Vorlesung Algebra I

Kapitel I - Ringkonstruktionen

In diesem Kapitel betrachten wir kommutative Ringe und Ringhomomorphismen, und zeigen wie man aus gegebenen Ringen neue Ringe konstruieren kann.

Jedes Ideal I in einem Ring R definiert zum Beispiel einen Restklassenring R/I. Der zugehörige Restklassenring ist nullteilerfrei bzw ein Körper genau dann, wenn das Ideal I ein Primideal respektive ein maximales Ideal des Ringes ist. Zur Konstruktion von Körpern ist daher die Bestimmung aller maximalen Ideale eines Rings von Bedeutung. In Hauptidealringen führt man dies zurück auf die Bestimmung aller Primelemente.

Eine weitere fundamentale Konstruktion neuer Ringe: Lokalisierung eines gegebenen kommutativen Ringes R. Die Lokalisierung R_S wird definiert durch Nenneraufnahme aus einer multiplikativ abgeschlossen Teilmenge S des Rings R. Schliesslich kann man durch das Tensorprodukt neue Ringe definieren. Wichtige Ringhomomorphismen, die wir in diesem Kapitel betrachten werden, sind die Quotientenabbildung, die Lokalisierungsabbildung, der Einsetzungshomomorphismus und der Frobeniushomomorphismus.

1 Kommutative Ringe

Für Ringe $(R, +, \cdot, 0, 1)$ fordern wir die Axiome eines kommutativen Körpers mit Ausnahme

1. des Axioms der Existenz des Inversen bezüglich der Multiplikation
2. des Axioms $0 \neq 1$.

Das heißt, alle Ringe seien im folgenden stillschweigend kommutative Ringe mit Einselement. Für die genauen Axiome siehe LA II, §56.

Beispiel: $\mathbb{Z}$ oder $K[x]$ (Polynomring über dem Körper K).

Definition 1.1. *Eine Teilmenge $I \neq \emptyset$ eines kommutativen Ringes R nennt man ein Ideal, falls gilt:*

1. $x, y \in I \Rightarrow x + y \in I$
2. $r \in R,\ x \in I \Rightarrow r \cdot x \in I.$

Es gilt dann automatisch auch $x - y \in I$.

Der Nullring besitzt nur ein Ideal, das Nullideal. Ist R nicht der Nullring, dann gibt es mindestens zwei verschiedene Ideale, nämlich das Nullideal $\{0\}$ und das Einsideal $I = R$.

Satz 1.2. *Ein kommutativer Ring R ist genau dann ein Körper, wenn R genau zwei verschiedene Ideale besitzt (nämlich $\{0\}$ und R).*

Beweis: Sei R ein Körper und $\{0\} \neq I \subset R$ ein Ideal. Wähle $x \neq 0$ in I. In dem Körper R existiert x^{-1}. Also

$$\underbrace{x^{-1}}_{\in R} \cdot \underbrace{x}_{\in I} = 1 \quad \in I \quad \text{(Wegen } x^{-1} \in R \text{ und } x \in I \text{ nach 2)}\ .$$

Aus $1 \in I$ folgt $I = R$, denn jedes $y \in R$ liegt in I wegen $y = y \cdot 1 \in R \cdot I \subset I$.

Sei umgekehrt R ein Ring mit den einzigen Idealen $\{0\}$ und R. Für $x \neq 0$ aus R ist $1 \cdot x = x \neq 0$, also das Ideal

$$(x) \;=\; \{r \cdot x \;,\; r \in R\} \;\neq\; \{0\} \;.$$

Somit gilt nach Annahme $(x) = R$. Wegen $1 \in R$ gibt es also ein $r \in R$ mit $r \cdot x = 1$. Daher ist x invertierbar in R. Da dann jedes Element $x \in R$ invertierbar ist und $0 \neq 1$ gilt, ist K ein Körper.

Definition 1.3. *Ein Ring R heißt nullteilerfrei, falls gilt*

1. $0 \;\neq\; 1$, *das heißt* $R \;\neq \{0\}$
2. *Aus* $r_1 \cdot r_2 \;=\; 0$ *folgt* $r_1 \;=\; 0$ *oder* $r_2 = 0$.

Beispiel: Die Ringe $\mathbb{Z}$ oder $K[x]$ (der Polynomring über dem Körper K) sind nullteilerfrei. Jeder Teilring eines Körpers ist nullteilerfrei.

2 Ringhomomorphismen

Seien R, S kommutative Ringe mit Einselement.

Definition 2.1. *Eine Abbildung $\varphi : R \to S$ heißt Ringhomomorphismus, falls für alle $r_1, r_2 \in R$ gilt:*

1. $\varphi(r_1 + r_2) \;=\; \varphi(r_1) \;+\; \varphi(r_2)$
2. $\varphi(r_1 \cdot r_2) \;=\; \varphi(r_1) \cdot \varphi(r_2)$
2*. $\varphi(1) \;=\; 1$ *(Dies gilt automatisch, wenn φ surjektiv ist).*

Wir nennen dann $\varphi : R \to S$ eine Ringerweiterung.

Bemerkung: Das Bild $\varphi(R)$ eines Ringhomomorphismus ist ein Unterring von S.

Satz 2.2. *Die Teilmenge $Kern(\varphi) \subset R$ eines Ringhomomorphismus $\varphi : R \to S$ ist ein Ideal von R.*

Beweis: (1) Aus $\varphi(x) = 0$, $\varphi(y) = 0$ folgt $\varphi(x + y) = \varphi(x) + \varphi(y) = 0$.

(2) Aus $\varphi(x) = 0$ folgt $\varphi(r \cdot x) = r \cdot \varphi(x) = r \cdot 0 = 0$. Es folgt $x, y \in I \;\Rightarrow$ $x + y \in I$ und $x \in I, r \in R \;\Rightarrow\; r \cdot x \in I$.

Aus Satz 1.2 folgt daher

Korollar 2.3. *Ein Homomorphismus $\varphi : R \to S$ von einem Körper R in einen Ring S ist entweder die Nullabbildung oder injektiv.*

3 Restklassenringe

Sei I ein Ideal des Ringes R. Dann definiert

$$r_1 \sim_I r_2 \Leftrightarrow r_1 - r_2 \in I$$

eine Äquivalenzrelation auf R. Auf den Äquivalenzklassen

$$[r] = \{r + x \mid x \in I\}$$

definiert man eine Addition und eine Multiplikation

$$[r_1] + [r_2] = [r_1 + r_2]$$

und eine Multiplikation

$$[r_1] \cdot [r_2] = [r_1 \cdot r_2] .$$

Diese Bildungen sind wohldefiniert.

Beweis: $r_1 + I = r_1' + I$, $r_2 + I = r_2' + I$ bedeutet $r_1 = r_1' + i_1$, $r_2 = r_2' + i_2$ mit $i_1, i_2 \in I$.
Somit gilt

$$(r_1 + r_2) - (r_1' + r_2') = i_1 + i_2 \in I$$

bzw.

$$r_1 r_2 - r_1' r_2' = r_1(r_2 - r_2') + r_2(r_1 - r_1') = r_1 i_2 + r_2' i_1 \in I .$$

Die Menge R/I der Äquivalenzklassen $[r]$ mit $r \in R$ bilden mit dieser Addition respektive Multiplikation einen Ring. Die Gültigkeit der Ringaxiome vererbt sich nämlich von R auf R/I.

Satz 3.1. *(Restklassenringe) Die natürliche Abbildung*

$$\pi : R \longrightarrow R/I$$

$$r \longmapsto [r] = r + I$$

ist ein surjektiver Ringhomomorphismus mit $Kern(\varphi) = I$.

Beweis: Trivial.

Satz 3.2. *(Idealkorrespondenz) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann gilt*

1. *$\varphi^{-1}(I)$ ist ein Ideal von R, falls I ein Ideal von S ist.*
2. *Ist φ surjektiv, dann ist $\varphi(I)$ ein Ideal von S, falls I ein Ideal von R ist. In diesem Fall gibt es eine bijektive Korrespondenz zwischen den Idealen in S und den Idealen in R, welche $Kern(\varphi)$ enthalten.*

Beweis:

$$\varphi(r_1), \varphi(r_2) \in I \;\Rightarrow\; \varphi(r_1 + r_2)$$

beziehungsweise

$$\varphi(r \cdot r_1) \;=\; \varphi(r) \cdot \varphi(r_1) \;\in\; I \;.$$

Daraus folgt (1).

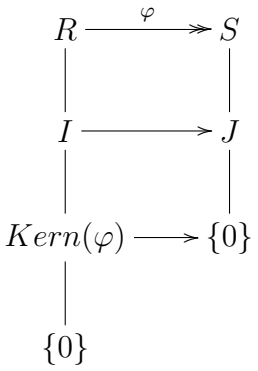
(2) Ist φ surjektiv, dann gilt

$$S \;\cdot\; \varphi(I) \;=\; \varphi(R) \cdot \varphi(I) \;\subseteq\; \varphi(R \cdot I) \;=\; \varphi(I)$$

$$\varphi(I) \;+ \varphi(I) \;\subseteq\; \varphi(I + I) \;\subseteq\; \varphi(I) \;.$$

Da $\varphi^{-1}(\varphi(I)) = I$ für jedes Ideal gilt, welches den Kern von φ enthält, liefert dies gewünschte Korrespondenz von Idealen.

Dagegen ist $\varphi(\varphi^{-1}(I)) = I$ trivialerweise erfüllt für eine beliebige Teilmenge $I \subseteq S$.



4 Primideale

Definition 4.1. *Ein Primideal I in einem kommutativen Ring ist ein vom Einsideal verschiedenes Ideal*

$$I \neq R \ ,$$

mit folgender Eigenschaft:

$$\boxed{\forall\ x, y \in R \quad (x \cdot y \in I \ \Rightarrow\ x \in I \text{ oder } y \in I)} \ .$$

Satz 4.2. *Sei $\varphi : R \twoheadrightarrow S$ ein surjektiver Ringhomomorphismus. Dann sind äquivalent*

1. *S ist nullteilerfrei*
2. *$I = Kern(\varphi)$ ist ein Primideal.*

Korollar 4.3. *R/I nullteilerfrei $\Leftrightarrow$ I Primideal.*

Beweis des Satzes

(1) $\Rightarrow$ (2): Für $x, y \in R$ mit $x \cdot y \in I$ gilt $\varphi(xy) = 0$. Wegen $\varphi(x) \cdot \varphi(y) = \varphi(xy) = 0$ und der Nullteilerfreiheit von S folgt daraus $\varphi(x) = 0$ oder $\varphi(y) = 0$. Also $x \in I$ oder $y \in I$. Aus $0 \neq 1$ in S folgt $I = Kern(\varphi) \neq R$.

(2) $\Rightarrow$ (1): Sei $I = Kern(\varphi)$ ein Primideal. Seien $\eta, \xi \in S$ gegeben mit $\eta \cdot \xi = 0$. Da φ surjektiv ist, existieren $y, x \in R$ mit $\eta = \varphi(y),\ \xi = \varphi(x)$. Also gilt

$$0 \ = \ \eta \cdot \xi \ = \ \varphi(y) \cdot \varphi(x) \ = \ \varphi(y \cdot x)$$

und somit $y \cdot x \in I = Kern(\varphi)$. Da I ein Primideal ist, folgt $y \in Kern(\varphi)$ oder $x \in Kern(\varphi)$. Also $\eta = 0$ oder $\xi = 0$.

Es bleibt $1 \neq 0$ in S zu zeigen. Wäre $1 = \varphi(1) = 0$, so wäre $1 \in I = Kern(\varphi)$. Daraus folgt $R \cdot 1 = R \subset Kern(\varphi) = I$. Nach Annahme gilt aber $I \neq R$. Das zeigt wie gewünscht $1 \neq 0$ in S.

Diagramm:

$$\begin{array}{ccc} R & \xrightarrow{\ \varphi\ } & S \\ I \ \neq \ R & \longleftrightarrow & 0 \ \neq 1 \end{array}$$

$$x \cdot y \in I \Rightarrow x \in I \text{ oder } y \in I \qquad \xi \cdot \eta = 0 \Rightarrow \xi = 0 \text{ oder } \eta = 0$$

5 Maximale Ideale

Definition: Ein Ideal I eines kommutativen Ringes R heißt maximal, falls gilt:

1. $I \neq R$
2. Jedes Ideal J mit $I \subsetneqq J \subsetneqq R$ erfüllt entweder $J = I$ oder $J = R$.

Satz 5.1. *Sei $\varphi : R \to S$ ein surjektiver Ringhomomorphismus. Dann sind äquivalent:*

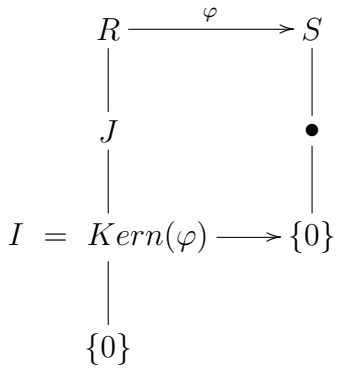
1. *$Kern(\varphi)$ ist ein maximales Ideal.*
2. *S ist ein Körper.*

Korollar 5.2. *R/I ist ein Körper, genau dann wenn I ein maximales Ideal ist.*

Korollar 5.3. *Jedes maximale Ideal ist ein Primideal.*

Beweis: (des Satzes) (1) $\Rightarrow$ (2): Gilt (1), dann besitzt S nach Satz 3.2(2) nur zwei Ideale, nämlich 0 und S. Somit ist S ein Körper (Satz 1.2).

Diagramm:



(2) $\Rightarrow$ (1): Ist S ein Körper und $I = Kern(\varphi)$, dann ist I maximal. Denn ein Ideal J mit $I \subseteq J \subseteq R$ entspricht einem Ideal $\varphi(J)$ in S nach Satz 3.2(2). Da ein Körper S nach Satz 1.2 nur die Ideale 0 und S besitzt, folgt daher $J = I$ oder $J = R$ aus Satz 3.2(1). Aus $S \neq \{0\}$ folgt $R \neq I$. (Beachte $1 \neq 0$ in S).

6 Anwendung auf Hauptidealringe

In diesem Abschnitt sei R ein Hauptidealring, d.h.

1. R sei nullteilerfrei und kommutativ.
2. Jedes Ideal $I \subset R$ ist von der Gestalt $I = (a)$ für ein Element $a \in R$.

$$(a) \;=\; \{a \cdot r \;\mid\; r \in R\}\ .$$

Die wichtigsten Beispiele sind euklidische Ringe wie etwa $\mathbb{Z}$ oder der Polynomring $K[x]$ über einem Körper (siehe LA II-Skript).

Zur Erinnerung (siehe LA II-Skript)
In einem Hauptidealring gilt

1. Kürzungslemma: $a_1 \cdot r \;=\; a_2 \cdot r \Rightarrow a_1 \;=\; a_2$ oder $r \;=\; 0$.
2. $(a_1) \;=\; (a_2)$ genau dann wenn gilt $\exists\, r \in R^*, a_1 \;=\; r \cdot a_2$.

R^* bezeichnet die Gruppe der invertierbaren Elemente in R, die sogenannte Gruppe der Einheiten.

Beispiel: Aus der Nullteilerfreiheit folgt, daß das Nullideal $I = \{0\}$ eines Hauptidealrings ein Primideal ist.

Für die verbleibenden Primideale gilt

Satz 6.1. *Für ein Ideal $I = (p)$, $I \neq \{0\}$ eines Hauptidealringes R sind äquivalent*

1. *I ist maximales Ideal.*
2. *I ist Primideal und $I \;\neq \{0\}$.*
3. *p ist ein Primelement von R, d.h. $p \notin R^*$, $p \neq 0$ sowie*

$$p \;\mid\; a \cdot b \quad\Longrightarrow\quad p \mid a \text{ oder } p \mid b.$$

Bemerkung: Wir sagen n teilt m und schreiben

$$n \mid m \ ,$$

falls ein $r \in R$ existiert mit der Eigenschaft $m = n \cdot r$.

Beweis:
(1) $\Rightarrow$ (2): folgt aus Korollar 5.3. (2) $\Leftrightarrow$ (3) ist klar. (3) $\Rightarrow$ (1): Sei p Primelement ($p \notin R^*, p \neq 0$) und $I = (a)$ ein maximales Ideal mit

$$(p) \ \subset \ I \ \subsetneq \ R \ , \quad I \ = \ (a) \ .$$

Dann gilt $p = r \cdot a$ und $a \notin R^*$.

Da p prim ist folgt entweder $p \mid a$ (und damit $(p) = I$, also (1)) oder es folgt $p \mid r$. Dann ist $r = b \cdot p$ und somit

$$p \ = \ r \ \cdot \ a \ = \ b \ \cdot a \ \cdot \ p$$

aus dem Kürzungslemma folgt

$$1 \ = \ b \cdot a$$

im Widerspruch zur $a \notin R^*$. Somit folgt $(p) = I$ und (p) ist maximal.

Beachte: (I Primideal) $\Leftrightarrow$ ($a \cdot b \in I$ impliziert $a \in I$ oder $b \in I$ und $I \neq R$) $\Leftrightarrow$ ($p \mid ab$ impliziert $p \mid a$ oder $p \mid b$ und $p \notin R^*$.)

Hierbei benutzen wir, daß $x \in I$ gleichbedeutend ist mit $x = r \cdot p$ (für ein $r \in R$) beziehungsweise gleichbedeutend mit $p \mid x$.

Definition: Ein Polynom $f(x)$ heißt normiert, wenn sein höchster Koeffizient 1 ist

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \quad , \quad a_i \ \in \ K.$$

Ein Polynom $f(x)$ in $K[x]$ vom Grad ≥ 1 heißt irreduzibel über dem Körper K, wenn aus $a(x) \cdot b(x) = f(x)$ (in $K[x]$) folgt $a(x) \in K$ oder $b(x) \in K$.

Beispiel: Die Primideale in $\mathbb{Z}$ entsprechen genau den Primzahlen $2, 3, 5, \cdots$ und die Primideale im Polynomring $K[x]$ über einem Körper K entsprechen genau den normierten irreduziblen Polynomen $f(x) \neq 0$.

Als Anwendung von Satz 6.1 und Korollar 5.1 erhalten wir die nächsten beiden Korollare

Korollar 6.2. *Ist p eine Primzahl, dann ist der Quotientenring*

$$\mathbb{F}_p = \mathbb{Z}/(p)$$

ein Körper (mit p Elementen).

Korollar 6.3. *Ist $f(x) \neq 0$ ein irreduzibles normiertes Polynom vom Grad $grad(f) \geqq 1$, dann ist der Quotientenring*

$$S = K[x]/(f(x))$$

ein Körper. Man hat einen natürlichen Ringhomomorphismus $\varphi : K \hookrightarrow S$

$$\begin{array}{ccc} K & \xrightarrow{\iota} & K[x] \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \pi} \\ & & S = K[x]/(f(x)) \end{array} ,$$

welcher nach Korollar 2.3 injektiv ist (beachte $1 \mapsto 1$ und somit ist die Abbildung nicht null).

S ist also ein Erweiterungskörper von K bezüglich der Einbettung φ von K in S. Wir nennen S/K eine primitive Körpererweiterung.

7 Bruchrechnen (Lokalisierung)

Sei S eine multiplikativ abgeschlossene Teilmenge eines kommutativen Rings R, d.h. es gelte

1. $s_1, s_2 \in S \implies s_1 \cdot s_2 \in S$
2. $1 \in S$.

Wir nennen dann zwei Ringelemente S-äquivalent, falls gilt

$$r_1 \sim_S r_2 \iff \exists s \in S \text{ mit } (r_1 - r_2) \cdot s = 0.$$

Bemerkung: $0 \in S \Leftrightarrow r \sim_S 0$ für alle $r \in R$.

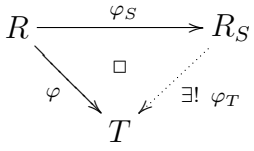
Bemerkung: Ist R nullteilerfrei und $0 \notin S$, dann gilt natürlich $r_1 \sim_S r_2 \Leftrightarrow r_1 = r_2$. Eine Richtung benutzt (2).

Satz: *Zu einer multiplikativ abgeschlossenen Teilmenge $S \subsetneqq R$ gibt es ein Paar (φ_S, R_S) bestehend aus einem Ring R_S und einem Ringhomomorphismus φ_S*

$$R \xrightarrow{\varphi_S} R_S$$

derart, daß gilt

1. *Alle Elemente $\varphi_S(s)$, $s \in S$ sind multiplikativ invertierbar in R_S.*
2. *Für jeden Ringhomomorphismus $\varphi : R \to T$, für den alle Elemente in $\varphi(S)$ multiplikativ invertierbar in T sind, gibt es genau einen Ringhomomorphimus φ_T, welcher das Diagramm*



kommutativ macht.

Bemerkung: Diese Eigenschaft charakterisiert R_S bis auf Ringisomorphie. Die sog. Lokalisierungsabbildung φ_S ist im allgemeinen aber nicht injektiv.

Beweis: Zum Beweis des Satzes konstruieren wir R_S als Menge der formalen Brüche

$$r/s \ , \ r \in R, s \in S$$

mit den Rechenregeln

$$r_1/s_1 + r_2/s_2 \ := \ (r_1 s_2 + r_2 s_1)/s_1 s_2$$

(*)

$$r_1/s_1 \cdot r_2/s_2 \ := \ r_1 r_2/s_1 s_2$$

und der Abbildung $\varphi_S(r) = r/1$.

Will man jetzt etwa das Distributivgesetz zeigen

$$(r_1/s_1 + r_2/s_2) \cdot r_3/s_3 \ = \ r_1/s_1 \cdot r_3/s_3 + r_2/s_2 \cdot r_3/s_3,$$

stößt man auf folgendes Problem: Links steht

$$(r_1 s_2 + r_2 s_1) r_3/s_1 s_2 s_3 \ ,$$

und rechts steht

$$(r_1 r_3 s_2 s_3 + r_2 r_3 s_1 s_3)/s_1 s_2 s_3^3 \ .$$

Um beide Seiten identifizieren zu können, sollte man daher rechts durch s_3 kürzen können oder alternativ links mit s_3 erweitern können. Dazu führt man per Definition eine Kürzungsregel ein, welche besagt

$$(**) \quad \boxed{r_1/s_1 \ \sim_S \ r_2/s_2 \iff \exists s \in S \quad (r_1 s_2 - r_2 s_1) \cdot s = 0} \ .$$

Wir überlassen es dem Leser als Übungsaufgabe zu überprüfen, daß $\sim_S$ eine Äquivalenzrelation definiert auf der Menge der formalen Brüche, und daß (*) auf den Äquivalenzklassen eine wohldefinierte Addition und Multiplikation induziert.

Bemerkung: Betrachte die Erweiterungsrelation $a/b \dashrightarrow as/bs$ (für beliebige $s \in S$). Die uns wohlvertraute Relation $\dashrightarrow$ ist leider keine Äquivalenzrelation. Sie ist zwar transitiv und reflexiv, aber sie ist nicht symmetrisch. Andererseits gilt auch $a/b \sim_S as/bs$, wie man sofort nachprüft. In der Situation von (**) gilt weiterhin

$$r_1/s_1 \ \dashrightarrow \ r_1 s_2 s/s_1 s_2 s \ = \ r_2 s_1 s/s_1 s_2 s \ \dashleftarrow \ r_2/s_2.$$

Dies zeigt daher leicht, daß die obige Äquivalenzrelation $\sim_S$ die von der vertrauten Erweiterungs-Relation $\dashrightarrow$ erzeugte Äquivalenzrelation ist.

Definition: R_S ist die Menge der Äquivalenzklassen formaler Brüche $r/s, r \in R, s \in S$ bezüglich der Äquivalenzrelation $\sim_S$.

Die universelle Eigenschaft: Gegeben sei $\varphi : R \to T$ mit $\varphi(S) \subset T^*$. Die invertierbaren Elemente T^* von T (die Einheiten von T) bilden ein Gruppe. Die inversen Elemente $t_s \in T$ mit

$$t_s \cdot \varphi(s) \;=\; 1 \;\text{ oder kurz }\; t_s \;=\; \varphi(s)^{-1}$$

sind eindeutig bestimmt in T. Die dann eindeutig bestimmte Abbildung $\varphi_T : R_S \to T$ ist definiert durch

$$\varphi_T(r/s) \;=\; \varphi(t) \;\cdot\; t_s \;=\; \varphi(s) \;\cdot\; \varphi(s)^{-1} \;.$$

Die Details werden dem Leser als Übungsaufgabe überlassen. Dies beendet den Beweis des Satzes.

Bemerkung: $R_S = \{0\}$ *genau dann, wenn* $0 \in S$.

Spezialfall: *Sei R nullteilerfrei. Dann ist $S = R \setminus \{0\}$ multiplikativ abgeschlossen in R. Der Ring R_S ist in diesem Fall ein Körper, der sogenannte Quotientenkörper $Q(R)$, und die natürliche Abbildung $\varphi_S : R \hookrightarrow Q(R)$ ist injektiv.*

Beweis: $r_1/s_1 \sim_S 0 \Leftrightarrow \exists s \in S : r_1 \cdot s = 0 \Leftrightarrow r_1 = 0$ (Nullteilerfreiheit). Somit ist für $r_1/s_1 \not\sim_S 0$ das Inverse s_1/r_1 definiert, $r_1 \in S = R \setminus \{0\}$. Weiterhin folgt aus $\varphi_S(r) = r/1 \equiv 0$ wie eben gezeigt $r = 0$. Somit ist φ_S ein injetiver Ringhomomorphismus. □

Korollar: *Ein nullteilerfreier Ring ist ein Unterring seines Quotientenkörpers.*

Beispiel:

1. $Q(\mathbb{Z}) = \mathbb{Q}$.
2. $Q(K[t]) = K(t)$, der Körper der gebrochen rationalen Funktionen mit Koeffizienten in K.

8 Die Charakteristik

Sei R ein Ring und 1_R das Einselement von R. Wir definieren eine Abbildung $\varphi : \mathbb{Z} \to R$ durch

$$\varphi(n) \;=\; \begin{cases} 1 + \cdots + 1, & \text{n} > 0; \\ 0, & \text{n} = 0; \\ -\varphi(|n|), & \text{n} < 0. \end{cases}$$

Aus den Ringaxiomen folgt, daß φ ein Ringhomomorphismus ist. Der Kern ist ein (Haupt-) Ideal I in $\mathbb{Z}$ und es gilt

$$\varphi(\mathbb{Z}) \;\cong\; \mathbb{Z}/I$$

als Unterring von R.

Lemma 8.1. *Ist R nullteilerfrei, dann ist I ein Primideal oder $I = \{0\}$.*

Beweis: $S = \mathbb{Z}/I$ ist als Teilring des nullteilerfreien Rings R wieder nullteilerfrei, da $\mathbb{Z}/I$ das Einselement 1_R enthält. Nach Satz 4.2 ist I daher ein Primideal. □

Definition: Das Bild $\varphi(\mathbb{Z})$ in einem nullteilerfreien Ring ist entweder $\mathbb{Z}$ oder der endliche Körper $\mathbb{F}_p = \mathbb{Z}/(p)$. Man macht nun folgende Definition: Die Charakteristik eines nullteilerfreien Ring ist 0 im ersten Fall und p im zweiten Fall.

9 Der Frobeniushomomorphismus

In jedem Ring gilt der

Binomialsatz 9.1. *Für alle $r, s \in R$ gilt*

$$(r+s)^n \;=\; \sum_{i=0}^{n} \varphi(\binom{n}{i}) \cdot r^i \cdot s^{n-i} \;.$$

Hierbei ist $\binom{n}{i} \in \mathbb{Z}$ ist der Binomialkoeffizient und $r^n = r \cdots r$ (n mal).

Beweis: Die Aussage folgt aus dem Distributivgesetz durch vollständige Induktion nach n. □

Annahme: Sei nun R ein kommutativer Ring mit der Eigenschaft

$$p \cdot r \;=\; 0 \quad , \quad \forall r \in R \;.$$

Hierbei sei p eine Primzahl.

Beispiel: R sei nullteilerfrei von der Charakteristik p.

Wir betrachten dann den Spezialfall $n = p$ des Binomialsatzes. Wegen

$$\binom{p}{i} \;=\; \frac{p!}{i!(p-i)!} \quad \in \mathbb{Q}$$

gilt dann für alle $0 < i < p$ in $\mathbb{Z}$ die Teilerbeziehung $p \mid \binom{p}{i}$, denn $p \mid p!$, aber $p \nmid (p-i)!$ und $p \nmid i!$. Dies benutzt natürlich implizit die Existenz und Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}$ (siehe LA II Skript).

Aus der obigen Annahme an R folgt daher aus dem Binomialsatz

Folgerung 9.2. *Im Ring R gilt $\varphi(\binom{p}{i}) = 0$ für alle $0 < i < p$ und somit*

$$\boxed{(r+s)^p = r^p + s^p}$$

für alle $r, s \in R$.

Folgerung 9.3. *Ist p eine Primzahl und gilt $p = 0$ in einem kommutativen Ring R, dann definiert die Abbildung $F : R \to R$*

$$F(r) \;=\; r^p$$

einen Ringhomomorphismus, den sogenannten Frobeniushomomorphismus.

Satz 9.4 (Kleiner Satz von Fermat)**.** *Der Frobeniushomomorphismus des Ringes $\mathbb{F}_p$ ist die Identität, d.h.*

$$r^p \;=\; r \quad (\forall\, r \in \mathbb{F}_p)\ .$$

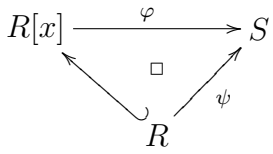
Beweis: Es gilt $F(i) = F(1 + \cdots + 1) = F(1) + \cdots + F(1) = i \cdot F(1) = i$ wegen $F(1) = 1$. □

Die Aussage von Satz 9.4 kann man auch so lesen:

> '*Für alle $r \in \mathbb{Z}$ haben die Zahl r und die Zahl r^p denselben Rest bei der Division durch p.*'

10 Einsetzungshomomorphismen

Sei R ein Ring, $R[x]$ der Polynomring über R und $R \xrightarrow{\psi} S$ ein Ringhomomorphismus. Ein Ringhomomorphismus φ, der das Diagramm



kommutativ macht, ist dann durch seinen Wert

$$x_0 = \varphi(x) \in S$$

eindeutig bestimmt. Umgekehrt gibt es für jedes x_0 genau einen Ringhomomorphismus φ wie oben mit $\varphi(x) = x_0$, nämlich

$$\varphi(\sum_i r_i x^i) \;=\; \sum_i \psi(r_i) x_0^i.$$

Man nennt φ auch den Einsetzungshomomorphismus: Die Variable X wird durch den Wert $x_0 \in S$ ersetzt.

11 *Das Tensorprodukt

Sei R ein kommutativer Ring. Seien $M_1, \cdots, M_n, N$ beliebige R-Moduln. Dann verstehen wir unter

$$\mathcal{L}^n(M_1, \cdots, M_n; N)$$

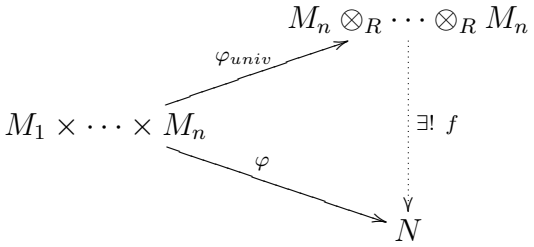
den R-Modul der n-fach R-multilinearen Abbildungen

$$\varphi : M_1 \times \cdots \times M_n \longrightarrow N \ .$$

Sind die R-Moduln $M_1, \cdots, M_n$ fest vorgegeben, dann gibt es unter all diesen Abbildungen φ eine universelle R-multilineare Abbildung

$$\varphi_{univ} : \ M_1 \times \cdots \times M_n \longrightarrow M_1 \otimes_R \cdots \otimes_R M_n \ ,$$

so daß jede andere R-multilineare Abildung φ von der Gestalt ist



für eine eindeutig bestimmte R-lineare Abbildung f.

Das bis auf Isormorphie eindeutig bestimmte universelle Objekt nennt man das Tensorprodukt $\varphi_{univ} : M_1 \times \cdots \times M_n \longrightarrow M_1 \otimes_R \cdots \otimes_R M_n$ der Moduln $M_1, ..., M_n$ über R.

Existenz: Der Einfachheit halber sei $n = 2$. Betrachte den freien R-Modul F erzeugt von allen Elementen (m_1, m_2), $m_1 \in M_1, m_2 \in M_2$. Sei U der R-Modul von F erzeugt von den Elementen $(m_1+m_1', m)-(m_1, m)-(m_1', m_2) \in F$, $(r \cdot m_1, m) - r(m_1, m) \in F$ und $(m_1, m_2 + m_2') - (m_1, m_2) - (m_1, m_2') \in F$, $(m_1, rm_2) - r(m_1, m_2) \in F$ für alle $m_1, m_1' \in M_1, m_2, m_2' \in M_2, r \in R$. Dann erfüllt F/U die gewünschte universelle Eigenschaft. Dies folgt unmittelbar aus der universellen Eigenschaft von Quotienten. Das Bild der Erzeuger (m_1, m_2) in F/U nennt man $m_1 \otimes_R m_2$. Nach Konstruktion gilt

Lemma: *Jedes Element von $M_1 \otimes_R M_2$ ist eine endliche Summe von Elementar-Tensoren der Gestalt $m_1 \otimes_R m_2$ ($m_1 \in M_1, \ m_2 \in M_2$).*

Kapitel II - Galois Theorie

In diesem Kapitel betrachten wir endliche Körpererweiterungen und Automorphismen von solchen Körpererweiterungen. Eine Körpererweiterung heisst Galoissch, wenn sie möglichst viele Automorphismen besitzt.

Das Ziel dieses Kapitel ist der Hauptsatz der Galoistheorie. Dieser besagt, dass man die Zwischenkörper einer Galoisschen Körpererweiterung aus der Galoisgruppe (der Automorphismengruppe der Körpererweiterung) ablesen kann.

12 Körpererweiterungen

Sei L ein Körper und K ein Teilkörper von L. Insbesondere ist L ein K-Vektorraum. Man nennt dann L/K eine Körpererweiterung sowie

$$[L:K] \;=\; dim_K(L)$$

den Grad der Körpererweiterung. L/K heißt endliche Körpererweiterung, wenn ihr Grad $[L:K] < \infty$ endlich ist.

Lemma 12.1. *Für Körpererweiterungen L/K und K/k gilt*

$$\boxed{[L:k] \;=\; [L:K]\cdot[K:k]}\;.$$

Beweis: Seien $b_1, \cdots, b_m \in L$ linear unabhängig über K und seien $b'_1, \cdots, b'_n \in K$ linear unabhängig über k. Dann sind $b'_i \cdot b_j$ $(1 \leqq i \leqq n, 1 \leqq j \leqq m)$ linear unabhängig über k, denn

$$\sum_{i,j} \mu_{ij} b'_i b_j \;=\; 0\;,\; (\mu_{ij} \in k)$$

impliziert $\sum_j (\sum_i \mu_{ij} b'_i) b_j = 0$, also $\sum_i \mu_{ij} b'_i = 0$ in K für alle j, sowie dann $\mu_{ij} = 0$ für alle i, j.

Dies beweist das Lemma, falls einer der beiden Grade $[L:K]$ oder $[K:k]$ unendlich ist.

Sind beiden Grade $[L:K] = m$ und $[K:k] = n$ endlich und seien $b_1, \cdots, b_m$ respektive $b'_1, \cdots, b'_n$ Vektorraumbasen, dann ist $\{b'_i b_j\}$ auch ein Erzeugendensystem, denn für $x \in L$ gilt

$$\begin{aligned} x \;&=\; \sum_{j=1}^{m} \lambda_j b_j \quad ,(\lambda_j \in K) \\ &=\; \sum_{j=1}^{m} (\sum_{i=1}^{n} \mu_{ij}\; b'_i)\; b_j \quad ,(\mu_{ij} \in k) \end{aligned}$$

für geeignete Koeffizienten $\lambda_j \in K$ respektive $\mu_{ij} \in k$. Zusammen mit der bereits bewiesenen linearen Unabhängigkeit folgt, daß die $b'_i b_j,\; 1 \leqq i \leqq n,\; 1 \leqq j \leqq m$ eine k-Basis von L mit $n \cdot m$ Elementen bilden. □

13 Körperautomorphismen

Sei L ein Körper. Ein Körperautomorphismus[1]

$$\sigma : L \longrightarrow L$$

ist eine Bijektion, welche die Körperstruktur respektiert:

$$\begin{aligned} \sigma(x+y) &= \sigma(x) + \sigma(y) \\ \sigma(x \cdot y) &= \sigma(x) \cdot \sigma(y) \ . \end{aligned}$$

Es gilt dann automatisch $\sigma(0) = 0$ und $\sigma(1) = 1$.

Ist $K \subset L$ ein Teilkörper, dann bezeichne

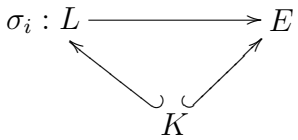
$$G(L/K)$$

die Gruppe aller Körperautomorphismen von L, welche auf K die identische Abbildung induzieren. Hierbei wird die Gruppenstruktur durch die Komposition von Abbildungen erklärt.

Lemma 13.1. [2]

$$\boxed{|G(L/K)| \leqq [L:K]} \ .$$

Zum Beweis betrachten wir allgemeiner Ringhomomorphismen σ_i



von L in einen Erweiterungskörper E von K mit $\sigma_i|_K = id_K$, und behaupten

Lemma 13.2 (Dedekind)**.** *Sind* $\sigma_1, \cdots, \sigma_n$ *paarweise verschieden, dann gilt*

$$\boxed{n \leqq [L:K]} \ .$$

[1] Jeder Ringhomomorphismus $\sigma : L \to L$ eines Körpers L ist wegen $\sigma(1) = 1$ automatisch injektiv und dann als L-lineare Abbildung aus Dimensionsgründen auch surjektiv!

[2] Wir zeigen in 15.2 sogar die Teilerbedingung: $|G(L/K)|$ teilt $[L:K]$

Beweis: OBdA ist $[L:K]=m$ endlich. Sei dann $x_1,\cdots,x_m$ ein K-Erzeugendensystem von L. Wäre $n>m$, gäbe es $0\neq(\lambda_1,\cdots,\lambda_n)\in E^n$ mit

$$(*)\qquad \sum_{i=1}^{n}\lambda_i\sigma_i(x) \;=\; 0 \quad , \quad x=x_1,\cdots,x_m$$

(ein lineares Gleichungssystem!). Da $\sum_{i=0}^{n}\lambda_i\sigma_i$ aber K-linear ist, gilt dann sogar (*) für alle $x\in L$. Dies wäre ein Widerspruch wegen dem folgenden

Hilfsatz 13.3 (Lineare Unabhängigkeit)**.** *Paarweise verschiedene Ringhomomorphismen*

$$\sigma_i : L\to E$$

eines Körpers L in einen Körper E sind E-linear unabhängig.

Beweis: Wir führen eine Induktion nach der Anzahl n der σ_i. Der Fall $n=1$ ist trivial. Sei daher $n>1$. Sei

$$\Sigma(x) \;=\; \lambda_1\sigma_1(x)+\cdots+\lambda_n\sigma_n(x) \;=\; 0 \quad , \quad x\in L$$

eine nichttriviale Relation mit $\lambda_i\in E$ und oBdA mit $\lambda_1\neq 0$. Wähle $\xi\in L$ mit $\sigma_1(\xi)\neq\sigma_n(\xi)$. Dann erhält man durch die Subtraktion $\Sigma(\xi x)-\sigma_n(\xi)\cdot\Sigma(x) = 0$ eine kürzere Relation der Länge $\leq n-1$

$$\begin{aligned}\lambda_1\big(\sigma_1(\xi)-\sigma_n(\xi)\big)\cdot\sigma_1(x) \;+\cdots+\; \lambda_{n-1}\big(\sigma_{n-1}(\xi)-\sigma_n(\xi)\big)\cdot\sigma_{n-1}(x)\\ =\; \Sigma(\xi x)-\sigma_n(\xi)\cdot\Sigma(x) \;=\; 0\ ,\end{aligned}$$

und somit per Induktion einen Widerspruch wegen

$$\lambda_1\big(\sigma_1(\xi)-\sigma_n(\xi)\big) \;\neq\; 0\ .$$

□

14 Galois Erweiterungen

Definition 14.1. *Eine endliche Körpererweiterung L/K mit der Eigenschaft*

$$\boxed{\left|G(L/K)\right| \;=\; [L:K]}$$

heißt Galoiserweiterung oder kurz galoissch.

Mit anderen Worten: L/K ist galoissch, wenn die Zahl der Automorphismen der Körpererweiterung maximal ist im Sinne, dass die obere Schranke in der Ungleichung von Lemma 2.1 angenommen wird.

Ist L ein Körper und sind $\sigma_1, \cdots, \sigma_n$ Körperautomorphismen von L, dann ist die Fixpunktmenge

$$Fix(\sigma_1, \cdots, \sigma_n) \;=\; \{x \in L \mid \sigma_i(x) \;=\; x\}$$

offensichtlich ein Teilkörper von L. Gilt $K \subsetneqq L$ und $\sigma_i|_K = id_K$ (für $i = 1, .., n$), dann enthält der Fixkörper natürlich den Körper K.

Sei $G = G(L/K)$, dann bezeichne L^G den Fixkörper aller $\sigma \in G$.

Satz 14.2. *Sei L/K galoissch und sei $G = G(L/K)$. Dann ist der Fixkörper L^G aller $\sigma \in G$ gleich dem Grundkörper K*

$$\boxed{L^G \;=\; K}\,.$$

Beweis: Per Definition gilt $G(L/K) \stackrel{!}{=} G(L/L^G)$ und

$$\begin{array}{c} L \\ \uparrow \\ L^G \\ \uparrow \\ K \end{array}$$

Lemma 13.1 angewendet auf $G = G(L/L^G)$ liefert $|G| \leqq [L : L^G]$.
L/K galoissch bedeutet per Definition $|G| = [L : K]$.
Die Gradformel für Körpererweiterungen $[L : L^G] \cdot [L^G : K] = [L : K]$ (Lemma 12.1) liefert daher sofort $[L^G : K] = 1$ oder $L^G = K$. □

15 Eine Verschärfung

Ziel dieses Abschnittes ist folgende Verschärfung von Satz 14.2.

Satz 15.1. *(Artin) Ist G eine Gruppe von Körperautomorphismen des Körpers L, dann gilt für den Fixkörper L^G*

$$\boxed{[L : L^G] \;=\; |G|} \; .$$

Folgerung: *Ist $|G|$ endlich, folgt $G(L/L^G) = G$ wegen Lemma 13.1, somit ist L/L^G galoissch.*

Beweis: (des Satzes) Wegen $|G| \leqq [L : L^G]$ (Lemma 13.1) genügt es die Ungleichung $|G| \geqq [L : K]$ für $K = L^G$ nachzuweisen. OBdA ist dabei G endlich mit $|G| = n$ Elementen.

Um $n \geqq [L : K]$ zu zeigen genügt es, daß je $n+1$ Elemente $x_1, \cdots, x_{n+1}$ von L über K linear abhängig sind. Das folgende L-lineare Gleichungssystem (aus n linearen Gleichungen über L)

$$\sum_{j=1}^{n+1} y_j \sigma_i(x_j) \;=\; 0 \quad , \quad (i = 1, \cdots, n)$$

hat aus Dimensionsgründen eine nichttriviale Lösung $(y_1, \cdots, y_{n+1}) \in L^{n+1}$. Da alle σ_i invertierbar sind, gilt für diese Lösung dann auch

$$\sum_{j=1}^{n+1} \sigma_i^{-1}(y_j) x_j \;=\; 0 \quad , \quad (i = 1, \cdots, n) \; .$$

Summiert man über alle $i = 1, \cdots, n$, erhält man

$$\sum_{j=1}^{n+1} \lambda_j x_j \;=\; 0 \quad , \quad \lambda_i \;=\; Spur(y_i) \; .$$

Aber $\lambda_j \in L^G = K$ wegen Satz 14.2. Ersetzt man die Lösung $(y_1, \cdots, y_n)$ durch $(yy_1, \cdots, yy_n)$, kann man bei geeigneter Wahl von $y \in L$ erreichen $\lambda_1 = Spur(yy_1) \neq 0$ (benutze Hilfssatz 13.3). Also sind $x_1, \cdots, x_{n+1} \in L$ linear abhängig über K. Es folgt somit $n \geqq [L : K]$. □

Korollar 15.2. *Für eine endliche Körpererweiterung L/K ist die Ordnung von $G = G(L/K)$ ein Teiler von $[L : K]$.*

Beweis: $[L : K] = [L : L^G] \cdot [L^G : K] = |G| \cdot [L^G : K]$ wegen Lemma 12.1 und Satz 15.1. □

16 Der Hauptsatz

Sei L/K eine galoissche Erweiterung, $G = G(L/K)$ die zugehörige Galoisgruppe und

$$\boxed{\mathcal{G} \;=\; \{U \mid U \subseteq G \text{ Untergruppe}\}}$$

die Menge der Untergruppen von G sowie

$$\boxed{\mathcal{K} \;=\; \{M \mid K \subseteq M \subseteq L \text{ Zwischenkörper}\}}$$

die Menge der Zwischenkörper von L/K.

Dann liefert die Zuordnung des **Fixkörpers** eine Injektion f

$$\begin{array}{ccc} \mathcal{G} & \overset{f}{\hookrightarrow} & \mathcal{K} \\ U & \longmapsto & L^U \end{array}$$

Wegen der Folgerung von Satz 15.1 ist nämlich die reziproke Abbildung g, welche einem Zwischenkörper M seine relative **Galoisgruppe** $G(L/M)$ zuordnet

$$\begin{array}{ccc} \mathcal{G} & \underset{g}{\longleftarrow} & \mathcal{K} \\ G(L/M) & \longleftarrow & M \end{array}$$

zu f linksinvers $U \mapsto L^U \mapsto G(L/L^U) = U$.

Satz 16.1. *(Hauptsatz der Galois Theorie) Die Abbildung f definiert eine Bijektion*

$$\boxed{f : \; \mathcal{G} \xrightarrow{\sim} \mathcal{K}}$$

mit der Umkehrabbildung g.

Das heißt: Die Zuordnung f des Fixkörpers zur Untergruppe U respektive die Zuordnung g der Galoisgruppe $Gal(L/M)$ zum Körper M induzieren eine Bijektion[3] zwischen der (endlichen !) Menge der Untergruppen von G und der Menge der Zwischenkörper von L/K.

[3]Wir zeigen im nächsten Abschnitt ausserdem, dass Inklusionrelationen bis auf Umkehrung dabei erhalten bleiben.

Beweis: Es verbleibt die Surjektivität von f zu beweisen. Wir müssen zeigen, daß jedes M aus $\mathcal{K}$ im Bild $f(\mathcal{G}) \subsetneqq \mathcal{K}$ liegt. Wäre dies nicht richtig, wählen wir ein minimales M aus $\mathcal{K} \setminus f(\mathcal{G})$, und zeigen damit einen Widerspruch!

1) Zu M wähle $U \in \mathcal{G}$ minimal[4] mit $K \subseteq L^U \subseteq M$.

Ersetzt man G durch U und damit L^U durch K, so ist M immer noch ein (minimales) Gegenbeispiel. Dadurch können wir für unseren Widerspruchsbeweis oBdA $G = U$ und $L^U = K$ annehmen. Wegen der Minimalität von M enthält jetzt M/K keinen echten Zwischenkörper mehr. Wegen $K = f(\mathcal{G})$ und $M \notin f(\mathcal{G})$ gilt $K \subsetneqq M$.

2) Wähle $\alpha \in M$ mit $\alpha \notin K$. Sei $K(\alpha)$ der kleinste Teilkörper von L, welcher K und α enthält. Aus $K \subsetneqq K(\alpha) \subseteq M$ folgt jetzt

$$M = K(\alpha) \ .$$

3) Sei G_α der Stabilisator von α in G (siehe Appendix). Da jedes Element von M sich in der Form $f(\alpha)/g(\alpha)$ für geeignete Polynome $f(x), g(x) \in K[X]$ schreiben lässt[5], folgt wegen $M = K(\alpha)$

$$K \subsetneqq M \subsetneqq L^{G_\alpha} \ .$$

Die Gradformel 12.1, Satz 15.1 und Lemma 16.2 (im Appendix) liefern

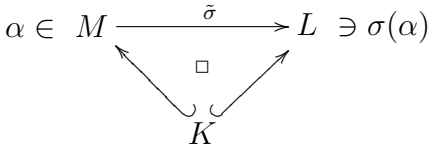
$$[L^{G_\alpha} : K] \overset{12.1}{=} \frac{[L:K]}{[L:L^{G_\alpha}]} \overset{15.1}{=} \frac{|G|}{|G_\alpha|} \overset{16.2}{=} |G \cdot \alpha| \ = \ \#Orbit(\alpha) \ .$$

4) Unter den Einschränkungen $\tilde{\sigma} = \sigma|_M$ der $\sigma \in G$ auf den Teilkörper $M = K(\alpha) \subsetneqq L$ befinden sich offensichtlich mindestens $\#Orbit(\alpha)$ paarweise

[4]Dies ist möglich wegen $L^G = K$.

[5]Dazu genügt es, dass dies einen Teilkörper definiert.

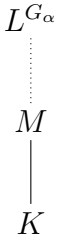
verschiedene Automorphismen $\tilde{\sigma}$



Aus dem Dedekind Lemma 13.2 folgt daher

$$\#Orbit(\alpha) \leqq [M : K] .$$

5) Die letzten beiden Schritte ergeben $[L^{G_\alpha} : K] = \#Orbit(\alpha) \leqq [M : K]$. Wegen



folgt daher $L^{G_\alpha} = M$. Also liegt $M = f(G_\alpha)$ in $f(\mathcal{G})$. Ein Widerspruch zur Annahme $M \notin f(\mathcal{G})$!

Damit ist der Hauptsatz gezeigt. $\square$

Appendix

Sei G eine Gruppe und X eine Menge. Eine Operation von G auf X ist eine Abbildung

$$G \times X \to X$$

$$(g, x) \mapsto g \cdot x$$

mit den Eigenschaften $1 \cdot x = x$ und $g \cdot (h \cdot x) = (gh) \cdot x$ für $g, h \in G$ und $x \in X$.

Ist eine Operation von G auf X gegeben, nennt man

$$G_x \;=\; \{g \in G \mid g \cdot x = x\}$$

den Stabilisator von x in G. Offensichtlich ist G_x eine Untergruppe von G. Die Teilmenge

$$G \cdot x \;=\; \{g \cdot x \mid g \in G\} \;\subseteq\; X$$

nennt man den Orbit von x in X unter G. Ist G endlich, dann ist auch der Orbit $G \cdot x$ endlich, und es gilt

Lemma 16.2.

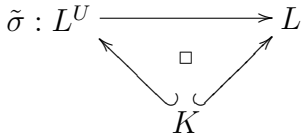
$$\boxed{|G \cdot x| \;=\; \tfrac{|G|}{|G_x|}}\,.$$

Beweis: Für $g_1, g_2 \in G$ gilt $g_1 \cdot x = g_2 \cdot x$ genau dann, wenn $g_2^{-1} g_1 \in G_x$; d.h. $g_2 = g_1 \cdot h$ mit $h \in G_x$. Somit hat jeder Punkt im Orbit genau $|G_x|$ Urbilder in G. Es folgt $|G_x| \cdot |G \cdot x| = |G|$.

17 Eigenschaften der Galois Korrespondenz

Für beliebige Untergruppen U von G gilt

(1) *Es gibt genau* $|G|/|U|$ *verschiedene Ringhomomorphismen* $\tilde{\sigma}$



Jedes solche $\tilde{\sigma}$ *wird von einem* $\sigma \in G$ *durch Einschränken* $\tilde{\sigma} = \sigma|_{L^U}$ *induziert.*

Beweis: Die Elemente τ der Gruppe G operieren auf der Menge aller solchen Abbildungen via $\tilde{\sigma} \mapsto \tau \circ \tilde{\sigma}$. Der Stabilisator der Inklusion $\tilde{\sigma} = i : L^U \subset L$ ist gerade U. Aus dem letzten Appendix folgt daher

$$\#\{\tilde{\sigma}\} \ \geqq \ \#\{\tilde{\sigma} = \sigma|_{L^U}, \sigma \in G\} \ \geqq \ \frac{|G|}{|U|} \ .$$

Wegen Lemma 13.2 gilt andererseits

$$\#\{\tilde{\sigma}\} \ \leqq \ [L^U : K] \ = \ \frac{[L : K]}{[L : L^U]} \ = \ \frac{|G|}{|U|} \ .$$

Es folgt $\#\{\tilde{\sigma}\} = \#\{\tilde{\sigma} = \sigma|_{L^U}, \sigma \in G\} = |G|/|U|$ wie behauptet.

Weiterhin gilt die offensichtliche Eigenschaft

(2) $$\textit{Es gilt } U_1 \subseteqq U_2 \quad \Longleftrightarrow \quad f(U_1) \supseteqq f(U_2)$$

sowie

(3) *Für* $\sigma \in G$ *ist der Bildkörper* $\sigma(L^U) \subseteqq L$ *von* L^U *unter* σ *gleich dem Fixkörper*

$$L^{\sigma U \sigma^{-1}} = \sigma(L^U)$$

der konjugierten Untergruppe $\sigma U \sigma^{-1} \subseteqq G$.

Beweis: von (3). $\tau x = x \Leftrightarrow \sigma\tau x = \sigma x \Leftrightarrow \sigma\tau\sigma^{-1} \cdot \sigma x = \sigma x$. Somit ist

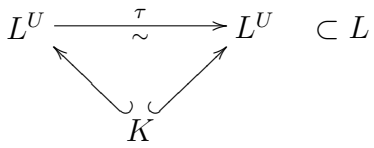
$$Fix(\sigma U \sigma^{-1}) \ = \ \sigma Fix(U) \ .$$

Während die Erweiterungen L/L^U immer galoissch sind mit Galoisgruppe U (Satz 15.1), ist dies für die Erweiterungen L^U/K im allgemeinen nicht mehr richtig! Vielmehr gilt

(4) $\qquad L^U/K$ *galoissch* $\Longleftrightarrow$ U *ist ein Normalteiler in* G.

Hierbei nennt man eine Untergruppe U von G einen Normalteiler, wenn gilt $\sigma U \sigma^{-1} = U$ für alle $\sigma \in G$.

Beweis: von (4). L^U/K ist galoissch genau dann, wenn es $[L^U : K] = |G|/|U|$ verschiedene Ringautomorphismen τ



gibt. Jedes solche τ ist durch seine Komposition $\sigma = i \circ \tau : L^U \hookrightarrow L$ mit der Inklusion $i : L^U \subset L$ vollkommen bestimmt. Nach Aussage (1) ist σ durch ein Element $\sigma \in G$ (durch Einschränken von L auf L^U) induziert, und es entstehen auf diese Weise höchstens $|G|/|U|$ verschiedene Ringhomomorphismen. Somit ist L^U/K galoissch genau dann wenn gilt

$$\sigma(L^U) \;=\; L^U \;\text{ für alle } \sigma \in G\ .$$

Wegen (3) ist dies gleichbedeutend mit der Normalteilereigenschaft von U.

Kapitel III - Zerfällungskörper

In diesem Kapitel zeigen wir, dass es zu jedem Polynom $f = f(X)$ über einem Körper K einen endlichen Erweiterungskörper gibt, in dem das Polynom in Linearfaktoren zerfällt. Wählt man einen solchen Körper kleinstmöglich, spricht man von einem Zerfällungskörper.

In der Tat sind je zwei Zerfällungskörper eines Polynoms über K zueinander K-isomorph. Ist das Polynom f separabel, dann ist der Zerfällungskörper von f über K eine galoissche Erweiterung von K. Die Umkehrung gilt auch: Jeder galoissche Erweiterungskörper von K ist der Zerfällungskörper eines geeigneten separablen Polynoms $f(X)$ über K.

18 Existenz von Zerfällungskörpern

Sei K ein Körper und $f \in K[x]$ ein Polynom. Wir suchen einen Körper $E \supseteq K$, in welchem $f(x)$ in ein Produkt von Linearfaktoren zerfällt. Sei $K_f \subseteq E$ der kleinste Teilkörper von E, welcher K und die Nullstellen von f enthält, dann nennt man K_f Zerfällungskörper von f. In der Tat zerfällt $f(x)$ ja bereits über K_f in ein Produkt von Linearfaktoren, und K_f ist kleinstmöglich in E mit dieser Eiegnschaft.

Satz 18.1. *Jedes Polynom f besitzt einen Zerfällungskörper K_f, welcher eine endliche Erweiterung von K ist.*

Bemerkung 18.2. *Besitzt $f(x)$ in E eine Nullstelle $\alpha \in E$, so spaltet $f(x)$ über E einen Linearfaktor $(x-\alpha)$, $\alpha \in E$ ab. D.h. es gilt*

$$f(x) \;=\; (x-\alpha)\; g(x)$$

(genau dann), wenn gilt $f(\alpha) = 0$. Aus $f(\alpha) = 0$ folgt nämlich

$$f(x) \;=\; f(x) - f(\alpha) \;=\; \sum_{i=0}^{n} a_i\; (x^i - \alpha^i)$$

$$=\; (x-\alpha) \cdot \sum_{i=0}^{n} a_i\; \Big(\sum_{j=0}^{i-1} x^{i-1-j} \alpha^j \Big)\; .$$

Es genügt also Erweiterungskörper zu finden, über denen f einen Nullstelle besitzt. Man erhält dann E durch Iteration der Konstruktion.

Bemerkung 18.3. *Sei $g(x)$ ein K-irreduzibler Faktor von $f(x)$. Es genügt einen Erweiterungskörper von K zu finden, in dem $g(x)$ eine Nullstelle hat. Wir können daher oBdA annehmen, $f(x)$ sei irreduzibel.*

Primitive Erweiterungen: Sei $f(x) \in K[x]$ ein irreduzibles Polynom vom $Grad \geqq 1$. Dann ist $K_1 = K[x]/(f)$ nach 6.3 ein Erweiterungskörper von K. Es bezeichne $\alpha = [x]$ die Restklasse von $x \in K[x]/f(x)$. Dann gilt

$$f([x]) \;=\; \sum a_i [x]^i \;=\; \sum [a_i][x]^i \;=\; \Big[\sum a_i x^i \Big] \;=\; [f(x)] \;=\; [0]\; .$$

Somit ist α eine Nullstelle von $f(x)$ über K_1. Es gilt $f(x) = (x-\alpha) \cdot g(x)$ für ein Polynom $g(x) \in K_1[x]$ vom $Grad < n$.

Lemma 18.4. *Für eine primitive Erweiterung K_1/K gilt*

$$[K_1 : K] \;=\; deg_x(f)\ .$$

Beweis: Sei $n = deg_x(f)$ und oBdA f normiert, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Dann ist $[1], [x], \cdots, [x]^{n-1}$ eine Basis von K_1 über K. (s. auch LA-I-Skript)
Dies ist ein Erzeugendensystem, denn

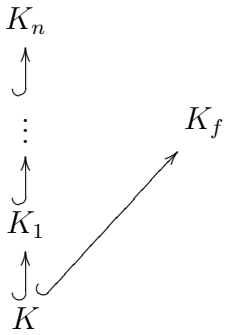
$$[x]^n \;=\; -a_{n-1}[x]^{n-1} \;-\; \cdots \;-\; a_0$$
$$[x]^{n+1} \;=\; \cdots\ .$$

Lineare Unabhängigkeit: Sei $(b_0, \cdots, b_{n-1}) \in K^n$ mit $\sum_{\nu=0}^{n-1} b_\nu [x]^\nu = 0$ in K_1, dann folgt $g(x) \in (f(x))$ für $g(x) = \sum_{\nu=0}^{n-1} b_\nu x^\nu$. Dies ist aber aus Gradgründen $deg_x(g) < deg_x(f)$ ist dies nur möglich für $g(x) = 0$ in $K[x]$ im Widerspruch zur Annahme $(b_0, \cdots, b_{n-1}) \neq 0$.

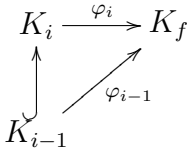
Alternativ: $K[x] = (f(x)) \oplus (K \cdot [1] + \cdots + K \cdot [x]^{n-1}) =: (f) \oplus V$. Für beliebiges $p(x) \in K[X]$ ist $p(x) = u(x)f(x) + r(x)$ mit $\deg_x(r) < n$, also $r(x) \in V$. Dies zeigt $K[x] = (f) + V$. Die Summe ist auch direkt. Ist nämlich $g(x) \in V \cap (f)$, so folgt wegen $f \mid g$ und $deg_x(g) < deg_x(f)$, dass gilt $g(x) = 0$. $\square$

19 Eindeutigkeit von Zerfällungskörpern

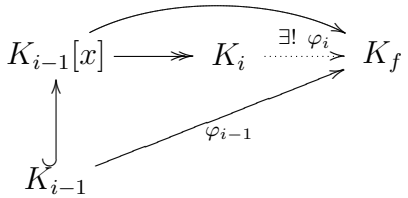
Wie wir gesehen haben, lässt sich ein Zerfällungskörper K_n durch sukzessive Iteration aus primitiven Körpererweiterungen gewinnen. Sei K_f ein zweiter Zerfällungskörper von f.



Dann lässt sich die Einbettung $K \hookrightarrow K_f$ sukzessive auf die primitiven Erweiterungen fortsetzen.

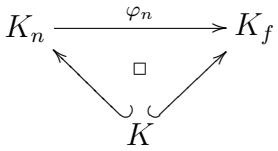


Angenommen, φ_{i-1} sei bereits konstruiert. Dann erhält man φ_i



mittels des Einsetzungshomomorphismus $K_{i-1}[x] \to K_f$, welcher x auf eine Nullstelle $\alpha \in K_f$ von f_i abbildet. Der Einsetzungshomomorphismus ist trivial auf dem Ideal $(f_i(x)) \subsetneqq K_{i-1}[x]$. Somit folgt aus der universellen Eigenschaft des Quotienten die Existenz eines Ringhomomorphismus $\varphi_i : K_i \to K_f$, welcher φ_{i-1} fortsetzt.

Durch Iteration folgt die Existenz eines Ringhomomorphismus



mit $\varphi_n|_K = id_K$. Da K_f von den Nullstellen von f erzeugt wird, ist φ_n surjektiv. Andererseits ist $\varphi_n(1) = 1$ und somit ist φ_n automatisch injektiv (Korollar 2.3), also sind K_n und K_f isomorphe Körpererweiterungen von K.

Satz 19.1. *Der Zerfällungskörper eines Polynoms $f(x) \in K[x]$ ist als Körpererweiterung von K eindeutig bestimmt bis auf Isomorphie.*

Beweis: Dies ist eine unmittelbare Folgerung aus der obigen Konstruktion von Ringhomomorphismen.

$$K_f \quad \cong \quad K_n \quad \cong \quad \tilde{K}_f \ .$$

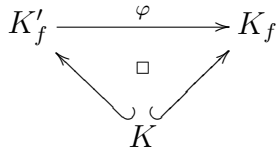
□

20 Separable Polynome

Ein Polynom $f(x) \in K[x]$ heißt separabel, falls jeder K-irreduzible Faktor von $f(x)$ in einem (und damit in jedem) Zerfällungskörper nur einfache Nullstellen besitzt.

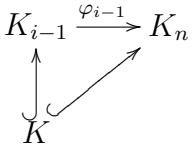
Betrachtet man die Konstruktion von §18 und §19, dann ist klar, daß ein separables Polynom $f(x) \in K[x]$ separabel über jedem der Körper K_i, $i = 1, \cdots, n$ bleibt! Wir schließen somit aus der Konstruktion von §19

Satz 20.1. *Seien K_f und K'_f zwei Zerfällungskörper eines separablen Polynoms $f(x) \in K[x]$. Dann gibt es mindestens $[K_f : K]$ verschiedene Isomorphien*

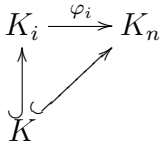


mit $\varphi|_K = id_K$.

Beweis: OBdA sei $K'_f = K_f = K_n$. Per Induktion zeigt man die Existenz von $[K_{i-1} : K]$ verschiedenen Ringhomomorphismen



Da man x auf jede der $Grad(f_i)$ Nullstellen in K_n des irreduziblen Polynoms $f_{i-1}(x) \in K_{i-1}[x]$ abbilden kann, lässt sich φ_{i-1} zu $grad(f_i) = [K_i : K_{i-1}]$ Ringhomomorphismen



fortsetzen. Wegen der Gradformel $[K_i : K] = [K_i : K_{i-1}] \cdot [K_{i-1} : K]$ (siehe Lemma 12.1), folgt daher die Existenz von mindestens $[K_i : K]$ verschiedenen Ringhomomorphismen $\varphi_i : K_i \to K_n$ mit $\varphi_i|_K = id_K$. $\square$

Korollar 20.2. *Der Zerfällungskörper K_f eines separablen Polynoms $f(x) \in K[x]$ ist eine galoissche Erweiterung von K.*

Wir beweisen im nächsten Abschnitt die Umkehrung dieser Aussage.

21 Charakterisierung von Galoissch

Satz 21.1. *Eine endliche Körpererweiterung L/K ist galoissch genau dann, wenn L Zerfällungskörper eines separablen Polynoms $f \in K[x]$ ist.*

Beweis: Wegen Korollar 20.2 genügt es zu zeigen, daß eine galoissche Erweiterung Zerfällungskörper eines separablen Polynoms f ist.

Sei L/K galoissch und $\alpha \in L$. Dann ist

$$f(x) \;=\; \prod_{\beta \in G(\alpha)} (x \;-\; \beta)$$

ein Polynom in $L[x]$, dessen Koeffizienten unter allen $\sigma \in G$ invariant sind. Es folgt daher aus Satz 3.2

$$f(x) \;\in\; K[x] \;.$$

Die Nullstellen $\beta \in G(\alpha)$ im G-Orbit von α (die sogenannten konjugierten Elemente) sind per Definition paarweise verschieden, und somit ist $f(x)$ separabel. Es folgt $K_f \subsetneqq L$ und $[L : K_f] < [L : K]$, falls $\alpha \notin K$. Wählt man dann sukzessiv weitere $\tilde{\alpha} \notin K_f$ und definiert analog $\tilde{f} \in K[x]$, sieht man leicht durch Induktion nach dem Grad, daß L der Zerfällungskörper des Produktes $f \cdot \tilde{f} \cdots$ ist.

Der Beweis des letzten Satzes zeigt sogar mehr

Satz 21.2. *(***Normalität***) Besitzt ein irreduzibles Polynom $f(x) \in K[x]$ in einer galoisschen Erweiterung L/K eine Nullstelle $\alpha \in L$, dann zerfällt $f(x) \in K[x]$ vollständig in Linearfaktoren (nämlich zu den Nullstellen β im Orbit $G(\alpha) \subsetneqq L$).*

22 Charakterisierung separabler Polynome

Satz 22.1. *Ein (K-irreduzibles) Polynom $f \in K[x]$ ist (genau dann) K-separabel, wenn gilt*

$$ggT\Big(f, \frac{d}{dx}f\Big) \;=\; 1 \;.$$

Bemerkung: Für ein Polynom $f(x) = \sum_{i=0}^{n} a_i x^i$ definiert man [6]

$$\frac{d}{dx}f(x) \;=\; \sum_{i=1}^{n} a_i \cdot i \cdot x^{i-1} \;.$$

Man zeigt leicht (*)

$$\begin{aligned} \frac{d}{dx}(f+g) \;&=\; \frac{d}{dx}f \;+\; \frac{d}{dx}g \\ \frac{d}{dx}(f\cdot g) \;&=\; \frac{d}{dx}f\cdot g \;+\; f\cdot\frac{d}{dx}g \end{aligned}$$

Beweis: [des Satzes] Gilt $f(x) = (x-\alpha)^2 \cdot g(x)$, dann ist wegen (*)

$$\begin{aligned} \frac{d}{dx}f \;&=\; 2(x-\alpha)\cdot g(x) \;+\; (x-\alpha)^2\Big(\frac{d}{dx}g\Big)(x) \\ &=\; (x-\alpha)\cdot h(x) \;. \end{aligned}$$

Betrachte den der Einsetzungshomomorphismus ψ

$$\begin{aligned} K[x] &\xrightarrow{\;\psi\;} K_n \\ x \;&\longmapsto\; \alpha \end{aligned}$$

mit $I = Kern(\psi)$. Dann ist $I = (p)$ ein Primideal in $K[x]$. Es folgt $p \mid f$ und $p \mid \frac{d}{dx}f$, da $\psi(f) = 0$ und $\psi(\frac{d}{dx}f) = 0$. Somit gilt

$$ggT\Big(f, \frac{d}{dx}f\Big) \;\neq\; 1 \;.$$

[6] Genauer $\sum_i a_i \varphi(i) x^{i-1}$ im Sinne von I §8.

Bemerkung 22.2. *Ist $f \in K[x]$ irreduzibel, dann gilt $Grad\big(\frac{d}{dx}f\big) < Grad(f)$. Aus $\frac{d}{dx}f \neq 0$, folgt somit $ggT\big(f, \frac{d}{dx}f\big) = 1$ aus Gradgründen. Somit ist ein irreduzibles Polynom f genau dann separabel, wenn gilt*

$$\frac{d}{dx}f(x) \not\equiv 0 \ .$$

(In Charakteristik Null ist daher f also automatisch separabel.)

Man sieht leicht

$$\frac{d}{dx}f \equiv 0 \Longleftrightarrow f(x) = g(x^p)$$

für ein Polynom $g \in K[x]$ über einem Körper K der Charakteristik $p = Char(K)$. Somit hat dann jede Nullstelle $\alpha \in L$ von f mindestens die Vielfachheit p.

Beweis: $f(\alpha) = 0 \ \Rightarrow g(\beta) = 0$ für $\beta = \alpha^p$. Also $g(y) = (y - \beta) \cdot h(y)$, beziehungsweise

$$f(\alpha) \ = \ (x^p - \beta) \cdot h(x^p) \ = \ (x - \alpha)^p \cdot h(x^p) \ .$$

Kapitel IV - Komplexe Zahlen

23 Fundamentalsatz der Algebra

Sei L eine galoissche Erweiterung von $\mathbb{R}$ von Grad $n = [L : \mathbb{R}]$ und sei M ein Zwischenkörper vom Grad $m = [M : \mathbb{R}]$. Sei N die Norm und Sp die Spur (siehe Appendix).

Lemma 23.1. *Ist $Sp(x \cdot y)$ definit auf M, dann gilt $M = \mathbb{R}$.*

Beweis: Jeder selbstadjungierte Endomorphismus φ von M besitzt dann einen Eigenvektor $x_0 \neq 0$ in M mit einem reellen Eigenwert λ_0 (Spektralsatz). Angewandt auf

$$\varphi_\beta(x) \;=\; \beta \cdot x \quad (\beta \in M)$$

liefert dies $\beta \cdot x_0 = \lambda_0 \cdot x_0$. Es folgt $\beta = \lambda_0 \in \mathbb{R}$ nach Kürzen von x_0 (in M).

Lemma 23.2. *Jede nichttriviale galoissche Körpererweiterung M von $\mathbb{R}$ enthält einen zu $\mathbb{C}$ isomorphen quadratischen Teilkörper $\mathbb{C}_M$.*

Beweis: Wegen $N(x^2) = N(x)^2 > 0$ für alle $x \in M^*$ definiert

$$x \longmapsto \frac{Sp(x^2)}{+\sqrt[n]{N(x)^2}}$$

eine stetige Funktion F auf $M^* \cong \mathbb{R}^m \setminus \{0\}$. Da F konstant ist auf allen Geraden $\{\lambda \cdot x \mid \lambda \in \mathbb{R}^*\}$, nimmt F sein Minimum an (Kompaktheit der Einheitssphäre in $\mathbb{R}^m$).

Für jeden Extremwert $\alpha \in M^*$ von F gilt [7] $\frac{d}{d\lambda} F(\alpha + \lambda\beta)|_{\lambda=0} = 2N(\alpha^2)^{\frac{1}{n}} \cdot Sp(\alpha \cdot \beta - \frac{Sp(\alpha^2)}{n} \cdot \alpha^{-1} \cdot \beta) = 0$ für alle $\beta \in L$. Da $Sp(x \cdot y)$ nichtausgeartet auf M ist (Lemma 24.2), folgt daraus $\alpha^2 = \frac{1}{n} \cdot Sp(\alpha^2)$ und somit $\alpha^2 \in \mathbb{R}$ sowie

$$F(\alpha) \;=\; \frac{n \cdot \alpha^2}{|\alpha^2|} \;.$$

Es gilt $\mathbb{R}(\alpha) = \mathbb{R} \iff \alpha^2 > 0$. Somit ist für das Minimum $\mathbb{C}_M = \mathbb{R}(\alpha)$ isomorph zu $\mathbb{C}$. Denn anderenfalls wäre der Zähler von F positiv, also

$$Sp(x^2) \;>\; 0 \quad , \quad \forall\, x \in M^*$$

im Widerspruch zum letzten Lemma definit.

[7] Benutze $\frac{d}{d\lambda} Sp(\alpha + \lambda\beta)^2 = 2Sp(\alpha\beta)$ und $\frac{d}{d\lambda} N(\alpha + \lambda\beta)^2 = 2N(\alpha^2) Sp(\alpha^{-1}\beta)$ bei $\lambda = 0$.

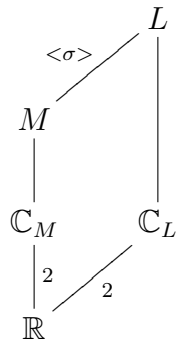
Bemerkung 23.3. *Da die Gleichung $x^2+1=0$ höchstens zwei Lösungen in M besitzt, ist der in Lemma 23.2 konstruierte Teilkörper $\mathbb{C}_M \subsetneqq M$ eindeutig bestimmt.*

Wir folgern daraus den

Satz 23.4 (Fundamentalsatz der Algebra)**.** *Jedes Polynom $f(X) \in \mathbb{C}[X]$ zerfällt in ein Produkt von Linearfaktoren. Das heißt, $\mathbb{C}$ besitzt keine echten endlichen Erweiterungskörper.*

Beweis: Anderenfalls gäbe es einen galoisschen Erweiterungskörper $L/\mathbb{R}$ mit Galoisgruppe G vom Grad $n > 2$. (Begründe dies!) Wir zeigen $G(L/\mathbb{R})$ ist zyklisch:

Sei $\mathbb{C}_L$ die eindeutige zu $\mathbb{C}$ isomorphe quadratische Erweiterung von $\mathbb{R}$ in L (Lemma 23.2). Wegen der Eindeutigkeit gilt $\sigma(\mathbb{C}_L) = \mathbb{C}_L$ für alle $\sigma \in G(L/\mathbb{R})$. Es gibt dann nach Satz ein $\sigma \in G(L/\mathbb{R})$ mit $\sigma|\mathbb{C}_L \neq id_{\mathbb{C}_L}$. Aber dann ist der Fixkörper $M = L^{<\sigma>}$ der Grundkörper $\mathbb{R}$. Denn anderenfalls existiert $\mathbb{C}_M \subseteq M$. Wegen der Eindeutigkeit in L gilt $\mathbb{C}_M = \mathbb{C}_L$ im Widerspruch zu der Tatsache, daß σ trivial auf $\mathbb{C}_M$ operiert.



Also $M = \mathbb{R}$. Nach dem Hauptsatz der Galoistheorie 16.1 ist also $G = <\sigma>$ zyklisch. Somit

$$G \;\cong\; \mathbb{Z}/n\mathbb{Z} \;\cong\; (\mathbb{Z}/2\mathbb{Z})^l \times \mathbb{Z}/k\mathbb{Z} \quad \text{(k ungerade)} \; .$$

Da der Fixkörper von $(\mathbb{Z}/2\mathbb{Z})^l$ eine Erweiterung von $\mathbb{R}$ von ungeradem Grad k wäre, folgt ein Widerspruch zu Lemma 23.2 im Fall $k \neq 1$. Also

$$G \;\cong\; (\mathbb{Z}/2\mathbb{Z})^l \quad , \quad (l \geqq 2) \; .$$

Der Fixkörper von $2^{l-2}\mathbb{Z}/2^l\mathbb{Z}$ in L definiert dann einen echten quadratischen Erweiterungskörper von $\mathbb{C}$. Dies liefert einen Widerspruch, da $\mathbb{C}$ keine quadratischen Erweiterungskörper besitzt. (Jedes quadratische Polynom in $\mathbb{C}[X]$ zerfällt in zwei Linearfaktoren. Begründe dies!).

Damit ist der Fundamentalsatz gezeigt.

24 Appendix (Norm und Spur)

Sei L/K eine Galoiserweiterung mit Galoisgruppe G. Für $x \in L$ setzen wir

$$N(x) = \prod_{\sigma \in G} \sigma(x)$$

$$Sp(x) = \sum_{\sigma \in G} \sigma(x),$$

welches nach 14.2 Werte in K liefert. Offensichtlich gilt $N(x \cdot y) = N(x) \cdot N(y)$ und $Sp(x + y) = Sp(x) + Sp(y)$ sowie $N(x) = 0 \Leftrightarrow x = 0$.

Lemma 24.1. *Für Galoiserweiterungen L/K definiert*

$$Sp(x \cdot y) \quad , \quad x, y \in L$$

eine nichtausgeartete symmetrische K-Bilinearform auf L.

Beweis: Wäre $Sp(x \cdot y) = 0$ für alle $y \in L$ und $x \neq 0$ erhielten wir einen Widerspruch zur 13.3 (lineare Unabhängigkeit der $\sigma \in G$).

Wir bemerken, daß dasselbe Argument auch zeigt

Lemma 24.2. *Sei M ein Zwischenkörper einer galoisschen Erweiterung L/K, dann ist*

$$Sp_M(x \cdot y) \quad , \quad x, y \in M$$

eine nichtausgeartete symmetrische Bilinearform auf M.

Hierbei ist entweder $char(K) = 0$ und Sp_M ist definiert wie oben, oder im Fall $char(K) \neq 0$ wird Sp_M definiert durch

$$Sp_M : M \longrightarrow K$$
$$x \longmapsto \sum_{\tilde{\sigma}} \tilde{\sigma}(x)$$

(Summe über alle paarweise verschiedene $\tilde{\sigma} = \sigma|_M$).

Kapitel V - Endliche Körper

25 Endliche Körper

Sei K ein endlicher Körper.

Die in § 7 definierte Charakteristik ist für einen endlichen Körper K ungleich Null. Ist p diese Charakteristik, dann erzeugen die Vielfachen des **1**-Elementes einen zu $\mathbb{F}_p$ isomorphen Teilkörper von $\mathbb{F}_p$, den sogenannten Primkörper.

$$\mathbb{F}_p \subseteq K .$$

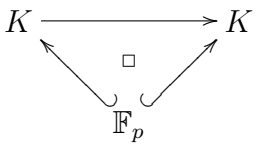
Da K endlich ist, ist die Dimension

$$n = [K : \mathbb{F}_p]$$

endlich. Somit $K \cong (\mathbb{F}_p)^n$ als $\mathbb{F}_p$-Vektorraum. Also

$$\#K = q = p^n \quad , \quad n = [K : \mathbb{F}_p] .$$

Aus § 8 folgt, daß der durch $F(x) = x^p$ definierte Frobeniushomomorphismus



ein Automorphismus (!) von K ist, welcher auf $\mathbb{F}_p$ die Identität ist

$$F \in G(K/\mathbb{F}_p) .$$

Aus Lemma 13.1 folgt $\#G(K/\mathbb{F}_p) \leqq n$. Somit ist unter den $n+1$ Automorphismen $id_K, F, F^2, \cdots, F^n$ ein gleiches Paar $F^i = F^j$.
Daraus folgt für $m = |j - i|$

$$1 \leqq m \leqq n \text{ mit } F^m = id_K .$$

Sei m kleinst möglich gewählt.

Behauptung: $m = n$.

Beweis: Es gilt $x^{p^m} - x = 0$ für alle $x \in K$. Das Polynom

$$x^{p^m} - x$$

besitzt höchstens p^m verschiedene Nullstellen in K (benutze 18.2 und die Nullteilerfreiheit). Daraus folgt $\#K = p^n \leqq p^m$, also $n \leqq m$ und somit dann sogar $m = n$.

Korollar 25.1. *Für einen endlichen Körper K mit $q = p^n$ Elementen gilt $n = \#G(K/\mathbb{F}_p) = [K : \mathbb{F}_p]$*

$$G(K/\mathbb{F}_p) \;=\; \{id_K, F, \cdots, F^{n-1}\}$$

und die Erweiterung $K/\mathbb{F}_p$ ist galoissch. Insbesondere gilt

$$F^n(x) - x = x^{p^n} - x = 0 \quad , \quad \forall x \in K \ .$$

Beweis: Eine unmittelbare Folgerung aus 13.1 und der obigen Behauptung, welche $\#\{id, F, \cdots, F^{n-1}\} \geqq n = [K : \mathbb{F}_p]$ impliziert.

Korollar 25.2. *Ein endlicher Körper K mit $q = p^n$ Elementen ist isomorph zum Zerfällungskörper $K = (\mathbb{F}_p)_f$ des Polynoms*

$$f(x) \;=\; x^{p^n} \;-\; x \ .$$

Beweis: Das Polynom f ist separabel wegen $\frac{d}{dx} f(x) = -1$, und besitzt somit mindestens p^n verschiedene Nullstellen. Anderseits gilt $(\mathbb{F}_p)_f \subseteqq K$ wie bereits in Korollar 25.1 gezeigt. Wegen $\#K = p^n$ folgt daher $(\mathbb{F}_p)_f = K$.

Korollar 25.3. *Je zwei endliche Körper mit p^n Elementen sind isomorph.*

Beweis: Eine unmittelbare Folgerung aus Korollar 25.2 und 19.1.

Korollar 25.4. *Für $q = p^n$ (p prim), gibt es einen Körper mit q Elementen.*

Beweis: Betrachte den Zerfällungskörper $(\mathbb{F}_p)_f$ des Polynoms $f(x) = x^q - x$. Die q Nullstellen von f (siehe Beweis von Korollar 25.2) in $(\mathbb{F}_p)_f$ sind genau die Fixpunkte von F^n in $(\mathbb{F}_p)_f$. Da die Fixpunkte von F^n einen Teilkörper L definieren erhält man auf diesem Weg den gesuchten Körper L mit q Elementen. (Der Schluß von Korollar 25.2 zeigt dann sogar $L = (\mathbb{F}_p)_f$).

Wir bemerken, daß die Zwischenkörper $\mathbb{F}_p \subseteqq M \subseteqq F_{p^n}$ genau den Teilern von n entsprechen. (Die Galoisgruppe $G = G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ ist zyklisch von der Ordnung n).

Somit ist $\mathbb{F}_{p^n}$ auf keinen Fall die Vereinigung seiner echten Teilkörper. [Benutze: $\#\mathbb{F}_p + \mathbb{F}_{p^2} + \cdots + \mathbb{F}_{p^{n-1}} < 1 + p + \cdots + p^{n-1} = \frac{(p^n-1)}{(p-1)} \leqq p^n - 1 < \#\mathbb{F}_{p^n}$]. Somit gibt es ein $\alpha \in \mathbb{F}_{p^n} \setminus \bigcup$ Teilkörper $K \subsetneqq \mathbb{F}_{p^n}$. Es gilt

$$\#Orbit(\alpha) \;=\; n$$

und daher ist $\mathbb{F}_{p^n}$ der kleinste Teilkörper, welcher $\mathbb{F}_p$ und α enthält

$$\mathbb{F}_{p^n} \;=\; \mathbb{F}_p(\alpha)\ .$$

Korollar 25.5. *Jede endliche Körpererweiterung $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$ wird als Körper von einem Element erzeugt.*

Kapitel VI Permutationsgruppen

26 Satz von primitiven Element

Sei K ein obdA[8] unendlicher Körper und L/K eine galoissche Körpererweiterung mit $G = G(L/K)$.

Jeder Zwischenkörper M von L/K kann aus K durch Hinzunahme von endlich vielen Elementen $\alpha_1, \cdots, \alpha_k \in L$ gewonnen werden. D.h. M ist der kleinste Teilkörper von L, welcher K und die Elemente $\alpha_1, \cdots, \alpha_k$ enthält. (Wegen $[M : K] < \infty$ folgt die Existenz solche Elemente leicht durch Induktion).

Offensichtlich gilt dann

$$M \;=\; L^U \quad , \; U \;=\; G_{\alpha_1} \cap \cdots \cap G_{\alpha_r}$$

da jedes Elemet aus M sich als ein Bruch $f(\alpha_1, \cdots, \alpha_r)/g(\alpha_1, \cdots, \alpha_r)$ für Polynome $f, g \in K[X_1, \cdots, X_k]$ schreiben läßt.

Wir wollen zeigen, daß es ein $\alpha \in L$ gibt mit

$$M \;=\; K(\alpha) \; .$$

Ein solches Element α nennt man ein <u>primitives</u> Element von M. Beachte $\alpha \in M$. OBdA genügt es dazu den Fall $k = 2$ zu behandeln (und dann Induktion nach k zu benutzen).

<u>Ansatz</u>: $\alpha = \alpha_1 + \lambda\alpha_2$ für geeignetes $\lambda \in K$.

Offensichtlich gilt dann $G_{\alpha_1} \cap G_{\alpha_2} \subseteqq G_\alpha$.
Wir müssen λ so wählen, daß umgekehrt gilt

$$\sigma(\alpha_1 \;+\; \lambda\alpha_2) \;=\; \alpha_1 \;+\; \lambda\alpha_2 \quad , \; \sigma \in G$$

impliziert $\sigma(\alpha_1) = \alpha_1$ und $\sigma(\alpha_2) = \alpha_2$. Dies gilt aber automatisch im Fall

$$\lambda \;\neq\; \frac{(\xi - \alpha_1)}{(\alpha_2 - \eta)} \quad , \; \xi \in \mathit{Orbit}(\alpha_1), \; \alpha_2 \neq \eta \in \mathit{Orbit}(\alpha_2) \; .$$

Da es also nur gilt eine endliche Menge von Zahlen zu meiden, folgt die Existenz eines solchen λ bereits aus der Annahme, daß K unendlich viele Elemente enthält.

[8] wegen Korollar 25.5 sind die Aussagen dieses Abschnitts für endliche Körper bereits bewiesen.

27 Die Operation von G

Annahme 27.1. *Sei $f \in K[x]$ ein (normiertes) irreduzibles separables Polynom von Grad n und $L = K_f$ sein Zerfällungskörper. Die Erweiterung L/K ist dann galoissch mit der Galoisgruppe $G = G(L/K)$.*

Es gilt

$$f(x) \;=\; \prod_{i=1}^{n}(x \;-\; \alpha_i) \quad , \; \alpha_i \in L$$

und wegen $f^\sigma = f$, $\sigma \in G$ permutiert σ die Nullstellen $\alpha_1, \cdots, \alpha_n$. Dies definiert einen Gruppenhomomorphismus von G in die symmetrische Gruppe S_n

$$G \longrightarrow S_n \;=\; Bij(\{\alpha_1, \cdots, \alpha_n\}) \; .$$

Wir behaupten

Lemma 27.2. *Die Operation von G auf $\{\alpha_1, \cdots, \alpha_n\}$ ist transitiv, d.h. für je zwei α_i, α_j gibt es mindestens ein $\sigma \in G$ mit $\sigma(\alpha_i) = \alpha_j$.*

Beweis: ObdA $i = 1$. Wäre die Aussage falsch, folgt $Orbit(\alpha) = G \cdot \alpha \subsetneqq \{\alpha_1, \cdots, \alpha_n\}$ und $\prod_{\beta \in G\cdot\alpha}(x - \beta) \in K[X]$ wäre ein echter Teiler von f im Widerspruch zur Irreduzibiltät von f.

Lemma 27.3. *Die Abbildung $G \longrightarrow S_n$ ist injektiv.*

Beweis: Da $L = K_f$ ein Zerfällungskörper von f ist, ist jedes Element von L von der Gestalt $f(\alpha_1, \cdots, \alpha_n)/g(\alpha_1, \cdots, \alpha_n)$ für Polynome $f, g \in K[X_1, \cdots, X_n]$. Somit operiert $\sigma \in G$ trivial auf L, falls $\sigma(\alpha_i) = \alpha_i$ gilt für alle $i = 1, \cdots, n$.

Also ist die Abbildung $G \longrightarrow S_n$ injektiv.

Lemma 27.4. *Für die Untergruppe $G \hookrightarrow S_n$ sind äquivalent*

1. *Es gilt $G \hookrightarrow A_n$*
2. $\Delta(\alpha_1, \cdots, \alpha_n) \;=\; \prod_{i<j}(\alpha_i - \alpha_j) \;\in\; K$.

Beweis: 1) $\Rightarrow$ 2) ist offensichtlich. Sei umgekehrt $\Delta \in K$. Wäre $G \not\subset A_n$, dann existiert ein $\sigma \in G$ mit $\sigma(\Delta) = -\Delta$ in Widerspruch zur Annahme.

Bemerkung: $\Delta^2 \in K$.

Beispiel ($n = 3$): Die Galoisgruppe G der Zerfällungskörper L eines irreduziblen separablen kubischen Polynom f ist daher entweder zyklisch von der Ordnung 3

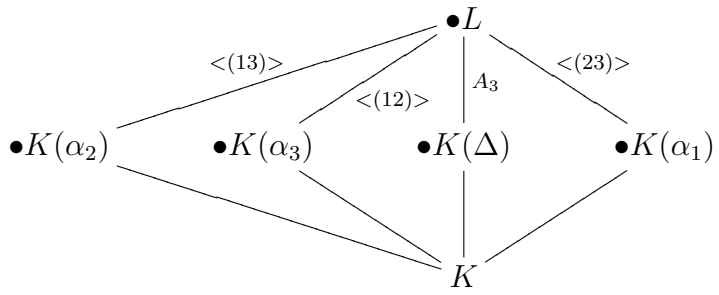
$$G \;=\; A_3 \;\cong\; \mathbb{Z}/3\mathbb{Z}$$

oder isomorph zur symmetrische Gruppe

$$G \;\cong\; S_3 \;,$$

je nach dem ob $\Delta^2 \in (K^*)^2$ oder $\Delta^2 \notin (K^*)^2$.

Im letzten Fall $\Delta^2 \notin (K^*)^2$ ergibt sich das Bild



Bemerkung: Man kann Δ^2 leicht aus den Koeffizienten des Polynoms $f(x)$ bestimmen. (Siehe Lemma 28.1). Im Fall $n = 3$ etwa ergibt sich für das Polynom $f(x) = x^3 + ax^2 + bx + c$

$$\Delta^2 \;=\; a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc \;.$$

Durch eine lineare Variablensubstitution kann man obdA annehmen $f(x) = x^3 + px + q$. Dann gilt:

$$\Delta^2 \;=\; -4p^3 \;-\; 27q^2 \;.$$

28 Die allgemeine Gleichung n-ten Grades

Sei R ein kommutativer Ring und $G = S_n$ die symmetrische Gruppe. Diese operiert auf dem Polynomring $R[x_1, \cdots, x_n]$ in n-Variablen vermöge

$$\tau(x_i) \;=\; x_{\tau^{-1}(i)} \quad , \; i = 1, \cdots, n \; .$$

Die Koeffizienten $\sigma_\nu(x_1, \cdots, x_n)$ des Polynoms

$$\prod_{\mu=1}^{n}(X - x_\mu) \;=\; \sum_{\nu=0}^{n}(-1)^\nu \sigma_\nu \cdot X^{n-\nu}$$

sind invariant unter G

$$\sigma_\nu \;\in\; R[x_1, \cdots, x_n]^G \; .$$

Lemma 28.1. *Es gilt* $R[x_1, \cdots, x_n]^G \;=\; R[\sigma_1, \cdots, \sigma_n]$.

Beweis: Induktion nach der lexikographischen Ordnung der Polynome nach dem Grad. Sei $f \in R[x_1, \cdots, x_n]$ G-invariant

$$f \;=\; r \cdot x_1^{m_1} \cdots x_n^{m_n} \;+\; \text{niedere Terme} \quad , \; (r \neq 0 \text{ in } R)$$

mit $m_1 \geqq m_2 \cdots \geqq m_n$. Dann ist

$$g \;=\; r \cdot \sigma_n^{m_n} \cdot \sigma_{n-1}^{m_{n-1}-m_n} \cdots \sigma_1^{m_1-m_2} \;=\; r \cdot x_1^{m_1} \cdots x_n^{m_n} + \text{ niedere Terme}$$

auch G-invariant. Somit ist $f - g \in R[x_1, \cdots, x_n]^G$ und von kleineren Grad als f. Somit nach Induktion in $R[\sigma_1, \cdots, \sigma_n]$.

Es folgt $f \in R[\sigma_1, \cdots, \sigma_n]$.

Bemerkung: Bei dem Einsetzungshomomorphismus

$$R[x_1, \cdots, x_n] \longrightarrow R[x_1, \cdots, x_{n-1}]$$

welcher x_n durch Null ersetzt gilt

$$\sigma_i \mapsto \sigma_i \quad , \quad i < n$$

$$\sigma_n \mapsto 0 \ .$$

Durch Induktion zeigt man damit leicht [9] die folgende Aussage: Ist ein Polynom $f(\sigma_1, \cdots, \sigma_n)$ der Variablen $\sigma_1, \cdots, \sigma_n$ aufgefaßt als Polynom in $R[x_1, \cdots, x_n]$ Null, dann ist bereits das Polynom $f \in R[\sigma_1, \cdots, \sigma_n]$ Null.
Das heißt, der Einsetzungshomomorphismus

$$R[\sigma_1, \cdots, \sigma_n] \longrightarrow R[x_1, \cdots, x_n]^G$$

$$\sigma_i \longmapsto \sigma_i(x_1, \cdots, x_n)$$

ist injektiv und surjektiv. Somit ist $R[x_1, \cdots, x_n]^G$ zum Polynomring $R[\sigma_1, \cdots, \sigma_n]$ isomorph.

Korollar 28.2. *Sei K ein Körper. Die symmetrische Gruppe $G = S_n$ operiert auf dem Quotientenkörper*

$$K(x_1, \cdots, x_n)$$

des Polynomringes $K[x_1, \cdots, x_n]$. Der Fixkörper ist der Quotientenkörper

$$K(\sigma_1, \cdots, \sigma_n)$$

des Polynomringes $K[\sigma_1, \cdots, \sigma_n]$.

Beweis: Klar ist die Inklusion $K(\sigma_1, \cdots, \sigma_n) \subseteq K(x_1, \cdots, x_n)$. Sei umgekehrt $f \in K(x_1, \cdots, x_n)^G$ und $f = g/h$ mit $g, h \in K[x_1, \cdots, x_n]$ oder

$$f \ = \ \frac{g \cdot \prod_{\sigma \neq id} \sigma(h)}{\prod_{\sigma \in G} \sigma(h)} \ = \ \frac{u}{v} \ .$$

Da $v \in K[x_1, \cdots, x_n]^G$ ist folgt aus der G-Invarianz von f also $u \in K[x_1, \cdots, x_n]^G$.
Das Korollar folgt somit aus dem vorigen Lemma.

Korollar 28.3. *S_n ist die Galoisgruppe der Erweiterung $K(x_1, \cdots, x_n)/K(\sigma_1, \cdots, \sigma_n)$.*

[9] Klammere die max. σ_n-Potenz aus und benutze, daß $x_1, \cdots, x_n$ keine Nullteiler in $R[x_1, \cdots, x_n]$ sind.

Korollar 28.4. *Jede endliche Gruppe U ist die Galoisgruppe einer Körpererweiterung.*

Beweis: Sei $n = \#U$, dann definiert die Operation von U auf U von links eine Injektion $U \hookrightarrow Bij(U) \cong S_n$. Die Körpererweiterung

$$K(x_1, \cdots, x_n)/K(x_1, \cdots, x_n)^U$$

ist Galoissch mit Galoisgruppe U.

Kapitel VII - Kreiskörper

Die n-ten Einheitswurzeln sind die Nullstellen des Polynoms $X^n - 1$, und damit die Lösungen ζ der Gleichung $\zeta^n = 1$. Im Körper der komplexen Zahlen sind die dies die Eckpunkte des regelmässigen n-Ecks auf dem Einheitskreis.

Adjungiert man zum Körper der rationalen Zahlen die n-ten Einheitswurzeln, d.h. betrachtet man den Zerfällungskörper des Polynoms $X^n - 1$ über dem Körper der rationalen Zahlen, dann erhält man den sogenannten Kreiskörper. Dies ist ein Galoisscher Erweiterungskörper von $\mathbb{Q}$. Das Hauptresultat dieses Kapitel ist die Bestimmung der Galoisgruppe dieser Körpererweiterung (eine abelsche Gruppe, wie sich herausstellen wird).

29 Einheitswurzeln

Sei K ein Körper und n eine natürliche Zahl. Es bezeichne $\mu_n(K)$ die Menge der n-ten Einheitswurzeln in K

$$\zeta \in \mu_n(K) \iff \zeta^n = 1 .$$

Beispiel 29.1.
$\mu_n(\mathbb{Q}) \subsetneqq \mu_n(\mathbb{R}) \subsetneqq \{\pm 1\}$.
$\mu_n(\mathbb{C}) = \{1, exp(\frac{2\pi i}{n}), \cdots, exp((n-1)\frac{2\pi i}{n})\}$.

Beachte, $\mu_n(K)$ ist eine Untergruppe der multiplikativen Gruppe K^* von K. Gilt $n = a \cdot b$, so sind $\mu_a(K)$ und $\mu_b(K)$ Untergruppen von $\mu_n(K)$.

Sind a und b teilerfremd, dann existieren ganze Zahlen α und β mit $\alpha a + \beta b = 1$ und es gilt

$$\begin{array}{c} \mu_n(K) \cong \mu_a(K) \times \mu_b(K) \\ \zeta \longmapsto (\zeta^b, \zeta^a) \end{array}$$

mit der Umkehrabbildung $(\zeta_1, \zeta_2) \mapsto \zeta_1^\beta \cdot \zeta_2^\alpha$. (Chinesischer Restsatz).

Satz 29.2. *Die Untergruppe $\mu_n(K)$ von K^* ist zyklisch.*

Beweis: Wegen der chinesischen Restsatzes genügt es den fall einer Primzahlpotenz zu betrachten. In diesem Fall genügt es wegen des Hauptsatzes für endlichen abelschen Gruppen zu zeigen, daß die Untergruppen der p-Torsionspunkte höchstens p Elemente besitzt.
Die Gruppe der p-Torsionspunkte in $\mu_n(K)$ ist aber gerade $\mu_p(K)$. Da die Gleichung

$$x^p - 1 = 0$$

in einen Körper K höchstens p Lösungen besitzt folgt die Behauptung.

Beispiel 29.3. $\mathbb{F}_p^* \cong (\mathbb{Z}/p\mathbb{Z})^*$ *ist zyklisch von der Ordnung p.*

allgemeiner

Satz 29.4. *Für einen endlichen Körper $\mathbb{F}_q$ mit q Elemente ist die multiplikative Gruppe $(\mathbb{F}_q)^*$ zyklisch von der Ordnung $q-1$.*

Beweis: Es gilt $(\mathbb{F}_q)^* = \mu_{q-1}(\mathbb{F}_q)$, da jedes Element in $\mathbb{F}_q^*$ der Gleichung $x(x^{q-1} - 1) = x^q - x = 0$ genügt.

30 Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^*$

Ist $n = a \cdot b$ eine Zerlegung von n in teilerfremde Zahlen a und b gilt nach dem chinesischen Restsatz

$$\mathbb{Z}/n\mathbb{Z} \;\cong\; \mathbb{Z}/a\mathbb{Z} \;\oplus\; \mathbb{Z}/b\mathbb{Z}$$

und daher für die Einheitengruppe

$$(\mathbb{Z}/n\mathbb{Z})^* \;\cong\; (\mathbb{Z}/a\mathbb{Z})^* \;\oplus\; (\mathbb{Z}/b\mathbb{Z})^* \;.$$

Sei daher $n = p^l$ eine Primzahlpotenz. Dann gilt folgender

Satz 30.1. *Ist $n > p^l$ eine Primzahlpotenz, dann gilt*

$$(\mathbb{Z}/p^l\mathbb{Z})^* \;\cong\; \mathbb{Z}/(p-1)\mathbb{Z} \;\times\; \mathbb{Z}/p^{l-1}\mathbb{Z} \quad (p \neq 2, l \geqq 1) \;,$$

$$(\mathbb{Z}/2^l\mathbb{Z})^* \;\cong\; \mathbb{Z}/2\mathbb{Z} \;\times\; \mathbb{Z}/2^{l-2}\mathbb{Z} \quad (p = 2, l \geqq 3) \;.$$

Zusatz 30.2. *Im Fall $p = 2$ wird die zyklische Gruppe der Ordnung 2^{l-2} in $(\mathbb{Z}/2^l\mathbb{Z})^*$ von der Restklassenpotenzen der Zahl 5 erzeugt.*

Trivial und für unsere Zwecke völlig ausreichend ist die Aussage über die Kardinalitäten $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

$$\varphi(ab) \;=\; \varphi(a)\varphi(b) \quad , \; (a,b) \;=\; 1$$

und

$$\varphi(p^n) \;=\; (p-1)p^{n-1} \quad , \; p \geqq 3$$

$$\varphi(2^l) \;=\; 2^{l-1} \quad .$$

Wir verzichten daher auf eine Beweis des obigen Satzes.

Beweisskizze (im Fall $p > 2$): Man hat im Ring $\mathbb{Z}/p^l\mathbb{Z}$ das von p erzeugte maximal Ideal mit dem Restklassen Homomorphismus

$$\mathbb{Z}/p^l\mathbb{Z} \;\twoheadrightarrow\; \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \;.$$

Offenischtlich bilden sich Einheiten auf Einheiten ab, und da jede zu p teilerfremde Zahl so auch zu p^l teilerfremd ist folgt

$$\pi : (\mathbb{Z}/p^l\mathbb{Z})^* \twoheadrightarrow \mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \ .$$

Der Kern dieser Abbildung besteht aus alle Elemente der Gestalt

$$1 - px \bmod p^l\mathbb{Z} \quad , \ (x \in \mathbb{Z}) \ .$$

Es genügt zu bemerken, daß jede solche Zahl modulo $p^l\mathbb{Z}$ ein Inverses besitzt, nämlich

$$1 + px + p^2x^2 + \cdots + p^{l-1}x^{l-1} \bmod p^l\mathbb{Z} \ .$$

Bestimmung von $Kern(\pi)$ Der ,,Logarithmus $log(1-px)$ "

$$1 - px \bmod p^l\mathbb{Z} \longmapsto \sum_{\nu=1}^{\infty}(-1)^{\nu-1}\frac{(xp)^\nu}{\nu} \bmod p^l\mathbb{Z}$$

ist ein expliziter Isomorphismus (im Fall $p \geqq 3$)

$$(Kern(\pi), \cdot) \ \cong \ (p\mathbb{Z}/p^l\mathbb{Z}, +) \ \cong \ \mathbb{Z}/p^{l-1}\mathbb{Z} \ .$$

Wir überlassen dies als Übungsaufgabe. Wegen $\#Kern(\pi) = p^{l-1} = \#(p\mathbb{Z}/p^l\mathbb{Z})$ genügt es die Surjektivität der Logarithmenabbildung und die Homomorphieeigenschaft zu zeigen (Sowie die Wohldefiniertheit!). Die erste Aussage zeigt man mit Hilfe einer ,,Exponentialabbildung".

Zusammenfassung: Da $Kern(\pi)$ und $\mathbb{F}_p^*$ abelsche Gruppen mit zueinander teilerfremde Ordnung sind, folgt für $p > 2$

$$(\mathbb{Z}/p^l\mathbb{Z})^* \ \cong \ Kern(\pi) \ \oplus \ Bild(\pi)$$

und daher

$$(\mathbb{Z}/p^l\mathbb{Z})^* \cong \ \mathbb{Z}/p^{l-1}\mathbb{Z} \ \oplus \ \mathbb{Z}/(p-1)\mathbb{Z}$$

bzw. wegen des chinesischen Restsatzes

$$(\mathbb{Z}/p^l\mathbb{Z})^* \ \cong \ \mathbb{Z}/p^{l-1}(p-1)\mathbb{Z} \ .$$

31 μ_n als Galoismodul

Sei L/K eine galoissche Körpererweiterung. Dann operiert $G = G(L/K)$ auf den n-ten Einheitswurzeln $\mu_n(L)$ von L.
Dabei gilt

$$ord(\zeta) \;=\; n \Longleftrightarrow ord(\sigma(\zeta)) \;=\; n$$

für alle $\sigma \in G$.

Bemerkung: Wie wir bereits wissen ist $\mu_n(L)$ eine zyklische Gruppe (29.2), somit erzeugt von einer Einheitswurzel $\zeta \in \mu_n(L)$. Indem man n durch $ord(\zeta)$ ersetzt, kann man annehmen $ord(\zeta) = n$. Das heißt oBdA gilt

$$\mu_n(L) \;= <\zeta> \cong\; \mathbb{Z}/n\mathbb{Z}\ .$$

Dann gilt offensichtlich

Lemma 31.1. *Für $\eta \in \mu_n(L)$ sind äquivalent*

(i) $<\eta> =\; \mu_n(L)$
(ii) $ord(\eta) \;=\; n$
(iii) $\eta \;= \zeta^m$ *für ein* $m \in \mathbb{N}$ *mit* $(m, n) = 1$.

Eine Einheitswurzel $\eta \in \mu_n(L)$ mit diesen äquivalenten Eigenschaften heißt primitive n-te Einheitswurzel.

Wir folgern daher, daß die Galoisgruppe primitive n-te Einheitswurzeln auf primitive n-te Einheitswurzeln abbildet. Das heißt für jedes $\sigma \in G$ gibt es ein $m = m(\sigma)$ so daß gilt

$$\sigma(\zeta) \;=\; \zeta^m \text{ mit } (m, n) = 1\ .$$

Die so definierte Galoisoperation auf $\mu_n(L)$ definiert daher einen Gruppenhomomorphismus

$$\phi : G \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

$$\sigma \longmapsto m(\sigma) \bmod n$$

von G in die Einheitengruppe des Ringes $\mathbb{Z}/n\mathbb{Z}$.

Zur Erinnerung: m ist invertierbar modulo n genau dann, wenn m und n teilerfremd sind (eine unmittelbare Folgerung aus dem Euklidischen Algorithmus).

Bemerkung 31.2. *Im Spezialfall, wo $L = K(\zeta)$ der Zerfällungskörper des Polynoms $x^n - 1$ über K ist, ist die Abbildung $\phi : G \to (\mathbb{Z}/n\mathbb{Z})^*$ injektiv. Man nennt dann L einen Kreiskörper über K erzeugt von den n-ten Einheitswurzeln.*

Beweis der Injektivität: Für $\sigma \in G(K(\zeta)/K) = G$ gilt

$$\phi(\sigma) \;=\; 1 \Longleftrightarrow \sigma(\zeta) = \zeta$$

oder damit

$$\sigma(\eta) \;=\; \eta \text{ für alle } \eta = \zeta^i \in \mu_n(K(\zeta)) \; .$$

Da G treu auf den Nullstellen η des Polynoms $f(x) = x^n - 1$ operiert (Lemma 27.3) ist somit $\phi(\sigma) = 1$ äquivalent zu $\sigma = id$.

32 Die Kreisgleichung über $\mathbb{Q}$

Sei

$$\phi_n(X) \;=\; \prod_{\zeta^n=1} (X-\zeta)\ ,\ \zeta \text{ primitiv}\ .$$

Offensichtlich gilt $\phi_n \in \mathbb{Q}[X]$.

Satz 32.1. *$\phi_n(X)$ ist über $\mathbb{Q}$ irreduzibel.*

Zum Beweis zeigen wir für jeden über $\mathbb{Q}$ irreduziblen Teiler f von ϕ_n:

$$(*) \quad f(\zeta) \;=\; 0 \Longrightarrow f(\zeta^l) \;=\; 0$$

für jede zu n teilerfremde Primzahl l.

Würde $(*)$ nicht gelten, folgt aus $\phi_n = f \cdot g$ dann $g(\zeta^l) = 0$, da ζ^l eine Nullstelle von ϕ_n ist. Somit wäre ζ eine Nullstelle von $g(X^l)$. Also

$$f \;=\; ggT(f, g(X^l))\ .$$

Falls $f, g \in \mathbb{Z}[X]$ [10] finden wir dann wie folgt einen Widerspruch:

Modulo l gilt [11] $\bar{g}(X)^l = \bar{g}(X^l)$, also wegen $\bar{g}^l = \bar{g}(X^l) = \bar{f} \cdot h \in \mathbb{F}_l[X]$

$$\bar{\phi}_n^l \;=\; \bar{f}^l \cdot \bar{g}^l \;=\; \bar{f}^{l+1} \cdot h\ .$$

Daraus folgt, daß $\bar{\phi_n}$ und damit $X^n - 1$ eine doppelte Nullstelle in einem geeigneten Erweiterungskörper von $\mathbb{F}_l$ besitzt.[12]
Dies steht im Widerspruch zu (beachte $ggT(n, l) = 1$!)

$$ggT(X^n - 1, nX^{n-1}) \;=\; 1 \quad (\text{in } \mathbb{F}_l[X])\ .$$

Beweis des Satzes. Sei ζ eine Nullstelle von f. Dann ist jede primitive n-te Einheitswurzel von der Gestalt ζ^m für eine zu n teilerfremde ganze Zahl. Wendet man (*) auf die Teiler von m an, zeigt dies, daß f und ϕ_n dieselben Nullstellen besitzen. Also gilt $f = \phi_n$ (bis auf eine Konstante).

[10] Dies folgt aus dem Gauß'schen Lemma!

[11] folgt aus dem kleinen Fermat

[12] Da f normiert ist, gilt $Grad_X(\bar{f}) = Grad_X(f) \geq 1$. $\bar{f}$ besitzt daher eine Nullstelle in einem Zerfällungskörper über $\mathbb{F}_p$.

Korollar 32.2. *Der Kreiskörper L der n-ten Einheitswurzeln über $\mathbb{Q}$ ist der Zerfällungskörper des Polynoms $\phi_n(X)$ über $\mathbb{Q}$. Für die Galoisgruppe G der Körpererweiterung $L/\mathbb{Q}$ gilt*

$$G \;\cong\; (\mathbb{Z}/n\mathbb{Z})^* \;.$$

Beweis: Da die primitiven n-ten Einheitswurzeln die Gruppe der n-ten Einheitswurzeln erzeugt, stimmen die Zerfällungskörper von $X^n - 1$ und $\phi_n(X)$ überein. Nach 31.2 gilt allgemein

$$\phi : G \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^* \;.$$

Anderseits gilt wegen $K = \mathbb{Q}$ und Satz 32.1

$$|G| \;\geqq\; deg_X(\phi_n) \;=\; \#(\mathbb{Z}/n\mathbb{Z})^*$$

und somit folgt, daß ϕ ein Isomorphismus ist.

33 Appendix (Das Gauß Lemma)

Für ein Polynom $f(X) \neq 0$ in $\mathbb{Q}[X]$ gibt es eine (bis auf das Vorzeichen) eindeutig bestimmte rationale Zahl $c(f) \in \mathbb{Q}^*$ so daß

$$f(X) \;=\; c(f) \cdot \sum_{i=0}^{n} a_i X^i \quad , \; a_i \in \mathbb{N}$$

gibt mit

$$ggT(a_0, \cdots, a_n) \;=\; 1 \; .$$

Lemma 33.1. *Für nicht verschwindende Polynome f, g in $\mathbb{Q}[X]$ gilt*

$$c(fg) = c(f) \cdot c(g) \; .$$

Beweis: OBdA $c(f) = c(g) = 1$. Dann ist $f \cdot g$ ganzzahlig und wir müssen nur zeigen, daß alle Koeffizienten von $f \cdot g$ teilerfremd sind. Wäre dies nicht der Fall gibt es ein Primzahl p mit

$$\overline{f \cdot g} \;=\; \bar{f} \cdot \bar{g} \;=\; 0 \quad \text{in } \mathbb{F}_p[X] \; .$$

Da $\mathbb{F}_p[X]$ nullteilerfrei ist, folgt $\bar{f} = 0$ oder $\bar{g} = 0$. Also ist entweder $c(f)$ oder $c(g)$ durch p teilbar im Widerspruch zur Annahme $c(f) = c(g) = 1$.

Das obige Argument benutzt das

Lemma 33.2. *Ist R nullteilerfrei, dann ist auch der Polynomring $R[X]$ nullteilerfrei.*

Beweis: Seien $f(X) = a_0 \cdot X^n + ..$ und $g(X) = b_0 \cdot X^m + ...$ nichtverschwindende Polynome vom Grad n resp. m. Dann gilt $a_0 \neq 0$ bzw. $b_0 \neq 0$ in R. Aus $0 = f(X) \cdot g(X) = a_0 b_0 \cdot X^{n+m} + ...$ würde folgen $a_0 b_0 = 0$. Wegen der Nullteilerfreiheit von R gilt daher $f(X)g(X) \neq 0$ in $R[X]$.

Kapitel VIII - Auflösbarkeit

Von historischer Bedeutung für das Lösen von Polynomgleichungen waren explizite Formel für die Nullstellen, welche in Termen von Wurzeln hingeschrieben werden können. Das klassische Beispiel ist die Formel von Vieta für die Nullstellen quadratischer Polynome. Ähnliche, aber komplizierte Formeln hat man für kubische Polynome und sogar für Polynome vierten Grades.

Es war eine bahnbrechende Leistung des Mathematikers N. Abel zu zeigen, dass es für die Nullstellen von Polynomen $f(X)$ fünften Grades im allgemeinen keine geschlossene Formeln mit iterierten Wurzeln mehr gibt. Gäbe es nämlich eine solche Formel, wäre der Zerfällungskörper von $f(X)$ in einem Turm von Radikalerweiterungen enthalten. Radikalerweiterung[13] entstehen durch Ziehen einer n-ten Wurzel aus einer Zahl, sind also Zerfällungskörper von Polynomen vom Typ $X^n - \alpha$.

Die Galoisgruppe des Zerfällungskörper eines solchen Radikalpolynoms, ist im Fall $\alpha = 1$ (Kreisgleichung) abelsch, im allgemeinen Fall fast abelsch (nämlich auflösbar). Tatsächlich kann man zeigen, dass der Zerfällungskörper eines separablen Polynoms f genau dann in einem Turm von Radikalerweiterungen liegt, wenn die Galoisgruppe des Zerfällungskörpers auflösbar ist. Der Satz von Abel reduziert sich damit auf die Aussage, dass die symmetrische Gruppe S_5 nicht auflösbar ist (es genügt dazu, dass der Normalteiler A_5 nicht auflösbar ist).

[13]Radikal kommt hier vom Wort Radix=Wurzel, da eine n-te Wurzel gezogen wird.

34 Radikalerweiterungen I

Sei n eine natürliche Zahl und K ein Körper. Wir machen die

Annahme 34.1. $char(K) \not| n$

Wir bemerken, daß für $a \in K$ und $char(K) \not| n$ das Radikalpolynom

$$f(X) = X^n - a$$

separabel über K ist. Auf Grund der obigen Annahme ist der Zerfällungskörper L des Polynoms

$$X^n - a \ , \ a \in K^*$$

daher eine galoissche Körpererweiterung von K.

Ist $\alpha \in L$, $\alpha^n = a$ eine Nullstelle des Polynoms, dann zeigt man mit Hilfe der Substitution $X \mapsto \alpha \cdot X$ leicht

$$X^n - a = \prod_{\zeta} (X - \zeta\alpha),$$

wobei das Produkt die Nullstellen ζ des Polynoms $X^n - 1$ durchläuft.

Folgerung 34.2. *Für den Zerfällungskörper L des Polynoms $X^n - a$ über K gilt:*

$$L = K(\zeta, \alpha)$$

wobei ζ eine positive n -te Einheitswurzel ist und α eine Nullstelle des Polynoms $X^n - a$ ist.

$$\begin{array}{c} L \\ | \\ K(\zeta) = K' \\ | \\ K \end{array}$$

Wir wissen bereits, daß $K(\zeta)/K$ galoissch ist mit abelscher Galoisgruppe (31.2).

Da L/K galoissch ist, ist auch L/K' galoissch. Wegen

$$L \ = \ K'(\alpha)$$

operiert die Galoisgruppe $G' = G(L/K')$ treu auf den Nullstellen des Polynoms $X^n - a$. Das heisst

$$\tau(\alpha) = \alpha \ \Rightarrow \tau = id$$

für $\tau \in G'$.

Lemma 34.3. *Die Galoisgruppe G' der Körpererweiterung L/K' ist abelsch und als Untergruppe der zyklischen Gruppe*

$$G' \hookrightarrow \mathbb{Z}/n\mathbb{Z}$$

sogar zyklisch.

Beweis: Für $\tau \in G$ gilt wegen $a \in K$

$$\tau(\alpha)^n \ = \ \tau(\alpha^n) \ = \ \tau(a) \ = \ a \ .$$

Somit folgt

$$\tau(\alpha) \ = \ \zeta_\tau \cdot \alpha$$

für ein $\zeta_\tau \in \mu_n(L) = \mu_n(K')$.

Für $\sigma, \tau \in G$ gilt

$$\sigma(\tau(\alpha)) \ = \ \sigma(\zeta_\tau \cdot \alpha) \ = \ \sigma(\zeta_\tau) \cdot \zeta_\sigma \cdot \alpha$$

oder mit anderen Worten ($a \neq 0, \alpha \neq 0$).

$$\zeta_{\sigma\tau} \ = \ \sigma(\zeta_\tau) \cdot \zeta_\sigma \ .$$

Spezialisiert man dies auf den Fall $\sigma, \tau \in G'$, folgt wegen $\zeta_\tau \in \mu_n(L) = \mu_n(K')$, daß

$$G' \longrightarrow \mu_n(K') \cong \mathbb{Z}/n\mathbb{Z}$$

$$\tau \longmapsto \zeta_\tau \ .$$

einen Gruppenhomomorphismus definiert. Wie bereits erwähnt gilt für $\tau \in G'$ aber $\tau = id \Leftrightarrow \tau(\alpha) = \alpha \Leftrightarrow \zeta_\tau = 1$. Somit ist die konstruierte Abbildung injektiv.

Übungsaufgabe 34.4. *Ist $m = |G'|$, dann ist L der Zerfällungskörper von $X^m - b$ über K', wobei $b^d = a$ für $n = d \cdot m$ und $b \in K'$.*

35 Radikalerweiterungen II

Wir betrachten nun eine Umkehrung der Aussage des letzten Abschnitts.

Annahme 35.1. *Sei K' ein Körper und $m \in \mathbb{N}$ gegeben mit den Eigenschaften*

- $char(K') \nmid m$
- $\mu_m(K') \cong \mathbb{Z}/m\mathbb{Z}$.

(Das heißt K' enthält alle m-ten Einheitswurzeln).

Bemerkung: Wir haben hier die Situation von $K' = K(\zeta)$ von VIII.1.3 im Auge. Mit den Bezeichnungen von 34.3 und 34.4 ist nämlich Annahme 35.1 erfüllt für jeden Teiler m von n, insbesondere also für $m = |G'|$ mit den Bezeichnungen aus 34.4.

Diagramm:

$$\begin{array}{c} L \\ | \\ | \ \mathbb{Z}/m\mathbb{Z} \\ | \\ K \end{array} \qquad , \quad \mu_m(K') \cong \mathbb{Z}/m\mathbb{Z} \ .$$

Sei nun L/K' eine zyklische Körpererweiterung mit Galoisgruppe $G' = G(L/K') \cong \mathbb{Z}/m\mathbb{Z}$, dann gilt

Satz 35.2. *Es gibt ein $b \in K'$, so daß L isomorph ist zum Zerfällungskörper des Polynoms*

$$X^m - b$$

über K'.

Beweis: Wir wählen eine primitive m-te Einheitswurzel ζ in K' und machen den Ansatz

$$\alpha \ = \ \sum_{i=0}^{m-1} \ \zeta^{-i} \cdot \tau^i(y)$$

wobei $y \in L$ und τ ein Erzeuger der zyklischen Gruppe G' ist.

Behauptung: $b = \alpha^m \in K'$ und $L = K'(\alpha)$, falls $\alpha \neq 0$.
Es gilt

$$\tau(\alpha) \;=\; \sum_{i=0}^{m-1} \zeta^{-i}\tau^{i+1}(y) \;=\; \zeta \cdot \sum_{i=0}^{m-1} \zeta^{-i} \cdot \tau^i(y) \;,$$

also

$$\tau(\alpha) \;=\; \zeta \cdot \alpha \;.$$

Daraus folgt für $b := \alpha^m$

$$b \;=\; \alpha^m \;\in\; K'$$

wegen $\tau(b) = \tau(\alpha^m) = \tau(\alpha)^m = \zeta^m\alpha^m = \alpha^m = b$ für alle $\tau \in G'$. Somit ist α eine Nullstelle von $f(X) = X^m - b \in K'[X]$, ebenso wie die Konjugierten $\tau(\alpha), \tau^2(\alpha), \cdots$. Wegen $\tau^i(\alpha) = \zeta^i \cdot \alpha$ liefert dies alle m Nullstellen von $f(X)$. Also ist$L$ der Zerfällungskörper L' [14] von $X^m - b$ über K'. Offensichtlich gilt $K' \subseteq L' \subseteq L$.

Beachte $[L : K'] = |G'| = m$ und $[L' : K'] = |G(L'/K')| \geqq m$, da die Automorphismen $id, \tau, \tau^2, \cdots$ eingeschränkt auf $L' = K'(\alpha)$ alle verschieden sind wegen

$$\tau^i(\alpha) \;=\; \zeta^i \cdot \alpha$$

Dazu ist aber nötig: $\alpha \neq 0$.

Wegen der linearen Unabhängigkeit der Automorphismen $1, \tau, \tau^2, \cdots$ ist es aber immer möglich $y \in L$ a priori so zu wählen, daß $\alpha \neq 0$ gilt (II.2.3).

[14] $f(X)$ ist separabel nach 35.1 wegen 34.1. Somit ist L'/K' galoissch.

36 Quotientengruppen

Sei G eine Gruppe und H eine Untergruppe von G. Wir definieren auf G eine Äquivalenzrelation durch

$$g_1 \ \sim_H \ g_2 \Leftrightarrow \exists\ h \in H\ ,\ g_1 = h \cdot g_2\ .$$

Die Menge der Äquivalenzklassen bezeichnen wir mit $H\backslash G$. Eine Äquivalenzklasse bezeichnen wir mit $H \cdot g$. Ist G endlich, gilt offensichtlich $|G| = |(H\backslash G)| \cdot |H|$.

Sei nun H ein Normalteiler in G. Wir schreiben dann auch

$$H \ \lhd \ G\ .$$

In diesem Fall kann man auf $H\backslash G$ in natürlicher Weise eine Gruppenstruktur definieren durch

$$Hg_1 \cdot Hg_2 \ = \ Hg_1g_2\ .$$

Wir müssen uns davon überzeugen, daß dies wohldefiniert ist:

Seien g_1' und g_2' so daß gilt $Hg_i = Hg_i'$. Dann gilt $g_i' = h_ig_i$ und somit $g_1'g_2' = h_1g_1 \cdot h_2g_2 = (h_1g_1 \cdot h_2g_1^{-1})g_1g_2$. Da $h_1 \in H$ und $g_1h_2g_1^{-1} \in H$ (Normalteiler !) folgt die Wohldefiniertheit

$$g_1'g_2' \ \in \ Hg_1g_2\ .$$

Es folgt dann sofort klar, daß $H \cdot 1$ das neutrale Element der Gruppe $H\backslash G$ ist und Hg^{-1} das inverse Element von Hg. Das Assoziativgesetz gilt automatisch. Mehr noch:

Die Abbildung

$$\pi_H : G \longrightarrow H\backslash G$$

$$g \longmapsto H \cdot g$$

ist ein surjektiver Gruppenhomomorphismus mit Kern $Kern(\pi_H) = H$.

Folgerung 36.1. *Für jeden Normalteiler $H \lhd G$ gibt es einen surjektiven Gruppenhomomorphismus $\pi_H : G \longrightarrow H\backslash G$ mit Kern H.*

Wir bemerken, daß der Kern eines Gruppenhomomorphismus

$$\pi : G \longrightarrow G'$$

immer ein Normalteiler in G ist

$$Kern(\pi) \ \lhd \ G$$

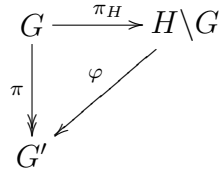
wegen $\pi(ghg^{-1}) = \pi(g)\pi(h)\pi(g^{-1}) = \pi(g)\pi(g^{-1}) = \pi(1) = 1$ für alle h aus $Kern(\pi)$.

Lemma 36.2. *Ist $\pi : G \twoheadrightarrow G'$ ein surjektiver Gruppenhomomorphismus, dann gilt*

$$G' \ \cong \ Kern(\pi)\backslash G$$

für den Normalteiler $H = Kern(\pi)$ in G.

Beweis: Dies folgt aus der "universellen Eigenschaft von Quotienten", welche wie im LAII Skript bewiesen wird:



Wir setzen $\varphi(H \cdot g) = \pi(g)$. Dies ist ein wohldefinierte surjektiver Gruppenhomomorphismus. Wegen $\varphi(H \cdot g) = 1 \Leftrightarrow g \in H \Leftrightarrow \pi(g) = 1$ ist φ auch injektiv, also ein Isomorphismus

$$\varphi : H\backslash G \xrightarrow{\sim} G'$$

Lemma 36.3. *Das Zentrum $Z(G) = \{g \in G | gh = hg \ \forall \ h \in G\}$ ist ein Normalteiler von G.*

Beweis: Trivial.

37 Anwendung auf Galoiserweiterungen

Ist L/K eine galoissche Körpererweiterung mit Galoisgruppe G und K'/K eine galoissche Körpererweiterung mit Galoisgruppe G' so, daß gilt

$$K \subseteq K' \subseteq L \ .$$

Nach §17, Aussage **(4)** gilt dann für jedes $\sigma \in G$

$$\sigma(K') \ = \ K' \ .$$

Somit definiert

$$\pi : G \longrightarrow G'$$
$$\sigma \longrightarrow \sigma|K'$$

einen Gruppenhomomorphismus. Nach Lemma 36.1 ist π surjektiv. Der Kern besteht aus allen Automorphismen von L/K, welche auf K' die Identität sind, also aus $Gal(L/K')$.

Aus 36.2 folgt

Folgerung 37.1. *Für $K \subseteq K' \subseteq L$ und K'/K sowie L/K galoissch gilt*

$$\boxed{Gal(K'/K) \ \cong \ Gal(L/K')\backslash Gal(L/K)} \ .$$

38 Auflösbare Gruppen

Definition 38.1. *Eine Gruppe G heißt auflösbar, wenn es eine aufsteigende Kette von Untergruppen*

$$1 \subseteq U_1 \subseteq U_2 \cdots \subseteq U_n = G$$

gibt, so daß gilt

- $U_{i-1} \lhd U_i$ *(Normalteiler)*
- $U_{i-1} \backslash U_i$ *ist eine zyklische Gruppe.*

Da in einer abelschen Gruppe jede Untergruppe ein Normalteiler ist, folgert man leicht aus dem Hauptsatz für endliche abelsche Gruppen:

Beispiel 38.2. *Jede abelsche Gruppe ist auflösbar.*

Lemma 38.3. *Ist $H \lhd G$ ein Normalteiler und $\pi : H \longrightarrow H\backslash G \cong Q$ der Quotientenhomomorphismus. Dann sind äquivalent:*

(i) G ist auflösbar
(ii) H und Q sind auflösbar.

Wir skizzieren den

Beweis: $(i) \Rightarrow (ii)$
Die Gruppen $\pi(U_i) = V_i$ bilden eine aufsteigende Kette von Untergruppen $1 \subseteq V_1 \subseteq V_2 \cdots \subseteq V_n = Q$ in Q mit $V_{i-1} \lhd V_i$ und $V_{i-1}\backslash V_i$ zyklisch.

$$\begin{array}{ccccc} U_{i-1} & \longrightarrow & U_i & \twoheadrightarrow & U_{i-1}\backslash U_i \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & \vdots{\scriptstyle \pi} \\ V_{i-1} & \longrightarrow & V_i & \overset{\pi}{\twoheadrightarrow} & V_{i-1}\backslash V_i \end{array}$$

Analog zu LAII konstruiert man nämlich eine Abbildung

$$\pi : U_{i-1}\backslash U_i \longrightarrow V_{i-1}\backslash V_i$$

$$U_{i-1} \cdot g \longmapsto V_{i-1} \cdot \pi(g)$$

Dies ist ein surjektiver Gruppenhomomorphismus. Da $U_{i-1}\backslash U_i$ zyklisch ist, ist somit der Quotient $V_{i-1}\backslash V_i$ wieder zyklisch. Daß V_{i-1} ein Normalteiler in V_i folgt aus $v_i V_{i-1} v_i^{-1} = \pi(u_i)\pi(U_{i-1})\pi(u_i)^{-1} = \pi(u_i U_{i-1} u_i^{-1}) \subseteq \pi(U_{i-1}) = V_{i-1}$. Es folgt, daß Q auflösbar ist.

Analog definiert $V_i' = U_i \cap H$ eine aufsteigende Kette $1 \subseteq V_1' \subseteq V_2' \cdots \subseteq V_n' = H$ von Untergruppen von H. Es gilt offensichtlich $V_{i-1}' \lhd V_i'$ und

$$V_{i-1}'\backslash V_i' \longrightarrow V_{i-1}\backslash V_i$$

$$V_{i-1}' \cdot v_i' \longmapsto V_{i-1} \cdot v_i'$$

definiert einen injektiven Gruppenhomomorphismus. Somit ist $V_{i-1}'\backslash V_i'$ als Untergruppe der zyklischen Gruppe $V_{i-1}\backslash V_i$ wieder zyklisch. Somit ist H auflösbar.

$(ii) \Rightarrow (i)$
Seien H und Q auflösbar und $1 \subseteq V_1' \subseteq V_2' \cdots \subseteq V_m' = H$ resp. $1 \subseteq V_1 \subseteq V_2 \cdots \subseteq V_n = Q$ die entsprechenden aufsteigenden Ketten.

Dann definiert

$$\begin{aligned} U_i &= V_i' \qquad i = 1, \cdots, m \\ U_{m+j} &= \pi^{-1}(V_j) \qquad j = 1, \cdots, n \end{aligned}$$

eine aufsteigende Kette von Untergruppen in G mit den gewünschten Eigenschaften. Die surjektive Abbildung

$$U_{m+j-1}\backslash U_{m+j} \twoheadrightarrow V_{j-1}\backslash V_j$$

definiert durch

$$U_{m+j-1} \cdot u \longmapsto V_{j-1} \cdot \pi(u)$$

ist ein injektiver Gruppenhomomorphismus. Somit ist die linke Seite $U_{m+j-1}\backslash U_{m+j}$ isomorph zu$V_{j-1}\backslash V_j$, also zyklisch. Man zeigt leicht, daß die Kette

$$1 \subseteq U_1 \subseteq \cdots \subseteq U_{m+n} = G$$

die gewünschten Eigenschaften $U_{i-1} \lhd U_i$ und $U_{i-1}\backslash U_i$ zyklisch besitzt. Somit ist G auflösbar.

39 Auflösbare Körpererweiterungen

Eine galoissche Körpererweiterung L/K heißt auflösbar, wenn die Galoisgruppe $G = Gal(L/K)$ eine auflösbare Gruppe ist.

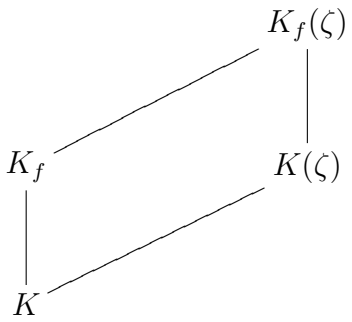
Beispiel: $K(\zeta)/K$ ist auflösbar, wenn $\zeta = \zeta_n$ eine primitive n-te Einheitswurzel ist (falls n eine zur Charakteristik von K teilerfremde Zahl ist).

Mit diese Bezeichnungen gilt

Lemma 39.1. *Äquivalent sind für eine galoissche Körpererweiterung L/K mit $L = K_f$*

(i) K_f/K *auflösbar.*
(ii) $K_f(\zeta)/K$ *auflösbar.*
(iii) $K_f(\zeta)/K(\zeta)$ *auflösbar.*

Beachte: $K_f(\zeta) = K_{(X^n-1)f}$ ist galoissch über K.



Beweis: Eine unmittelbare Folgerung aus Lemma 38.3.

40 p -Sylowsätze

Eine Untergruppe $P \subseteqq G$ eine endlichen Gruppe G heißt p -Sylowgruppe, wenn p teilerfremd zu $|G|/|P|$ ist und $|P|$ eine Potenz von p ist.

Satz 40.1. *G besitzt p -Sylowgruppen für jede Primzahl p.*

Beweis: Wir schließen durch Induktion nach $|G|$. Für abelsche Gruppen folgt die Aussage unmittelbar aus dem Hauptsatz für endlich erzeugte abelsche Gruppen. Somit gilt die Aussage für das Zentrum $Z(G)$ von G.

Sei $Z_p(G)$ die p -Sylowgruppe von $Z(G)$. Offensichtlich ist dann $Z_p(G)$ ein Normalteiler

$$Z_p(G) \ \lhd \ G \ .$$

Sei $\pi : G \longrightarrow Q = G/Z_p(G)$ die Quotientenabbildung. Dann ist $P = \pi^{-1}(P_Q)$ eine p-Sylowgruppe von G, falls P_Q eine p-Sylowgruppe von Q ist. Per Induktion können wir daher annehmen, daß $Z_p(G) = \{1\}$ trivial ist. Mit anderen Worten:

$$\text{obdA} \ \ (|Z(G)|, p) \ = \ 1 \ .$$

Wir betrachten nun die Konjugationsoperation von G auf G. Es gilt

$$|G| \ = \ |Z(G)| \ + \ \sum_x |G|/|G_x| \ ,$$

wobei die Summe über Konjugationsklassen von G erstreckt wird für die gilt $G_x \neq G$.

ObdA gilt weiterhin $p \,||G|$, da anderenfalls die Aussage des Satzes trivial ist.

Folgerung 40.2. *Für mindestens eine Konjugationsklasse x gilt*

$$(p, |G|/|G_x|) \ = \ 1$$

wegen $p \mid |G|$ und $p \not| \, |Z(G)|$.

Eine p-Sylowgruppe von G_x, welche wegen $G_x \nsubseteqq G$ per Induktion existiert, ist somit auch eine p -Sylowgruppe von G.

□

Satz 40.3. *Je zwei p -Sylowgruppen P und P' einer endlichen Gruppe G sind konjugiert.*

Beweis: Betrachte die Operation von P auf $X = G/P'$ durch Multiplikation von links. Wegen

$$(p\ ,\ |X|)\ =\ 1\ ,$$

und da die Orbiten der p -Sylowgruppe P entweder aus Fixpunkten bestehen oder eine durch p teilbare Kardinalität besitzen folgt

$$|X|\ =\ |\text{P-Fixpunkte in X}| \bmod p\ .$$

Aus $p \not| |X|$ folgt daher die Existenz eines Fixpunktes gP' in X. Mit anderen Worten:

$$P \cdot g \cdot P'\ =\ g \cdot P'$$

beziehungsweise $\forall p \in P\ \exists p' \in P'$ mit $p \cdot g = g \cdot p'$.
Damit gilt $g^{-1}Pg \subseteq P'$ und aus Kardinalitätsgründen $g^{-1}Pg = P'$. □

Analog zeigt man folgende

Variante: *Jede p -Gruppe P von G ist in einer p -Sylowgruppe enthalten.*

Beweis: Wie oben zeigt man, daß gPg^{-1} für geeignetes $g \in G$ in einer gegebenen p -Sylowgruppe P' enthalten ist. Somit ist P in der p -Sylowgruppe $g^{-1}P'G$ von G enthalten.

41 Die Gruppe A_5

In einer auflösbaren endlichen Gruppe G gilt [15]:

$$[G, G] \subsetneqq G \ .$$

Wir zeigen

Lemma 41.1. $[A_5, A_5] = A_5$ *oder* $[A_n, A_n] = A_n$ *für* $n \geqq 5$

und folgern daraus

Lemma 41.2. A_5 *und damit auch* S_5 *sind nicht auflösbare Gruppen.*

Beweisansatz: Jedes Element von A_n schreibt sich als Produkt von einer geraden Anzahl von Transpositionen.
Es genügt daher

$$(a\ b)\ (c\ d)\ \in\ [A_n, A_n]$$

Zwei Fälle:

- $b = c$, dann gilt $(a\ b)(c\ d)\ =\ (abc)$
- a, b, c, d paarweise verschieden, dann gilt

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd) \ .$$

Es genügt daher

$$(abc) \in [A_n, A_n] \ .$$

Aber

$$(abc)\ =\ [(ac)(de)\ ,\ (cb)(de)]\ \in [A_n, A_n]$$

für paarweise verschiedene Elemente a, b, c, d, e! □

[15] in einer Normalteilerkette $\{1\} \subsetneqq U_1 \subsetneqq U_2 \cdots \subsetneqq U_n = G$ mit $U_{i-1} \lhd U_i$ und zyklischen Subquotienten U_i/U_{i-1} gilt notwendigerweise $[G, G] \subseteqq U_{n-1}$.

42 Dreiteilung des Winkels

Es gilt

$$\cos(3\alpha) \;=\; 4\cos(\alpha)^3 \;-\; 3\cos(\alpha)$$

und somit führt die Dreiteilung des Winkels $\beta = 3\alpha$ auf die Lösung einer Gleichung

$$4X^3 - 3X - a \;=\; 0$$

oder für $Y = 2X$

$$Y^3 - 3Y - 2a \;=\; 0\ .$$

Ist a ganz und $a = 2$, so ist die obige Gleichung irreduzibel über $\mathbb{Q}$, da $Y = \pm 1, \pm 2, \pm 4$ keine Nullstellen sind (Lemma von Gauß).

Folgerung: *Im allgemeinen ist die Dreiteilung eines Winkels mit Zirkel und Lineal nicht möglich.*

43 Körper der mit ZL konstruierte Punkte

$z, w \in \mathbb{C}$ konstruierbar $\Rightarrow z \pm w$ konstruierbar $\Rightarrow z/w$ konstruierbar.
Wegen Winkeladdition ObdA $z, w \in \mathbb{R}$.
Dann schließt man aus dem Struktursatz $\frac{x}{a} = \frac{z}{w}$. Setze $a = 1$, dann ist x der gesuchte Punkt.

Kapitel IX - Differentiale

44 Universelle Derivationen

Sie $R \to S$ ein Ringhomomorphismus und sei M ein S-Modul (und somit auch ein R-Modul).

Wir betrachten die Gruppe $Der_R(S, M)$ der R-Derivationen

$$D : S \to M \ ,$$

d.h. R-lineare Abbildungen mit der Eigenschaft

$$(*) \quad D(s_1 \cdot s_2) \ = \ s_1 \cdot D(s_2) + s_2 \cdot D(s_1) \ .$$

Bemerkung: Es folgt $D(r) = r \cdot D(1) + 1 \cdot D(r)$ und wegen der R-Linearität somit $D(r) = 0$ für alle $r \in R$. Umgekehrt ist eine additive Abbildung mit der Eigenschaft $(*)$ eine R-Derivation, falls gilt $D(r) = 0$ für $r \in R$.

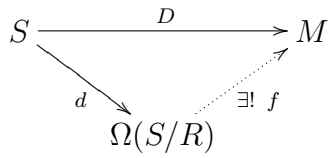
Bemerkung: Aus $(*)$ folgt durch Induktion nach n sofort

$$D(s^n) \ = \ n \ \cdot s^{n-1} \ \cdot D(s).$$

Satz 44.1. *Es gibt eine universelle R-Derivation*

$$d : S \to \Omega(S/R)$$

so, daß jede andere R-Derivation $D : S \to M$ durch eine eindeutig bestimmte S-lineare Abbildung $f : \Omega(S/R) \to M$ induziert wird



Beweis: Setze $\Omega(S/R) \ = \ \bigoplus_{s \in S} S \cdot ds/(Relationen)$, wobei geteilt wird durch den von den Relationen $(*)$

$$d(s_1 \cdot s_2) \ = \ s_1 \cdot ds_2 + s_2 \cdot ds_1$$

$$d(s_1 + s_2) \ = \ ds_1 + ds_2$$

$$dr \;=\; 0\ ,\ r \in R$$

erzeugten S-Untermodul von $\bigoplus_{s\in S} S \cdot ds$. Setze $d : s \mapsto ds$. Die universelle Eigenschaft von $\Omega(S/R)$ folgt dann unmittelbar aus der universellen Eigenschaft von Quotienten.

Für die Gruppe der R-Derivation gilt also

$$Der_R(S, M) \;\cong\; Hom_S(\Omega(S/R), M)\ .$$

Bemerkung 44.2. *Es gilt $Der_R(S, M) = 0$ für alle S-Moduln M dann und nur dann, wenn gilt $\Omega(S/R) = \{0\}$. (Setze nämlich $M = \Omega(S/R)$).*

Bemerkung 44.3. *Aus der Konstruktion von $\Omega(S/R)$ folgt $\Omega(S/R) = 0$, falls $R \to S$ surjektiv ist.*

Behauptung 44.4. *Für den Polynomring $S = R[X]$ ist*

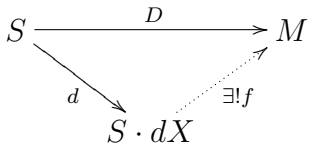
$$\Omega(S/R) \;=\; S \cdot dX$$

ein freier S-Modul vom Rang 1.

Beweis: Sei $D : S \to M$ eine R-Derivation, dann gilt für $s = \sum a_i X^i, a_i \in R$

$$D(\sum_i a_i X^i) \;=\; \sum_i a_i \cdot i \cdot X^i \cdot D(X).$$

Setzt man daher $ds = \sum a_i\ i\ X^i \cdot dX \in S \cdot dX$



so folgt aus der Freiheit des Moduls $S \cdot dX$, daß $f(s \cdot dX) = s \cdot D(X)$ wohldefiniert ist. Dies zeigt die universelle Eigenschaft.
Mit anderen Worten: Die universelle R-Derivation auf $R[X]$ wird einfach durch formales Ableiten nach X gegeben!

$$df(X) \;=\; f'(X) \cdot dX$$

45 Die Quotientenregel

Lemma 45.1. *Für Lokalisierungsabbildungen $R \to R_S$ gilt $\Omega(R_S/R) = 0$.*

Allgemeiner sogar

Lemma 45.2. *Es gilt $\Omega(R_S/R') = R_S \otimes_R \Omega(R/R')$ für beliebige Ringhomomorphismen $R' \to R$. Genauer: Man hat ein kommutatives Diagramm*

$$\begin{array}{ccc} R & \xrightarrow{\quad d \quad} & \Omega(R/R') \\ \downarrow & & \downarrow{\scriptstyle 1\otimes_R id} \\ R_S & \xrightarrow{\exists!\ ds} & R_S \bigotimes_R \Omega(R/R') \end{array}$$

Beweis: Beachte, Regel $(*)$ angewendet auf $s \cdot r/s = r$ für eine beliebige Derivation $D : R_S \to M$ impliziert

$$D(r/s) \;=\; s^{-1} \cdot D(r) - r/s^2 \cdot D(s)\ .$$

Dies erzwingt den Ansatz

$$d_S(r/s) = s^{-1} \otimes_R dr - r/s^2 \otimes_R ds\ .$$

Mehr noch : Zwei Derivationen $D_i : R_S \to M$ welche auf R übereinstimmen sind gleich. Man muß zeigen, daß der Ansatz wohldefiniert ist und eine R'-Derivation $d_S : R_S \to R_S \bigotimes_R \Omega(R/R')$ liefert.

Wohldefiniertheit: Es gilt für $s, \tilde{s} \in S$ und $r \in R$

$$\begin{aligned} d_S(r\tilde{s}/s\tilde{s}) \;&=\; (s\tilde{s})^{-1} \otimes_R d(r\tilde{s}) \;-\; r\tilde{s}/(s\tilde{s})^2 \otimes_R d(s\tilde{s}) \\ =\; (s\tilde{s})^{-1} \otimes_R (\tilde{s}dr + rd\tilde{s}) \;&-\; r\tilde{s}/(s\tilde{s})^2 \otimes_R (sd\tilde{s} + \tilde{s}ds) \\ =\; s^{-1} \otimes_R dr \;&-\; r/s^2 \otimes_R ds \\ =\; d_S(r/s).& \end{aligned}$$

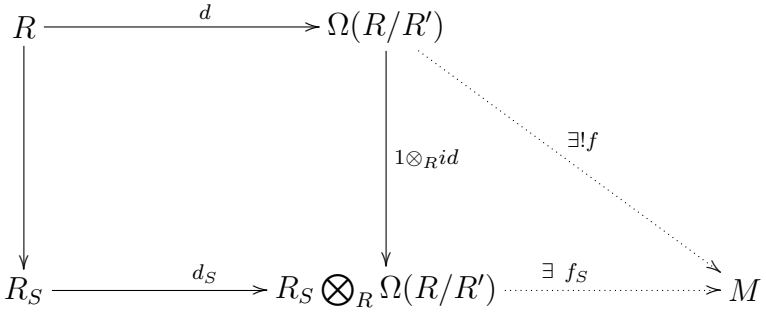
Dies genügt, da $(r\tilde{s} - \tilde{r}s)\tilde{\tilde{s}} = 0$ impliziert

$$r/s \;\sim\; r\tilde{\tilde{s}}s/s\tilde{\tilde{s}}s \;\sim\; \tilde{r}s\tilde{\tilde{s}}/s\tilde{\tilde{s}}s \;\sim\; \tilde{r}/\tilde{s}\ .$$

Produktregel: Offensichtlich gilt $d_S(r'/1) = 0$ für $r' \in R'$. Weiterhin gilt

$$\begin{aligned} d_S(r_1/s_1 \cdot r_2/s_2) \;&:=\; (s_1s_2)^{-1} \otimes_R d(r_1r_2) \;-\; r_1r_2/(s_1s_2)^2 \otimes_R d(s_1s_2) \\ &=\; (s_1s_2)^{-1} \otimes_R (r_1dr_2 + r_2dr_1) \;-\; r_1r_2/(s_1s_2)^2 \otimes_R (s_1ds_2 + s_2ds_1) \\ =\; r_1/s_1 \cdot (s_2^{-1} \otimes_R dr_2 - r_2/s_2^2 \otimes_R ds_2) \;&+\; r_2/s_2 \cdot (s_1^{-1} \otimes_R dr_1 - r_1/s_1^2 \otimes_R ds_1) \\ &=\; r_1/s_1 \cdot d_S(r_2/s_2) \;+\; r_2/s_2 \cdot d_S(r_1/s_1) \;. \end{aligned}$$

Zum Beweis von Lemma 45.2 verbleibt noch der Nachweis der universellen Eigenschaft von $d_S : R_S \to R_S \bigotimes_R \Omega(R/R')$. Betrachte dazu eine R'-Derivation $D : R_S \to M$ und das Diagramm



Die universelle Eigenschaft von d liefert eine eindeutige R-lineare Abbildung

$$f \in Hom(\Omega(R/R'), M) \;,$$

so daß $f \circ d$ auf R mit D übereinstimmt.

Wir benutzen nun die folgende

Übungsaufgabe: Sei N ein R-Modul, M ein R_S-Modul. Dann stiftet die Zuordnung $f_S \mapsto f := f_S \circ (1 \otimes_R id)$ eine Bijektion

$$\boxed{Hom_{R_S}(R_S \otimes_R N, M) \;=\; Hom_R(N, M)} \;.$$

Dies liefert $f_S \in Hom_{R_S}(R_S \otimes_R \Omega(R/R'), M)$.

Da D und $f_S \circ d_S$ auf R übereinstimmen und Derivationen sind, gilt

$$D \;=\; f_S \circ d_S \;.$$

Die Eindeutigkeit von f_S folgt aus obiger Übungsaufgabe und der universellen Eigenschaft von $d : R \to \Omega(R/R')$, d.h. der Eindeutigkeit von f. □

46 Transitivität

Lemma 46.1. *Seien $R \to S$ und $S \to T$ Ringhomomorphismen, dann gibt es eine exakte Sequenz von T-Moduln*

$$T \otimes_S \Omega(S/R) \longrightarrow \Omega(T/R) \longrightarrow \Omega(T/S) \to 0 \ .$$

Beweis: Dies folgt unmittelbar aus der Konstruktion in § 43 in der Form der Sequenz

$$T \otimes_S \Omega(S/R) \longrightarrow^{\varphi} \bigoplus_{t \in T} T \cdot dt/(\text{R-Relationen}) \twoheadrightarrow \bigoplus_{t \in T} T \cdot dt/(\text{S-Relationen})$$

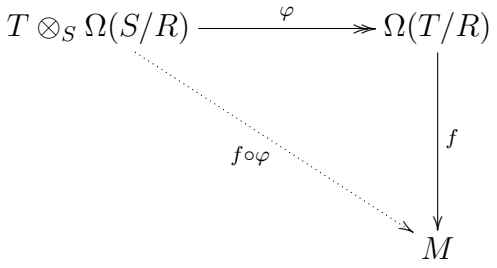
gegeben durch die Abbildung

$$\varphi : t \otimes_S s_1 ds_2 \mapsto t s_1 \cdot ds_2 \ ,$$

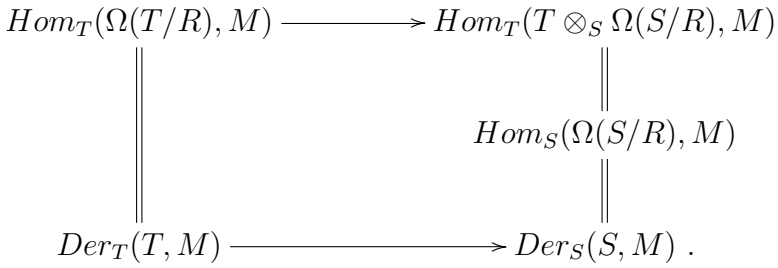
da die S-Relationen aus den R-Relationen durch Hinzunahme der Bedingungen $ds = 0,\ s \in S$ entstehen. Dies sind genau die Erzeuger des T-Moduls $Bild(\varphi)$.

□

Im Fall, wo $\pi : S \twoheadrightarrow T$ ein surjektiver Ringhomomorphismus mit Kernideal I ist, gilt natürlich $\Omega(T/S) = 0$. Man hat also dann



und man erhält eine induzierte Abbildung



welche direkt durch $D_T \mapsto D_S = D_T \circ \pi$ beschrieben werden kann. Hierbei ist M ein beliebiger T-Modul (und somit auch ein S-Modul).

Sei nun umgekehrt

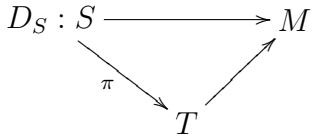
$$D_S : S \longrightarrow M$$

eine beliebige R-Derivation in den T-Modul M. Dann gilt für $s = s_1 \cdot s_2 \in I^2$ wegen $(*)$

$$D(s) \;=\; s_1 D(s_2) \;+\; s_2 D(s_1) \;=\; 0\ ,$$

da s_1 und s_2 null in T sind und daher wie die Null auf M operieren.

Weiterhin faktorisiert D_S über die Quotientenabbildung $\pi : S \to T$



genau dann, wenn gilt $D_S(I) = 0$. Somit liegt das Hindernis für das Faktorisieren in dem $T = S/I$-Modul

$$I/I^2\ .$$

Dies führt unschwer zu der Beobachtung

Lemma 46.2. *Für einen surjektiven Ringhomomorphismus $\pi : S \to T$ mit $Kern(\pi) = I$ existiert eine exakte Sequenz von T-Moduln*

$$I/I^2 \xrightarrow{\ \delta\ } T \otimes_S \Omega(S/R) \xrightarrow{\ \varphi\ } \Omega(T/R)$$

$$s \longmapsto 1 \otimes_S ds\ .$$

47 Separable Ringerweiterungen

Definition 47.1. *Ein Ringhomomorphismus $R \to T$ heißt separabel, wenn gilt*

$$\Omega(T/R) \;=\; 0 \;.$$

Lemma 47.2. *Sind $R \to S$ und $S \to T$ separable Ringhomomorphismen, dann ist auch die Komposition $R \to T$ separabel.*

Beweis: Lemma 45.1. □

Wir betrachten nun einen Spezialfall, nämlich

$$R \to T \;=\; R[X]/f(X) \;.$$

Wir wollen entscheiden, wann dieser Ringhomomorphismus separabel ist.

Wir setzen dazu $S = R[X]$ und $I = (f(X))$ und benutzen Lemma 45.2. Dies liefert die exakte Sequenz

$$I/I^2 \xrightarrow{\quad\delta\quad} T \cdot dX \longrightarrow\!\!\!\!\!\rightarrow \Omega(T/R)$$

$$\delta : \quad g(x) \cdot f(x) \; mod \; I^2 \longmapsto g(x) \cdot df \;.$$

Es folgt also

$$\Omega(T/R) \;=\; T \cdot dX/T \cdot df \;\cong\; T/[f'] \cdot T$$

wobei $f' = \sum a_i i X^{i-1}$ für $f = \sum a_i X^i$ (und $a_i \in R$).
Mit anderen Worten: $[f'] \in T$ ist die Restklasse in $T = R[X]/f(X)$ des Polynoms $f' \in R[X]$, welches durch formales Ableiten des Polynoms $f \in R[X]$ entsteht.

Hilfsatz 47.3. *Für ein Element $\xi \in T$ gilt $T/\xi \cdot T = 0$ genau dann, wenn gilt $\xi \in T^*$.*

Beweis: Ein Element $\xi \in T$ ist eine Einheit genau dann, wenn gilt $(\xi) = T$.

Es folgt somit

Korollar 47.4. *Der Ringhomomorphismus*

$$R \to R[X]/f(X) \;=\; T$$

ist genau dann separabel, wenn das von $f(X)$ und $f'(X)$ in $R[X]$ erzeugte Ideal ganz $R[X]$ ist

$$(f(X), f'(X)) \;=\; R[X].$$

Äquivalent: Für die Restklasse von $f'(X)$ in T gilt $[f'] \in T^*$.

Lemma 47.5. *Seien $R \to S$ und $S \to T$ Ringhomomorphismen, so daß die Komposition $R \to T$ separabel ist. Dann ist auch $S \to T$ separabel.*

Beweis: Lemma 45.1. □

Leider ist im allgemeinen in der Situation von Lemma 47.5 nicht klar, wann $R \to S$ separabel ist. Wir werden aber einen wichtigen Spezialfall im nächsten Abschnitt behandeln.

48 Ein Separabilitätskriterium

Wir betrachten in diesem Abschnitt Ringhomomorphismen

$$R \to S \quad \text{und} \quad S \to T$$

für die die Zusammensetzung

$$R \to T \ ,$$

separabel ist, d.h. für die gilt $\Omega(T/R) = 0$.

Wir bemerken: Ist $S \to T = \{0\}$ die Nullabbildung, dann ist $R \to T$ immer separabel. Über die Separabilität von $R \to S$ kann jedoch nichts ausgesagt werden !

Wir wollen aber zeigen, daß unter der

zusätzlichen Annahme: $S \to T$ sei eine primitive Ringerweiterung, d.h.

- $T \ = \ S[X]/f \ , \ f = \sum a_i X^i$ mit $a_i \in S$.
- f normiert in $S[X]$ vom $N \ = \ grad_X(f) \geq 1$,

die Separabilität von $R \to T$ nicht nur die Separabilität von $S \to T$, sondern auch die folgende Aussage impliziert

Lemma 48.1. *Aus $\Omega(T/R) = 0$ und der obigen zusätzlichen Annahme folgt $\Omega(S/R) = 0$. D.h. $R \to S$ ist wieder separabel.*

Beweis: Nach Lemma 47.5 gilt $\Omega(T/S) = 0$ und somit wegen Korollar 3.4

$$[f'] \ \in \ T^* \text{ für } T \ = \ S[X]/f \ .$$

Wir müssen $\Omega(S/R) = 0$ zeigen. Oder wegen Bemerkung 44, daß jede R-Derivation von S verschwindet. Eine solche Derivation

$$D : S \longrightarrow M$$

lässt sich vermöge

$$\widetilde{D}(s_i X^i) \ = \ s_i \cdot i \cdot X^{i-1} \cdot \widetilde{D}(X) \ + \ X^i \otimes_S D(s_i)$$

zu einer R-Derivation

$$\widetilde{D} : S[X] \longrightarrow S[X] \otimes_S M$$

fortsetzen. Hierbei kann über den Wert $\widetilde{D}(X)$ frei verfügt werden.

Wir betrachten nun die Zusammensetzung $(\pi \otimes_S id) \circ \widetilde{D}$, welche ein Diagramm

$$\begin{array}{ccc} S[X] & \xrightarrow{\widetilde{D}} & S[X] \bigotimes_S M \\ \Big\downarrow{\scriptstyle \pi} & & \Big\downarrow{\scriptstyle \pi \otimes_S id} \\ S[X]/f = T & \xrightarrow{D_T} & T \bigotimes_S M \end{array}$$

und eine Derivation $D_T : T \to T \otimes_S M$ induziert, falls gilt

$$(\pi \otimes_S id)(\widetilde{D}(f)) \;=\; 0 \; .$$

Dazu reicht aus

$$f' \cdot \widetilde{D} \;+\; \sum_i [X]^i \otimes_S D(s_i) \;=\; 0 \text{ in } T \otimes_S M \; .$$

Wie bereits gezeigt, gibt es $g, h \in S[X]$ mit $f' \cdot g + f \cdot h = 1$ und somit können wir setzen

$$\widetilde{D}(X) \;:=\; -g(X) \cdot \sum_i X^i \otimes_S D(s_i) \;\in\; S[X] \otimes_S M$$

um D_T zu konstruieren.

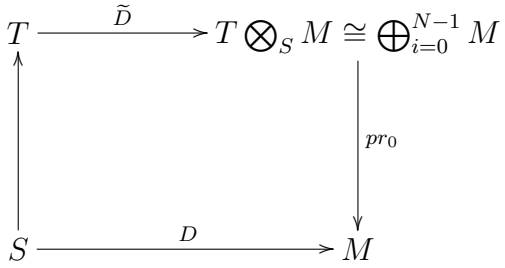
Nun kommt das entscheidende

Lemma 48.2. *Als S-Modul ist der T-Modul $T \otimes_S M$ isomorph zur direkten Summe $\bigoplus_{i=0}^{N-1} M$. Also gilt*

$$T \bigotimes_S M \;=\; M \oplus [X] \cdot M \oplus \cdots \oplus [X^{N-1}] \cdot M \;\cong\; \bigoplus_{i=0}^{N-1} M \; .$$

Beweis: Dies folgt wegen der Normiertheit von f aus $S[X]/f(X) = S \oplus [X] \cdot S \oplus \cdots \oplus [X^{N-1}] \cdot S$ somit aus der Identität $S \otimes_S M = M$.

Wir bemerken, daß gilt



Somit impliziert $D \neq 0$ sofort $\widetilde{D} \neq 0$.

Aus $\Omega(S/R) \neq 0$ folgt daher $\Omega(T/R) \neq 0$. Wegen der Annahme $\Omega(T/R) = 0$ gilt somit $\Omega(S/R) = 0$. $\square$