der Tat, die Faktorisierung in irreduzible Faktoren von $x^{15}-1$ ist wie folgt gegeben:

$$x^{15}-1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)$$
$$(x^4+x^3+x^2+x+1).$$

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 $g(x) \mid x^5-1$. Hier ist eine kleine Tabelle mit einigen Beispielen primitiver Polynome über $\mathbb{F}_2$:

$\ell \geq 2$	$f(x)$
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	$x^{10}+x^3+1$

Für den nächsten Abschnitt brauchen wir noch folgendes Resultat:

Satz 4.5.21. *Es seien $C \trianglelefteq R_n$ ein zyklischer $[n,k]_q$-Code mit Nullstellenmenge $U(C)$ und u eine primitive n-te Einheitswurzel. 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 die Minimaldistanz mindestens d, d.h. $d(C) \geq d$.*

Beweis. Angenommen es gilt $d(C) < d$. Dann gibt wegen

$$d(C) = \min\{w(x) \mid 0 \neq x \in C\}$$

ein Wort $c(x) = \sum_{j=1}^{r} a_j x^j$ aus C vom Gewicht $w(c) = r$ mit $0 < r < d$. Dann ist nach Voraussetzung $\{u^b, \ldots, u^{b+r-1}\}$ in der Nullstellenmenge $U(C)$ enthalten, und $(a_1, \ldots, a_r)$ eine nichttriviale Lösung des homogenen linearen Gleichungssystems

$$\begin{aligned} x_1(u^b)^1 + \cdots + x_r(u^b)^r &= 0, \\ \vdots \qquad\qquad \vdots &\quad \vdots \\ x_1(u^{b+r-1})^1 + \cdots + x_r(u^{b+r-1})^r &= 0. \end{aligned}$$

Deshalb verschindet die Determinante von

$$L = \begin{pmatrix} u^b & \cdots & u^{br} \\ \vdots & & \vdots \\ u^{b+r-1} & \cdots & u^{(b+r-1)r} \end{pmatrix}.$$

Andererseits gilt nach dem Satz über Vandermonde Determinanten

$$\begin{aligned} \det(L) &= \prod_{j=1}^{r} u^{bj} \cdot \det \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ (u^1)^{r-1} & \cdots & (u^r)^{r-1} \end{pmatrix} \\ &= \prod_{j=1}^{r} u^{bj} \cdot \prod_{j<k} (u^k - u^j) \neq 0, \end{aligned}$$

welches ein Widerspruch ist. □

4.6 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 und 1959 unabhängig voneinander entdeckt haben. Wir erinnern noch einmal an folgende Definition.

Definition 4.15. Ein *Minimalpolynom* eines Elementes $\alpha \in \mathbb{F}_{q^m}$ über $\mathbb{F}_q$ ist ein normiertes Polynom $m(x) \in \mathbb{F}_q[x]$ kleinsten Grades mit $m(\alpha) = 0$.

Dazu ist folgender Satz zu nennen.

Satz 4.6.1. *Zu jedem $\alpha \in \mathbb{F}_{q^m}$ existiert ein eindeutig bestimmtes Minimalpolynom $m_\alpha(x)$ über $\mathbb{F}_q$. Es ist irreduzibel über $\mathbb{F}_q$ und teilt jedes andere normierte Polynom $f(x) \in \mathbb{F}_q[x]$ mit $f(\alpha) = 0$.*

Natürlich ist $m_\alpha(t) = t - \alpha$ das Minimalpolynom von $\alpha \in \mathbb{F}_q$ über $\mathbb{F}_q$.

Beispiel 4.6.2. *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 $m_\alpha(t)$ für $\alpha = 0, 1, 2$ sind t, $t+2$, $t+1$, die für $x, 2x$ sind t^2+1, die für $x+1, 2x+1$ sind t^2+t+2, und die für $x+2, 2x+2$ sind t^2+2t+2.

Die angegebenen Polynome sind irreduzibel und haben α als Nullstelle. Deswegen sind sie die Minimalpolynome. Zum Beispiel gilt, mit $m(t) = t^2+2t+2$ 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 $\mathbb{F}_9$.

Kommen wir nun zur Definition eines BCH-Codes. Die multiplikative Gruppe des endlichen Körpers $\mathbb{F}_{q^m}$ ist zyklisch, siehe Satz 4.3.7. Es sei u ein Erzeuger dieser Gruppe, d.h., $(\mathbb{F}_{q^m})^\times = \langle u \rangle$. Ferner bezeichne $m_i(x)$ das Minimalpolynom von u^i.

Definition 4.16 (BCH-Code)**.** Es sei u ein Erzeuger von $(\mathbb{F}_{q^m})^\times$ und

$$U_{b,d} = \{u^b, \ldots, u^{b+d-2}\}$$

mit $2 \leq d \leq q^m - 1$ und $b \geq 0$. Sei $g(x)$ das kleinste gemeinsame Vielfache aller Minimalpolynome der $u^j \in U_{b,d}$ über $\mathbb{F}_q$, d.h.,

$$g(x) = \mathrm{kgV}(m_b(x), m_{b+1}(x), \ldots, m_{b+d-2}(x)).$$

Ein *BCH-Code über $\mathbb{F}_q$ mit garantierter Minimaldistanz d* ist der zyklische Code, der durch das Polynom $g(x)$ erzeugt wird.

Bemerkung 4.6.3. Ein BCH-Code C heißt *primitiv*, falls er Länge $n = q^m - 1$ hat, und u^b ebenfalls ein Erzeuger der Gruppe $(\mathbb{F}_{q^m})^\times$ ist. Für primitive BCH-Codes kann man also o.E. $b = 1$ annehmen.

Die Bezeichnung *mit garantierter Minimaldistanz* hat ihre Berechtigung, weil ein BCH-Code C wegen Satz 4.5.21 eine Minimaldistanz $d(C) \geq d$ hat.

Satz 4.6.4 (BCH-Schranke)**.** *Ein BCH-Code C der Länge n mit Parameter $d \geq 2$ hat Minimaldistanz $d(C) \geq d$. Seine Dimension ist mindenstens $n - m(d-1)$. Im Fall $q = 2$ und $b = 1$ gilt sogar*

$$\dim(C) \geq n - m \left\lfloor \frac{d}{2} \right\rfloor.$$

Beweis. Wegen $[\mathbb{F}_q(u) : \mathbb{F}_q] = m$ ist der Grad der Mininmalpolynome $m_i(x)$ zu $u^i \in U_{b,d}$ nicht größer als m, so daß $\deg(g(x)) \leq m(d-1)$ wegen $|U_{b,d}| = d-1$ folgt. Für $q = 2$ stimmen die Minimalpolynome $m_i(x)$ und $m_{2i}(x)$ überein wegen $m_i(u^{2i}) = (m_i(u^i))^2 = 0$. Somit hat das Erzeugerpolynom $g(x)$ eines binären BCH-Codes C, der $U_{1,d} \subseteq U(C)$ erfüllt, die Gestalt

$$g(x) = \mathrm{kg}V(m_j(x) \mid j = 1, 3, 5, \ldots, 2\left\lfloor \frac{d}{2} \right\rfloor - 1)$$

und höchstens Grad $m\lfloor d/2 \rfloor$. Die Behauptungen folgen nun wegen

$$\dim(C) = n - \deg(g(x)).$$

□

Korollar 4.6.5. *Für $q = 2$, $n = 2^m - 1$ und $t < 2^{m-1}$ existiert ein t-fehlerkorrigierender BCH-Code C der Länge n mit* $\dim(C) \geq n - mt$.

Beweis. Es sei C ein binärer BCH-Code mit $U_{1,2t} \subseteq U(C)$. Wegen $m_i(u^{2t}) = 0$ und $m_t(x) \mid g(x)$ ist u^{2t} eine weitere Nullstelle von C. Daher gilt sogar $U_{1,2t+1} \subseteq U(C)$. Somit besitzt C die garantierte Minimaldistanz $d = 2t+1$, und es folgt $\dim(C) \geq n - m\lfloor d/2 \rfloor = n - mt$. □

Definition 4.17. Sei u eine primitive n-te Einheitswurzel über $\mathbb{F}_q$, und $b \geq 0$, $2 \leq d \leq q-1$. Ein BCH-Code der Länge $n = q - 1$ mit Generatorpolynom

$$g(x) = (x - u^b)(x - u^{b+1}) \cdots (x - u^{b+d-2})$$

heißt *Reed-Solomon-Code* mit garantierter Minimaldistanz d.

Es gilt $n = ord(u) \mid ord(\mathbb{F}_q^\times) = q - 1$. Ein Reed-Solomon-Code ist ein primitiver BCH-Code. Wir können ohne Einschränkung $b = 1$ und $g(x) = \prod_{i=1}^{d-1}(x - u^i)$ wählen; oder $b = 0$ und $g(x) = \prod_{i=0}^{d-2}(x - u^i)$.

Für lineare $[n, k, d]$-Codes C folgt aus der Singleton-Schranke

$$\dim(C) = k \leq n - d + 1,$$

siehe Satz 4.1.8. Codes, die diese Schranke erreichen, erhalten einen besonderen Namen.

Definition 4.18. Ein linearer $[n, k, d]$-Code C heißt *MDS-Code*, falls $k = n - d + 1$ gilt.

Dabei steht MDS für *maximum distance separable code.*

Satz 4.6.6. *Ein Reed-Solomon-Code über 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 aus Satz 4.6.4 mit $m = 1$ gerade $k \geq n - d + 1$. □

Anders ausgedrückt haben wir eine scharfe Schranke für die Größe $A_q(n,d)$ von Codes über q der Länge n und Minimaldistanz d für eine unendliche Serie von Werten $d \leq n \leq q-1$ gefunden:

Korollar 4.6.7. *Sei q eine Primzahlpotenz, und sei $d \leq n \leq q-1$. Dann gilt $A_q(n,d) = q^{n-d+1}$.*

Die zu MDS-Codes dualen Codes sind wieder MDS-Codes.

Satz 4.6.8. *Sei C ein MDS-$[n, n-r, r+1]$-Code. Dann ist der duale Code $C^\perp$ ein MDS-$[n, r, n-r+1]$-Code.*

Beweis. Sei C ein MDS-$[n, n-r]$-Code über $\mathbb{F}_q$. Es ist $d = n-(n-r)+1 = r+1$. Zu zeigen ist, daß der $[n,r]$-Code $C^\perp$ die Minimaldistanz $d = n-r+1$ hat. 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 $y \in \mathbb{F}_q^r$ mit $x = y^t H$. Wenn x höchstens Gewicht $n-r$ hat, dann gibt es eine $(r \times r)$-Untermatrix H' von H mit $y^t H' = 0$. Da aber je r Spalten von H linear unabhängig sind, ist $\det(H') \neq 0$, und es folgt $y = 0$. Das ist ein Widerspruch. Es folgt $d(C^\perp) = \min\{w(x) \mid 0 \neq x \in C^\perp\} \geq n-r+1$. Also ist die Minimaldistanz von $C^\perp$ mindestens $n-r+1$. □

Bemerkung 4.6.9. Ein Reed-Solomon-Code mit garantierter Minimaldistanz d besitzt die Kontrollmatrix

$$H = \begin{pmatrix} 1 & u & \cdots & u^{q-2} \\ 1 & u^2 & \cdots & u^{2(q-2)} \\ \vdots & \vdots & \vdots & \\ 1 & u^{d-1} & \cdots & u^{(d-1)(q-2)} \end{pmatrix}.$$

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 4.6.10. *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 $d = 5$.

Das primitive Element $u \in \mathbb{F}_{2^3}$ ist Nullstelle des primitiven Polynoms $p(x) = x^3+x+1 \in \mathbb{F}_2[x]$. Wir haben $u^3 = u+1$, $u^4 = u^2+u$, $u^5 = u^2+u+1$, $u^6 = u^2+1$ und $u^7 = 1$, siehe Beispiel 4.5.19. Das Generatorpolynom ist

$$\begin{aligned} g(x) &= (x-1)(x-u)(x-u^2)(x-u^3) \\ &= x^4 + u^2x^3 + u^5x^2 + u^5x + u^6. \end{aligned}$$

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 4.6.11. 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 die Tabelle nach Bemerkung 4.5.20. Zunächst konstruiert man damit über dem Körper $\mathbb{F}_{256}$ einen primitiven $[255, 251, 5]_{256}$-Reed-Solomon-Code der Länge $n = 255$, Dimension $k = n-d+1 = 251$ und Minimaldistanz $d = 5$. Daraus formt man durch gewisse Streichungen einen $[28, 24, 5]$-Code C_1, und einen $[32, 28, 5]$-Code C_2, aus denen man durch Produktbildung $C_1 \otimes C_2$ den *Interleaved Reed-Solomon Code* der Audio CD erhält.

Literaturverzeichnis

[1] T. Janssen: *Crystallographic groups.* North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing, New York (1973).

[2] D. Cox, J. Little, D. O'Shea: *Ideals, varieties and algorithms.* Springer-Verlag (1997).

[3] K. Lamotke: *Die Symmetriegruppen der ebenen Ornamente.* Math. Semesterber. **52** (2005), 153–174.

[4] J. H. van Lint: *Introduction to Coding Theory.* Third edition. Graduate Texts in Mathematics, 86. Springer-Verlag (1999).

[5] G. Mackiw: *Finite Groups of* 2×2 *Integer Matrices.* Math. Magazine **69**, No. 5 (1996), 356–361.

[6] J. C. Jantzen, J. Schwermer: *Algebra.* Springer-Verlag (2006).