UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Bachelorarbeit

Algebraische Zahlkörper in der Codierungstheorie

Vorgelegt der
Fakultät für Mathematik
der Universität Duisburg-Essen

Von:
Florian Hennecke
Matr.-Nr. 2274073

Betreut von:
Prof. Dr. J. Kohlhaase

23. Juli 2021

Inhaltsverzeichnis

1 Einleitung

In der vorliegenden Bachelorarbeit geht es darum, mithilfe von algebraischen Zahlkörpern einen „guten“ Code mit einem möglichst kleinen Alphabet zu erzeugen. „Gut“ bedeutet hier, dass dieser Code sowohl sinnvoll Informationen übertragen soll, als auch Fehler erkennen soll. Wir identifizieren dies anhand der Informationsrate und der relativen Minimaldistanz des Codes.
Um dort hinzugelangen, fassen wir zunächst die nötigen Grundlagen der Codierungstheorie und der algebraischen Zahlentheorie zusammen, um uns anschließend an eine erste Konstruktion zu wagen. Dort stellen wir fest, dass $size(x) := \|x\|$ für uns keine geeignete Definition der Größe eines Elements ist, da wir nachfolgende zwei Eigenschaften an unsere Größe eines Elements fordern. Zum einen, dass $size(a-b)$ klein ist, wenn auch $size(a)$ und $size(b)$ klein ist, zum anderem, dass $size(f)$ sehr klein sein soll, falls $f \neq 0$ in vielen Idealen $I_1, \ldots, I_n$ enthalten ist, wobei eine Nachricht $m \in R$ durch $Enc(m) = (m/I_1, \ldots, m/I_n)$ codiert wird. Mithilfe der Bewertungstheorie bei Zahlkörpern finden wir eine geeignete Definition für die Größe eines Elements: $size(x) := \sum_{i=1}^{r} |x|_{\mathfrak{q}_i} + \sum_{i=1}^{s} 2\sqrt{|x|_{\mathfrak{q}_{r+i}}}$. Mithilfe dieser machen wir uns an die Konstruktion eines Zahlkörpercodes $\mathcal{C}_K$ und berechnen für diesen in Abhängigkeit seiner Parameter die Minimaldistanz und Informationsrate. Anschließend machen wir einen Exkurs in die Klassenkörpertheorie. Von dort benötigen wir spezielle Klassenkörpertürme, die unsere konkreten Familien von guten Zahlkörpercodes erzeugen. Deren Existenzen sind dann zum Abschluss unsere beiden Haupttheoreme der Arbeit. Wir erzeugen zunächst die Familie von asymptotisch guten Zahlkörpercodes über dem Alphabet $\mathbb{F}_{29}$. Das Ziel für unser zweites Theorem ist es, die Größe des Alphabets von 29 zu verringern. Dies gelingt uns, indem wir keine linearen Codes mehr betrachten und eine weitere Familie von asymptotisch guten Codes erzeugen, aber diesmal über $\mathbb{F}_{17}$ und $\mathbb{F}_{19}$, was uns zu einer Alphabetgröße von 19 bringt.
Wir beziehen uns dabei hauptsächlich auf das Paper [Gur00a] „Constructions of Codes from Number Fields“ von Venkatesan Guruswami, veröffentlicht im Electronic Colloquium on Computational Complexity, Report No. 2 (2001) und dessen Korrektur von 2003.

2 Grundlagen

In diesem Kapitel werden die notwendigen Grundlagen der Codierungstheorie und der algebraischen Zahlentheorie zusammengetragen, wobei wir im Laufe dieser Arbeit immer wieder auf Teile davon zurückkommen werden und entsprechend verweisen. Dabei stützt sich das Unterkapitel der Codierungstheorie im Wesentlichen auf die Vorlesung „Codierungstheorie“ von Herrn Dr. Staszewski aus dem Sommersemester 2017 und das Unterkapitel der algebraischen Zahlentheorie auf das Buch „Algebraische Zahlentheorie“ von Herrn Jürgen Neukirch [Neu92] und auf die Vorlesung „Algebraische Zahlentheorie I“ von Herrn Professor Kohlhaase aus dem Sommersemester 2014.

2.1 Codierungstheorie

Die Codierungstheorie befasst sich mit dem Generieren von fehlererkennenden und -korrigierenden Codes. Hierbei wird eine bereits bestehende digitale Nachricht „codiert“, indem zusätzliche Informationen zur ursprünglichen Nachricht hinzugefügt werden. Diese sogenannten Kontrollstellen sollen später dabei helfen, Übertragungsfehler zu erkennen oder sogar zu korrigieren. Oft ist das Ziel, für eine bestimmte Anwendung einen optimalen Code zu erzeugen. Dieser soll dann die nötige Anzahl an Fehlern korrigieren bzw. erkennen, aber im Gegenzug auch nicht zu viele Kontrollstellen haben, da diese das Datenvolumen der Nachricht vergrößern. Es geht also darum, mit den gegebenen Bedingungen den jeweils effizientesten Code zu finden.
Dies veranschaulichen wir nachfolgend an drei simplen Beispielen, doch zunächst definieren wir, was wir unter einem Code verstehen.

Definition 2.1
Sei F eine endliche Menge mit $|F| = q$ und für $n \in \mathbb{N}$ sei $F^n := \{(u_1, \dots, u_n) \mid u_1, \dots, u_n \in F\}$. Ferner sei $F^* := \cup_{n=0}^{\infty} F^n$. Dann versteht man unter einem Code über dem Alphabet F eine Teilmenge $\mathcal{C} \neq \emptyset$ von F^* und bezeichnet C als q-nären Code. Ist $|\mathcal{C}| = 1$, so heißt $\mathcal{C}$ trivial. Sollte $\mathcal{C} \subseteq F^n$ gelten, nennen wir $\mathcal{C}$ einen Blockcode der Länge n.

Beispiel 2.2
Betrachte hierfür die Nachrichtenmenge $\{00, 01, 10, 11\}$. Sollte man nun - ohne zu codieren - eine der Nachrichten verschicken und es taucht durch sogenanntes Rauschen (zum Beispiel durch Interferenzen, einem Kratzer auf einer CD oder anderen Übertragungsfehlern) genau ein Fehler auf, dann wird der Empfänger nicht bemerken, dass ein Fehler aufgetreten ist.

1. Sei $\mathcal{C}_1$ der binäre Code der Länge 3, der an die ursprüngliche Nachricht die Anzahl (modulo 2) der vorhandenen Einsen anhängt. Also

$$\text{Enc}(00) = 000,\ \text{Enc}(01) = 011,\ \text{Enc}(10) = 101,\ \text{Enc}(11) = 110,$$

   wobei Enc(m) eine Nachricht m auf ein Codewort $c \in \mathcal{C}$ codiert.

2. Sei $\mathcal{C}_2$ der binäre Code der Länge 6, der die ursprüngliche Nachricht dreimal wiederholt. Also

$$\text{Enc}(00) = 000000,\ \text{Enc}(01) = 010101,\ \text{Enc}(10) = 101010,\ \text{Enc}(11) = 111111.$$

3. Sei $\mathcal{C}_3$ der binäre Code der Länge 5, der an die ursprüngliche Nachricht die Anzahl (modulo 2) der vorhandenen Einsen anhängt und anschließend die ursprüngliche Nachricht einmal wiederholt. Also

$$\text{Enc}(00) = 00000,\ \text{Enc}(01) = 01101,\ \text{Enc}(10) = 10110,\ \text{Enc}(11) = 11011.$$

Der Code $\mathcal{C}_1$ ist ein Beispiel für einen fehlererkennenden Code, da die Summe über die Ziffern modulo 2 Null ergibt. Sollte hier genau ein Fehler auftreten, kann der Empfänger erkennen, dass eine Stelle des Codeworts nicht richtig sein kann und zum Beispiel die Nachricht erneut anfordern. Der Code $\mathcal{C}_2$ ist ein Code bei dem der Empfänger diesen Fehler nicht nur erkennen, sondern auch eigenständig korrigieren kann. Der Code $\mathcal{C}_3$ soll hier veranschaulichen, dass es anschließend auch um Effizienz geht, denn dieser Code kann das Gleiche wie $\mathcal{C}_2$, benötigt aber nur 5-Bit anstatt 6-Bit zur Datenübertragung.

Das Verhältnis zwischen Informations- und Kontrollstellen eines Codes wird durch die Informationsrate gegeben.

Definition 2.3
Sei $\mathcal{C}$ ein q-närer Code der Länge n. Dann definiert die Anzahl der übertragenen Informationsstellen im Verhältnis zur Länge der Wörter die Informationsrate $R = \frac{\log_q(|\mathcal{C}|)}{n}$ des Codes $\mathcal{C}$.

Nachfolgend möchten wir betrachten, wie erhaltene gegebenenfalls fehlerhafte Nachrichten sinnvoll decodiert werden können. Dies geschieht im Normalfall mit der Maximum-Likelihood-Decodierung. Um diese genauer zu beschreiben, benötigen wir jedoch noch einen Abstandsbegriff für zwei Codeworte $u, v \in F^n$.

Definition 2.4
Sei F ein Alphabet, $n \in \mathbb{N}$ und seien $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in F^n$. Dann heißt $d(u, v) := |\{i \in \{1, \ldots, n\} \mid u_i \neq v_i\}|$ die Hamming-Distanz zwischen u und v.
Sei weiterhin $r \in \mathbb{N}_0$. Dann definiert $B_r(u) := \{v \in F^n \mid d(u, v) \leq r\}$ eine Kugel vom Radius r um den Mittelpunkt u in F^n. Dabei gilt für $|F| > 1$, dass $|B_r(u)| = 1$ genau dann, wenn $r = 0$ ist.

Satz 2.5
Sei F ein Alphabet und $n \in \mathbb{N}$. Dann definiert die Hamming-Distanz auf F^n eine Metrik, d.h. für alle $u, v, w \in F^n$ gilt:

i) $d(u, v) \geq 0$ *und* $d(u, v) = 0 \iff u = v$,

ii) $d(u, v) = d(v, u)$,

iii) $d(u, v) \leq d(u, w) + d(w, v)$.

Ist $(F, +)$ eine abelsche Gruppe, so ist die Hamming-Distanz translationsinvariant, also

iv) $d(u + w, v + w) = d(u, v)$.

Beweis: Die Teile i) und ii) folgen direkt aus der Definition der Hamming-Distanz. Mithilfe der Interpretation, dass $d(u, v)$ die kleinste Anzahl von Koordinatenänderungen ist, folgen Teil iii) und iv). □

Lemma 2.6
Sei F ein q-näres Alphabet und $r \in \mathbb{N}_0$. Dann hat für jedes Element $u \in F^n$ die Kugel $B_r(u)$ genau $\sum_{j=0}^{r} \binom{n}{j}(q-1)^j$ Elemente.

Beweis: Das Lemma folgt aus der Gleichungskette

$$B_r(u) = |\{v \in F^n \mid d(u,v) \leq r\}| = \sum_{j=0}^{r} |\{v \in F^n \mid d(u,v) = j\}| = \sum_{j=0}^{r} \binom{n}{j}(q-1)^j,$$

wobei die letzte Gleichung mithilfe der Kombinatorik folgendermaßen zu erklären ist. Es gibt $\binom{n}{j}$ Möglichkeiten genau j beliebige Stellen des Codewortes auszuwählen, welche dann jeweils $(q-1)$ Möglichkeiten haben sich von den Stellen des Codewortes u zu unterscheiden. □

Definition 2.7
Sei $\mathcal{C} \subseteq F^n$ ein q-närer Blockcode über F. Für $c \in \mathcal{C}$ und $v \in F^n$ sei $P(v|c)$ die bedingte Wahrscheinlichkeit, dass v empfangen wird, falls c gesendet wird. Eine Maximum-Likelihood-Decodierung decodiert die empfangene Nachricht v nun zu einem Codewort c beziehungsweise dessen Nachricht, für welches $P(v|c) = \max_{c' \in \mathcal{C}} P(v|c')$ gilt.

Also wird eine fehlerhafte Nachricht immer auf das Codewort zurückgeführt, welches mit höchster Wahrscheinlichkeit das ursprüngliche Codewort war.
In der Praxis sind die meisten Kanäle symmetrisch, das bedeutet zum einen, dass für alle Buchstaben die Wahrscheinlickeit gleich groß ist, richtig übermittelt zu werden, also $P(c_1|c_1) = P(c_2|c_2)$ für alle $c_1, c_2 \in \mathcal{C}$ und zum anderen, dass für alle Fehler die Wahrscheinlichkeit gleich groß ist, also $P(v|c) = P(u|c)$ für alle $u, v, c \in F^n$ mit $u \neq c \neq v$. Zusätzlich zur Symmetrie des Kanals nehmen wir weiterhin an, dass die Wahrscheinlichkeit p für die Verfälschung eines Symbols $a \in F$ kleiner als $\frac{q-1}{q}$ ist. Diese Annahme ist realistisch, da anderenfalls der Kanal zu schlecht für eine sinnvolle Übertragung wäre. Somit wird jedes $a \in F$ mit Wahrscheinlichkeit $1 - p > \frac{1}{q}$ richtig übertragen.

Satz 2.8
In diesem Fall verlangt die Maximum-Likelihood-Decodierung eine Decodierung zum nächstgelegenem Codewort, d.h. zum Codewort mit minimalem Hammingabstand zum empfangenem Wort.

Beweis: Betrachte für ein festes $v \in F^n$ und beliebiges $c' \in \mathcal{C}$ mit $d(v,c') = l$ die Wahrscheinlichkeit

$$P(v|c') = (\frac{p}{q-1})^l (1-p)^{n-l} = (\frac{p}{(q-1)(1-p)})^l (1-p)^n.$$

Mit obigen Ungleichungen für p und $1-p$ gilt $\frac{p}{q-1} \cdot \frac{1}{1-p} < \frac{1}{q} \cdot \frac{1}{1-p} < \frac{1}{q} \cdot q = 1$. Mithilfe dieser Ungleichung erkennen wir, dass die Funktion $f(l) \coloneqq (\frac{p}{q-1})^l (1-p)^{n-l} = (\frac{p}{(q-1)(1-p)})^l (1-p)^n$ mit wachsendem l monoton fallend ist. Demnach gilt $P(v|c) = \max_{c' \in \mathcal{C}} P(v|c')$ genau für die Codeworte $c \in \mathcal{C}$, für die $d(v,c) = \min_{c' \in \mathcal{C}} d(v,c')$ gilt. □

Korollar 2.9
Ist $B_l(c) \cap B_l(c') = \emptyset$ für alle $c, c' \in \mathcal{C}$ mit $c \neq c'$, so werden mit der Maximum-Likelihood-Decodierung bis zu l Fehler korrigiert.

Diese Erkenntnis führt uns zu folgender wichtigen Definition.

Definition 2.10
Sei $\mathcal{C} \subseteq F^n$ ein q-närer Blockcode der Länge n über F.

i) $\mathcal{C}$ heißt t-fehlererkennend, falls $B_t(c) \cap \mathcal{C} = \{c\}$ für alle $c \in \mathcal{C}$.

ii) $\mathcal{C}$ heißt e-fehlerkorrigierend, falls $B_e(c) \cap B_e(c') = \emptyset$ für alle $c, c' \in \mathcal{C}$ mit $c \neq c'$.

iii) Ist $|\mathcal{C}| > 1$, dann nennen wir $d(\mathcal{C}) := \min\{d(c, c') \mid c, c' \in \mathcal{C} \text{ mit } c \neq c'\}$ die Minimaldistanz von $\mathcal{C}$.

iv) Ist $d(\mathcal{C}) = d$ und $|\mathcal{C}| = M$, so nennen wir $\mathcal{C}$ einen $(n, M, d)_q$- Code über F.

Satz 2.11
Sei $\mathcal{C}$ ein Blockcode mit Minimaldistanz $d(\mathcal{C}) = d$ und $t, e \in \mathbb{N}$.

i) Falls $d \geq t + 1$, so ist $\mathcal{C}$ t-fehlererkennend.

ii) Falls $d \geq 2e + 1$, so ist $\mathcal{C}$ e-fehlerkorrigierend.

Beweis: Sei für den ersten Teil $c \in \mathcal{C}$ und $v \in B_t(c)$, dann gilt für die Hamming-Distanz $d(v, c) \leq t \leq d - 1$. Somit muss $v = c$ oder $v \notin \mathcal{C}$ gelten und es folgt $B_t(c) \cap \mathcal{C} = \{c\}$. Für den zweiten Teil sei zusätzlich $c' \in \mathcal{C}$ mit $c \neq c'$, somit gilt $2e + 1 \leq d \leq d(c, c')$. Nun folgt mit der Annahme, dass $v \in B_e(c) \cap B_e(c')$ existiert und mit Satz 2.5 iii), dass $d(c, c') \leq d(c, v) + d(v, c') \leq 2e$. Dies führt zum Widerspruch und somit ist $B_e(c) \cap B_e(c') = \emptyset$. □

2.2 Algebraische Zahlentheorie

Zunächst erinnern wir an die Definitionen eines algebraischen Zahlkörpers und seines Ganzheitsrings $\mathcal{O}_K$.

Definition 2.12

i) Als (algebraischen) Zahlkörper K bezeichnet man eine endliche Körpererweiterung des Körpers $\mathbb{Q}$ der rationalen Zahlen.

ii) Ein Element $x \in K$ heißt ganz über $\mathbb{Z}$, falls x eine Nullstelle eines normierten Polynoms $f \in \mathbb{Z}[t]$ ist. Der ganze Abschluss von $\mathbb{Z}$ in K sind alle Elemente $x \in K$, die ganz über $\mathbb{Z}$ sind.

iii) Ist K ein Zahlkörper, so heißt der ganze Abschluss von $\mathbb{Z}$ in K Ganzheitsring von K und wird als $\mathcal{O}_K \subseteq K$ notiert.

Zahlkörper sind als endliche Körpererweiterungen algebraisch. Außerdem lässt sich ein Zahlkörper K mit einem Körpererweiterungsgrad $[K : \mathbb{Q}] = m$ nach dem Satz vom primitiven Element schreiben als $K = \mathbb{Q}(\alpha)$, wobei α eine Nullstelle eines irreduziblen Polynoms vom Grad m über $\mathbb{Q}$ ist.

Anschließend wiederholen wir einige weitere wichtige Grundlagen über den Ganzheitsring $\mathcal{O}_K$ und dessen (Prim-)Ideale.

Satz 2.13

i) Der Ganzheitsring $\mathcal{O}_K$ eines Zahlkörpers K ist ein Dedekindring der Krulldimension Eins, d.h. er ist ein ganzabgeschlossener, noetherscher Integritätsring, der kein Körper ist und in dem jedes von Null verschiedene Primideal $\mathfrak{P}$ von $\mathcal{O}_K$ maximal ist.

ii) Jedes von (0) verschiedene Ideal $I \subset \mathcal{O}_K$ kann bis auf Reihenfolge eindeutig als endliches Produkt von Primidealen dargestellt werden.

Bemerkung 2.14

Ein Primideal $\mathfrak{P}$ ist genau dann in I enthalten, wenn $\mathfrak{P}$ in der Primidealzerlegung von I vorkommt.

Beweis: Für einen Beweis von i) sei auf Satz 8.1 auf Seite 47 des [Neu92] verwiesen, wobei $\mathfrak{o} = \mathbb{Z}$ ein Dedekindring ist. Teil ii) ist ebenfalls mit Beweis im [Neu92] auf Seite 19ff. unter Theorem 3.3 zu finden. □

Definition 2.15

Sei $L|K$ eine endliche Körpererweiterung von Zahlkörpern. Mit Satz 2.13ii) können wir ein Primideal aus $\mathcal{O}_K$ in $\mathcal{O}_L$ faktorisieren als $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdot \mathfrak{P}_2^{e_2} \cdot \ldots \cdot \mathfrak{P}_n^{e_n}$ mit $\mathfrak{P}_i \neq \mathfrak{P}_j$ für $i \neq j$. Wir nennen $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n$ die über $\mathfrak{p}$ liegenden Primideale in $\mathcal{O}_L$ und die Zahl $e_i = e(\mathfrak{P}_i|\mathfrak{p})$ den Verzweigungsindex des Primideals $\mathfrak{P}_i$ über $\mathfrak{p}$. Den Körpererweiterungsgrad $f_i = f(\mathfrak{P}_i|\mathfrak{p}) \coloneqq [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ nennen wir Trägheitsgrad von $\mathfrak{P}_i$ über $\mathfrak{p}$.
Ein Primideal $\mathfrak{P}_i$ heißt verzweigt über $\mathfrak{p}$, falls $e_i > 1$, ansonsten ist es unverzweigt. Das Primideal $\mathfrak{p}$ heißt verzweigt, wenn es ein $e_i > 1$ gibt, ansonsten ist $\mathfrak{p}$ unverzweigt. Man sagt, ein Primideal $\mathfrak{p}$ aus $\mathcal{O}_K$ ist voll zerlegt, falls jedes $e_i = f_i = 1$ für alle i.

Satz 2.16

Die Zahlen e_i und f_i aus Definition 2.15 genügen der fundamentalen Gleichung $\sum_{i=1}^{n} e_i f_i = m$, wobei m der Grad der Körpererweiterung von L über K ist. Die Zahlen e_i, f_i sind in Körpertürmen multiplikativ, d.h. für einen Körperturm von endlichen Körpererweiterungen $M|L|K|\mathbb{Q}$, ihren Ganzheitsringen $\mathcal{O}_M, \mathcal{O}_L, \mathcal{O}_K$ und einem Primideal $\mathfrak{P}$ in $\mathcal{O}_M$ mit $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_L$ und $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \cap \mathcal{O}_K$, s.d. $\mathfrak{P}|\mathfrak{p}|\mathfrak{q}$ übereinanderliegen, gilt, dass $e(\mathfrak{P}|\mathfrak{q}) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|\mathfrak{q})$ und $f(\mathfrak{P}|\mathfrak{q}) = f(\mathfrak{P}|\mathfrak{p})f(\mathfrak{p}|\mathfrak{q})$.

Beweis: Ein Beweis der fundamentalen Gleichung $\sum_{i=1}^{n} e_i f_i = m$ ist zu finden in Satz 8.2 auf den Seiten 48f. in [Neu92]. Die Multiplikativität der Trägheitsgrade entspricht dem Gradsatz bei Körpererweiterungen. Betrachte nun mithilfe von Satz 2.13ii) $\mathfrak{q}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_n^{e_n} \cdot \mathfrak{p}^{e}$ und $\mathfrak{p}\mathcal{O}_M = \mathfrak{P}_1^{e_1{}'} \cdot \ldots \cdot \mathfrak{P}_n^{e_n{}'} \cdot \mathfrak{P}^{e'}$, da hier $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_L$, folgt mit der Eindeutigkeit der Primidealzerlegung, dass $\mathfrak{p}_i \nsubseteq \mathfrak{P} \cap \mathcal{O}_L$ für $i = 1, \ldots, n$. Daher können wir festhalten, dass $\mathfrak{P}$ nicht über $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ liegt und beim Betrachten von $\mathfrak{q}\mathcal{O}_M = \prod_{i=1}^{n} (\prod_{j=1}^{m_i} \mathfrak{P}'^{e_j''}_j)^{e_i} \cdot (\mathfrak{P}_1^{e_1{}'} \cdot \ldots \cdot \mathfrak{P}_n^{e_n{}'} \cdot \mathfrak{P}^{e'})^{e}$ folgern, dass $\mathfrak{P}$ im linken Faktor nicht auftritt, weswegen $e(\mathfrak{P}|\mathfrak{q}) = e' \cdot e = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|\mathfrak{q})$ gilt. Dabei haben wir benutzt, dass für zwei Ideale I, J eines kommutativen Ringes $IJ = JI$ gilt. □

Nachfolgend definieren wir eine Normfunktion für Ideale und Elemente von $\mathcal{O}_K$.

Definition 2.17

i) Die Norm eines von Null verschiedenen Ideals $I \subset \mathcal{O}_K$ ist definiert als $\|I\| \coloneqq |\mathcal{O}_K/I|$, d.h. als die Mächtigkeit von $\mathcal{O}_K/I$.

ii) Die Norm eines von Null verschiedenen Elementes $x \in \mathcal{O}_K$ ist definiert als $\|x\| := \|(x)\|$, d.h. als die Norm des von x erzeugten Ideals. Wir definieren $\|0\| := 0$.

Sei $p \in \mathbb{Z}$ eine Primzahl. Da jedes über p liegende Primideal $\mathfrak{p}_i$ maximal ist, ist $\mathcal{O}_K/\mathfrak{p}_i$ als endliche Körpererweiterung von $\mathbb{Z}/(p)$ selbst ein endlicher Körper und hat nach Definition 2.15 einen Erweiterungsgrad von f_i und somit eine Mächtigkeit von p^{f_i}. Also gilt für ein Primideal $\mathfrak{p}$ das über $p \in \mathbb{Z}$ liegt, dass $\|\mathfrak{p}\| = p^{f(\mathfrak{p}|p)}$.

Definition 2.18
Seien I, J von Null verschiedene Ideale aus $\mathcal{O}_K$, dann sagen wir J teilt I genau dann, wenn $I \subset J$, und notieren dies als $J|I$.

Satz 2.19

i) Sei I ein von Null verschiedenes Ideal aus $\mathcal{O}_K$ und $0 \neq x \in I$. Dann gilt $\|I\|$ teilt $\|x\|$.

ii) Für zwei von Null verschiedene Ideale I und J aus $\mathcal{O}_K$ gilt $\|I \cdot J\| = \|I\| \cdot \|J\|$.

Beweis: Betrachte für i) zunächst die surjektive Abbildung $\pi\colon \mathcal{O}_K \to \mathcal{O}_K/I$ mit $r \mapsto [r]$. Nun folgt mit der universellen Eigenschaft der Faktorgruppe, dass ein Homomorphismus

$$\phi\colon G := \mathcal{O}_K/(x) \to G' := \mathcal{O}_K/I \text{ mit } [r] \mapsto [r]$$

existiert, da $(x) \subset \ker(\pi) = I$. Die Abbildung ϕ ist offensichtlich surjektiv. Weiterhin gilt mithilfe des Homomorphiesatzes die Isomorphie $G/\ker(\phi) \cong \mathrm{im}(\phi) = G'$, was insbesondere bedeutet, dass $|G'| = |G/\ker(\phi)| = \frac{|G|}{|\ker(\phi)|}$. Daraus folgt $|G'| = \|I\|$ teilt $|G| = \|x\|$. Für den Beweis von ii) sei auf Satz 6.1 auf Seite 37 des [Neu92] verwiesen. □

3 Grundidee der Konstruktion algebraischer Codes

In diesem Kapitel betrachten wir das Grundprinzip der Konstruktion von algebraischen-fehlerkorrigierenden Codes. Dazu gehören beispielsweise folgende bekannte Codes: Hamming-Code, Reed-Muller-Code, Reed-Solomon-Code, Simplex Codes, Algebraisch-Geometrische Codes und die Chinese-Remainder Codes.
Grundsätzlich wird ein algebraischer-fehlerkorrigierender Code auf einem zugrunde liegenden (Integritäts-) Ring R definiert, dessen Elemente $r \in R$ eine gewisse „Größe“ haben, welche wir als $size(r)$ notieren. Dies betrachten wir am Beispiel des Reed-Solomon-Codes.

Definition 3.1
Sei $\mathbb{F}_q$ der endliche Körper mit $q = p^m$ Elementen mit p prim und $m, k \in \mathbb{N}$. Seien $u_1, \ldots, u_n \in \mathbb{F}_q$ paarweise verschieden und fest. Dann ist

$$\mathcal{C} = \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid a_i = f(u_i),\ i = 1, \ldots, n, \text{ für ein } f \in \mathbb{F}_q[x] \text{ mit } \deg(f) < k\}$$

ein Reed-Solomon-Code $RS(q, k, n)$ der Länge n für Nachrichten der Größe k über $\mathbb{F}_q$ mit den Wertetupeln aller Polynome aus $\mathbb{F}_q[x]$ mit Grad kleiner k an den gewählten Stützstellen.

Hier ist der zugrunde liegende Ring der Polynomring $\mathbb{F}_q[X]$ und die „Größe“ eines Elements f aus $\mathbb{F}_q[X]$ gleich dem Grad von f, also $size(f) = \deg(f)$ mit $f \in \mathbb{F}_q[X]$. Ähnlich ist es beim Chinese Remainder Code (kurz CRT-Code vgl. dazu [Gur00b]), hier ist der zugrundeliegende Ring $\mathbb{Z}$ und $size(z)$ mit $z \in \mathbb{Z}$ ist die Betragsfunktion. Allgemein gilt, die Nachrichten eines Codes sind all diejenigen Elemente des Rings R, die eine maximale Größe Λ haben.
Eine Codierung der Nachricht $m \in R$ ist gegeben durch eine Abbildung

$$m \mapsto \text{Enc}(m) = (m/I_1, \ldots, m/I_n)$$

wobei I_i mit $1 \leq i \leq n$ verschiedene Primideale von R sind. So können wir in einem Spezialfall des Reed-Solomon-Codes $RS(q, q-1, n)$ (Definition 3.1) zum Beispiel $R = \mathbb{F}_q[X]$ und $I_i = (X - u_i)$ für $1 \leq i \leq n$ setzen. Wobei $u_1, \ldots, u_n$ verschiedene Elemente von $\mathbb{F}_q$ sind.
Für die Konstruktion eines Codes sind für uns zwei Eigenschaften von besonderem Interesse, zum einen die Informationsrate des Codes (Definition 2.3) und zum anderem seine Minimaldistanz (Definition 2.10iii)). Dabei werden wir feststellen, dass für unsere $size(\cdot)$-Funktion die Erfüllung der nachfolgenden zwei Eigenschaften essentiell ist, um das entsprechende Resultat zur Informationsrate und Minimaldistanz aus Satz 4.29 herzuleiten.

1. Mit $a, b \in R$ ist $size(a-b)$ immer dann „klein“, wenn sowohl $size(a)$ als auch $size(b)$ „klein“ ist.
2. Falls $f \neq 0$ mit $f \in R$ in „vielen“ Idealen $I_1, I_2, \ldots, I_n$ enthalten ist, ist $size(f)$ nicht zu „klein“.

4 Konstruktion von Codes mit algebraischen Zahlkörpern

Im vorangehendem Kapitel haben wir gesehen wie algebraische Codes über Ringen konstruiert werden. Dort benötigen wir zusätzlich zu einem Ring R noch eine geeignete „Größe“ für Elemente dieses Rings. In diesem Kapitel werden wir algebraische Codes über einem Zahlkörper K beziehungsweise seinem Ganzheitsring $\mathcal{O}_K$ konstruieren und dazu zunächst eine geeignete $size(\cdot)$-Funktion für Elemente aus K definieren.

4.1 Definition der „Größe“ eines Elements

Mit dem Wissen aus Kapitel 3 und den Grundlagen aus Kapitel 2 würde es sich anbieten, die „Größe“ eines Elements $x \in \mathcal{O}_K$ als $size(x) := \|x\|$ zu definieren. Dies würde tatsächlich unsere zweite geforderte Eigenschaft aus Kapitel 3 an die $size(\cdot)$-Funktion erfüllen. Eigenschaft 1 wird allerdings nicht erfüllt, dies verdeutlichen wir am nachfolgendem Beispiel.

Beispiel 4.1
Sei $K = \mathbb{Q}(\alpha)$, wobei $\alpha \in \mathbb{R}$ eine Nullstelle von $x^2 + Dx + 1$ mit $D \in \mathbb{Z}_{>2}$. Sei $\beta \in \mathbb{R}$ die andere Nullstelle, also gilt $x^2+Dx+1 = (x-\alpha)(x-\beta)$. Wegen $1 = ||1|| = ||\alpha\beta|| = ||\alpha|| \cdot ||\beta||$ mit $||\alpha||, ||\beta|| \in \mathbb{Z}$ (da $\alpha, \beta \in \mathcal{O}_K$) gilt $||\alpha|| = ||\beta|| = 1$. Außerdem gilt $D + 2 = ||D + 2|| = ||\alpha - 1|| \cdot ||\beta - 1||$. Da $D + 2$ beliebig groß werden kann, kann $||\alpha - 1||$ oder $||\beta - 1||$ beliebig groß werden. Also widerspricht eines der Paare $(\alpha, \alpha - 1)$ oder $(\beta, \beta - 1)$ Eigenschaft 1.

Daher werden wir uns in diesem Unterkapitel hauptsächlich damit beschäftigen, eine besser geeignete $size(\cdot)$-Funktion zu finden. Dazu machen wir uns die Bewertungstheorie von Zahlkörpern zunutze.

4.1.1 Bewertung eines Zahlkörpers

Definition 4.2
Eine Bewertung (später auch Stelle (eng. place)) oder auch Absolutbetrag eines Körpers K ist eine Funktion $|\cdot| : K \to \mathbb{R}$, für die für $x, y \in K$ gilt

i) $|x| \geq 0$ und $|x| = 0$ genau dann, wenn $x = 0$,

ii) $|xy| = |x||y|$ und

iii) $|x - y| \leq |x| + |y|$.

Von nun an schließen wir stets aus, dass $|\cdot|$ die triviale Bewertung ($|x| = 1$ für alle $x \neq 0$) von K ist.

Definition 4.3
Zwei Bewertungen $|\cdot|_1$ und $|\cdot|_2$ von K heißen äquivalent, wenn sie die gleiche Topologie auf K definieren.

Satz 4.4
Zwei Bewertungen $|\cdot|_1$ und $|\cdot|_2$ sind genau dann äquivalent, wenn ein $s > 0$ in $\mathbb{R}$ existiert, sodass für alle $x \in K$ bereits $|x|_1 = |x|_2^s$ gilt.

Beweis: Für den Beweis sei auf Satz 3.3 auf den Seiten 121f. des [Neu92] verwiesen. □

Definition 4.5
Eine Stelle von K ist eine Äquivalenzklasse von Bewertungen von K.

Definition 4.6
Eine Bewertung $|\cdot|$ heißt nicht-archimedisch, wenn $|n|$ für alle $n \in \mathbb{N}$ beschränkt ist, sonst heißt sie archimedisch.

Satz 4.7
Eine Bewertung $|\cdot|$ ist genau dann nicht-archimedisch, wenn sie der verschärften Dreiecksungleichung

$$|x + y| \leq \max\{|x|, |y|\}$$

genügt.

Beweis: Für den Beweis sei auf Satz 3.6 auf den Seiten 123f. des [Neu92] verwiesen. □

Beispiel 4.8

1. Der gewöhnliche Absolutbetrag auf $\mathbb{Q}$ ist eine archimedische Bewertung.

2. Sei p eine Primzahl und sei $v_p(a/b)$ die höchste p-Potenz die $a/b \in \mathbb{Q}$ teilt, genauer sei $v_p(a/b) := n - m$ für $a = p^n z \in \mathbb{Z}$ und $b = p^m z' \in \mathbb{Z}$ mit $ggt(p, z) = 1 = ggt(p, z')$. Dann ist die für die Zahlentheorie wichtige Bewertung $|x|_p = p^{-v_p(x)}$ eine nicht-archimedische Bewertung auf $\mathbb{Q}$.

3. Sei $h(x) = f(x)/g(x) \in \mathbb{Q}(X)$ mit $f(x), g(x) \in \mathbb{Q}(X)$ und sei $\deg(h) \coloneqq \deg(f) - \deg(g)$, dann ist die Bewertung $|h| = e^{\deg(h)}$ auf dem Körper der ganzrationalen Funktionen $\mathbb{Q}(X)$ über $\mathbb{Q}$ ebenfalls nicht-archimedisch.

4.1.2 Unendliche Stellen

Betrachten wir zunächst eine Körpererweiterung $K|\mathbb{Q}$ mit Grad $[K : \mathbb{Q}] = m$. Dann gibt es $r + 2s$ verschiedene Körperhomomorphismen von K nach $\mathbb{C}$ die $\mathbb{Q}$ festhalten. Davon sind r der Einbettungen reell, namentlich $\tau_i : K \to \mathbb{R}$ mit $1 \leq i \leq r$ und die anderen $2s$ Einbettungen sind als s Paare komplex konjugierte nicht-reelle Einbettungen nach $\mathbb{C}$, namentlich $\sigma_j, \overline{\sigma}_j : K \to \mathbb{C}$ mit $1 \leq j \leq s$. Die Zahlen r und s definieren die Signatur (r, s).
Die nachfolgende Definition gibt uns den nützlichen Zusammenhang zwischen diesen Einbettungen und den archimedischen Stellen.

Definition 4.9
Sei $K|\mathbb{Q}$ eine endliche Galoiserweiterung vom Grad m mit Signatur (r, s). Dann gilt nach dem Hauptsatz der Galoistheorie $m = r + 2s$ und wir erhalten genau $r + s$ unendliche Stellen, welche wir mit $\mathfrak{q}_1, \ldots, \mathfrak{q}_{r+s}$ bezeichnen. Die r unendlichen Stellen $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ entsprechen den durch die r reellen Einbettungen $\tau_1, \ldots, \tau_r$ gegebenen archimedischen Bewertungen $|x|_{\mathfrak{q}_i} \coloneqq |\tau_i(x)|$ mit $1 \leq i \leq r$ und die s unendlichen Stellen $\mathfrak{q}_{r+1}, \ldots, \mathfrak{q}_{r+s}$ entsprechen den durch die s Paare von komplex konjugierten Einbettungen $\sigma_j, \overline{\sigma}_j$ gegebenen archimedischen Bewertungen $|x|_{\mathfrak{q}_{r+j}} \coloneqq |\sigma_j(x)|^2$ mit $1 \leq j \leq s$.

Bemerkung 4.10
Die Normierung über das Quadrat $|\sigma_j(x)|^2$ ist eine wichtige Konvention. Allerdings erfüllt diese Abbildung nicht mehr Bedingung iii) in Definiton 4.2. Da wir mit der Wurzel arbeiten werden, spielt das aber keine Rolle.

4.1.3 „Größe“ eines Elements

Als Nächstes folgt unsere neue Definition von $size(x)$ für Elemente x eines Zahlkörpers K. Diese erfüllt dann Eigenschaft 1 im Gegensatz zu unserer anfänglichen „Definition“ von $size(x) = \|x\|$, was wir im anschließendem Lemma zeigen werden.

Definition 4.11
Sei K ein Zahlkörper der Signatur (r, s). Dann sei die „Größe“ eines Elements $x \in K$ definiert als

$$size(x) \coloneqq \sum_{i=1}^{r} |x|_{\mathfrak{q}_i} + \sum_{i=1}^{s} 2\sqrt{|x|_{\mathfrak{q}_{r+i}}}.$$

Lemma 4.12
Sei K ein Zahlkörper mit Signatur (r, s) und seien $a, b \in \mathcal{O}_K$. Dann gilt $size(a-b) \leq size(a)+size(b)$.

Beweis: Für den Beweis benötigen wir für die dritte Zeile der abschließenden Ungleichungskette, dass $\sqrt{|a|_{\mathfrak{q}_i} + |b|_{\mathfrak{q}_i}} \leq \sqrt{|a|_{\mathfrak{q}_i}} + \sqrt{|b|_{\mathfrak{q}_i}}$. Dazu betrachte man die Ungleichung

$$(\sqrt{|a|_{\mathfrak{q}_i} + |b|_{\mathfrak{q}_i}})^2 = |a|_{\mathfrak{q}_i} + |b|_{\mathfrak{q}_i} \leq |a|_{\mathfrak{q}_i} + 2\sqrt{|a|_{\mathfrak{q}_i}}\sqrt{|b|_{\mathfrak{q}_i}} + |b|_{\mathfrak{q}_i} = (\sqrt{|a|_{\mathfrak{q}_i}} + \sqrt{|b|_{\mathfrak{q}_i}})^2.$$

Nun gilt mit der Definition von $size(\cdot)$ aus 4.11, der Dreiecksungleichung aus Definition 4.2iii) und obiger Ungleichung

$$\begin{aligned}
size(a-b) &= \sum_{i=1}^{r} |a-b|_{\mathfrak{q}_i} + \sum_{i=1}^{s} 2\sqrt{|a-b|_{\mathfrak{q}_{r+i}}} \\
&\leq \sum_{i=1}^{r} (|a|_{\mathfrak{q}_i} + |b|_{\mathfrak{q}_i}) + \sum_{i=1}^{s} 2\sqrt{|a|_{\mathfrak{q}_{r+i}} + |b|_{\mathfrak{q}_{r+i}}} \\
&\leq \sum_{i=1}^{r} (|a|_{\mathfrak{q}_i} + |b|_{\mathfrak{q}_i}) + \sum_{i=1}^{s} 2(\sqrt{|a|_{\mathfrak{q}_{r+i}}} + \sqrt{|b|_{\mathfrak{q}_{r+i}}}) \\
&= \sum_{i=1}^{r} |a|_{\mathfrak{q}_i} + \sum_{i=1}^{r} |b|_{\mathfrak{q}_i} + \sum_{i=1}^{s} 2\sqrt{|a|_{\mathfrak{q}_{r+i}}} + \sum_{i=1}^{s} 2\sqrt{|b|_{\mathfrak{q}_{r+i}}} \\
&= \sum_{i=1}^{r} |a|_{\mathfrak{q}_i} + \sum_{i=1}^{s} 2\sqrt{|a|_{\mathfrak{q}_{r+i}}} + \sum_{i=1}^{r} |b|_{\mathfrak{q}_i} + \sum_{i=1}^{s} 2\sqrt{|b|_{\mathfrak{q}_{r+i}}} \\
&= size(a) + size(b). \qquad \square
\end{aligned}$$

Nachfolgende Proposition und anschließendes Lemma geben uns den Zusammenhang zwischen unserer „Größe“ und der Norm eines Elements und weiterhin eine von $size(\cdot)$ abhängige obere Schranke für $\|x\|$.

Proposition 4.13
Sei K ein Zahlkörper mit der Signatur (r,s) und sei $x \in \mathcal{O}_K$. Dann gilt

$$\|x\| = \prod_{i=1}^{r+s} |x|_{\mathfrak{q}_i},$$

mit den archimedischen Stellen $|\cdot|_{\mathfrak{q}_i}$ von oben für $1 \leq i \leq r+s$.

Beweis: Mithilfe des 1. Kapitels §6 auf Seite 36f. des [Neu92] können wir folgern, dass unsere Absolutnorm $\|x\|$ gleich dem Betrag der Norm der Erweiterung $K|Q$ ist, also $\|x\| = |N_{K|\mathbb{Q}}(x)|$ für alle $x \in K$. Für diese gilt nach Satz 2.6 auf Seite 9f. des [Neu92], dass $N_{K|\mathbb{Q}} = \prod_{\pi} \pi(x)$, wobei π genau unsere $(r+2s)$ verschiedenen Einbettungen vom Beginn dieses Kapitels durchläuft. Diese definieren exakt die archimedischen Stellen $|\cdot|_{\mathfrak{q}_i}$. $\square$

Lemma 4.14
Sei K ein Zahlkörper mit der Signatur (r,s) und sei $x \in \mathcal{O}_K$. Dann gilt $\|x\| \leq (\frac{size(x)}{M})^M$ mit $M = r+2s$.

Beweis: Für den Beweis nutzen wir die Ungleichung des arithmetischen und geometrischen Mittels, nach der das geometrische Mittel kleiner oder gleich dem arithmetischem Mittel ist. Diese kann einschließlich eines Beweises in [Cau21] auf Seite 457ff. nachgelesen werden.
Zunächst betrachten wir mithilfe von Proposition 4.13

$$\|x\| = \prod_{i=1}^{r} |x|_{\mathfrak{q}_i} \prod_{i=1}^{s} |x|_{\mathfrak{q}_{r+i}} = \prod_{i=1}^{r} |x|_{\mathfrak{q}_i} \prod_{i=1}^{s} \sqrt{|x|_{\mathfrak{q}_{r+i}}} \prod_{i=1}^{s} \sqrt{|x|_{\mathfrak{q}_{r+i}}},$$

anschließend können wir die M-te Wurzel ziehen und zum arithmetischem Mittel abschätzen

$$\sqrt[M]{\|x\|} = \left(\prod_{i=1}^{r} |x|_{\mathfrak{q}_i} \prod_{i=1}^{s} \sqrt{|x|_{\mathfrak{q}_{r+i}}} \prod_{i=1}^{s} \sqrt{|x|_{\mathfrak{q}_{r+i}}}\right)^{\frac{1}{M}}$$
$$\leq \frac{\sum_{i=1}^{r} |x|_{\mathfrak{q}_i} + \sum_{i=1}^{s} \sqrt{|x|_{\mathfrak{q}_{r+i}}} + \sum_{i=1}^{s} \sqrt{|x|_{\mathfrak{q}_{r+i}}}}{M} = \frac{size(x)}{M}.$$

Daraus folgt schließlich $\|x\| \leq (\frac{size(x)}{M})^M$. □

Mit diesem Lemma und Lemma 4.12, können wir anschließend etwas über die Größe des Abstands zweier Elemente aus $\mathcal{O}_K$ folgern.

Korollar 4.15
Sei K ein Zahlkörper vom Grad $[K : \mathbb{Q}] = M$, $B \in \mathbb{R}$ und $a, b \in \mathcal{O}_K$ mit $size(a) \leq B$ und $size(b) \leq B$. Dann gilt $\|a - b\| \leq (\frac{2B}{M})^M$.

Beweis: Es gilt mit Lemma 4.12, dass $size(a - b) \leq size(a) + size(b) \leq 2B$ und mit Lemma 4.14 folgt $\|a - b\| \leq (\frac{size(a-b)}{M})^M \leq (\frac{2B}{M})^M$. □

4.1.4 Verschiebung der „Größe“

Wir haben nun alle Grundlagen zur Konstruktion unseres Codes zusammengetragen, benötigen allerdings später aus technischen Gründen noch einen zusätzlichen Verschiebungsparameter $\mathfrak{z}$, der die Größe $size(\cdot)$ verschiebt. Diesen führen wir der Vollständigkeit halber bereits jetzt ein. Aus dem Unterkapitel 4.4 zur Informationsrate des Codes geht hervor, warum wir diesen benötigen.

Definition 4.16
Sei K ein Zahlkörper der Signatur (r, s) und sei $\mathfrak{z} \in \mathbb{R}^r \times \mathbb{C}^s$ also $\mathfrak{z} = (z_1, \ldots, z_{r+s})$ der Verschiebungsparameter mit $z_i \in \mathbb{R}$ für $1 \leq i \leq r$ und $z_{r+j} \in \mathbb{C}$ für $1 \leq j \leq s$. Seien weiterhin wie in Kapitel 4.1.2 τ_i und σ_j die Körperhomomorphismen, die $\mathbb{Q}$ festhalten, und $x \in \mathcal{O}_K$. Dann definiere $a_i^{(x)} \coloneqq |\tau_i(x) - z_i|$ für $1 \leq i \leq r$, $b_j^{(x)} \coloneqq |\sigma_j(x) - z_{r+j}|^2$ für $1 \leq j \leq s$ und

$$size_{\mathfrak{z}}(x) \coloneqq \sum_{i=1}^{r} a_i^{(x)} + \sum_{j=1}^{s} 2\sqrt{b_j^{(x)}}.$$

Diese Definition von $size_{\mathfrak{z}}(\cdot)$ ist unserer vorherigen Definition also sehr ähnlich, trotzdem müssen wir im nächstem Lemma prüfen, dass das Ergebnis aus Korollar 4.15 auch für diese Verschiebung gilt.

Lemma 4.17
Sei K ein Zahlkörper vom Grad $[K : \mathbb{Q}] = r + 2s = M$ mit Signatur (r, s), sei $\mathfrak{z} \in \mathbb{R}^r \times \mathbb{C}^s$, $B \in \mathbb{R}$ und $a, b \in \mathcal{O}_K$ mit $size_{\mathfrak{z}}(a) \leq B$ und $size_{\mathfrak{z}}(b) \leq B$. Dann gilt $\|a - b\| \leq (\frac{2B}{M})^M$.

Beweis: Zu Beginn zeigen wir, dass aus $size_{\mathfrak{z}}(a) \leq B$ und $size_{\mathfrak{z}}(b) \leq B$ folgt, dass $size(a - b) \leq 2B$ gilt. Dazu folgen wir der Beweisstruktur von Lemma 4.12 und nutzen weiterhin aus, dass unsere

Einbettungen τ_i und σ_j linear sind, somit gilt

$$\begin{aligned}
size(a-b) &= \sum_{i=1}^{r} |a-b|_{\mathfrak{q}_i} + \sum_{i=1}^{s} 2\sqrt{|a-b|_{\mathfrak{q}_{r+i}}} \\
&= \sum_{i=1}^{r} |\tau_i(a-b) - z_i + z_i| + \sum_{i=1}^{s} 2|\sigma_i(a-b) - z_{r+i} + z_{r+i}| \\
&= \sum_{i=1}^{r} |(\tau_i(a) - z_i) - (\tau_i(b) - z_i)| + \sum_{i=1}^{s} 2|(\sigma_i(a) - z_{r+i}) - (\sigma_i(b) - z_{r+i})| \\
&\leq \sum_{i=1}^{r} (|\tau_i(a) - z_i| + |\tau_i(b) - z_i|) + \sum_{i=1}^{s} (2|\sigma_i(a) - z_{r+i}| + 2|\sigma_i(b) - z_{r+i}|) \\
&= \sum_{i=1}^{r} |\tau_i(a) - z_i| + \sum_{i=1}^{s} 2|\sigma_i(a) - z_{r+i}| + \sum_{i=1}^{r} |\tau_i(b) - z_i| + \sum_{i=1}^{s} 2|\sigma_i(b) - z_{r+i}| \\
&= \sum_{i=1}^{r} a_i^{(a)} + \sum_{i=1}^{s} 2\sqrt{b_j^{(a)}} + \sum_{i=1}^{r} a_i^{(b)} + \sum_{i=1}^{s} 2\sqrt{b_j^{(b)}} \\
&= size_{\mathfrak{z}}(a) + size_{\mathfrak{z}}(b).
\end{aligned}$$

Es folgt $size(a-b) \leq size_{\mathfrak{z}}(a) + size_{\mathfrak{z}}(b) \leq 2B$ und wir können Lemma 4.14 nutzen, um die gewünschte Aussage zu erhalten. □

4.2 NF-Code-Konstruktion

Nun sind wir bei der Konstruktion unseres Zahlkörper-Codes angekommen, hierfür sei K ein Zahlkörper vom Grad $[K : \mathbb{Q}] = M$ mit der Signatur (r, s). Ein Zahlkörpercode, kurz NF-Code (Numberfield-Code), basiert auf dem Zahlkörper K und hat die Parameter $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; \mathfrak{z})$, wobei n die Blocklänge des Codes ist, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ unterschiedliche von Null verschiedene Primideale von $\mathcal{O}_K$ sind, B eine positive reelle Zahl ist und $\mathfrak{z}$ der Verschiebungsparamter aus $\mathbb{R}^r \times \mathbb{C}^s$ ist. Die i-te Position eines Codewortes aus $\mathcal{C}$ ist definiert über einem Alphabet der Größe $\|\mathfrak{p}_i\|$ mit $1 \leq i \leq n$, daher nehmen wir o.B.d.A. an, dass $\|\mathfrak{p}_1\| \leq \cdots \leq \|\mathfrak{p}_n\|$. Wir definieren nun formal unseren Zahlkörpercode.

Definition 4.18
Der Zahlkörpercode $\mathcal{C} = \mathcal{C}_K$ mit obigen Parametern $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; \mathfrak{z})$ und einem Zahlkörper K ist wie folgt definert. Die Nachrichtenmenge von $\mathcal{C}$ ist $\{m \in \mathcal{O}_K \mid size_{\mathfrak{z}}(m) \leq B\}$ und die Kodierungsfunktion ist gegeben durch $\text{Enc}(m) = (m/\mathfrak{p}_1, \ldots, m/\mathfrak{p}_n)$.

Bemerkung 4.19
Wir gehen stets davon aus, dass unser Zahlkörpercode $\mathcal{C}_K$ nicht trivial ist, d.h., dass es mindestens zwei unterschiedliche Codeworte m_1 und m_2 gibt. Daraus folgt mit Lemma 4.17, dass $B \geq M/2$.

In den nächsten beiden Unterkapiteln betrachten wir die Distanz und die Informationsrate des NF-Codes diese gehören zu den beiden wichtigsten Eigenschaften eines Codes und sollten daher gesondert betrachten werden.

4.3 Minimaldistanz des NF-Codes

Lemma 4.20
Sei $\mathcal{C} = \mathcal{C}_K$ ein NF-Code mit dem Zahlkörper K des Grads $[K : \mathbb{Q}] = M$ und den Parametern $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; \mathfrak{z})$. Ist $t \in \mathbb{N}$ mit $1 \leq t \leq n$ und $\prod_{i=1}^{t} \|\mathfrak{p}_i\| > (\frac{2B}{M})^M$, dann gilt, dass die Minimaldistanz $d(\mathcal{C})$ von $\mathcal{C}$ mindestens $(n - t + 1)$ beträgt. Insbesondere gilt

$$d(\mathcal{C}) \geq n - \frac{M \log \frac{2B}{M}}{\log \|\mathfrak{p}_1\|},$$

falls mindestens ein solches t existiert.

Beweis: Wir betrachten zunächst zwei Codewörter $\text{Enc}(m_1)$ und $\text{Enc}(m_2)$, die in t Stellen übereinstimmen, seien diese Stellen $1 \leq i_1 < i_2 < \cdots < i_t \leq n$. Damit folgt für diese Stellen i_j, dass $m_1 \equiv m_2 \mod \mathfrak{p}_{i_j}$ und daher $m_1 - m_2 \in \mathfrak{p}_{i_j}$ und $I \coloneqq \langle m_1 - m_2 \rangle \subseteq \mathfrak{p}_{i_j}$ für alle $1 \leq j \leq t$. Folglich tauchen nach Bemerkung 2.14 alle $\mathfrak{p}_{i_j}$ in der Primidealzerlegung von I auf und, da diese paarweise verschieden sind, teilt auch dessen Produkt $J \coloneqq \prod_{j=1}^{t} \mathfrak{p}_{i_j}$ das Ideal I. Dies impliziert wieder nach Bemerkung 2.14, dass $I \subseteq J$ und demnach auch $m_1 - m_2 \in J = \prod_{j=1}^{t} \mathfrak{p}_{i_j}$. Also wird nach Satz 2.19 $\|m_1 - m_2\|$ von $\| \prod_{j=1}^{t} \mathfrak{p}_{i_j} \|$ geteilt und $\|m_1 - m_2\| \geq \| \prod_{j=1}^{t} \mathfrak{p}_{i_j} \|$. Nach Korollar 4.15 gilt aber auch, dass $\|m_1 - m_2\| \leq (\frac{2B}{M})^M$ und infolgedessen

$$(\frac{2B}{M})^M \geq \|m_1 - m_2\| \geq \prod_{j=1}^{t} \|\mathfrak{p}_{i_j}\| \geq \prod_{i=1}^{t} \|\mathfrak{p}_i\|.$$

Die Eigenschaft $\prod_{i=1}^{t} \|\mathfrak{p}_i\| > (\frac{2B}{M})^M$ führt dies nun zum Widerspruch und es folgt, dass die Codewörter höchstens in $(t - 1)$ Stellen übereinstimmen und wir demzufolge eine Minimaldistanz von mindestens $(n - t + 1)$ haben.
Nun wählen wir $1 \leq t \leq n$ minimal mit der Eigenschaft, dass $\prod_{i=1}^{t} \|\mathfrak{p}_i\| > (\frac{2B}{M})^M$, insbesondere ist $t \geq 1$. Dann gilt

$$\prod_{i=1}^{t} \|\mathfrak{p}_i\| > (\frac{2B}{M})^M \geq \prod_{i=1}^{t-1} \|\mathfrak{p}_i\|,$$

wobei wir die rechte Ungleichung wie folgt ergänzen

$$\begin{aligned}
(\frac{2B}{M})^M \geq \prod_{i=1}^{t-1} \|\mathfrak{p}_i\| \geq \|\mathfrak{p}_1\|^{t-1} &\iff M \log(\frac{2B}{M}) \quad \geq (t-1) \log \|\mathfrak{p}_1\| \\
&\iff \frac{M \log(\frac{2B}{M})}{\log \|\mathfrak{p}_1\|} \quad \geq t - 1 \\
&\iff n - \frac{M \log(\frac{2B}{M})}{\log \|\mathfrak{p}_1\|} \leq n - t + 1.
\end{aligned}$$

Dabei ist $\log \|\mathfrak{p}_1\| > 0$, da $\mathcal{O}_K / \mathfrak{p}_1$ ein Körper ist und daher $\|\mathfrak{p}_1\| > 1$. Folglich gilt $d(\mathcal{C}) \geq n - t + 1 \geq n - \frac{M \log \frac{2B}{M}}{\log \|\mathfrak{p}_1\|}$. □

4.4 Informationsrate des NF-Codes

Um in diesem Unterkapitel die Informationsrate des NF-Codes zu berechnen, benötigen wir zunächst eine untere Schranke für die Anzahl der Elemente x aus $\mathcal{O}_K$ mit der Größe $size_{\mathfrak{z}}(x) \leq B$. Dafür verwenden wir die Diskriminante eines Zahlkörpers, die Definition eines Gitters, dessen Volumenberechnung und wie angekündigt unseren Verschiebungsparamter $\mathfrak{z}$.

Definition 4.21
Sei K ein Zahlkörper vom Grad $[K : \mathbb{Q}] = M$ mit M Einbettungen $\zeta_1, \ldots, \zeta_M \colon K \to \mathbb{C}$. Dann definiere

i) die Diskriminante $\text{disc}(\alpha_1, \ldots, \alpha_M)$ eines M-Tupels von Elementen $\alpha_1, \ldots, \alpha_M \in \mathcal{O}_K$ als Quadrat der Determinante der $M \times M$ Matrix mit $\zeta_i(\alpha_j)$ als (i, j)-ter Eintrag,

ii) die Diskriminante $D_K \coloneqq D_{K|\mathbb{Q}}$ von K als $\text{disc}(\beta_1, \ldots, \beta_M)$, wobei $\beta_1, \ldots, \beta_M$ eine beliebige Ganzheitsbasis von $\mathcal{O}_K$ über $\mathbb{Z}$ ist und

iii) die Wurzeldiskriminante von K als $rd_K \coloneqq |D_K|^{\frac{1}{M}}$.

Bemerkung 4.22
Hier benutzen wir die Tatsache, dass $\mathcal{O}_K$ ein freier $\mathbb{Z}$-Modul vom Rang M ist (vgl. dazu Satz 2.10 auf Seite 13 des [Neu92]). Die Wahl der Ganzheitsbasis spielt für D_K deswegen keine Rolle, denn eine Übergangsmatrix T zwischen zwei Ganzheitsbasen hätte wie ihre Inverse die Determinante ± 1. Daraus folgt, dass das von allen disc$(\beta_1 \ldots, \beta_M)$ erzeugte Ideal dem Hauptideal (D_K) entspricht.

Lemma 4.23
Für einen Körperturm $K \subseteq L \subseteq M$ von Zahlkörpern gilt

$$D_{M|K} = {D_{L|K}}^{[M:L]} \cdot ||(D_{M|L})||.$$

Beweis: Für den Beweis sei auf Korollar 2.10 auf Seite 213 des [Neu92] verwiesen. Hier verwenden wir außerdem das Zusammenspiel der verschiedenen Normbegriffe aus §6 „Die Klassenzahl“ auf den Seiten 36f. des [Neu92]. □

Definition 4.24
Sei V ein n-dimensionaler $\mathbb{R}$-Vektorraum. Dann heißt $\Lambda \subseteq V$ Gitter, wenn es von der Form $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ ist mit $v_1, \ldots, v_m$ linear unabhängige Vektoren von V. Dabei heißt die Menge $F = \{x_1v_1 + \cdots + x_mv_m \mid x_i \in \mathbb{R}, 0 \leq x_i < 1\}$ Grundmasche oder auch fundamentales Parallelogramm von Λ. Ein Gitter heißt vollständig, wenn $m = n$ gilt, was gleichbedeutend damit ist, dass sämtliche Verschiebungen der Grundmasche F um $\lambda \in \Lambda$ den Vektorraum V überdecken.

Definition 4.25
Das Volumen des fundamentalen Parallelogramms F eines vollständigen Gitters über einem n-dimensionalen $\mathbb{R}$-Vektorraum ist definiert als $\text{Vol}(F) \coloneqq |\det(A)|$, wobei $A = (a_{ik})$ die Übergangsmatrix der Standardbasis $e_1, \ldots, e_n$ hin zu $v_1, \ldots, v_n$ ist, also mit $v_i = \sum_{k=1}^{n} a_{ik}e_k$.

Weiterhin werden wir für den Beweis der nachfolgenden Proposition zwei Volumina berechnen, wobei uns folgende Lemmata helfen.

Lemma 4.26
Die Abbildung $\rho\colon K \to \mathbb{R}^{r+2s}$ mit

$$\alpha \mapsto (\tau_1(\alpha), \dots, \tau_r(\alpha), \mathit{Re}(\sigma_1(\alpha)), \mathit{Im}(\sigma_1(\alpha)), \dots, \mathit{Re}(\sigma_s(\alpha)), \mathit{Im}(\sigma_s(\alpha))),$$

wobei $\tau_1, \dots \tau_r, \sigma_1 \dots \sigma_s$ die bekannten Einbettungen von K sind, bildet $\mathcal{O}_K$ auf ein vollständiges Gitter ab mit $n = r + 2s$. Dessen fundamentales Parallelogramm F hat dann ein Volumen von $\mathit{Vol}(F) = \frac{1}{2^s}\sqrt{|(D_K)|}$.

Beweis: Für den Beweis sei auf Theorem 36 auf Seite 94 des [Mar18] verwiesen. □

Lemma 4.27
Sei U eine Teilmenge von $\mathbb{R}^{r+2s}$ mit

$$U = \{(x_1, \dots, x_{r+2s}) \mid |x_1| + \dots + |x_r| + \sum_{i=1}^{s} 2\sqrt{x_{r+2i-1}^2 + x_{r+2i}^2} \leq t\}.$$

Dann gilt $\mathit{Vol}(U) = 2^r(\frac{\pi}{2})^s \frac{t^{r+2s}}{(r+2s)!}$.

Beweis: Für den Beweis sei auf die Seiten 98f. des [Mar18] verwiesen. □

Proposition 4.28
Sei K ein Zahlkörper vom Grad $[K : \mathbb{Q}] = M$ mit der Signatur (r, s), der Diskriminante D_K und einem $B \in \mathbb{R}_{>0}$. Dann gibt es ein $\mathfrak{z} \in \mathbb{R}^r \times \mathbb{C}^s$, sodass

$$|\{x \in \mathcal{O}_K \mid size_{\mathfrak{z}}(x) \leq B\}| \geq \frac{2^r \pi^s B^M}{M!\sqrt{|D_K|}}.$$

Beweis: Zunächst benötigen wir die Abbildung $\rho\colon K \to \mathbb{R}^M$ aus Lemma 4.26 mit

$$\alpha \mapsto (\tau_1(\alpha), \dots, \tau_r(\alpha), \mathrm{Re}(\sigma_1(\alpha)), \mathrm{Im}(\sigma_1(\alpha)), \dots, \mathrm{Re}(\sigma_s(\alpha)), \mathrm{Im}(\sigma_s(\alpha))).$$

Des Weiteren betrachten wir nun die Bilder von $\mathcal{O}_K$ und $S = \{x \in \mathcal{O}_K \mid size(x) \leq B\}$ unter dieser Abbildung. Nach Lemma 4.26 wird $\mathcal{O}_K$ auf ein vollständiges Gitter Λ abgebildet, dessen fundamentales Parallelogramm F dann das Volumen $\mathrm{Vol}(F) = 2^{-s}\sqrt{|D_K|}$ hat.
Das Bild von S liegt in der Menge $U \subset \mathbb{R}^M$ gegeben durch

$$U = \{(x_1, \dots x_M) \mid |x_1| + \dots + |x_r| + \sum_{i=1}^{s} 2\sqrt{x_{r+2i-1}^2 + x_{r+2i}^2} \leq B\}.$$

Betrachte dazu $\rho(\alpha)$ mit $\alpha \in S$

$$\rho(\alpha) = (\tau_1(\alpha), \dots, \tau_r(\alpha), \mathrm{Re}(\sigma_1(\alpha)), \mathrm{Im}(\sigma_1(\alpha)), \dots, \mathrm{Re}(\sigma_s(\alpha)), \mathrm{Im}(\sigma_s(\alpha))) = (x_1, \dots, x_M).$$

Anschließend erhält man durch Einsetzen

$$|\tau_1(\alpha)|+\cdots+|\tau_r(\alpha)|+\sum_{i=1}^{s}2\sqrt{\mathrm{Re}(\sigma_i(\alpha))^2+\mathrm{Im}(\sigma_i(\alpha))^2}=\sum_{i=1}^{r}|\tau_i(\alpha)|+\sum_{i=1}^{s}2\sqrt{|\sigma_i(\alpha)|^2}=size(\alpha),$$

was mit $size(\alpha) \leq B$ für $\alpha \in S$ zeigt, dass das Bild von S in U liegt. Nachfolgend berechnen wir noch das Volumen von U. Dazu nutzen wir Lemma 4.27 und erhalten $\mathrm{Vol}(U) = 2^r(\frac{\pi}{2})^s\frac{B^M}{M!}$. Somit gibt es ungefähr $\frac{Vol(U)}{Vol(F)} = \frac{2^r\pi^s B^M}{M!\sqrt{|D_K|}}$ Elemente in S. Ganz ähnlich wie in Theorem 2.1 und dessen Beweis von [Len86] ist dies nur der Fall, wenn der Fehlerterm nicht dominant ist. Um dieses Problem zu lösen, nimmt man den Durchschnitt aller Verschiebungen von U um $y \in \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^M$. Nachfolgend ist χ die charakteristische Funktion von U. Dann gilt

$$\begin{aligned}\int_{y\in F}|(y+U)\cap\Lambda|dy &= \int_{y\in F}\sum_{x\in\Lambda}\chi(x-y)dy=\sum_{x\in\Lambda}\int_{y\in F}\chi(x-y)dy\\ &=\sum_{x\in\Lambda}\int_{y\in x-F}\chi(y)dy=\int_{y\in\mathbb{R}^M}\chi(y)dy\\ &=Vol(U)=Vol(U)\int_{y\in F}1dy\frac{1}{Vol(F)}\\ &=\int_{y\in F}\frac{Vol(U)}{Vol(F)}dy,\end{aligned}$$

dabei dürfen mithilfe des Satzes der monotonen Konvergenz Reihe und Integral vertauscht werden, denn wenn man die Reihe als Folge von Partialsummen auffasst, ist diese monoton steigend. Dieser Satz ist inklusive eines Beweises zu finden auf Seite 54 des [For11]. Des Weiteren nutzen wir für die vierte Umformung aus, dass Λ vollständig ist und somit $\mathbb{R}^M$ die disjunkte Vereinigung von $x - F$ mit $x \in \Lambda$ ist.

Demnach gibt es also ein $\mathfrak{z} := y \in F \subset \mathbb{R}^M \simeq \mathbb{R}^r \times \mathbb{C}^s$, sodass $|(y + U) \cap \rho(\mathcal{O}_K)| \geq \frac{Vol(U)}{Vol(F)} = \frac{2^r\pi^s B^M}{M!\sqrt{|D_K|}}$ □

Der nachfolgende Satz soll noch einmal die Parameter Informationsrate und Minimaldistanz des konstruierten NF-Codes zusammentragen. Sofern nicht anders angegeben, sind alle Logarithmen zur Basis 2.

Satz 4.29

Sei K ein Zahlkörper vom Grad $[K : \mathbb{Q}] = M$ mit der Signatur (r, s) und sei $\mathcal{C} = \mathcal{C}_K$ der NF-Code mit den Parametern $(n, \mathfrak{p}_1, \ldots, \mathfrak{p}_n; B; \mathfrak{z})$ mit $\|\mathfrak{p}_1\| \leq \cdots \leq \|\mathfrak{p}_n\|$ und B, sodass $1 \leq t \leq n$ existiert mit $\prod_{i=1}^{t} ||\mathfrak{p}_i|| > (2B/M)^M$. Dann existiert eine Verschiebung $\mathfrak{z} \in \mathbb{R}^r \times \mathbb{C}^s$, sodass für die Informationsrate $R(\mathcal{C})$ von $\mathcal{C}$ gilt

$$R(\mathcal{C}) \geq \frac{\log(2^r\pi^s B^M) - \log M! - \log\sqrt{|D_K|}}{n\log\|\mathfrak{p}_n\|}.$$

Nach Lemma 4.20 erfüllt die Minimaldistanz $d(\mathcal{C})$ von $\mathcal{C}$, dass $d(\mathcal{C}) \geq d'(\mathcal{C}) := n - \frac{M\log(2B/M)}{\log\|\mathfrak{p}_1\|}$.

Insbesondere gilt dann

$$R(\mathcal{C}) \geq \frac{(n - d'(\mathcal{C}))\log\|\mathfrak{p}_1\| + s\log(\pi/4) + M\log e - M\log\sqrt{rd_K} - \log(3M)}{n\log\|\mathfrak{p}_n\|}$$
$$\geq \frac{(n - d(\mathcal{C}))\log\|\mathfrak{p}_1\| + s\log(\pi/4) + M\log e - M\log\sqrt{rd_K} - \log(3M)}{n\log\|\mathfrak{p}_n\|}.$$

Beweis: Für die erste Abschätzung von $R(\mathcal{C})$ betrachten wir die Definition der Informationsrate, nach der gilt $R(\mathcal{C}) = \frac{\log_q(|\mathcal{C}|)}{n}$, wobei q die Mächtigkeit des genutzten Alphabets ist. Aus Proposition 4.28 kennen wir eine Abschätzung für die Mächtigkeit von $\mathcal{C}$. Des Weiteren wissen wir aus der Konstruktion unseres Codes, dass unsere Alphabetgröße durch $\|\mathfrak{p}_n\|$ beschränkt ist. Daher können wir mithilfe eines Basiswechsels zu $\log_2$ wie folgt abschätzen

$$R(\mathcal{C}) = \frac{\log_q(|\mathcal{C}|)}{n} = \frac{\log(|\mathcal{C}|)}{n\log(q)} \geq \frac{\log(|\mathcal{C}|)}{n\log(\|\mathfrak{p}_n\|)}$$
$$\geq \frac{\log(|\frac{2^r\pi^s B^M}{M!\sqrt{|D_K|}}|)}{n\log(\|\mathfrak{p}_n\|)} = \frac{\log(2^r\pi^s B^M) - \log M! - \log\sqrt{|D_K|}}{n\log\|\mathfrak{p}_n\|}.$$

Für die weitere Abschätzung von $R(\mathcal{C})$ benötigen wir zunächst eine Abschätzung für $M!$. Dafür nutzen wir eine Modifizierung der Stirling Approximation, $M! \leq \sqrt{2\pi}M^{M+\frac{1}{2}}e^{-M}e^{\frac{1}{12M}}$, welche auch für kleine $M \geq 1$ gilt und mit Beweis in [Rob55] auf den Seiten 26ff. zu finden ist. Weiterhin schätzen wir sie wie folgt ab

$$M! \leq \sqrt{2\pi}M^{M+\frac{1}{2}}e^{-M}e^{\frac{1}{12M}} \leq \sqrt{2\pi}\sqrt{M}(\frac{M}{e})^M e^{\frac{1}{12}} = \sqrt{2\pi e^{\frac{1}{6}}}\sqrt{M}(\frac{M}{e})^M \leq 3M(\frac{M}{e})^M.$$

Betrachte nun

$$R(\mathcal{C}) \geq \frac{\log(2^r\pi^s B^M) - \log M! - \log\sqrt{|D_K|}}{n\log\|\mathfrak{p}_n\|}$$
$$\geq \frac{\log(2^M B^M) + (\log\frac{\pi^s}{2^{2s}}) - \log(3M(\frac{M}{e})^M) - M\log\sqrt{|D_K|^{\frac{1}{M}}}}{n\log\|\mathfrak{p}_n\|}$$
$$= \frac{M\log(2B) + s\log(\frac{\pi}{4}) - \log(3M) - M\log M + M\log e - M\log\sqrt{rd_K}}{n\log\|\mathfrak{p}_n\|}$$
$$= \frac{M\log(\frac{2B}{M}) + s\log(\frac{\pi}{4}) - \log(3M) + M\log e - M\log\sqrt{rd_K}}{n\log\|\mathfrak{p}_n\|}$$
$$= \frac{(n - d'(\mathcal{C}))\log\|\mathfrak{p}_1\| + s\log(\frac{\pi}{4}) - \log(3M) + M\log e - M\log\sqrt{rd_K}}{n\log\|\mathfrak{p}_n\|}$$
$$\overset{4.20}{\geq} \frac{(n - d(\mathcal{C}))\log\|\mathfrak{p}_1\| + s\log(\frac{\pi}{4}) - \log(3M) + M\log e - M\log\sqrt{rd_K}}{n\log\|\mathfrak{p}_n\|},$$

was unsere gewünschte Abschätzung gibt. □

Damit haben wir in diesem Kapitel unseren NF-Code sowohl konstruiert als auch auf seine wichtigsten Eigenschaften, sprich der Minimaldistanz und Informationsrate, untersucht und im letztem Satz noch einmal zusammengefasst.

5 Konstruktion eines asymptotisch guten Codes

In diesem Kapitel wollen wir einen Schritt weiter gehen und besonders gute NF-Codes bzw. sogar Familien von asymptotisch guten Codes konstruieren. Dazu betrachten wir das Ergebnis aus Satz 4.29, welches besagt, dass die Informationsrate eines NF-Codes groß ist, falls die Wurzeldiskriminante des Zahlkörpers K klein ist. Weiterhin gilt, dass wir für einen Code der Blocklänge n über einem Alphabet mit maximaler Größe q einen Ganzheitsring $\mathcal{O}_K$ benötigen, der n Primideale der Norm maximal q hat. Insbesondere brauchen wir eine Familie von Zahlkörpern $\{K_n\}$, sodass K_n eine kleine Wurzeldiskriminante, bestmöglich sogar eine Konstante c als Schranke für alle K_n und $\Omega([K_n : \mathbb{Q}])$ Primideale der Norm maximal q hat, wobei $\Omega(m)$ die Anzahl der Primfaktoren von m angibt. Für die Konstruktion solcher Familien machen wir uns die Klassenkörpertheorie zunutze, denn mit der Existenz von unendlichen Hilbert'schen Klassenkörpertürmen für Zahlkörper können wir Sequenzen von Zahlkörpern mit beschränkter Wurzeldiskriminante konstruieren. Hierzu wiederholen wir im nachfolgendem Unterkapitel einige Ergebnisse aus der Klassenkörpertheorie. Doch zunächst definieren wir was eine Familie von asymptotisch guten NF-Codes ist.

Definition 5.1
Die relative Minimaldistanz eines Codes der Blocklänge n und der Minimaldistanz d ist durch dessen Quotienten $\frac{d}{n}$ gegeben.

Definition 5.2
Eine Familie von NF-Codes $\{\mathcal{C}_i\}_{i\geq 0}$ mit den Informationsraten $R(\mathcal{C}_i)$ und den relativen Minimaldistanzen $\frac{d_i}{n_i}$ heißt asymptotisch gut, falls $\liminf R(\mathcal{C}_i) > 0$ und $\liminf \frac{d_i}{n_i} > 0$, wobei die Blocklänge $n_i \to \infty$ konvergiert.

5.1 Klassenkörper

Definition 5.3
Eine endliche Körpererweiterung von Zahlkörpern K über k heißt

i) unverzweigt, falls kein Primideal von $\mathcal{O}_k$ verzweigt ist;

ii) abelsch, falls $K|k$ galois mit abelscher Galoisgruppe ist;

iii) p-Erweiterung, falls $K|k$ galois und $[K : k]$ eine Potenz von p ist.

Lemma 5.4
Ein Primideal $\mathfrak{p}$ von K ist genau dann verzweigt in L, wenn $\mathfrak{p}|(D_{L|K})$. Insbesondere ist die Erweiterung $L|K$ genau dann unverzweigt, wenn die Diskriminante $D_{L|K} = 1$ ist.

Beweis: Die Aussage findet sich in Korollar 2.12 auf Seite 213 des [Neu92]. □

Definition 5.5
Sei k ein Zahlkörper und p eine Primzahl. Dann heißt die maximale unverzweigte abelsche Erweiterung k^1 von k Hilbert'scher Klassenkörper (oder Klassenkörper). Ein p-Hilbert-Klassenkörper (oder p-Klassenkörper) ist die maximale p-Erweiterung von k die in k^1 enthalten ist.

Definition 5.6
Sei k ein Zahlkörper und p eine Primzahl. Dann ist der Hilbert'sche Klassenkörperturm (oder Klassenkörperturm) von k eine Sequenz von Körpern $k_0 = k; k_1 = k^1$ der Klassenkörper von $k; k_i = (k_{i-1})^1$ der Klassenkörper von k_{i-1} für $i \geq 2$. Die Sequenz bzw. der Turm endet bei j, falls k_j sich selbst als Klassenkörper hat und somit $k_j = k_{j+1}$ gilt. Man spricht von einem unendlichen Turm, falls er nicht abbricht. Der p-Hilbert-Klassenkörperturm (oder p-Klassenkörperturm) von k ist durch wiederholtes Nutzen von p-Klassenkörpern analog zum Klassenkörperturm definiert.

5.2 Klassenkörpertürme mit voll zerlegten Primidealen

Wie bereits erwähnt ist für uns die wichtigste Eigenschaft von Klassenkörpertürmen, dass die Unverzweigtheit der Erweiterungen dafür sorgt, dass die Wurzeldiskriminante $rd(k_i)$ den gesamten Weg des Turms unverändert bleibt. Um so durch die unendlichen Klassenkörpertürme unsere unendlichen Familien von guten NF-Codes zu erhalten, benötigen wir einen unendlichen Turm von Zahlkörpern, welche verschiedene Primideale von kleiner Norm haben. Dies ist möglich, wenn K einen unendlichen Klassenkörperturm hat, indem „spezielle" Primideale von K von kleiner Norm sind und auf dem Weg des Turms voll zerlegt werden.

Definition 5.7
Sei k ein Zahlkörper, T eine Menge von Primidealen aus $\mathcal{O}_K$ und p eine Primzahl. Dann heißt die maximale, unverzweigte, abelsche p-Erweiterung von k, in welcher jedes Primideal aus T voll zerlegt ist, T-zerlegender p-Klassenkörper von k und wird als k_p^T notiert.

Definition 5.8
Sei k ein Zahlkörper, T eine Menge von Primidealen aus $\mathcal{O}_K$ und p eine Primzahl. Dann heißt die nachfolgende Sequenz von Körpern T-zerlegender p-Klassenkörperturm von k, $k_0 = k; k_1 = k_p^T$ der T-zerlegende p-Klassenkörper von $k; k_i = (k_{i-1})_p^{T_{i-1}}$ der T_{i-1}-zerlegende p-Klassenkörper von k_{i-1} für $i \geq 2$, wobei T_i die Menge der über T liegenden Primideale in k_i ist. Wir sagen, dass k einen unendlichen T-zerlegenden p-Klassenkörperturm hat, falls der Turm nicht abbricht, d.h. $k_i \neq k_{i+1}$ für alle $i \in \mathbb{N}$.

Unser nächstes Ziel besteht darin einen passenden Zahlkörper K zu finden, der eine „kleine" Wurzeldiskriminante, eine Menge T von Primidealen von kleiner Norm in K und einen unendlichen T-zerlegenden p-Klassenkörperturm hat.

5.3 Konstruktion eines passenden Zahlkörpers

Die Konstruktionsidee für einen Zahlkörper K, der einen unendlichen Klassenkörperturm besitzt, entnehmen wir der Golod-Šafarevič Theorie [Ga64], welche eine hinreichende Bedingung für die Unendlichkeit eines p-Klassenkörperturms basierend auf einem Zahlkörper K gibt. Wir werden für unsere Zwecke nur einen Spezialfall für quadratische Körpererweiterungen nutzen, die unendliche 2-Klassenkörpertürme besitzen.

Proposition 5.9
Seien $P = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ und $Q = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$ disjunkte Mengen von Primidealen von $\mathbb{Z}$. Sei weiterhin K eine quadratische Erweiterung über $\mathbb{Q}$, die genau bei den Primidealen aus Q verzweigt ist. Sei T die

Menge von Primidealen aus $\mathcal{O}_K$, die über den Primidealen aus P liegen und setze $|T| = t$. Zusätzlich nehmen wir an, dass $r \geq 3 + t - s + 2\sqrt{2+t}$. Dann hat K einen unendlichen T-zerlegenden 2-Klassenkörperturm.

Beweis: Für den Beweis dieses Spezialfalls siehe Korollar 9.2 auf Seite 69 des [Tsf00]. □

Die Vermutung an dieser Stelle ist, dass durch die Nutzung verschiedener Werte viele asymptotisch gute NF-Codekonstruktionen entstehen, was genau das Ziel dieser Arbeit ist. Aus diesem Grund werden wir nachfolgend versuchen, konkrete asymptotisch gute Codes über einem sinnvollem Alphabet zu konstruieren.

5.4 Konkrete Codekonstruktion

Für unsere erste konkrete Codekonstruktion benötigen wir noch folgende Lemmata und Sätze aus dem [Neu92] und der Vorlesung zur algebraischen Zahlentheorie aus dem Sommersemester 2014.

Lemma 5.10
Sei $K = \mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Z}$ quadratfrei. Setzen wir $\delta := \sqrt{d}$, falls $d \equiv 2 \mod 4$ oder $d \equiv 3 \mod 4$, bzw. $\delta := \frac{1}{2}(1+\sqrt{d})$, falls $d \equiv 1 \mod 4$. Dann ist $(1, \delta)$ eine Ganzheitsbasis von $K = \mathbb{Q}(\sqrt{d})$ und der Zahlkörper K hat die Diskriminante $4d$, falls $d \equiv 2 \mod 4$ oder $d \equiv 3 \mod 4$, bzw. die Diskriminante d, falls $d \equiv 1 \mod 4$.

Beweis: Für $x = a + b\sqrt{d}$ mit $a, b \in \mathbb{Q}$ und $b \neq 0$ ist das Minimalpolynom von x über $\mathbb{Q}$ gegeben durch $\mu_x(t) = (t - (a + b\sqrt{d}))(t - (a - b\sqrt{d})) = t^2 - 2at + a^2 - db^2$, sodass δ ganz über $\mathbb{Z}$ ist, da

$$\mu_\delta(t) = \begin{cases} t^2 - t + \frac{1-d}{4} & d \equiv 1 \mod 4 \\ t^2 - d & d \equiv 2 \mod 4 \\ t^2 - d & d \equiv 3 \mod 4 \end{cases}$$

in $\mathbb{Z}[t]$. Daher gilt $\mathcal{O}_K \supset \mathbb{Z} + \delta\mathbb{Z}$. Ist umgekehrt $x \in K$ ganz über $\mathbb{Z}$, so gilt nach dem Lemma von Gauß $\mu_x(t) \in \mathbb{Z}[t]$ und daher $2a \in \mathbb{Z}$ und $a^2 - b^2 d \in \mathbb{Z}$. Somit ist auch $d \cdot (2b)^2 = 4(db^2 - a^2) + (2a)^2 \in \mathbb{Z}$. Daraus folgt $2b \in \mathbb{Z}$, da d quadratfrei. Ist nun $a \notin \mathbb{Z}$, so muss auch $2b$ ungerade sein. Andernfalls gilt $b \in \mathbb{Z}$ und mit $a^2 - b^2 d \in \mathbb{Z}$ auch $a^2 \in \mathbb{Z}$, ein Widerspruch zu $a \notin \mathbb{Z}$. Ist umgekehrt $b \notin \mathbb{Z}$, also $2b = 1 + 2m$ mit $m \in \mathbb{Z}$, so muss auch $2a$ ungerade sein. Anderenfalls gilt $a \in \mathbb{Z}$ und man erhält $0 \equiv 4(db^2 - a^2) \equiv d(2b)^2 = d(1+2m)^2 \equiv d \mod 4$ im Widerspruch dazu, dass d quadratfrei ist. Daher ist entweder $a, b \in \mathbb{Z}$ und damit $x = a + b\sqrt{d} \in \mathbb{Z} + \delta\mathbb{Z}$ oder $2a = 1 + 2n$ und $2b = 1 + 2m$. Dies kann nur der Fall sein, wenn $d \equiv 1 \mod 4$, denn $a^2 - b^2 d = \frac{1-d}{4} + n + n^2 - d(m + m^2) \in \mathbb{Z}$ und mit $n + n^2 - d(m + m^2) \in \mathbb{Z}$ folgt, dass $\frac{1-d}{4} \in \mathbb{Z}$ und daher $d \equiv 1 \mod 4$. Dann gilt auch $x = a + b\sqrt{d} = \frac{1+2n}{2} + \frac{1+2m}{2}\sqrt{d} = n - m + \frac{1}{2}(1 + \sqrt{d} + 2m\sqrt{d} + 2m) = (n - m) + (1 + 2m)\frac{1}{2}(1 + \sqrt{d}) \in \mathbb{Z} + \delta\mathbb{Z}$. Folglich ist $\mathcal{O}_K = \mathbb{Z}[\delta]$.
Sei τ der nichttriviale Galoisautomorphismus von $\mathbb{Q}[\sqrt{d}]$ über $\mathbb{Q}$ mit $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. Wir erhalten mit

$$D_K = (\det \begin{pmatrix} id(1) & id(\delta) \\ \tau(1) & \tau(\delta) \end{pmatrix})^2,$$

dass $D_K = (-\sqrt{d} - \sqrt{d})^2 = 4d$, falls $d \equiv 2 \mod 4$ bzw. falls $d \equiv 3 \mod 4$ und $D_K = (\frac{1}{2}(1+\sqrt{d}) - \frac{1}{2}(1-\sqrt{d}))^2 = d$, falls $d \equiv 1 \mod 4$. □

Definition 5.11
Für eine ganze Zahl $a \in \mathbb{Z}$ und eine Primzahl $p \in \mathbb{Z}$ bezeichne $\left(\frac{a}{p}\right)$ als das Legendre-Symbol mit

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \not\equiv 0 \mod p \text{ und } \exists x \in \mathbb{Z} : x^2 \equiv a \mod p \\ -1 & \text{falls } a \not\equiv 0 \mod p \text{ und } \forall x \in \mathbb{Z} : x^2 \not\equiv a \mod p \\ 0 & \text{falls } a \equiv 0 \mod p, \end{cases}$$

also 1, wenn a ein quadratischer Rest modulo p ist, -1 wenn a ein nicht-quadratischer Rest modulo p ist und 0 wenn a Vielfaches von p ist.

Satz 5.12
Für quadratfreies a und ggT$(p, 2a) = 1$ gilt

$$\left(\frac{a}{p}\right) = 1 \iff \textit{p ist voll zerlegt in } \mathbb{Q}(\sqrt{d})$$

Beweis: Für einen Beweis dieses Satzes sei auf Satz 8.5 und dessen vorrangehenden Beweis auf den Seiten 52f. des [Neu92] verwiesen. □

5.4.1 Erhalt einer Familie von asymptotisch guten Codes

Im folgenden Lemma werden wir für das konkrete Beispiel $K = \mathbb{Q}(\sqrt{-4849845})$ zeigen, dass ein T-zerlegender 2-Klassenkörperturm existiert.

Lemma 5.13
Sei $d = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 4849845$ und $K = \mathbb{Q}(\sqrt{-d})$. Dann gilt:

i) $rd_K = \sqrt{4d} \approx 4404,4727$

ii) $\mathcal{O}_K$ *hat eine Menge* T *mit* 2 *Primidealen der Norm* 29.

iii) K *hat einen unendlichen* T*-zerlegenden* 2*-Klassenkörperturm.*

Beweis: Betrachten wir für Teil i) zunächst $-d = -4849845 = -1212461 \cdot 4 - 1 \equiv 3 \mod 4$ somit folgt mithilfe von Lemma 5.10 bereits $D_K = -4d$ also $rd_K = \sqrt{|D_K|} = \sqrt{4d} \approx 4404,4727$.
Für Teil ii) nutzen wir Lemma 5.12. Hierfür halten wir fest, dass $-d = -3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ quadratfrei ist und dass ggT$(29; -2d) = 1$. Durch Nutzung des Euler-Kriteriums (vgl. Seite 53 des [Neu92]) können wir zeigen, dass das Legendre-Symbol $\left(\frac{-d}{p}\right) = 1$, denn $(-4849845)^{14} = (-167236 \cdot 29 - 1)^{14} \equiv (-1)^{14} = 1 \mod 29$. Somit folgt mit Lemma 5.12, dass $(29) = \mathfrak{p}_1\mathfrak{p}_2$ mit $\mathfrak{p}_1 \neq \mathfrak{p}_2$ gilt, welche Primideale nach Definition 2.17 die Norm $\|\mathfrak{p}_1\| = \|\mathfrak{p}_2\| = 29$ haben. Sei $T \coloneqq \{\mathfrak{p}_1, \mathfrak{p}_2\}$.
Der Beweis für Teil iii) nutzt Lemma 5.4, um die verzweigten Primideale in $\mathbb{Q}(\sqrt{-d})|\mathbb{Q}$ zu bestimmen. Diese sind demnach genau die Primideale $Q = \{2, 3, 5, 7, 11, 13, 17, 19\}$ aus $\mathbb{Z}$, die $|D_K| = 4d$ teilen. Mit diesem Wissen können wir nun Proposition 5.9 auf $P = \{29\}$, $Q = \{2, 3, 5, 7, 11, 13, 17, 19\}$,

$T = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ und $K = \mathbb{Q}(\sqrt{-d})$ anwenden. Des Weiteren erfüllen dann $r = 8, s = 1$ und $t = 2$ die erforderliche Ungleichung $r \geq 3 + t - s + 2\sqrt{2+t}$ und somit auch iii). □

Nun möchten wir mit diesem Wissen eine ganze Familie von asymptotisch guten Zahlkörper-Codes generieren. Dazu betrachten wir $K_0 = K$ aus Lemma 5.13 und sei $K_0 \subset K_1 \subset K_2 \subset \dots$ sein unendlicher T-zerlegender 2-Klassenkörperturm, wobei jedes K_n einen Code $\mathcal{C}_n$ erzeugen wird. Nachfolgend werden wir für ein festes n einen solchen Code $\mathcal{C}_n$ konstruieren. Sei dazu $[K_n : \mathbb{Q}] = M$, da K_n in unserem Fall vollständig komplex ist, ist seine Signatur $(0, \frac{M}{2})$. Nach Lemma 5.13 wird das Primideal 29 in der Erweiterung von K_n über $\mathbb{Q}$ voll zerlegt und daher hat $\mathcal{O}_K$ M Primideale der Norm 29, diese nennen wir $\mathfrak{p}_1, \dots, \mathfrak{p}_M$. Sei nun $\mathcal{C}_n$ der NF-Code mit den Parametern $(M; \mathfrak{p}_1, \dots, \mathfrak{p}_M; B; \mathfrak{z})$ mit $B = c_0 M$ für eine geeignete Konstante c_0 und $\mathfrak{z} \in \mathbb{C}^{M/2}$ der Verschiebungsparameter aus 4.29. Damit Satz 4.29 anwendbar ist, muss ein t existieren mit $1 \leq t \leq M$ und $\prod_{i=1}^{t} ||\mathfrak{p}_i|| = 29^t > (2B/M)^M = (2c_0)^M$. Wir können $0 < c_0 < 14,5$ unabhängig von n wählen, denn $t = M$ erfüllt für solches c_0 die notwendige Ungleichung.
Nun bestimmen wir sowohl die Minimaldistanz als auch die Informationsrate der Codes aus der Familie $\{\mathcal{C}_n\}_{n\geq 0}$ mithilfe von Satz 4.29. So ist die Minimaldistanz

$$d(\mathcal{C}_n) \geq M - \frac{M \log(2c_0)}{\log(29)} = d'(C_n) \tag{1}$$

und für die Informationsrate gilt

$$\begin{aligned}
R(\mathcal{C}_n) &\geq \frac{(M - d'(\mathcal{C}_n)) \log \|\mathfrak{p}_1\| + s \log(\pi/4) + M \log e - M \log \sqrt{r d_{K_n}} - \log(3M)}{n \log \|\mathfrak{p}_M\|} \\
&= \frac{(M - d'(\mathcal{C}_n)) \log(29) + \frac{M}{2} \log(\pi/4) + M \log e - M \log \sqrt{r d_{K_n}} - \log(3M)}{M \log(29)} \\
&= 1 - \frac{d'(\mathcal{C}_n)}{M} + \frac{M \log(\sqrt{\pi/4}) + M \log e - M \log \sqrt{r d_{K_n}}}{M \log(29)} - \frac{\log(3M)}{M \log(29)} \\
&= 1 - \frac{d'(\mathcal{C}_n)}{M} + \frac{\log(\frac{e}{2}\sqrt{\frac{\pi}{r d_{K_n}}})}{\log(29)} - \frac{\log(3M)}{M \log(29)} \\
&= 1 - \frac{d'(\mathcal{C}_n)}{M} - \frac{\log(\frac{2}{e}\sqrt{\frac{r d_{K_n}}{\pi}})}{\log(29)} - \frac{\log(3M)}{M \log(29)}.
\end{aligned}$$

Durch Einsetzen von

$$r d_{K_n} = |D_{K_n}|^{\frac{1}{[K_n:\mathbb{Q}]}} \overset{4.23}{=} |D_K|^{\frac{[K_n:K]}{[K_n:\mathbb{Q}]}} = r d_K \approx 4404,4727$$

erhalten wir für große M, wodurch $-\frac{\log(3M)}{M \log(29)}$ kleiner als der Rundungsfehler von $1 - \frac{\log(27,55)}{\log(29)}$ ist,

$$R(\mathcal{C}_n) \geq 1 - \frac{d'(\mathcal{C}_n)}{M} - \frac{\log(27,55)}{\log(29)} - \frac{\log(3M)}{M \log(29)} > 0,015 - \frac{d'(\mathcal{C}_n)}{M}.$$

Wegen $r d_{K_n} = r d_K$ und $\frac{d'(\mathcal{C}_n)}{M} = 1 - \frac{\log(2c_0)}{\log(29)}$ haben wir für die Informationsrate und die relative

Minimaldistanz nur von c_0 abhängige untere Schranken gefunden, von denen wir zeigen, dass sie größer als 0 sind. Wir erhalten hier daher asymptotisch gute Codes, falls $0 < \frac{d'(\mathcal{C}_n)}{M} \leq 0,015$. Um das zu gewährleisten, ist hier das letzte Ziel, c_0 so zu bestimmen, dass beide Ungleichungen erfüllt sind. Dazu betrachten wir Gleichung (1), nach der zum einen $0,015 \geq 1 - \frac{\log(2c_0)}{\log(29)} \iff \log(c_0) \geq \log(29^{0,985}/2)$, was für $c_0 \geq 13,79$ gilt, und zum anderen $0 < \frac{d'(\mathcal{C}_n)}{M} = 1 - \frac{\log(2c_0)}{\log(29)} \iff \log(c_0) < \log(29/2) \iff c_0 < 14,5$. Somit erhalten wir für $13,79 \leq c_0 < 14,5$ asymptotisch gute NF-Codes über einem Alphabet der Größe 29 mit einer relativen Minimaldistanz δ mit $0 < \delta \leq 0,015$.
Hier war unser Ziel, die Alphabetgröße minimal zu halten. Mit deutlich größeren Alphabeten hätten wir auch eine deutlich größere Minimaldistanz erreichen können, wir hätten sogar beliebig nah an die Singleton-Schranke kommen können.
Dies beweist eines der wichtigsten Ergebnisse dieser Arbeit.

Theorem 5.14
Es existieren Familien von asymptotisch guten Zahlkörpercodes. Insbesondere existieren solche Codes über $\mathbb{F}_{29}$.

Beweis: Siehe oben. □

5.4.2 Erhalt einer Familie von asymptotisch guten Codes mit kleinerem Alphabet

Da es unser Ziel ist, die Größe des Alphabets niedrig zu halten, werden wir unser Augenmerk in diesem Abschnitt darauf wenden, eine Familie von asymptotisch guten Codes mit einer kleineren Alphabetgröße als 29 zu konstruieren. Es zeigt sich, dass dies schwierig wird, falls wir unsere Herangehensweise nicht ändern. Es scheint nämlich so, als bräuchten wir für die Anwendung von Proposition 5.9, sprich die Existenz eines unendlichen T-zerlegenden 2-Klassenkörperturms, eine Verzweigung an mindestens acht Stellen. Das führt uns zu einer gewissen Minimalgröße der Diskriminante und lässt somit keine kleinere Primzahl als 29 für Lemma 5.13 ii) zu. Wir werden später kurz darauf eingehen, dass es eine andere Beweismethode gibt, um eine Alphabetgröße von 17 zu ermöglichen, diese bleibt uns mit unserem Wissen aber vorenthalten. Allerdings können wir mit einer kleinen Änderung bereits eine Alphabetgröße von 19 erreichen. NF-Codes müssen nicht zwangsweise linear sein, was für uns bedeutet, dass wir uns nicht auf Primideale aus $\mathcal{O}_K$ beschränken müssen, die nur über einer Primzahl liegen. Wir nutzen im Folgenden zwei Primzahlen, genauer die Primzahlen 17 und 19.

Lemma 5.15
Sei $d = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29 \cdot 37 \cdot 41 = 15192762585$ *und* $K = \mathbb{Q}(\sqrt{-d})$. *Dann gilt:*

i) $rd_K = \sqrt{4d} \approx 246515,72$

ii) $\mathcal{O}_K$ *hat eine Menge* T *mit* 4 *Primidealen, zwei der Norm* 17 *und zwei der Norm* 19.

iii) K *hat einen unendlichen* T*-zerlegenden* 2*-Klassenkörperturm.*

Beweis: Dieser Beweis verläuft analog zum Beweis von Lemma 5.13. Wir nutzen für Teil i) Lemma 5.10 mit $-d = -15192762585 = -3798190646 \cdot 4 - 1 \equiv 3 \mod 4$. Für Teil ii) zeigen wir, dass beide Legendre-Symbole $(\frac{-d}{17}) = (\frac{-d}{19}) = 1$, wodurch mit Lemma 5.12 und Definition 2.17 folgt, dass es

$\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_3, \mathfrak{q}_4$ gibt mit $\|\mathfrak{p}_1\| = \|\mathfrak{p}_2\| = 17$ und $\|\mathfrak{q}_3\| = \|\mathfrak{q}_4\| = 19$, dann sei $T \coloneqq \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_3, \mathfrak{q}_4\}$. Teil iii) ergibt sich mit Proposition 5.9, da die nötige Abschätzung $r \geq 3 + t - s + 2\sqrt{2+t}$ mit $r = 10, s = 2$ und $t = 4$ erfüllt ist. □

Das führt uns zum zweiten Hauptsatz unserer Arbeit.

Theorem 5.16

Es existieren asymptotisch gute Zahlkörpercodes über einem Alphabet der Größe 19.

Beweis: Dieser Beweis basiert erneut auf der Konstruktion einer Familie von NF-Codes und ist somit ähnlich zum Beweis von Theorem 5.14.
Sei $K_0 = K \subset K_1 \subset K_2 \subset \dots$ ein unendlicher T-zerlegender 2-Klassenkörperturm aus Lemma 5.15. Jedes dieser K_n erzeugt einen Code $\mathcal{C}_n$. Für die Konstruktion von $\mathcal{C}_n$ halten wir n fest. Sei dazu $[K_n : \mathbb{Q}] = M$. Da K_n vollständig komplex ist, ist seine Signatur $(0, \frac{M}{2})$. Nach Lemma 5.15 sind die Primideale 17 und 19 in der Erweiterung von K_n über $\mathbb{Q}$ voll zerlegt, daher hat $\mathcal{O}_K$ M Primideale $\mathfrak{p}_1, \dots \mathfrak{p}_M$ der Norm 17 und M Primideale $\mathfrak{q}_1, \dots, \mathfrak{q}_M$ der Norm 19. Sei nun $\mathcal{C}_n$ der NF-Code mit den Parametern $(N; \mathfrak{p}_1, \dots, \mathfrak{p}_M, \mathfrak{q}_1 \dots, \mathfrak{q}_M; B; \mathfrak{z})$ mit $N = 2M$, $B = c_0 M$ für eine geeignete Konstante c_0 und $\mathfrak{z} \in \mathbb{C}^{M/2}$ der Verschiebungsparameter aus Satz 4.29. Dabei existiert mindestens ein t mit $\prod_{i=1}^{t} ||\mathfrak{p}_i|| > (2B/M)^M = (2c_0)^M$, falls $0 < c_0 < (17 \cdot 19)/2 = 161,5$. Wir bemerken wieder, dass c_0 unabhängig von n gewählt werden kann.
Nachfolgend bestimmen wir erneut unter Verwendung von Satz 4.29 sowohl die Minimaldistanz als auch die Informationsrate der Codes $\mathcal{C}_n$. So ergibt sich für die Minimaldistanz

$$d(\mathcal{C}_n) \geq 2M - \frac{M \log(2c_0)}{\log(17)} = d'(C_n). \tag{2}$$

Des Weiteren gilt für die Informationsrate

$$\begin{aligned}
R(\mathcal{C}_n) &\geq \frac{(N - d'(\mathcal{C}_n)) \log \|\mathfrak{p}_1\| + s \log(\pi/4) + M \log e - M \log \sqrt{rd_{K_n}} - \log(3M)}{N \log \|\mathfrak{q}_M\|} \\
&= \frac{(2M - d'(\mathcal{C}_n)) \log(17) + \frac{M}{2} \log(\pi/4) + M \log e - M \log \sqrt{rd_{K_n}} - \log(3M)}{2M \log(19)} \\
&= \left(1 - \frac{d'(\mathcal{C}_n)}{2M}\right) \frac{\log(17)}{\log(19)} + \frac{M \log(\sqrt{\pi/4}) + M \log e - M \log \sqrt{rd_{K_n}}}{2M \log(19)} - \frac{\log(3M)}{2M \log(19)} \\
&= \left(1 - \frac{d'(\mathcal{C}_n)}{2M}\right) \frac{\log(17)}{\log(19)} + \frac{\log(\frac{e}{2}\sqrt{\frac{\pi}{rd_{K_n}}})}{2 \log(19)} - \frac{\log(3M)}{2M \log(19)} \\
&= \left(1 - \frac{d'(\mathcal{C}_n)}{2M}\right) \frac{\log(17)}{\log(19)} - \frac{\log(\frac{2}{e}\sqrt{\frac{rd_{K_n}}{\pi}})}{2 \log(19)} - \frac{\log(3M)}{2M \log(19)}.
\end{aligned}$$

Da für große M der Term $-\frac{\log(3M)}{2M \log(19)}$ gegen 0 geht, erhalten wir durch Einsetzen von $rd_{K_n} = rd_K =$

$246515,72$

$$\begin{aligned} R(\mathcal{C}_n) &\geq \left(1 - \frac{d'(\mathcal{C}_n)}{2M}\right) \frac{\log(17)}{\log(19)} - \frac{\log(206,11)}{2\log(19)} - \frac{\log(3M)}{2M\log(19)} \\ &= \frac{\log(17)}{\log(19)} \left(1 - \frac{d'(\mathcal{C}_n)}{2M} - \frac{\log(206,11)}{2\log(17)}\right) - \frac{\log(3M)}{2M\log(19)} \\ &> \frac{\log(17)}{\log(19)} \left(1 - \frac{d'(\mathcal{C}_n)}{2M} - 0,941\right), \end{aligned}$$

wobei wir im letztem Schritt erneut den Rundungsfehler abschätzen (vgl. Rechnung in Kapitel 5.4.1) Die Codes sind demnach asymptotisch gut, falls $\frac{d(\mathcal{C}_n)}{2M} \geq \frac{d'(\mathcal{C}_n)}{2M} > 0$ und $1 - \frac{d'(\mathcal{C}_n)}{2M} - 0,941 \geq 0 \iff \frac{d'(\mathcal{C}_n)}{M} \leq 1 - 0,941 = 0,059$, denn auch hier hängen die unteren Schranken der Informationsrate und der relativen Minimaldistanz nicht mehr von n ab. Wir müssen also $0 < c_0 < 161,5$ so bestimmen, dass $0 < \frac{d'(\mathcal{C}_n)}{M} \leq 0,059$ gilt. Dazu betrachten wir die Gleichung (2), nach der zum einen $0,059 \geq 2 - \frac{\log(2c_0)}{\log(17)} \iff \log(c_0) \geq \log(17^{1,941}/2)$ gilt, woraus wir die Bedingung $c_0 \geq 122,26$ erhalten, und zum anderen $0 < \frac{d'(\mathcal{C}_n)}{M} = 2 - \frac{\log(2c_0)}{\log(17)} \iff \log(c_0) < \log(17^2/2) \iff c_0 < 144,5$. Somit erhalten wir für die c_0 mit $122,26 \leq c_0 < 144,5$ asymptotisch gute NF-Codes über einem Alphabet der Größe 19 und einer relativen Minimaldistanz von δ mit $0 < \delta \leq 0,059$. □

Wie bereits erwähnt würde auch die Möglichkeit bestehen, zu zeigen, dass es sogar asymptotisch gute NF-Codes der Alphabet Größe 17 gibt. Dafür würde man in der Konstruktion auf jegliche Ideale anderer Norm als 17 verzichten. Dies ist mit unserer Konstruktionsidee nicht zu verwirklichen. Hierzu müssten wir wissen, wie man archimedische Stellen zum codieren nutzt. Gleichzeitig möchten wir erwähnen, dass der zugrunde liegende Körper $K := \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29})$ ist, welcher einen unendlichen 2-Klassenkörperturm hat, in dem das Primideal 17 den Weg hinauf voll zerlegt wird.

Literatur

[Cau21] Cauchy, Augustin Louis: *cours d'analyse de l'école royale polytechnique*. DE L'IMPRIMERIE ROYALE, Paris, 1821, ISBN 978-1-160-84277-8.

[For11] Forster, Otto: *Analysis 3*. Vieweg+Teubner, Wiesbaden, 2011, ISBN 978-3-8348-1232-2.

[Ga64] Golod-Šafarevič: *On the class field tower*. Izv. Akad. Nauk SSSR, 28:261–272, 1964.

[Gur00a] Guruswami, Venkatesan: *Constructions of Codes from Number Fields*. MIT Laboratory for Computer Science, Cambridge, 2000. `https://eccc.weizmann.ac.il/report/2001/002/`, (zuletzt aufgerufen am 22.07.2021).

[Gur00b] Guruswami, Venkatesan: *"Soft-decision" Decoding of Chinese Remainder Codes*. MIT Laboratory for Computer Science, Cambridge, 2000. `http://madhu.seas.harvard.edu/papers/2000/gss-conf.pdf`, (zuletzt aufgerufen am 22.07.2021).

[Len86] Lenstra, Hendrik: *Codes from Algebraic Number Fields*. Mathematics and computer science II: fundamental contributions in the Netherlands since 1945, 4:95 – 104, 1986.

[Mar18] Marcus, Daniel A.: *Number Fields*. Springer-Verlag, Berlin; Heidelberg; New York, 2018, ISBN 978-3-319-90232-6.

[Neu92] Neukirch, Jürgen: *Algebraische Zahlentheorie*. Springer-Verlag, Berlin; Heidelberg; New York, 1992, ISBN 978-3-540-37547-0.

[Rob55] Robbins, Herbert: *A Remark On Stirling's Formula*. Mathematical Association of America, The American Mathematical Monthly, Vol. 62, No. 1 (Jan., 1955), pp. 26-29, 1955.

[Tsf00] Tsfasman, Michael; Vladut, Serge: *Infinite Global Fields and the Generalized Brauer-Siegel Theorem*. 2000. `https://arxiv.org/abs/math/0205129v1`, (zuletzt aufgerufen am 22.07.2021).

Versicherung an Eides Statt

Ich versichere an Eides statt durch meine untenstehende Unterschrift,

- dass ich die vorliegende Arbeit - mit Ausnahme der Anleitung durch die Betreuer - selbstständig ohne fremde Hilfe angefertigt habe und
- dass ich alle Stellen, die wörtlich oder annähernd wörtlich aus fremden Quellen entnommen sind, entsprechend als Zitate gekennzeichnet habe und
- dass ich ausschließlich die angegebenen Quellen (Literatur, Internetseiten, sonstige Hilfsmittel) verwendet habe und
- dass ich alle entsprechenden Angaben nach bestem Wissen und Gewissen vorgenommen habe, dass sie der Wahrheit entsprechen und dass ich nichts verschwiegen habe.

Mir ist bekannt, dass eine falsche Versicherung an Eides Statt nach §156 und nach §163 Abs. 1 des Strafgesetzbuches mit Freiheitsstrafe oder Geldstrafe bestraft wird.

Ort, Datum	Unterschrift