Algebra II

Lukas Meinschad

Contents

0.1 Körpertheorie

0.1.1 Normale und separable Erweiterungen

Definition 0.1.1: Normale Körpererweiterung

Eine algebraische Körpererweiterung $k \subset K$ heißt **normal** falls jedes irreduzible Polynom $p \in k[t]$ welches in K eine Nullstelle hat in K bereits zerfällt

Example 0.1.1

- ISt K algebraisch abgeschlossen, so ist die Erweiterung $k \subset K$ trivialerweise normal. Beispielsweise ist $\mathbb{R} \subset \mathbb{C}$ normal
- $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ist nicht normal.

Theorem 0.1.1 Charakterisierung Normaler Körpererweiterungen

Für eine algebraische Körpererweiterung $k \subset K \subset \bar{k}$ ist äquivalent:

1. $k \subset K$ ist normal
2. K ist der Zerfällungskörper einer Menge von Polynomen über k
3. Jeder k-Homomorphismus $\varphi : K \to \bar{k}$ erfüllt $\varphi(K) \subset K$

Damit findet man leicht einige Beispiele für normale Körpererweiterungen:

- $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$
- $\mathbb{Q} \subset \mathbb{Q}(\exp 2\pi i/d)$

Definition 0.1.2: Separabel

- Ein irreduzibles Polynom $p \in k[x]$ heißt separabel, fals p in $\bar{k}$ oder einem Zerfällungskörper $deg(p)$ viele verschiedene Nullstellen besitzt
- Für eine Körpererweiterung $k \subset K$ heißt $a \in K$ separabel über k, falls a algebraisch über k ist und $Min(a, k)$ separabel ist
- Eine algebraische Körpererweiterung $k \subset K$ heißt separabel falls jedes $a \in K$ separabel über k ist

Definition 0.1.3: Formale Ableitung

Sei R ein kommutativer Ring. Dann heißt die Abbildung

$$\partial : R[x] \to R[x] \tag{1}$$

$$\sum_{i=0}^{d} c_i x^i \to \sum_{i=1}^{d} i c_i x^{i-1} \tag{2}$$

die formale Ableitung

Lemma 0.1.1

Sei R ein kommutativer Ring und ∂ die formale Ableitung auf $R[x]$ dann gilt für $r, s \in R, p, q \in R[x]$

$$\partial(rp + sq) = r\partial(q) + s\partial(q) \tag{3}$$

$$\partial(pq) = p\partial(q) + q\partial(p) \tag{4}$$

$$\partial(r) = 0 \tag{5}$$

Theorem 0.1.2 Separabel und die Formale Ableitung

Sei k ein Körper und $p \in k[x]$ irreduzibel dann gilt:

$$p \; separabel \Leftrightarrow \partial(p) \neq 0 \tag{6}$$

Man sollte sich hier als Fact merken dass im Fall $char(k) = 0$ gilt das jedes irreduzible Polynom $p \in k[x]$ bereits separabel ist. Insbesndere ist in diesem Fall jede algebraische Körpererweiterung $k \subset K$ separabel. Ist nun $char(k) = d$ so ist ein irreduzibles $p \in k[x]$ genau dann inseparabel wenn es ein $q \in k[x]$ gibt mit $p(x) = q(x^d)$

Definition 0.1.4: Vollkommen

Ein Körper k heißt **vollkommen** falls jedes irreduzible Polynom $p \in k[x]$ separabel ist

Damit ist also auch jeder Körper mit Charakteristik 0 vollkommen da die irreduziblen Polynome separabel sind. Als Abschluss betrachten wir noch die Aussage des **Satzes des Primitiven Elements**

Theorem 0.1.3 Satz vom Primitiven Element

Sei $k \in K$ eine endliche separable Körpererweiterung. Dann gibt es ein $a \in K$ mit $K = k(a)$

0.1.2 Galoistheorie

Die Galoistheorie erlaubt es uns die Fragen der Körpertheorie in die Fragen der Gruppentheorie zu übersetzen. Damit kann man auch die Lösbarkeit von Polynomialen Gleichungen betrachten.

Definition 0.1.5: Galoisgruppe

Sei $k \subset K$ eine Körpererweiterung. Wir definieren die Galoisgruppe

$$Gal(K,k) := \{\varphi : K \to K | \varphi \; k - Isomorphismus\} \tag{7}$$

Die Elemente nennt man hier dann k-Automorphismen

Bestimmen wir zuerst $Gal(\mathbb{C},\mathbb{R})$ hierzu gilt $\mathbb{C} = \mathbb{R}$. Es gibt genau so viele $\mathbb{R}$-Homomorphismen wie es Nullstellen von $x^2 + 1$ in $\mathbb{C}$ gibt damit sind das $i, -i$. Man erhält als Elemente die Identität und die komplexe Konjugation.

$$Gal(\mathbb{C},\mathbb{R}) = \{id_{\mathbb{C}}, \kappa\} \cong \mathbb{Z}/2\mathbb{Z} \tag{8}$$

Lemma 0.1.2

Sei $p \in k[x]$ und K der Zerfällungskörper

1. Es gilt $\#Gal(K,k) \leq [K : k]$ insbesondere ist die Galoisgruppe der Erweiterung endlich
2. Fall alle Nullstellen von p verschieden sind gilt $\#Gal(K,k) = [K : k]$

Definition 0.1.6: Fixkörper

Sei $k \subset K$ eine Körpererweiterung, $G = Gal(K,k)$ und $H < G$ eine Untergruppe. Dann definieren wir

$$Fix(H) := \{b \in K | \varphi(b) = b \; \forall \varphi \in H\} \tag{9}$$

Man sieht hierbei leicht das $Fix(H)$ für jede Untergruppe H der Galoisgruppe ein Zwischenkörper der Erweiterung ist. $k \subset Fix(H) \subset K$

Umgekehrt gilt für jeden Zwischenkörper offensichtlich $Gal(K,L) < Gal(K,k)$

Damit erhalten wir eine Zuordnung zwischen den Untergruppen der Galoisgruppe und der Zwischenkörpern:

Diese Zuordnung ist inklusionsumkehrend:

- Für $H_1 < H_2 < Gal(K,k)$ gilt $Fix(H_2) \subset Fix(H_1)$
- Für $L_1 \subset L_2 \subset K$ gilt $Gal(K,L_2) \subset Gal(K,L_1)$
- Weiteres gilt $H \subset Gal(K, Fix(H))$ und $L \subset Fix(Gal(K,L))$

Proposition 0.1.1 Lemma von Artin

Sei $k \subset K$ eine Körpererweiterung und $H \subset Gal(K,k)$ endlich. Dann gilt $[K : Fix(H)] \leq \#H$

: Sei $n = \#H$ und $H = \{\varphi_1, ..., \varphi_n\}$. Sei $m > n$ und $a_1, ..., a_m \in K$. Wir zeigen dass $a_1, ..., a_m$ linear abhängig über $Fix(H)$ sein müssen. Dazu betrachtet man folgendes Gleichungsystem

$$\varphi_1(a_1)x_1 + ... + \varphi_1(a_m)x_m = 0 \tag{10}$$
$$... \tag{11}$$
$$\varphi_n(a_1)x_1 + ... + \varphi_n(a_m)x_m = 0 \tag{12}$$

Nun ist $m > n$ und es gibt nicht triviale Lösung $(b_1, ..., b_m) \in K^m$ und wir wählen jene mit maximaler Anzahl von Nullen in den Einträgen. Sei außerdem o.b.d.A $b_1 = 1$. Für alle i, j gilt:

$$0 = \varphi_j(0) = \varphi_j(\sum_k \varphi_i(a_k)b_k) = \sum_k (\varphi_j \circ \varphi_i)(a_k)\varphi_j(b_k) \tag{13}$$

Damit durchlaufen für festes j die Elemente $\varphi_j \circ \varphi_j$ die ganze Gruppe und auch $(\varphi_j(b_1), ..., \varphi_j(b_m) \in K^m$ eine Lösung durch Homogenität ist auch

$$(b_1 - \varphi_j(b_1)...b_m - \varphi_j(b_m)) \in K^m \tag{14}$$

eine Lösung. Angenommen es gilt nun $b_i \notin Fix(H)$ dann gibt es ein j mit $\varphi_j(b_i) \neq b_i$ damit

$$(b_1 - \varphi_j(b_1), ..., b_m - \varphi_j(b_m) = (1 - 1, ..., b_i - \varphi_j(b_i), ..., b_m - \varphi_j(b_m)) \tag{15}$$

eine nichttriviale Lösung mit einer Null mehr. Das ist ein Widerspruch und zeigt $b_i \in Fix(H)$ für alle i. Daraus folgt der Beweis. □

Definition 0.1.7: Galois-Erweiterung

Eine Körpererweiterung heißt **Galois-Erweiterung** falls sie endlich, normal und separabel ist

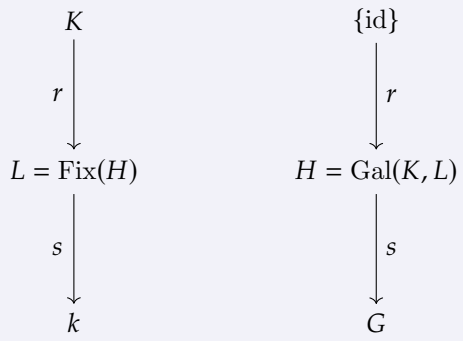
Mit $char(k) = 0, p \in k[x]$ sind also folgende Erweiterungen Galoiserweiterungen:

- $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$
- $\mathbb{Q} \subset \mathbb{Q}(\exp(2\pi i/d))$
- $\mathbb{R} \subset \mathbb{C}$

Theorem 0.1.4 Hauptsatz der Galoistheorie

Es sei $k \subset K$ eine Galois-Erweiterung. Dann sind die Zuordnungen $Fix(*)$ und $Gal(K,*)$ zueinander inverse inklusionsumkehrende Bijektionen zwischen Untergruppen von $G = Gal(K,k)$ und den Zwischenkörpern von k und K. Zudem gilt für $H < G$:

1. $\#H = [K : Fix(H)]$ und $|G : H| = [Fix(H) : k]$
2. $H \lhd G \Leftrightarrow Fix(H)$ normal über k. In diesem Fall ist $k \subset Fix(H)$ wieder eine Galois-Erweiterung und es gilt $Gal(Fix(H), k) \cong G/H$



: Mit dem Satz vom primitiven Element ist K als Galoiserweiterung der Zerfällungskörper eines separablen Polynoms über k. Es gilt also $\#Gal(K,k) = [K:k]$. Dieses Argument kann man auch auf jeden Zwischenkörper $k \subset L \subset K$ anwenden und erhält $\#Gal(K,L) = [K:L]$. Sei nun $H < G := Gal(K,k)$ eine Untergruppe nun gilt $H \subset Gal(K, Fix(H))$ und mit dem **Lemma von Artin**

$$\#H \leqslant \#Gal(K, Fix(H)) = [K : Fix(H)] \leq \#H \tag{16}$$

Das beweis $Gal(K, Fix(H)) = H$ und die erste Gleichung die zweite Gleichung folgt aus

$$\#G = [K:k] = [K : Fix(H)] * [Fix(H) : k] = \#H * [Fix(H) : k] \tag{17}$$

Nun gilt offensichtlich $Gal(K, Fix(Gal(K,k))) = Gal(K,k)$ damit

$$[K:k] = \#Gal(K,k) = \#Gal(K, Fix(Gal(K,k))) = [K : Fix(Gal(K,k))] \tag{18}$$

damit gilt $Fix(Gal(K,k)) = k$ und man sieht das die Zuordnungen zueinander beidseitig invers sind.

Für die zweite Aussage betrachtet man $H < G$ und $L = Fix(H)$ dann gilt für $\varphi \in G : \varphi(L) = Fix(\varphi H \varphi^{-1})$

$$\begin{aligned} a \ \in Fix(\varphi H \varphi^{-1}) &\Leftrightarrow (\varphi\tau\varphi^{-1})(a) = a \forall \tau \in H && (19)\\ &\Leftrightarrow (\tau\varphi^{-1})(a) = \varphi^{-1}(a) \forall \tau \in H && (20)\\ &\Leftrightarrow \varphi^{-1}(a) \in Fix(H) = L && (21)\\ &\Leftrightarrow a \in \varphi(L) && (22) \end{aligned}$$

Ist nun H eine normale Untergruppe in G so gilt $\varphi H \varphi^{-1} = H$ und somit $\varphi(L) = L$ für alle $\varphi \in G$ nun kann man noch auf die Normalität von L über k diskutieren dazu betrachtet man die Kette

$$k \subset L \subset K \subset \hat{k} \tag{23}$$

und einen Homomorphismus $\varphi : L \to \bar{k}$ nun kann man die Fortsetzung bilden $\varphi : K \to \bar{k}$ und da K normal über k ist gilt sogar $\varphi : K \to K$.

Ist umgekehrt L normal über k dann gilt wieder $\varphi(L) \subset L$ für alle $\varphi \in G$ also $Fix(\varphi H \varphi^{-1}) \subset Fix(H)$ nach Anwendung von $Gal(K, *)$ erhält man $H \subset \varphi H \varphi^{-1}$ und aufgrund der Mächtigkeit natürlich $H = \varphi H \varphi^{-1}$. Damit ist H eine normale Untergruppe.

Konkret betrachtet man nun noch den Gruppenhomomorphismus

$$\begin{aligned} \pi : G &\to Gal(L,k) && (24)\\ \varphi &\to \varphi_{|L} && (25) \end{aligned}$$

Dies ist wohldefiniert und aufgrund der Noramlität von L über k gilt stets $\varphi(L) \subset L$. Es gilt $ker(\pi) = Gal(K, L) = Gal(K, Fix(H)) = H$ dann gilt mit den Homomorphiesatz

$$G/H \cong Gal(L, k) \tag{26}$$

□

0.1.3 Unlösbarkeit von Polynomialen Gleichungen

Definition 0.1.8: Mit Radikalen Auflösbar

Eine Körpererweiterung $k \subset K$ heißt mit Radikalen auflösbar, falls es eine Körperkette

$$k = k_0 \subset k_1 \subset ... \subset k_m = K \tag{27}$$

gibt mit $k_{i+1} = k_i(a_i)$ mit $a_i^{d_i} \in k_i$ für alle $i = 0, ..., m. - 1.$
Für $p \in k[x]$ ist die Gleichung $p = 0$ mit Radikalen auflösbar wenn es eine Körpererweiterung $k \subset K$ gibt die mit Radikalen auflösbar ist und p über K in Linearfaktoren zerfällt

Lemma 0.1.3

Sei $k \subset K$ mit Radikalen auflösbar. Dann gibt es einen Erweiterungskörper L von K sodass die Erweiterung $k \subset L$ mit Radikalen auflösbar und zusätzlich normal ist. Dabei bleiben die verwendeten Exponenten gleich

: Da $k \subset K$ mit Radikalen auflösbar ist, können wir k_i, a_i und d_i wie in der Definition wählen. Für jedes $i = 0, ..., m - 1$ seien

$$a_i = a_{i1}, a_{i2}, ..., a_{in_i} \tag{28}$$

die Nullstellen von $Min(a_i, k)$ in $\bar{K}$. Nun ist p_i ein Teiler von $x^{d_i} - a_i^{d_i}$ es gilt $a_{ij}^{d_i} = a_i^{d_i} \in k_i = k(a_0, ..., a_{i-1})$ für alle i, j

Man kann eine neue Körperkette konstruieren indem man die ELemente iterativ adjungiert. Da nun dieser Körper L der Zerfällungskörper von Polynome $p_0, ..., p_{m-1}$ über k ist ist die Erweiterung $k \subset L$ normal. □

Theorem 0.1.5 Gleichung $p = 0$ auflösbar $\implies$ Gal ist auflösbar

Sei $p \in \mathbb{Q}^x$ und K der Zerfällungskörper von p über $\mathbb{Q}$. Falls die Gleichung $p = 0$ mit Radikalen auflösbar ist so ist $Gal(K, \mathbb{Q})$ eine auflösbare Gruppe

Theorem 0.1.6

Sei d eine Primzahl $p \in \mathbb{Q}^x$ irreduzibel vom Grad d und habe genau 2 Nullstellen in $\mathbb{C} \setminus \mathbb{R}$. Dann gilt für den Zerfällngskörper K von p über $\mathbb{Q}$:

$$Gal(K, \mathbb{Q}) \cong S_d \tag{29}$$

: Das Polynom p hat in $\mathbb{C}$ die verschiedenen Nullstellen $a_1, ..., a_n$ und $\varphi \in Gal(K, \mathbb{Q})$ permutiert diese. Man erhält einen injektiven Gruppenhomomorphismus

$$\iota : G \to S_d \tag{30}$$

Nun hat p reelle Koeffizienten damit gilt $0 = \bar{0} = p(\bar{a}_i) = p(\bar{a}_i)$ damit ist $\bar{a}_i$ wieder eine Nullstelle, komplexe Konjugation κ ist in G und $\iota \in S_d$ ist eine Transposition da p genau zwei nichtreelle Nullstellen hat.

$$\#G = [K : \mathbb{Q}] = [K : \mathbb{Q}(a_1)][\mathbb{Q}(a_1) : \mathbb{Q}] = d[K : \mathbb{Q}(a_1)] \tag{31}$$

Zeigt das G nach dem 1.Sylowsatz eine Untergruppe der Mächtigkeit d besitztund ein Element der Ordnung d. Nun ist d prim und $\iota(\varphi) \in S_d$ muss ein Zyklus der Länge d sein. Die Transposition und der d-Zyklus erzeugen die Gruppe. Damit bekommt man die Isomorphie. □

Corollary 0.1.1

Für $p = x^5 - 4x + 2 \in \mathbb{Q}^x$ ist die Gleichung $p = 0$ nicht mit Radikalen auflösbar

: Mit dem Eisensteinkriterium und $d = 2$ einer Primzahl sieht man das p irreduzibelist die Ableitung $p' = 5x^4 - 4$ ist negativ im Intervall $I = [-\sqrt[4]{4/5}, \sqrt[4]{4/5}]$ und positiv außerhalb. Damit hat man höchstens 3 reelle Nullstellen. Man berechnet.

$$p(-2) < 0, p(-1) > 0, p(1) < 0, p(2) > 0 \tag{32}$$

nach dem Zwischenwertsatz hat p also genau drei Reelle Nullstelle und es gilt für den Zerfällungskörper K von p

$$Gal(K, \mathbb{Q}) \cong S_5 \tag{33}$$

Diese Gruppe ist jedoch nich auflösbar! Damit ist $p = 0$ nicht auflösbar nicht auflösbar □

0.2 Moduln

In der linearen Algebra untersucht man lineare Gleichungssysteme über Körpern. Dafür gibt es Lösungsalgorithmen z.b. den Gauß Algorithmus. Möchte man nun ein lineares Gleichungssystem über einen Ring lösen, so funktioniert das nicht so einfach da man durch Skalare nicht mehr teilen kann.

Der Begriff des Moduls ist hierbei eine Verallgemeinerung des Vektorraums, man legt nun als Skalarkörper einen Ring zu Grunde.

0.2.1 Grundlagen

Definition 0.2.1: R-Modul

Sei R ein kommutativer Ring. Ein R-Modul ist eine abelsche Gruppe $(M, +)$ mit einer Operation genannt Skalarmultiplikation

$$R \times M \to M \tag{34}$$
$$(r, m) \to r * m \tag{35}$$

Dabei gilt für $r, s \in R; m, n \in M$

- $r * (m + n) = (r * m) + (r * n)$
- $(r + s) * m = (r * m) + (s * m)$
- $(rs) * m = r * (s * m)$

Example 0.2.1

- Ist $R = k$ ein Körper so ist ein R Modul genau das gleiche wie ein K-Vektorraum.
- Für jeden Ring R ist R^n auf kanonische Weise ein R Modul
- Ist $I \lhd R$ ein Ideal so ist I ein R-Modul wobei die Skalarmultiplikation dann einfach die Ringmultiplikation ist. Ein Beispiel ist $3\mathbb{Z}$ ein $\mathbb{Z}$-Modul und (x, y) ein $k[x, y]$ Modul.
- Ist $I \lhd R$ ein Ideal so ist der Faktorring R/I auf kanonische Weise ein R-Modul.

Definition 0.2.2: R-Untermodul

Sei M ein R-Modul. Ein R-Untermodul U von M ist eine Untergruppe U von M mit $ru \in U, \forall r \in R, u \in U$

Definition 0.2.3: R-Modulhomomorphismus

Seien M, N zwei R-Modul ein **Modulhomomorphismus** ist eine Abbildung $f : M \to N$ mit

$$f(m+n) = f(m) + f(n) \wedge f(rm) = rf(m) \tag{36}$$

Example 0.2.2

- Sei R ein Ring und $A \in Mat_{m,n}(R)$ dann ist die Lösungsmenge des linearen Gleichungsystems $Ax = 0$ ein Untermodul von R^n
- Nicht jeder Untermodul von R^n ist die Lösungsmenge eines linearen Gleichungssystems (im Gegensatz zum Vektorraumfall). Beispiel ist $2\mathbb{Z} \subset \mathbb{Z}$
- Für jeden Modulhomomorphismus $f : M \to N$ ist $f(M)$ ein Untermodul von N
- Es ist $ker(f) := \{m \in M | f(m) = 0\}$ ein Untermodul von M

Note:-

Gleich wie in der Gruppentheorie gilt der Homomorphiesatz. Ist $f : M \to N$ ein Homomorphismus von R Modulen so ist der folgende Hmomorphismus wohldefiniert und injektiv

$$\bar{f} : M/ker(f) \to N \tag{37}$$
$$m + ker(f) \to f(m) \tag{38}$$

Gleich wie in der linearen Algebra kann man den $span$ definieren als den kleinsten Untermodul von M der eine Teilmenge $W \subset M$ enthält

$$span_R(W) := \{\sum_{i=1}^{d} r_i w_i | d \in \mathbb{N}, r_i \in R, w_i \in W\} \tag{39}$$

Definition 0.2.4: Endlich erzeugt, Basis, Frei

- Ein R Modul M heißt **endlich erzeugt**, falls es eine endliche Teilmenge $W \subset M$ gibt mit $M = span_R(W)$
- Eine Familie $(b_i)_{i \in I}$ mit $b_i \in M$ heißt Basis von M falls es für alle $m \in M$ eine *eindeutig bestimme* $r_i \in R$ exestieren mit $m = \sum_{i \in I} r_i b_i$
- Ein Modul heißt **frei** falls er eine Basis besitzt.

Ebenfalls wie im Vektorraumfall können wir auch Summen von Modulen definieren hierbei gilt:

$$M_1 + ... + M_d := \{m_1 + ... + m_d | m_i \in M_i\} \tag{40}$$

hat jeds Element von $m \in M_1 + ... + M_d$ eine *eindeutige* Darstellung

$$m = m_1 + ... + m_d \tag{41}$$

mit $m_i \in M_i$ so schreibt man $M_1 \bigoplus ... \bigoplus M_d$ und nennt die Summe **direkt**

Example 0.2.3

- Jeder k-Vektorraum ist ein freier k-Modul
- Für jeden Ring R ist R^n ein freier R-Modul, man wählt die Standardbasis $e_1, ..., e_n$
- Ist M ein freier R-Modul mit Basis $(b_1, ..., b_m)$ so ist M isomorph zu R^n
- **Nicht jeder Modul besitzt eine Basis**, ein Beispiel wäre $M = \mathbb{Z}/2\mathbb{Z}$ man könnte $b_1 = 1$ wählen und dann gilt $0 = 0 * b_1 = 2 * b_1$ ein Widerspruch zu Eindeutigkeit.
- Ist $(b_1, ..., b_d)$ eine basis von M so gilt $M = span_R(b_1) \bigoplus ... \bigoplus span_R(b_d)$

Note:-

Es gilt folgende Äquivalenz für die Untermodule M_1, M_2 von M:

$$M = M_1 \bigoplus M_2 \Leftrightarrow M = M_1 + M_2 \wedge M_1 \cap M_2 = \{0\} \tag{42}$$

Des weiteren muss ein Untermodul eines freien Moduls nicht selbst wieder frei sein. Auch der Untermodul eines endlich erzeugten Moduls muss selbst nicht wieder endlich erzeugt sein.

Proposition 0.2.1

Sei R ein noetherscher Ring, M ein endlich erzeugter R-Modul sowie $N \subset M$ ein R-Untermodul. Dann ist N selbst endlich erzeugt

: Beweise die Aussage zunächst im Fall $M = R^n$ über Induktion über n. Im Fall $n = 1$ ist R noethersch daraus folgt die Aussage. Im Allgemeinen Fall betrachte die Projektion auf die erste Koordinate $\pi : R^n \to R$ und das Ideal

$$I := \pi(N) \subset R \tag{43}$$

sowie den Untermodul

$$K := N \cap ker(\pi) \subset N \tag{44}$$

Da R noethersch ist gibt es $n_1, ..., n_d \in N$ mit $I = (\pi(n_1), ..., \pi(n_d)$ damit gilt nun:

$$N = span_R\{n_1, ..., n_d\} + K \tag{45}$$

Nun besteht aber K genau aus den Komponenten mit Null in der ersten Komponente damit ist K ein Untermodul von R^{n-1} und N ist endlich erzeugt. Im allgemeinen Fall gelte $M = span_R\{m_1, ..., m_n\}$ und wir betrachten den surjektiven Modulhomomorphismus:

$$\varphi : R^n \to M; (r_1, ..., r_n) \to r_1 m_1 + ... + r_n m_n \tag{46}$$

Dann ist $\varphi^{-1}(N) \subset R^n$ ein Untermodul und somit endlich erzeugt. Dann gilt jedoch

$$N = \varphi(\varphi^{-1}(N)) \tag{47}$$

und N selbst ist endlich erzeugt. □

Lemma 0.2.1

Sei M ein R Modul, $M \subset M$ und $I \lhd R$ ein Ideal

1. Es ist $IM := \{\sum_{k=1}^{d} i_k m_k | d \in \mathbb{N}, i_k \in I, m_k \in M\}$ ein R Untermodul von M
2. Es ist die folgende Skalarmultiplikation wohldefiniert und macht den R-Modul M/IM zu einen R/I

Modul

$$R/I \times M/IM \to M/IM \tag{48}$$
$$(r+I, m+IM) \to rm+IM \tag{49}$$

3. $M = span_R(W)$ folgt $M/IM = span_{R/I}(w+IM|w \in W)$
4. Ist $(b_j)_{j\in J}$ eine Basis des R Modul M so ist $(b_j+IM)_{j\in J}$ eine Basis des R/I Moduls M/IM

Theorem 0.2.1 Mächtigkeit der Basen

Sei $R \neq 0$ und M ein freier R-Modul. Dann haben je zwei Basen von M dieselbe Mächtigkeit. Jedes Erzeugendensystem hat mindestens diese Mächtigkeit.

: Man kann die Aussage mit dem Lemma auf den Vektorraumfall zurückfuhren. Dazu seien also $(a_i)_{i\in I}$ und $(b_j)_{j\in J}$ zwei Basen des R-Moduls M sowie $W \subset M$ ein Erzeugendensystem. Wähle nun ein Maximales Ideal $m \subset R$ und erhalte aus dem Lemma:

$$(a_i+mM)_{i\in I} \wedge (b_j+mM)_{j\in J} \tag{50}$$

sind Basen des R/m Moduls M/mM und man bekommt auch ein Erzeugendensystem. Nun ist R/m ein Körper hier wissen wir das M/mM ein Vektorraum ist und es gilt

$$\#I = \#J \leqslant \#\{w+mM|w \in W\} \leqslant \#W \tag{51}$$

□

0.2.2 Tensorprodukt

Tensorprodukte sind Konstruktionen mit denen man Bilinearität in Linearität verwandeltn kann. Die explizite Konstruktion ist meist mühsam, man führt sie oft erst über ihre wichtigste Eigenschaft (*universelle Eigenschaft*) ein.

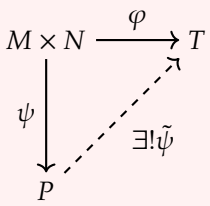
Definition 0.2.5: Tensorprodukt

Seien M, N zwei R Module. Ein Tensorprodukt von M und N ist ein R Modul T gemeinsam mit einer R bilinearen Abbildung

$$\varphi : M \times N \to T \tag{52}$$

sodass jede andere R-bilineare Abbildung $\psi : M \times N \to P$ eindeutig linearr über T faktorisiert.

$$\exists!\tilde{\psi} \implies \psi = \tilde{\psi} \circ \varphi \tag{53}$$



Theorem 0.2.2 Existenz und Eindeutigkeit

Für je zwei R-Moduln M, N exestiert ein Tensorprodukt. Dieses ist bis auf eindeutige Isomorphie eindeutig bestimmt es gilt:

$$M \otimes_R N \tag{54}$$

: **Existenz:** Sei F der freie R-Modul mit Basis $((m,n))_{(m,n)\in M\times N}$. Damit sind die Elemente endliche R Linearkombination von Elementen aus $M \times N$. Betrachte nun den Untermodul U der von folgenden Elementen erzeugt wird.

$$(m+m',n)-(m,n)-(m',n) \tag{55}$$
$$(m,n+n')-(m,n)-(m,n') \tag{56}$$
$$(rm,n)-r(m,n) \tag{57}$$
$$(m,rn)-r(m,n) \tag{58}$$

Dabei gilt $m,m' \in M; n,n' \in N, r \in R$ nun ist F/U ein Tensorprodukt und sehen dass folgende Abbildung bilinear ist.

$$\varphi : M \times N \to F/U \tag{59}$$
$$(m,n) \to (m,n)+U \tag{60}$$

Sei nun $\psi : M \times N \to P$ eine weitere R-Bilineare Abbildung wir erhalten zunächst eine wohldefinierte Lineare Abbildung durch

$$\Psi : F \to P \tag{61}$$
$$(m,n) \to \psi(m,n) \tag{62}$$

Aufgrund der Bilinearität liegt U im Kern von Ψ damit gibt es den Morphismus

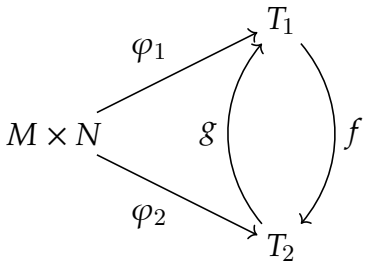
$$\tilde{\psi} : F/U \to P \tag{63}$$
$$(m,n)+U \to \psi(m,n) \tag{64}$$

wo offensichtlich $\psi = \tilde{\psi} \circ \varphi$ gilt. Durch die Bedingung ist $\tilde{\psi}$ auch eindeutig bestimmt mit Elementen F/U und $\varphi(m,n) = (m,n)+U$

Eindeutigkeit: Dazu betrachtet man einfach zwei Tensorprodukte

$$\varphi_1 : M \times N \to T_1 \wedge \varphi_2 : M \times N \to T_2 \tag{65}$$

Nun ist φ_2 bilinear damit $\exists! f : T_1 \to T_2$ mit $\varphi_2 = f \circ \varphi_1$. Umgekehrt gibt es auch $g : T_2 \to T_1$ mit $\varphi_1 = g \circ \varphi_2$



□

Note:-

Die Restklassen $(m,n)+U$ des Tensors bezeichnet man mit $m \otimes n$ und nennt sie **Elementartensor**. Es ist jedoch nicht jedes Element in $M \otimes_R N$ ein Elementartensor man muss auch Summen zulassen

$$M \otimes_R N = \{\sum_{i=1}^{d} m_i \otimes n_i | d \in \mathbb{N}, m_i \in M, n_i \in N\} \tag{66}$$

Wichtig sind hier die Rechenregeln welche aus der Konstruktion hervorgehen:

$$(m+m') \otimes n = m \otimes n + m' \otimes n \tag{67}$$
$$m \otimes (n+n') = m \otimes n + m \otimes n' \tag{68}$$
$$(rm) \otimes n = r(m \otimes n) = m \otimes (rn) \tag{69}$$

Example 0.2.4

Wir betrachten noch einige konkretere Tensorprodukte

- Beispielswiese gilt $R^m \otimes_R R^n \cong Mat_{m,n}(R) \cong R^{mn}$ indem man die Abbildung $R^m \times R^n \longrightarrow Mat_{m,n}(R); (v,t) \longrightarrow vw^t$ betrachtet
- Ähnlich gilt $R[x] \otimes_R R[y] \cong R[x,y]$

0.2.3 Ganze Ringerweiterungen und Hilberts Nullstellensatz

Nun verallgemeinern wir den Begriff einer algebraischen Körpererweiterung auf Ringe. Problem an den Gleichungen in der Körpertheorie ist dass man diese meist normiert indem man durch den Leitkoeffizienten eines Polynoms dividiert. Dies ist in Ringen allgemein nicht möglich deshalb muss man die Normiertheit vorraussetzen. *Anstelle von algebraisch spricht man hier von ganz*

Definition 0.2.6: Ganzheitsgleichung, ganz über

Sei $R \subset S$ eine Ringerweiterung

1. Ein Element $b \in S$ heißt **ganz über R** falls $a_0, ..., a_{n-1} \in R$ exestieren mit $a_0 + a_1 b + ... + a_{n-1} b^{n-1} + b^n = 0$
2. S heißt **ganz über R** falls jedes Element $b \in S$ ganz über R ist.

Theorem 0.2.3 Charakterisierung von ganzen Ringwerweiterungen

Sei $R \subset S$ eine Ringerweiterung und $b_1, ..., b_m \in S$. Dann sind folgende Aussagen äquivalent:

1. $b_1, ..., b_m$ sind ganz über R
2. $R[b_1, .., b_m]$ ist als R Modul endlich erzeugt
3. $R[b_1, ..., b_m]$ ist ganz über R

: $(i) \implies (ii)$ Durch Auflösen einer Ganzheitsgleichung für b_1 nach b_1^n gilt

$$b_1^n = -(a_{n-1} b_1^{n-1} + ... + a_0) \tag{70}$$

für gewisse $a_i \in R$. Man kann die n-te Potenz von b_1 also immer durch niedrigere Potentzen von b_1 und Koeffizienten aus R ersetzen. Man sieht also das $R[b_1, ..., b_m]$ von endlich vielen Produkten $b_1^{e_1} ... b_m^{e_m}$ erzeugt wird.

$(ii) \implies (iii)$ Da endlich viele Elemente $1 = c_1, ..., c_n$ den R Modul $M := R[b_1, ..., b_m]$ erzeugen kann man $c \in M$ wählen und da M ein Ring ist auch $c * c_i \in M$ und es gibt $a_{ij} \in R$ mit

$$c * c_i = \sum_{j=1}^{n} a_{ij} c_j \tag{71}$$

Für die Matrix $A = (a_{ij})_{i,j} \in Mat_n(R)$ gilt dann

$$A(c_1, ...c_n)^T = c(c_1, ...c_n)^T \tag{72}$$

und es liegt $(c_1, ..., c_n)^T$ im Kern von $N := cI_n - A$. Durch die Formel

$$det(N) \cdot (c_1, ..., c_n) = 0 \tag{73}$$

folgt dann $det(N) = 0$ was aus der Leibnitzformel

$$det(N) = c^n + a_{n-1}c^{n-1} + ... + a_m \tag{74}$$

eine Ganzheitsgleichung liefert □

Theorem 0.2.4 Hilberts Nullstellensatz, körpertheoretische Form

Sei $k \subset K$ eine Körpererweiterung und K sei als Ring über k endlich erzeugt. Dann ist die Erweiterung $k \subset K$ endlich und damit algebraisch

: Es gibt $\alpha_1, ..., \alpha_n \in K$ mit $K = k[\alpha_1, ..., \alpha_n]$. Wir beweisen die Aussage per Induktion über n. Im Fall $n = 1$ gilt $K = k[\alpha]$ dies ist ein Körper damit gibt es ein Polynom $p \in k[t]$ mit $\alpha^{-1} = p(\alpha)$ i Daraus folgt $\alpha p(\alpha) - 1 = 0$ was eine algebraische Gleichung ist. Damit ist die Erweiterung algebraisch, endlich. Im Fall $n - 1 \to n$ betrachte $K = k(\alpha_1)[\alpha_2, ..., \alpha_n]$ denn K ist ein Körper nun sind nach Induktionsannahme $\alpha_2, ..., \alpha_n$ algebraisch über $k(\alpha_1)$ man zeigt nun dass α_1 algebraisch über k ist. Dann ist die gesamte Erweiterung algebraisch und damit endlich.

Nun sind $\alpha_2, ..., \alpha_n$ algebraisch über $k(\alpha_1)$ erfüllen also:

$$u_i \alpha_i^d + \sum_{j=0}^{d-1} r_{ij} \alpha_i^j = 0 \tag{75}$$

mit $u_i, r_{ij} \in k[\alpha_1]$ man definiert nun $u := u_2 * * * u_n \in k[\alpha_1]$ nun sind $\alpha_2, ..., \alpha_n$ ganz über den Ring $k[\alpha_1, 1/u]$ und es ist K eine ganze Ringerweiterung von $k[\alpha_1, 1/u]$. Angenommen α_1 ist transzendent sprich $k[\alpha_1] \cong k[t]$ dann könne wir ein irreduzibles Polynom $p \in k[\alpha_1]$ wählen mit $p \nmid u$. Dann gibt es auch für p^{-1} eine Ganzheitsgleichung

$$p^{-m} + b_1 p^{-(m-1)} + ... + b_m = 0 \tag{76}$$

Multiplikation mit p^m in einer genügend hohen Potenz und mit u liefert

$$u^r + a_1 p + ... + a_m p^m = 0 \tag{77}$$

was zeigt $p \nmid u$ ein Widerspruch und es ist nicht transzendent sondern algebraisch.

□

Corollary 0.2.1

Sei R als Ring über k endlich erzeugt und m ein maximales Ideal in R dann ist R/m eine endliche Körpererweiterung

: Es ist R/m als Ring über k immer noch endlich erzeugt und andererseits ein Körper. □

Corollary 0.2.2 Hilberts Nullstellensaz, geometrische Form

Sei k ein algebraisch abgeschlossener Körper und $I \lhd k[x_1, ..., x_n]$ ein echtes Ideal. Dann exestiert ein $a \in k^n$ mit $p(a) = 0$ für alle $p \in I$. *Damit hat das von I definierte polynomiale Gleichungsystem über k eine Lösung*

: Wähle ein maximales Indeal m von $k[x_1, ..., x_n]$ mit $I \subset m$. Nach Korrollar ist $k[x_1, ..., x_n]/m$ eine endliche Körpererweiterung von k. Nun ist k algebraisch abgeschlossen damit gilt $k[x_1, ..., x_n]/m = k$. Setze nun $a_i := \bar{x_i}$ die Restklasse von x_i. Für jedes $p \in k[x_1, .., x_n]$ gilt dann

$$p(a) = p(\bar{x}) = \bar{p} \tag{78}$$

damit gilt für $p \in I$ klarer Weise $p(a) = 0$ □

0.3 Cyclotromic Polynomials

This section should give a small revision of cylcotromic polynomials

0.4 Quaterionen

Definition 0.4.1: Quaterionen

Seien K ein Körper und $a, b \in K \setminus \{0\}$ Der Ring der Quaterionen $Q_K(a, b)$ is der K^4 mit den Basisvektoren

$$1, i, j, k \tag{79}$$

Mit den Multiplikationsregeln

$$ij = k = -ij, i^2 = a * 1, j^2 = b * 1 \tag{80}$$

Diese oben definierte Rechenregel gibt uns eine Ringstruktur auf K^4 dabei ist der erste Basisvektor das neutrale Element es ergeben sich weitere Multiplikationsregel automatisch

$$ik = iij = a1j = aj \tag{81}$$

Oft schreibt man anstatt des Tuples (v, w, x, y) auch die Vektorenschreibweise

$$v + wi + xj + yk \tag{82}$$

Definition 0.4.2: Konjugierte Elemente und Norm

Für eine Element $p = v + swi + xj + yk \in Q_K(a, b)$ der Quaterionen definieren wir das konjugierte Element als

$$\bar{p} := v - wi - xj - yk \in Q_K(a, b) \tag{83}$$

und die Norm

$$N(p) := p\bar{p} = v^2 - aw^2 - bx^2 + aby^2 \in K \tag{84}$$

Lemma 0.4.1

1. Für $p, q \in Q_K(a, b)$ gilt $p\bar{q} = \bar{q}\bar{p}$
2. Für $p, q \in Q_K(a, b)$ gilt $N(pq) = N(p)N(q)$
3. Es gilt $p \in Q_k(a, b)^\times \Leftrightarrow N(p) \neq 0$

: 1. Kann man einfach nachrechnen und sieht dann die Aussage sofort

2. $N(pq) = pq\bar{p}\bar{q} = pq\bar{q}\bar{p} = pN(q)\bar{p} = N(p)N(q)$ dies geht da $N(q) \in K \subset Z(Q_K(a,b))$
3. Aus $pq = 1$ folgt $1 = N(1) = N(pq) = N(p)N(q)$ und daraus $N(p) \neq 0$ gilt umgekehrt das $N(p) \neq 0$ so setzen wir $q = \frac{1}{N(p)}\bar{p}$ dann ist $pq = 1$

□

Theorem 0.4.1

Sei $char(K) \neq 2$
1. $Q_K(a,b)$ ist einfach
2. Für jeden Teilkörper $K \subset \mathbb{R}$ ist $Q_K(-1,-1)$ ein Schiefkörper
3. Für $0 \neq b \in K$ gilt $Q_K(1,b) \cong Mat_2(K)$ insbesondere ist $Q_K(1,b)$ kein Schiefkörper

: Für (i) stellt man fest dass der Quaterionenring eine K-Algebra bildet man zeigt dann $Z(A) = K$ damit ist diese Algebra zentral. Für (ii) betrachtet man ein Element $0 \neq (v,w,x,w) \in K^4$ und stellt fest:

$$v^2 - (-1)w^2 - (-1)x^2 + (-1)(-1)y^2 = v^2 + w^2 + x^2 + y^2 \neq 0 \tag{85}$$

Für (iii) betrachtet man den Isomorphismus:

$$Q_K(1,b) \to Mat_2(K) \tag{86}$$

$$i \to \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{87}$$

$$j \to \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \tag{88}$$

□

0.5 Algebren

In diesem Abschnitt sei nun K ein Körper. Eine K-Algebra ist im Grunde ein Vektorraum in welchen multipliziert werden darf. Alternativ kann man es als Ring mit skalaren Multiplikation definieren

Definition 0.5.1: K-Algebra und K-Unteralgebra

- Eine K-Algebra ist ein Ring A zusammen mit einem Ringhomomorphismus $K \to Z(A)$
- eine K-Unteralgebra der K-Algebra A ist ein Teilring $B \subset A$ der das Bild von K unter dem Homomorphismus erhält.

Example 0.5.1

- Man kann also Elemente von K mit Elementen von A multiplizieren und erhält Elemente von A als Ergebnis. Damit bildet A einen K-Vektorraum. Gleichzeitig kann man aber auch zwei ELemente aus A miteinander Multiplizieren da A ein Ring ist.
- Der Matrixring $Mat_m(K$ wird zu einer K-Algebra indem man Elemente von k als Konstante Diagonalmatrizen der Größe m auffasst.
- Der Polynomring $K[t]$ ist eine Kommutative k-Algebra.
- Der Quaterionenring $Q_K(a,b)$ ist eine K-Algebra.

Im folgenden betrachten wir Unteralgebren von Matrix-Algebren. Für eine K-Unteralgebra $A \subset Mat_m(K)$ nennt man einen Untervektorraum **invariant** falls $Mv \in K$ gilt

Theorem 0.5.1 Satz von Burnside

Sei K ein algebraisch abgeschlossener Körper. Falls die K-Unteralgebra $A \subset Mat_m(K)$ nur die beiden trivialen invarianten Unterräume besitzt gilt $A = Mat_m(K)$

: A operiert transitiv auf K^m: für jedes $0 \neq v \in K^m$ ist

$$\{0\} \subset \{Mv | M \in A\} \tag{89}$$

ein A invarianter Unterraum stimmt also mit K^m überein. Nun zeigt man das A eine Matrix vom Rang 1 enthält. sei $0 \neq P \in A$ falls $rang(P) \geqslant 2$ ist wähle $v_1, v_2 \in K^m$ mit Pv_1, Pv_2 linear unabhängig.

Wähle dann $MPv_1 = v_2$ das geht da A transitiv operiert. Dann ist $PMPv_1$ und Pv_1 linear unabhängig es gilt $PMP - \lambda P \neq 0$ für alle $\lambda in K$. Nun gibt es ein $\lambda_0 \in K$ sodass $PM - \lambda_0 I_d$ auf den Raum $P(K^m)$ nicht invertierbar ist, denn K ist algebraisch abgeschlossen und jede lineare Abbildung hat einen Eigenwert.

$$(PM - \lambda_0 I_d)P \tag{90}$$

hat echt kleineren Rang als P, ist aber nicht Null. Iterativ erhält man also eine Matrix Q vom Rang 1 in A. Dann ist jedoch auch jede beliebige Rang 1 Matrix in A und es gilt $A = Mat_m(K)$

□

Example 0.5.2

Sei $A \subset Mat_m(\mathbb{C})$ sogar eine $*$-Unteralgebra, dh mit M gehört auch M^* zu A. Falls A einen echten invarianten Unterraum $V \subset \mathbb{C}^m$ besitzt, so ist auch $V^\perp$ ein solcher invarianter Unterraum. Man verwendet das A abgeschlossen unter $*$ ist nach einen unitären Basiswechsel haben alle Matrizen in A Blockgestalt damit gilt

$$Mat_{m_1}(\mathbb{C}) \oplus Mat_{m_2}(\mathbb{C}) \tag{91}$$

Definition 0.5.2: Zentral

Eine K-Algebra A heißt zentral, wenn $Z(A) = A$ gilt

So ist beispielsweise für Körper K, $Mat_m(K)$ eine zentrale K-Algebra. Für $char(K) \neq 2$ ist $Q_K(a, b)$ eine zentrale K-Algebra.

0.6 Kodierungstheorie

Ziel der Kodierungstheorie ist es Daten so aufzubereiten dass Fehler welche bei der Übertragung gemacht werden erkannt und bestenfalls verbessert werden können.

Example 0.6.1 (ISBN-10)

Die ISBN-10 Nummer eines Buchs besteht aus einer Zahl mit 10 Ziffern

$$x_1 x_2 ... x_{10} \tag{92}$$

Dabei tragen nur die ersten 9 Ziffern wirkliche Information die x_{10} ist eine Prüfziffer. Sie wird durch die folgende Prüfgleichung erfüllt:

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} = 0 \mod 11 \tag{93}$$

Dies kann man da $10 = -1 \mod 11$ gilt umformen zu

$$x_{10} = x_1 + 2x_2 ... + 9x_9 \mod 11 \tag{94}$$

Man macht hierbei folgende Beobachtungen

- Wird genau eine Ziffer einer gültigen ISBN-10 Nummer abgeändert, ist die Prüfgleichung nicht mehr erfüllt. Solch ein einfacher Fehler wird also immer endteckt.
- Wird genau eine Ziffer abgeändert, und weiß man um welche es sich handelt so kann sie aus der Prüfgleichung rekonstruiert werden

Um mehr Ziffern zu Vefügung zu haben wurde die **ISBN-13** Nummer eingeführt diese besteht aus 13 Ziffern $x_1 ... x_{13}$ wobei nur 12 Ziffern die eigentliche Information tragen und x_{12} über die Prüfgleichung

$$x_1 + 3x_2 + x_3 + ... + x_{12} = 0 \mod 10 \tag{95}$$

bestimmt wird

Definition 0.6.1: Alphabet, Code

1. Ein Alphabet A ist eine endliche Menge
2. Ein Wort über A ist ein Tupel $x = (x_1, ..., x_k) \in A^k$ dabei heißt k die Wortlänge
3. Eine Kodierungsregel ist eine injektive Abbildung $\varphi : A^k \to A^n$ für $k, n \in \mathbb{N}$.
4. Für eine Kodierungsregel $\varphi : A^k \to A^n$ nennt man die Elemente von A^k Informationswörter und $\varphi(x) \in A^n, x \in A^k$ nennt man Codewort. Die Menge $\varphi(A^k)$ aller Codewörter ist der Code

Die Idee ist also. Die Informationswörter tragen die eigentliche Information, die gespeichert und oder übermittelt werden soll, man erhält das Codewort. Aufgrund der **Injektivität** von φ kann die eigentliche Infromation aus einem Codewort zurückermittelt werden.

Example 0.6.2

FÜr den ISBN-10 Code ist $A = \mathbb{F}_{11}$ und

$$\varphi F_{11}^9 \to F_{11}^{10} \tag{96}$$
$$(x_1, ..., x_9) \to (x_1, ..., x_9, x_{10}) \tag{97}$$

Der d-Wiederholungscode hat die Kodierungsregel:

$$\varphi : A^k \to A^{dk}(x_1, ..., x_k) \to (x_1, ..., x_k, x_1, ..., x_k, x_1, ..., x_k) \tag{98}$$

Definition 0.6.2: Hamming-Distanz

Sei A ein Alphabet und $n \in \mathbb{N}$. Die Hamming Distanz zweier Elemente $v = (v_1, ..., v_n), w = (w_1, ..., w_n) \in A^n$ ist definiert durch

$$d(v, w) := \#\{i | 1 \leqslant i \leqslant n, v_i \neq w_i\} \tag{99}$$

Die Hamming-Distanz ist eine Metrik auf A^n

In der Praxis geht man also folgendermaßen vor: Es wird die Information $x \in A^k$ kodiert und das Codewort $\varphi(x) \in A^n$ versendet. Der Empfänger erhält dann ein Wort $r \in A^n$ dass aufgrund von Fehlern in der Übertragung von $\varphi(x)$ verschieden sein kann. Es sucht nun mit der Hamming Distanz das nächstgelegende Codewort $c = \varphi(y) \in \varphi(A^k)$ und schließt mit der Injektivität auf die ursprüngliche Information

Definition 0.6.3: e-fehlerkorrigierend

Sei $e \in \mathbb{N}$ ein Code $C \subset A^n$ heißt **e-fehlerkorrigierend** falls die abegschlossenen Bälle in A^n mit Radius e um Elemente von C paarweise disjunkt sind.

Wird also bei einen Code C der e-fehlerkorrigierend ist nur an e-Stellen ein Fehler gemacht dann liefert die Vorgehensweise die richtige Information zurück.

Definition 0.6.4: Minimaldistanz von C

Für $C \subset A^k$ definieren wir die Minimaldistanz von C als

$$d_{min}(C) := min\{d(v,w)|v,w \in C, v \neq w\} \tag{100}$$

Lemma 0.6.1

Ein Code mit Minimaldistanz d ist genau dann e-fehlerkorrigierend, wenn $e \leqslant [\frac{d-1}{2}]$ gilt

Die Minimaldistanz des d Wiederhilungscodes ist gerade d fpr $d = 2e + 1$ ist dieser Code also e fehlererkennend. Wenn man also bei der Kodierung e fehler gemacht hat so müssen $d - e = 2e + 1 - e = e + 1$ der Wiederholungen übereinstimmen.

Definition 0.6.5: Linearer (n,k)-Code

EIn linearer (n,k) Code über $\mathbb{F}_q$ ist ein k dimensionaler F_q Untervektorraum von $\mathbb{F}_q^n$

0.7 Kryptographie

Man möchte hier eine Nachricht so verschlüsseln das man sie einen Empfänger zukommen lassen kann, ohne das ein eventuell unerwünschter Zuhörer den Inhalt versteht. Man verschlüsselt also die eigentliche Information der Empfänger muss die Nachricht dann wieder entschlüsseln.

Cäsar Verschlüsselung die Idee hierbei ist das sich Senderin Alice (A) und Empfänger Bob (B) eine Ersetzungsregel für Buchstaben ausdenken. Jeder Buchstabe der eigentlichen Nachricht (Klartext) wird in Geheimtext verschlüsselt

$$a \rightarrow d, b \rightarrow jx \rightarrow t... \tag{101}$$

Wird dabei nur eine Verschiebung von Buchstaben verwendet kann man dies durch probieren aller 26 Möglichkeiten sehr einfach lösen. Hat die dritte Person Eve keine Kenntnis über die verwendete Ersetzungsregel so gibt es

$$26! \sim 2^{88} \tag{102}$$

mögliche Kombinationen, was nicht möglich ist. Knacken kann man diesen Code jedoch durch **Häufigkeitsanalyse** so kommen die Buchstaben in verschiedenen Sprachen in unterschiedlicher Häufigkeit vor. In Deutsch sind beispielsweise e, n, i häufig vorkommende Buchstaben. Durch das Zuordnen diesr kann der Code dann geknackt werden.

Um dieses Problem zu umgehen werden meist **Vigenere Verschlüsselungen** verwendet hier bekommt jeder Buchstabe eine eigene Ersetzungsregel. Es vereinbaren Alice und Bob dann ein Schlüsselwort (z.b BACH)

- Erster Buchstabe wird mit zweiter Zeile verschlüsselt
- Zweiter Buchstabe wird mit erster Zeile verschlüsselt
- Dritter Buchstabe wird mit dritter Zeile verschlüsselt

Man wiederholt dieses Verfahren mit dem gesamten Klartext, hier versagt die klassische Häufigkeitsanalyse komplett. Man kann, falls das Schlüsselwort eher kurz ist jedoch eine andere Taktik verwenden. So gibt es in jeder Sprache einige kurze Wörter die relativ häufig vorkommen, im Deutschen beispielsweise "und", "der", "die. Es kommen in diesem Fall mit einger Wahrscheinlichkeit eines dieser Worter in einen Abstand vor der ein vielfaches der Schlüsselwortlänge ist. Dann wendet man auf die kurzen Buchstabenketten im Geheimtext die Häufigkeitsanalyse an.

Ist der Geheimtext und das Schlüsselwort jedoch gleich lang so ist der Code in der Tat unknackbar!

Diffie-Hellmann-Verfahren ist ein Pulic Key Verfahren hier können A und B über einen unsicheren Kanal Informationen austauschen. Es kommt zu einer Erstellung eines Schlüssels den E nicht kennt.

- Alice und Bob vereinbaren öffentlich eine Primzahl p und ein Element $g \in \mathbb{Z}/p\mathbb{Z}$
- Alice wählt eine Zahl $a \in \{1, ..., p-1\}$ die sie geheim hält.
- Bob wählt eine Zahl $b \in \{1, ..., p-1\}$ die er geheim hält.
- Alice sendet Bob $g^a \in \mathbb{Z}/p\mathbb{Z}$
- Bob sendet Alice $g^b \in \mathbb{Z}/p\mathbb{Z}$
- Sowohl Alice als auch Bob können über $(g^a)^b = (g^b)^a = g^{ab}$ den Code entschlüsseln

Möchte Eve nun g^{ab} bestimmen so muss sie den Logarithmus zur Basis g von g^a ausrechnen. Normal ist dies kein Problem und kann durch ein Schachtelungs-Algorithmus erledigt werden. Problematisch ist nur das die Exponentialfunktion in $(\mathbb{Z}/p\mathbb{Z})^\times$ ein Sprungverhalten zeigt und die Berechnung ist für großes p praktisch unmöglich. In der Praxis verwendet man auch gerne den Körper der elliptischen Kurven:

Definition 0.7.1: Elliptische Kurve

Seien $r, s \in K$ dann heißt die Menge

$$C = \{(a, b) \in \bar{K}^2 | b^2 = a^3 + ra + s\} \tag{103}$$

eine elliptische Kurve über K. Falls für einen Punkt $(a, b) \in C$ sogar $a, b \in K$ gilt so heißen (a, b) ein rationaler Punkt der Kurve

0.8 Kategorientheorie

Definition 0.8.1: Kategorie

Eine **Kategorie** C besteht aus eine Klasse

$$Obj(C) \tag{104}$$

von sogenannten Objekten und für alle $X, Y \in Obj(C)$ jeweils aus einer Menge von Morphismen

$$C(X, Y) \tag{105}$$

und partiellen Verknüpfungen von Morphismen

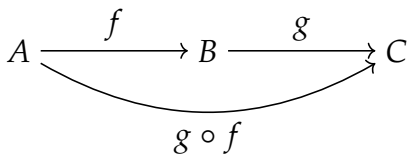
$$C(X, Y) \times C(Y, Z) \to C(X, Z) \tag{106}$$
$$(f, g) \to g \circ f \tag{107}$$

diese erfüllen jeweils zwei Bedingungen:

1. $\forall X \in Obj(C) \exists id_X \in C(X, X)$ mit $id_x \circ f = f, g \circ id_x = g$ für alle $f \in C(Y, X), g \in C(X, Y)$
2. Für alle $f \in C(W, X), g \in C(X, Y), h \in C(Y, Z)$ gilt $h \circ (g \circ f) = (h \circ g) \circ f$

Man nennt $f \in C(X, Y)$ einen Isomorphismus, falls $g \in C(Y, X)$ exestiert mit $g \circ f = Id_x, f \circ g = id_Y$

Ausschnitte aus den Kategorien stellt man gewöhlich durch kommutative Pfeildiagramme dar, unten gezeigt die Komposition von Morphismen.



Example 0.8.1

- Die Kategorie Men hat also Objekte die Mengen und als Morphismen die Abbildungen. Die Verknüpfungen sind hier die Hintereinanderausführungen
- Für jeden festen Körper K gibt es die Kategorie $K-Vec$ der Vektorräume hier sind die Morphismen die K-linearen Abbildungen
- Die Kategorie Top der topologischen Räume hat als Morphismen die stetigen Abbildungen. Hier wird der Isomorphismus gerade Homöomorphismus genannt.

Definition 0.8.2: Kovarianter und Kontravarianter Funktor

Ein **kovarianter bzw. kontravarianter** Funktor von der Kategorie C in die Kategorie D besteht aus einer Abbildung

$$F : Obj(C) \to Obj(D) \tag{108}$$

und jeweils Abbildungen

$$F : C(X,Y) \to D(F(X),F(Y)) \tag{109}$$
$$F : C(X,Y) \to D(F(Y),F(X)) \tag{110}$$

mit

- $F(id_X) = id_{F(x)}$
- $F(g \circ f) = F(g) \circ F(f)$
- $F(g \circ f) = F(f) \circ F(g)$

Example 0.8.2

- Die Bildung des Dualraums ist ein kontravarianter Funktor von $K-Vec$ in sich selbst
- Sei X ein fest gewählter K-Vektorraum. Dann ist die Zuordnung $V \to X \otimes V$ ein kovarianter Funktor von $K-Vec$ in sich selbst. Dabei wird eine lineare Abbildung $\varphi : V \to W$ auf $id_X \otimes \varphi : X \otimes V \to X \otimes W$ abgebildet
- Es gibt kovarianten Funktor $Top \to Men$ der jedem topologischen Raum die Menge seiner Zusammenhangskomponenten abbildet. Stetige Abbildungen erhalten den Zusammenhang
- Es gibt den kovarianten Vergiss Funktor $C \to Men$ der eventuelle Zusatzstruktur auf den Objekten der Kategorie einfach vergisst.

Lemma 0.8.1

Sei $F : C \to D$ ein Funktor und in C gelte $X \cong Y$ Dann gilt in D

$$F(X) \cong F(Y) \tag{111}$$

: Sei o.B.d.A F kovariant. Sei $f \in C(X,Y)$ ein Isomorphismus mit $g in C(Y,X)$ und $g \circ f = id_X$ nach Anwendung des Funktors:

$$id_{F(x)} = F(id_X) = F(g \circ f) = F(g) \circ F(f) \tag{112}$$

Analog bekommt man $F(f) \circ F(g) = id_{F(Y)}$ und die gewünschte Aussage □

0.9 Garbentheorie

Definition 0.9.1: Ring-Prägarbe

Sei X ein topologischer Raum. Eine **Ring-Prägarbe** F auf X besteht aus den Daten:
- Für jede offene Teilmenge $U \subset X$ einen Ring $F(U)$ wobei $F(\emptyset) = \{0\}$
- Für je zwei offene Teilmengen $U \subset V$ einen Ringhomomorphismus $r_{V,U} : F(V) \to F(U)$

Diesen Ringhomomorphismus nennt man **Restriktion von V auf U** dabei gilt für drei offene Mengen $U \subset V \subset W$ stets

$$f_{V,U} \circ r_{W,V} = r_{W,U} \tag{113}$$

und $r_{U,U} = id_{F(U)}$

Example 0.9.1

Seien X, W zwei topologische Räume. Für $U \subset X$ offen sei $C(U, W)$ die Menge aller stetigen Funktionen von U nach W. Wiederum mit den Restriktionen von Funktionen auf kleinere Definitionsbereiche erhalten wir eine Prägarbe C auf X.

Um nun die *Lokalität* der Bedingung an den Funktionen axiomatisch zu erfassen definiert man den Begriff einer Garbe.

Definition 0.9.2: Garbe

Sei X ein topologischer Raum. Eine **Garbe** auf X ist eine Prägarbe F die zusätzlich folgende Bedingung erfüllt:
FÜr jedes offene $U \subset X$, jede offene Überdeckung $U = \bigcup_{i \in I} U_i$ und jede Auswahl von Elementen $s_i \in F(U_i)$ mit

$$r_{U_i, U_i \cap U_j}(s_i) = r_{U_j, U_i \cap U_j}(s_j) \tag{114}$$

für alle $i, j \in I$ gibt es genau ein $s \in F(U)$ mit $r_{U,U_i}(s) = s_i, \forall I$

Denkt man sich die $F(U)$ jeweils als Menge von auf U definierten Funktionen, so sagt die Garbeneigenschaft, dass die Bedingung an die betrachteten Funktionen **lokal** ist. Für vorgegebene Funktionen s_i auf U_i welche auf paarweisen Schnitten übereinstimmen gibt es genau eine global auf U definierte Funktion s die alle s_i fortsetzt. Dieses s muss nun automatisch auf die Bedingung in F erfüllen.

Ein konkretes Beispiel ist die Garbe C mit stetigen Funktionen zwischen topologischen Räumen. Auf die Einschränkung $F_{|U}$ einer Garbe auf eine offene Teilmenge $U \subset X$ ist offensichtlich wieder eine Garbe.

Definition 0.9.3: Morphismus von Garben

Seien $(X, F), (Y, G)$ topologische Räume mit Garben. Ein Morphismus von Garben besteht aus den Daten
- Stetige Abbildung $f : X \to Y$
- Für jede offene Menge $U \subset Y$ einen Ringhomomorphismus $f^*_U : G(U) \to F(f^{-1}(U))$

Man nennt hier die Abbildung f^*_U auch die Zurückziehung von Elementen aus $G(U)$ nach $F(f^{-1}(U)$. Sind X, Y topologische Räume mit der Garbe der Stetigen Funktionen mit Werten in W dann erhält man fpr jede stetige Funktion $f : X \to Y$ einen Morphismus indem man f^* als Zurückziehung mittels f definiert

Definition 0.9.4: Halm

Um das lokale Verhalten einer Garbe an einem Punkt zu erfassen, definiert man den Begriff eines Halms. Sei (X, F) eine (Prä)-Garbe und $x \in X$. Auf der Menge

$$M := \{(U, s) | x \in U, U \subset X \ offen, s \in F(U)\} \tag{115}$$

definiert man eine Äquivalenzrelation

$$(U, s) \sim (V, t) :\Leftrightarrow \exists W \subset U \cap V \ offen, x \in W, r_{U,W}(s) = r_{V,W}(t) \tag{116}$$

Konkret für Garben von Funktionen sagt dies das zwei auf Umgebungen von x definierte Funktionen äquivalent sind wenn sie auf einer kleinen offenen Umgebung von x übereinstimmen. Die Menge

$$F_x := M/\sim = \{[(U, s)] | (U, s) \in M\} \tag{117}$$

der Äquivalenzklassen trägt eine kanonische Ringstruktur

$$[(U, s)] + [(V, t)] := [(U \cap V, r_{U,U\cap V}(s) + r_{V,U\cap V}(t))] \tag{118}$$

Dies nennt man dann Halm der Garbe F am Punkt x

Für jedes $U \subset X$ mit $x \in U$ gibt es den kanonischen Homomorphismus

$$F(U) \to F_x \tag{119}$$
$$s \to [(U, s)] \tag{120}$$

Weiteres ist $\varphi = (f, f^*) : (X, F) \to (Y, G)$ ein Garbenmorphismus, so induziert er für jedes $x \in X$ einen kanonischen Morphismus der Halme

$$\varphi_x : G_{f(x)} \to F_x \tag{121}$$
$$[(U, s)] \to [(f^{-1}(U), f^*(s)] \tag{122}$$

Theorem 0.9.1 Isomorphismus der Halme

Sei $\varphi(f, f^*) : (X, F) \to (Y, G)$ ein Morphismus von Garben, wobei f ein Homöomorphismus der topologischen Räume sei. Dann ist φ genau dann ein Isomorphismus, wenn für alle $x \in X$ die induzierten Morphismen φ_x der Halme Isomorphismen sind.