Zahlentheorie

Vorlesungszeiten
Dienstag 9.15-10.45 Uhr Hörsaal 19 Augustusplatz
Donnerstag 9.15-10.45 Uhr Hörsaal 19 Augustusplatz

Bezeichnungen

c	Inhaltsabbildung auf der Idele-Gruppe eines globalen Körpers, vgl. 4.5.5.
D_k	Gruppe der Divisoren des Funktionenkörpers k, vgl. 4.6.3.
D_k^0	Gruppe der Divisoren des Grades 0 des Funktionenkörpers k, vgl. 4.6.3.
d_v	Grad des Primdivisors v des Funktionenkörpers k, vgl. 4.6.3.
deg	Grad eines Divisors eines Funktionenkörpers, vgl. 4.6.3.
$D_R(T)$	Dual des erzeugenden R-Teilmoduls T eines Q(R)-Vektorraums, vgl. 1.6.9.
$\mathcal{D}(S/R)$	Differente der ganzen Abschließung S des Dedekind-Rings R in einer endlichen separablen Abschließung des Quotientenkörpers von R, vgl. 3.2.7.
$\mathcal{D}(L/K)$	die Differente des Bewertungsrings des vollständigen bewerteten Körpers K in der endlichen Erweiterung L von K, vgl. 3.3.6.
$\delta(M/R)$	die Diskriminante des R-Gitters M, vgl. 1.6.12.
$\delta(L/K)$	die Diskriminante des Bewertungsrings des vollständigen bewerteten Körpers K in der endlichen Erweiterung L von K,, vgl. 3.3.6.
F(R)	die freie abelsche Gruppe der gebrochenen Ideale des Dedekind-Rings R, vgl. 1.5.3.
e	Verzweigungsindex der Fortsetzung einer Bewertung, vgl. 2.3.8.
e(K/k)	Verzweigungsindex des vollständigen diskret bewerteten Körpers k in der endlichen separablen Körpererweiterung K, vgl. 3.1.5 und 3.3.6.
e(p"/p')	Verzweigungsindex des maximalen Ideals p' im maximalen Ideal p", vgl. 3.3.1.
f(K/k)	Relativgrad des vollständigen diskret bewerteten Körpers k in der endlichen separablen Körpererweiterung K, vgl. 3.1.5 und 3.3.6.
f(p"/p')	Relativegrad des maximalen Ideals p' im maximalen Ideal p", vgl. 3.3.1
$\phi(x)$	Herbrand-Index der Verzweigungsgruppe Γ_x. vg. 3.7.15.
G(m)	Gruppe der primen Restklassen modulo m, vgl. 5.1.1.
G(L/K)	Galois-Gruppe der Galois-Erweiterung L/K.
G_0(L/K)	Trägheitsgruppe der Galois-Erweiterung L/K, vgl. 3.5.9.
g_i	die Ordnung der i-ten Verzweigungsgruppe Γ_i, vgl. 3.7.2.
Γ_i	die i-te Verzweigungsgruppe im Fall κ_L/κ separabel, vgl. 3.7.2 und 3.7.14.
Γ_{i*}	die i-te (kleine) Verzweigungsgruppe, vgl. 3.7.9.
Γ_i^*	die i-te (große) Verzweigungsgruppe, vgl. 3.7.9.
Γ_P	Zerlegungsgruppe des von Primideals P, vgl. 3.8.4.
H_S	Gruppe der S-Einheiten eines globalen Körpers, vgl. 4.7.1
$H_{S,k}$	Gruppe der S-Einheiten des globalen Körpers k, vgl. 4.7.1
I_k	Gruppe der Ideale eines Zahlenkörpers, vgl. 4.6.1
J_k	Idele-Gruppe des globalen Körpers k, vgl. 4.5.2.

J_k^1 der Kern der Inhaltsabbildung c: $J_k \longrightarrow \mathbb{R}_{>0}$ auf der Idele-Gruppe J_k, vgl. 4.5.9.

κ_K Restekörper des diskret bewerteten vollständigen Körpers K, vgl. 3.3.6.

L(κ') die unverzweigte Körpererweiterung mit vorgegebener Erweiterung κ' des Restkörpers, vgl. 3.5.7.

N(A) Norm der linearen Abbildung A, vgl. 1.7.2

$ord_v\alpha$ Bild des Elements α eines globalen Körpers bei der additiven Bewertung zu einer normalisierten archimedischen Bewertung dieses Körpers, vgl. 4.6.1.

$\mathcal{O}_K$ der Ring der ganzen Zahlen des Zahlenkörpers K, vgl. 1.3.6. und 1.9.5, bzw. der Bewertungsring des diskret bewerteten vollständigen Körpers K,, vgl. 3.3.6.

p_v Bewertungideal der diskreten Bewertung v, vgl. 1.4.11.

$\wp_K$ maximales Ideal des Bewertungsrings $\mathcal{O}_K$, vgl. 3.3.6.

Q(R) Quotientenkörper des Integritätsbereiches R, vgl. 1.4.1.

$\mathbb{Q}$ Körper der rationalen Zahlen.

R_v Bewertungsring der Bewertung v, vgl. 1.4.8.

Tr(A) Spur der linearen Abbildung A, vgl. 1.7.2.

U_v Einheitengruppe der diskreten Bewertung v, vgl. 1.4.13.

U Einheitengruppe einer additiven Bewertung, vgl. 1.4.13

U Einheitengruppe einer multiplikativen Bewertung, vgl. 2.4.5

U_1 Gruppe der 1-Einheiten einer additiven Bewertung, vgl. 1.4.14.

U_1 Gruppe der 1-Einheiten einer multiplikativen Bewertung, vgl. 2.4.5.

U_n Gruppe der n-Einheiten einer additiven Bewertung, vgl. 1.4.14.

U_K Gruppe der Einheiten des vollständigen diskret bewerteten Körpers K, vgl. 3.5.14.

$U_{K,n}$ Gruppe der n-Einheiten des vollständigen diskret bewerteten Körpers K, vgl. 3.5.14.

V_k Adele-Ring des globalen Körpers k, vgl. 4.4.1.

V_k^+ Additive Gruppe des Adele-Rings des globalen Körpers k, vgl.4.4.3.

v_p die diskrete Bewertung des Quotientenkörpers eines Dedekind-Rings R mit dem maximalen Ideal $p \subseteq R$, deren Bewertungsring gerade die Lokalisierung R_p von R in p ist, vgl. 1.5.2.

v_K die additive Bewertung des vollständigen bewerteten Körpers K, vgl. 3.3.6.

$\mathbb{Z}$ Ring der ganzen rationalen Zahlen.

$\mathbb{Z}^+$ additive Gruppe der ganzen Zahlen, vgl. 2.4.5.

$|?|_v$ multiplikative Bewertung zur diskreten Bewertung v, vgl. 1.4.12.

$|?|_p$ die Bewertung des Körpers der rationalen Zahlen zur Primzahl p, die p-adische Bewertung von $\mathbb{Q}$, vgl. 2.3.12.

[x] größtes Ganzes der reellen Zahl x, vgl. 3.7.14.

(M:N) Index des Gitters N im Gitter M, vgl. 1.6.5.

E^s separable Abschließung eines Teilkörpers $F \subseteq E$ in E, vgl. 3.5.3.

$F((t))$ Körper der formalen Laurent-Reihen über dem Körper F, vgl. 1.4.7.

$F[[t]]$ Körper der formalen Potenzreihen über dem Körper F, vgl. 1.4.7.

$\phi(x)$ Herbrand-Index der Verzweigungsgruppe Γ_x, vgl. 3.7.15.

$K(\sqrt[m]{1})$ Körpererweiterung des Körpers K der Charakteristik Null, welche durch Adjunktion einer primitiven m-ten Einheitswurzel entsteht, vgl. 5.1.1.

K_p Vervollständigung des Körpers K, welcher Quotientenkörper eines Bewertungsrings mit dem Bewertungsideal p ist, bezüglich der p-adischen Topologie, vgl. 3.2.3.

R_p Lokalisierung des Integritätsbereichst R im Primideal p, vgl. 1.4.18

$\overline{R}_p$ Vervollständigung des Dedekind-Rings R bezüglich der p-adischen Topologie, wobei $p \subseteq R$ ein maximales Ideal von R bezeichne, vgl. 3.2.3.

T_p Lokalisierung des Moduls T über einem kommutativen Ring im Primideal p dieses Rings, vgl. 1.6.3.

Einleitung

Die Zahlentheorie ist voller eigenartig anmutender Sätze und Probleme, die sich jeder Systematik zu entziehen scheinen, isoliert nur für sich dastehen und sich weigern Teil eines größeren Ganzen zu sein. Oft besteht die Lösung der Probleme gerade in der Einordung in einen größeren Zusammenhang.

Ein ein typisches Beispiel ist der große Fermatsche Satz:
die Gleichungen

$$x^n + y^n = z^n \text{ mit } n = 3, 4, 5.... \tag{1}$$

besitzen nur die trivialen ganzzahligen Lösungen, d.h. die mit

$$x, y, z \in \{0, \pm 1\}.$$

Es stellt sich sofort die Frage, wie es mit den anderen diophantischen Gleichungen steht.

Die Zahlentheorie hat etwa 300 Jahre gebraucht, um eine Einordnung in einen größeren Zusammenhang zu finden und so das Problem zu lösen. Der entscheidende Teil der Antwort ist ein Satz über alle diophantischen Gleichungen.

1. Schritt. Man betrachte anstelle von (1) die Gleichung

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1,$$

d.h. man untersuche rationalen Punkte der ebenen Kurve

$$X: x^2 + y^2 = 1 \tag{2}$$

d.h. die Punkte (x,y) mit $x, y \in \mathbb{Q}$. Um diese Kurve zu verstehen, muß man auch die komplexwertigen Lösungen dieser Gleichung untersuchen. Und man muß sie in den projektiven Raum einbetten.
2. Schritt. Man betrachte zusätzlich die geometrischen Punkte der Kurve (2), d.h. die Punkte

$$(x, y) \in X$$

mit x, y $\in \mathbb{C}$.

3. Schritt. Man betrachte zusätzlich die projektive Abschließung der Kurve, d.h. die Abschließung von

$$X \subseteq \mathbb{C}^2 \subseteq \mathbb{P}^2_{\mathbb{C}} \text{ , } (x,y) \mapsto [1, x, y], \tag{3}$$

im projektiven Raum $\mathbb{P}^2_{\mathbb{C}}$. Zur Erinnerung, der projektive Raum $\mathbb{P}^n_K$ der Dimension n über dem Körper K besteht aus allen Geraden des K^{n+1}, die durch den Ursprung gehen. Im Fall K = $\mathbb{R}$ kann man sich $\mathbb{P}^n_K$ auch als Einheitssphäre $S^n \subseteq \mathbb{R}^{n+1}$ vorstellen, bei der gegenüberliegende Punkte identifiziert sind (jede Gerade im $\mathbb{R}^{n+1}$ schneidet S^n in einem Paar gegenüberliegender Punkte). Mit

$$[x_0, \dots , x_n] \in \mathbb{P}^n_K$$

bezeichnet man die Gerade des K^{n+1} durch den Ursprung und durch $(x_0, \dots , x_n)$. Kehren wir zu unserem Ausgangsproblem zurück. Abbildung (3) identifiziert jeden Punkt der komplexen Ebene $\mathbb{C}^2$ mit einem Punkt der projektiven Ebene

$$\mathbb{P}^2_{\mathbb{C}} = \{ [z, x, y] \mid (z, x, y) \in \mathbb{C}^3 - \{(0,0,0)\}\}$$

und damit X mit einer Teilmenge der letzteren. Die komplexe projektive Ebene ist ein topologischer Raum. Wir bezeichnen mit

$$\overline{X} \subseteq \mathbb{P}^2_{\mathbb{C}}$$

die Abschließung von X in $\mathbb{P}^2_{\mathbb{C}}$ genannt die projektive Abschließung von X. Diese Menge kann man (wie man leicht sieht) durch eine Gleichung beschreiben, nämlich die Gleichung (1): die Menge $\overline{X}$ besteht aus allen Punkten [z, x, y] der komplexen projektiven Ebene, die der Gleichung (1) genügen,

$$\overline{X}: x^n + y^n = z^n.$$

Der der komplexe projektive Raum $\mathbb{P}^N_{\mathbb{C}}$ hat gegenüber dem affinen Raum $\mathbb{C}^N$ den Vorteil, daß er kompakt ist. Wir können deshalb alle möglichen Sätze der Analysis über kompakte Mengen anwenden.

4. Schritt. Man betrachte die projektive Abschießung

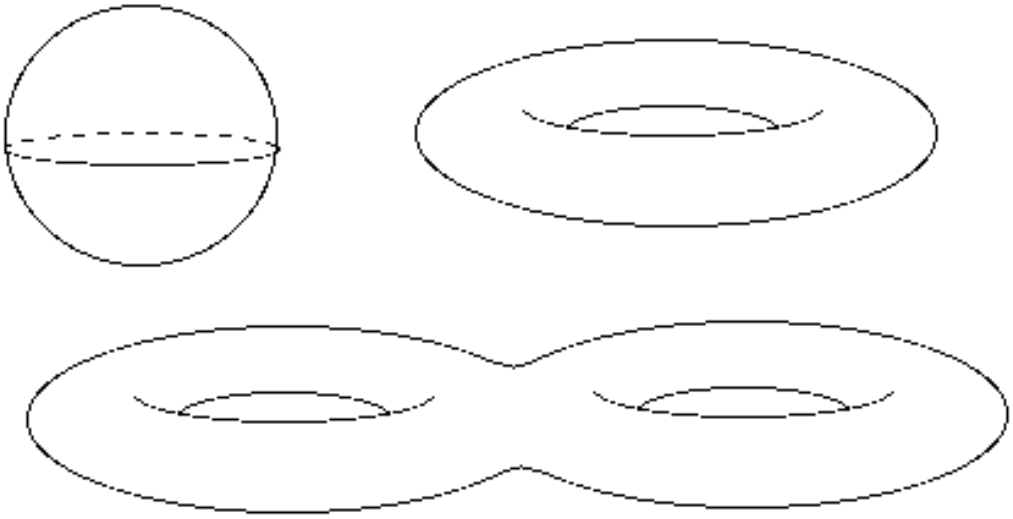
$$\overline{X} \subseteq \mathbb{P}^2_{\mathbb{C}}$$

X als Riemannsche Fläche. Die Menge $\mathbb{P}^2_{\mathbb{C}}$ ist komplex zwei-dimensional, also reell vier-dimensional. Die Teilmenge $\overline{X}$ ist durch eine (komplexe) Gleichung gegeben. Reell gesehen bedeutet dies, man hat zwei Gleichungen: der Realteil und der Imaginärteil eines Ausdrucks werden Null gesetzt. Das bedeutet, $\overline{X}$ ist reell gesehen zwei-dimensional. Man kann sich leicht davon überzeugen, daß $\overline{X}$ eine zwei-dimensionale reelle Teilmannigfaltigkeit der vierdimensionalen Mannigfaltigkeit $\mathbb{P}^2_{\mathbb{C}}$ (d.h. in jedem Punkt kann man $\overline{X}$ mit einer offenen Menge im $\mathbb{R}^2$ identifizieren, man verwende den Satz über implizite Funktionen). Dasselbe funktioniert sogar über dem komplexen Zahlen: $\overline{X}$ ist eine (ein-dimensionale) komplexe Teilmannigfaltigkeit von $\mathbb{P}^2_{\mathbb{C}}$.

Weil $\mathbb{P}^2_{\mathbb{C}}$ kompakt ist und $\overline{X}$ durch die Gleichung (1) gegeben ist, ist $\overline{X}$ eine abgeschlossene Teilmenge von $\mathbb{P}^2_{\mathbb{C}}$, mit anderen Worten,

$\overline{X}$ ist eine kompakte Riemannsche Fläche.

Die kompakten Riemannschen Flächen sind als topologische Räume (und als differenzierbare Mannigfaltigkeiten) wohlbekannt. Man kann sie mit der Oberfläche einer 2-Sphäre identifizieren, in welche endlich viele Löcher gebohrt wurden.



Die Anzahl der Löcher nennt man Geschlecht. Unsere "Kurve" $\overline{X}$ ist eine Riemannsche Fläche vom Geschlecht 0 im Fall n = 1 und n = 2 und vom Geschlecht > 1 im allen anderen Fällen.

Diophantische Gleichungen vom Geschleicht 0.

Die Fälle n = 1 und n = 2 sind in Sonderfälle: der Satz von Fermat ist falsch für diese n. Für n = 1 ist das trivial und für n = 2 ist dies seit Urzeiten bekannt: es gibt unendlich viele Pythagoräsiche Zahlentripel (vgl. z.B. Bundschuh [1], Kapitel 4, §2.1). Es ist klar, daß diese Fälle in der Formulierung des großen Fermatschen Satzes ausgeschlossen werden müssen.

Diophantische Gleichungen vom Geschlecht 1.

Das Geschlecht 1 kommt unter den betrachteten diophantischen Gleichungen nicht vor. Man kann sich leicht überlegen, daß andernfalls die Aussage des Fermatschen Satzes fallsch wäre. Topologisch kann man eine Riemannsche Fläche vom Geschlecht 1 identifizieren mit

$$g(\overline{X}) = 1 \Rightarrow \overline{X} \approx S^1 \times S^1$$

und S^1 mit dem Einheitskreis in der komplexen Ebene,

$$S^1 = \{ z \in \mathbb{C} \mid |z| = 1\}.$$

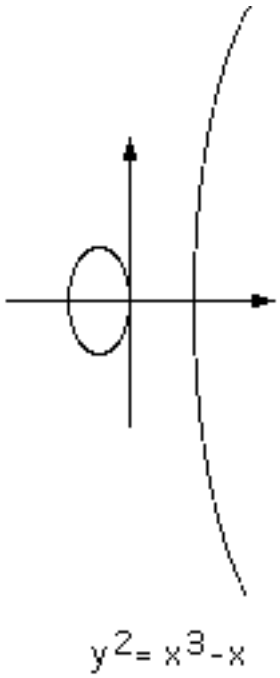
Aus dieser Beschreibung ergibt sich insbesondere, daß S^1 eine multiplikative Gruppe ist: das Produkt von zwei komplexen Zahlen vom Betrag 1 hat den Betrag 1. Dann ist aber auch $\overline{X} \approx S^1 \times S^1$ eine Gruppe. Man kann in dieser Situation sogar mehr zeigen:

$\overline{X}$ ist eine algebraische Gruppe,

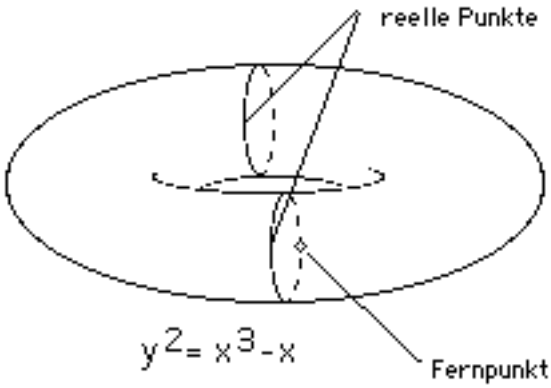
d.h. die Multiplikation und der Übergang zum inversen Element sind algebraische Operaatgionen, sie lassen sich mit Hilfe von Polynomen beschreiben. Nehmen wir zum Beispiel die projektive Abschließung der Kurve

$$X: y^2 = x(x-1)(x-\lambda)$$

mit einem Paramter λ.



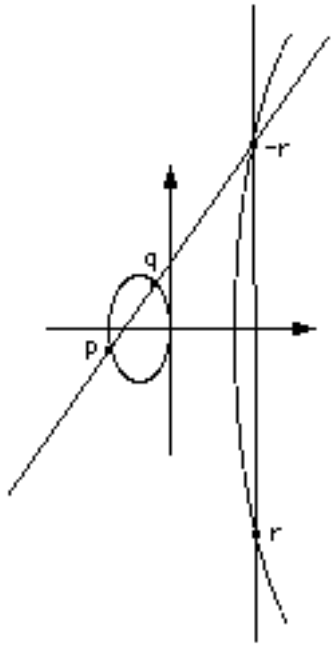
Beim Übergang zur projektiven Abschließung dieser Kurve kommt ein weiterer Punkt hinzu. Er liegt im Unendlichen und zwar in der Richtung der y-Achse. Der rechte Zweig der Kurve ist gewissermaßen ebenfalls ein Kreis, wobei ein Punkt des Kreises im Unendlichen liegt. Komplex gesehen ist die projektive Abschließung ein Torus (d.h. eine Riemannsche Fläche vom Geschlecht 1).



Die Gruppen-Operation auf dieser Kurve - die wir als Addition schreiben wollen - läßt sich wie folgt beschreiben. Als neutrales Element der Gruppe verwenden wir den Punkt im Unendlichen,

$$0 \in \overline{X} - X.$$

Für je zwei Punkte p, q auf $\overline{X}$ geht die Verbindunggerade durch einen dritten Punkt dieser Kurve, den wir mit -r bezeichnen wollen (er ist gleich dem Negativen der gesuchten Summe).



Durch -r legen wir eine Gerade, die parallel zur y-Achse ist. Diese Gerade geht außer durch -r noch durch den Fernpunkt 0 und einen weiteren Punkt, den wir mit r bezeichnen. Dieser ist gleich der gesuchten Summe,

$$r = p + q. \qquad (4)$$

Es ist nicht schwer einzusehen, daß die Koordinaten von r rationale Funktionen der Koordinaten von p und q sind,

$$r = \left(\frac{f(p,q)}{h(p,q)}, \frac{g(p,q)}{h(p,q)}\right) \text{ mit Polynomen f, g und h.}$$

Es gilt sogar mehr (vgl. z.B. Siverman [1]):

> Ist die Kurve X über einem Körper K definiert,
>
> $$\mathbb{Q} \subseteq K \subseteq \mathbb{C},$$
>
> d.h. liegen die Koeffizienten der Gleichung von X in K, so haben die Koeffizienten der rationalen Funktionen, welche die Addition (4) beschreiben, ebenfalls Koeffizienten in K,
>
> $$f, g, h \in K[p_1, p_2, q_1, q_2],\ p = (p_1, p_2),\ q = (q_1, q_2).$$

Sind p und q K-rationale Punkte von $\overline{X}$, d.h. liegen deren Koordinaten in K, so gilt also dasselbe für r. Mit anderen Worten,

Die Menge der K-rationalen Punkte von $\overline{X}$ ist eine Untergruppe von $\overline{X}$.

Für jeden K-rationalen Punkt p von $\overline{X}$ sind also 2p, 3p, 4p, ... ebenfalls K-rationale Punkte von $\overline{X}$. Aus der Gruppeneigenschaft folgt damit im wesentlichen[1], daß eine diophantische Gleichung vom Geschleicht 1 entweder überhaupt keine Lösung besitzt oder unendlich viele.

---

[1] Wir vernachlässigen hier die Frage, daß p ein Punkt endlicher Ordnung sein könnte.

Das finale Ergebnis bei der Lösung des großen Fermatschen Problems besagt nun, daß die Gruppeneigenschaft der einzige Grund dafür ist, daß eine diophantische Gleichung unendlich viele Lösungen haben kann (sieht man vom Geschlecht-0-Fall ab).

Eine über $\mathbb{Q}$ definierte algebraische Kurve vom Geschlecht > 1 hat nur endlich viele $\mathbb{Q}$-rationale Punkte.

Die Antwort auf das große Fermatsche Problem ist also eine Aussage der arithmetischen algebraischen Geometrie. Der Weg zum Beweis geht allerdings weit über die Möglichkeiten dieser Vorlesung hinaus. Wir beschränken uns deshalb auf einen bescheideneren Problemkreis. Er hat mit den Fragestellungen der folgenden Art zu tun.

1. Wie entscheidet man, ob eine diophantische Gleichung über einem endlichen Körper lösbar ist ?

2. Ist die gibt es außer den Hamiltonschen Quaternionen weitere reelle Vektorräume endlicher Dimension, welche die Struktur einer zentralen Divisionsalgebra über $\mathbb{R}$ haben, d.h. welche Schiefkörper sind bezüglich einer $\mathbb{R}$-bilinearen Multiplikation und das Zentrum $\mathbb{R}$?

3. Welche Strutkur besitzt die Galois-Gruppe einer (möglicherweise unendlichen) Körpererweiterung ? Tritt jede Gruppe als Galois-Gruppe auf ?

4. Behauptung: jede Primzahl p, welche kongruent 1 modulo 6 ist, hat die Gestalt

$$p = \frac{x^2+27\cdot y^2}{4}$$

Beispiele:

$$7 = \frac{1^2+27\cdot 1^2}{4},\ 13 = \frac{5^2+27\cdot 1^2}{4},\ 19 = \frac{7^2+27\cdot 1^2}{4},\ 31 = \frac{8^2+27\cdot 2^2}{4},\ \ldots$$

Der Beweis von Aussage 4 ist einfach. Frage 3 ist ein ungelöstes Problem.

Die Antwort auf Frage 2 heist nein. Man kann heute für jeden Körper die Gesamtheit der Divisionsalgebren über diesen Körper berechnen: diese Algebren bilden eine Gruppe, die Brauer-Gruppe. Die Brauer-Gruppe von $\mathbb{R}$ besteht aus zwei Elementen. Diese ensprechen den Divisionsalgebren $\mathbb{R}$ und $\mathbb{H}$.

Die Antwort auf Frage 1 ist bekannt, wenn die diophantische Gleichung den Grad 2 hat und besteht im Gaußschen Reziprozitätsgesetz. Siehe zum Beispiel Pieper [1]. Das Buch ist eine Sammlung von Beweisen des Reziprozitätsgesetzes.Die Antwort auf Frage 1 ist ebenfalls bekannt, wenn die zur diophantischen Gleichung gehörige Galois-Gruppe kommutativ ist: sie stammt ebenfalls von Gauß und heißt heute Klassenkörper-Theorie. Im allgemeinen Fall ist die Antwort auf diese Frage Gegenstand moderner Forschung und die zugehörige Theorie heißt Langlands-Theorie.

Die vorliegende Vorlesung versteht sich als eine Vorbereitung auf die Klassenkörper-Theorie. Alle vier angegebenen Fragestellungen haben mit der Tatsache zu tun, daß sich ganze Zahlen in eindeutiger Weise als Produkte von Primzahlpotenzen schreiben lassen, und daß sich dieses Phänomen auf von $\mathbb{Z}$ verschieden Ringe verallgemeinern läßt. Wir beginnen mit einem einfachen Beispiel.

1. Dedekind-Ringe

1.1 Die ganzen Gaußschen Zahlen[2]

1.1.1 Definition und grundlegenden Eigenschaften

Die ganzen Gaußschen Zahlen sind die komplexen Zahlen, deren Real- und Imaginärteil ganz ist. Sie werden hier mit

$$\Gamma := \mathbb{Z} + i\bullet\mathbb{Z} \subseteq \mathbb{C}$$

bezeichnet. Sie bilden offensichtlich einen kommutischen Ring mit 1 (und ohne Nullteiler, also einen Integritätsbereich[3]).

Bemerkung

Aus der Grundvorlesung Algebra wissen wir, Γ ist ein Euklidischer Ring mit der Norm

$$N: \Gamma \longrightarrow \mathbb{Z},\ z = a + ib \mapsto z\bullet\overline{z} = (a + bi)\bullet(a - bi) = a^2 + b^2.$$

Mit anderen Worten, der Ring der ganzen Gaußschen Zahlen gestattet eine Division mit Rest: für je zwei ganze Gaußsche Zahlen

$$u, v \in \Gamma - \{0\}$$

gibt es ganze Gaußsche Zahlen $q, r \in \Gamma$ mit

$$u = q\bullet v + r \text{ und } N(r) < N(v).$$

Die Beweisidee besteht darin, für q eine ganze Gaußsche Zahl zu wählen, die möglichst nahe bei der komplexen Zahl $\frac{u}{v}$ liegt. Man kann immer dafür sorgen, daß Real- und Imaginärteil von q und $\frac{u}{v}$ sich höchstens um den Wert $\frac{1}{2}$ unterscheiden, also

$$|q - \frac{u}{v}|^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

gilt. Mit $r = u - q\bullet v = v\bullet(\frac{u}{v} - q)$ erhält man

$$N(r) = |r|^2 = |v|^2\bullet|\frac{u}{v} - q|^2 \leq |v|^2\bullet\frac{1}{2} < |v| = N(v).$$

Wir haben damit erneut gezeigt, daß Γ ein Euklidischer Ring ist, und damit insbesonder ein ZPE-Ring: Γ gestattet eine eindeutige Zerlegung in Primelemente.

1.1.2 Die Einheiten von Γ

Für jede ganze Gaußsche Zahl $u \in \Gamma$ sind folgende Aussagen äquivalent.

(i) u ist eine Einheit von Γ.
(ii) $N(u) = 1$.
(iii) $u \in \{+1, -1, +i, -i\}$

Beweis. (i) $\Rightarrow$ (ii). Nach Voraussetzung gibt es eine ganze Gaußsche Zahl $v \in \Gamma$ mit

$$u\bullet v = 1.$$

Wir wenden N an und erhalten

$$N(u)\bullet N(v) = N(1) = 1,$$

d.h. N(u) und N(v) sind nicht-negative ganze Zahlen, deren Produkt gleich 1 ist. Das ist nur möglich, wenn gilt

$$N(u) = N(v) = 1.$$

---

[2] Wir folgen hier der Darstellung von Kochendörffer [1].
[3] Ein Integritätsbereich ist ein kommutativer Ring mit 1 ohne Nullteiler.

(ii) $\Rightarrow$ (i). Wir schreiben u in der Gestalt

$$u = x + i \bullet y$$

mit ganzen Zahlen x und y. Nach Voraussetzung gilt

$$1 = N(u) = x^2 + y^2.$$

Das eine Quadrat auf der rechten Seite muß somit 1 sein und das andere 0. Daraus ergeben sich die angegebenen vier Möglichkeiten für u.

(iii) $\Rightarrow$ (i). Wegen

$$1 = 1 \bullet 1 = (-1) \bullet (-1) = i \bullet (-i)$$

sind 1, -1, i und -i Einheiten von Γ.

QED.

Bemerkung

Die nächste zu stellende Frage ist die nach den Primelementen. Welches sind die Primelemente von Γ ? Bei der Beantwortung wird sich das folgende hinreichende Kriterium als nützlich erweisen.

Eine ganze Gaußsche Zahl u, für welche

$$p = N(u) \in \mathbb{Z}$$

eine Primzahl ist, ist ein Primelement von Γ.

Beweis. Andernfalls ließe sich u in der Gestalt

$$u = \alpha \bullet \beta$$

schreiben mit ganzen Gaußschen Zahlen α und β, die keine Einheiten sind. Es folgte

$$p = N(u) = N(\alpha) \bullet N(\beta)$$

mit von 1 verschiedenen nicht-negativen ganzen Zahlen $N(\alpha)$ und $N(\beta)$. Dann kann aber p keine Primzahl sein.

QED.

1.1.3 Die Primelemente von Γ

Die Primelemente von Γ sind gerade diejenigen ganzen Gaußschen Zahlen die assoziiert[4] sind zu einer der folgenden ganzen Gaußschen Zahlen:

(i) zu i + 1

(ii) zu einer Primzahl p, die kongruent -1 modulo 4 ist

(iii) zu x + i•y, wobei $x^2 + y^2 = p$ eine Primzahl ist, die kongruent 1 modulo 4 ist.

Beweis. Zeigen wir zunächst, daß jedes Primelement von Γ assoziiert ist zu einer der angegebenen ganzen Gaußschen Zahlen. Sei π eine Primzahl von Γ. Dann gilt

$$\pi \mid \pi \bullet \overline{\pi} = N(\pi).$$

Nun ist die ganze Zahl $N(\pi)$ Produkt von Primzahlen. Es gibt also eine Primzahl $p \in \mathbb{Z}$ mit

$$\pi \mid p.$$

1. Fall: p = 2.

Wegen

$$2 = (1 + i) \bullet (1 - i)$$

folgt

$$\pi \mid 1 + i \text{ oder } \pi \mid 1 - i.$$

---

[4] Zwei Zahlen von Γ heißen assoziiert, wenn ihr Quotient eine Einheit von Γ ist.

Wegen N(1+i) = N(1-i) = 2 sind aber 1 + i und 1 - i Primelemente von Γ (vgl. die Bemerkung von 0.2). Die beiden Teilbarkeitsbeziehungen bedeuten damit,

$$\pi \text{ ist assoziiert zu } 1 + i \text{ oder } 1 - i.$$

Wegen

$$1 - i = (1 + i)(-i)$$

sind aber 1 + i und 1 - i assoziiert, d.h. π ist assoziert zu i + 1. Es tritt der Fall (i) ein.

2. Fall: $p \equiv -1 \pmod 4$.

Aus $\pi \mid p$ folgt

$$N(\pi) \mid N(p) = p^2,$$

also

$$N(\pi) = p \text{ oder } N(\pi) = p^2.$$

Zeigen wir, der erste Fall ist nicht möglich. Andernfalls wäre

$$p = N(\pi) = x^2 + y^2$$

mit ganzen Zahlen $x, y \in \mathbb{Z}$. Durch direktes Nachrechnen sieht man, jedes Quadrat ist kongruent 0 oder 1 modulo 4. Also ist die Summe von zwei Quadraten immer

x	0	1	2	3
$\mathbf{x^2}$	0	1	0	1

kongruent 0, 1 oder 2 modulo 4 und niemals kongruent $-1 \equiv 3$. Der erste Fall ist somit nicht möglich, und wir erhalten

$$N(\pi) = p^2.$$

Schreiben wir jetzt

$$p = \pi \bullet \alpha$$

mit einer ganzen Gaußschen Zahl. Dann gilt

$$p^2 = N(p) = N(\pi) \bullet N(\alpha) = p^2 \bullet N(\alpha),$$

also $N(\alpha) = 1$, d.h. α ist eine Einheit. Mit anderen Worten π ist assoziiert zu p, des tritt der Fall (ii) ein.

Wir haben außerdem gezeigt, jeder Primteiler von p ist in Γ assoziiert zu p. Das bedeutet, die Primzahlen der Gestalt (ii) sind tatsächlich auch Primelemente von Γ.

3. Fall: $p \equiv +1 \pmod 4$.

Aus der Theorie der endlichen Körper wissen wir, die von Null verschiedenen Elemente des Körpers

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

besteht gerade aus den Nullstellen des Polynoms $x^{p-1} - 1$ (weil die multiplikative Gruppe dieses Körpers die Ordnung p-1 hat). Deshalb gilt modulo p

$$x^{p-1} - 1 = (x - 1)(x - 2) \bullet \ldots \bullet (x - p-1)$$

Für x = 0 ergibt dies (weil p eine ungerade Primzahl ist) den Satz von Wilson:

$$-1 \equiv (p-1)! \bmod p.$$

Modulo p können wir damit die folgende Rechnung durchführen

$$\begin{aligned} -1 &= (p-1)! \\ &= \prod_{k=1}^{\frac{p-1}{2}} k \bullet \prod_{k=1}^{\frac{p-1}{2}} (p - k) \end{aligned}$$

$$= \prod_{k=1}^{\frac{p-1}{2}} k \cdot \prod_{k=1}^{\frac{p-1}{2}} (- k)$$

$$= (-1)^{\frac{p-1}{2}} \cdot \left(\prod_{i=1}^{\frac{p-1}{2}} k \right)^2$$

$$= (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2} ! \right)^2$$

Wegen $p \equiv 1 \pmod 4$ folgt

$$-1 \equiv \left(\frac{p-1}{2} ! \right)^2 \bmod p,$$

d.h. -1 ist modulo 4 ein Quadrat,

$$-1 \equiv z^2 \bmod p$$

mit einer ganzen Zahl z. Es folgt

$$p \mid z^2 + 1$$

und wegen $\pi \mid p$ auch

$$\pi \mid z^2 + 1 = (z + i)(z - i)$$

also

$$\pi \mid z + i \text{ oder } \pi \mid z - i.$$

Wir schreiben jetzt wieder

$$p = \pi \cdot \alpha$$

mit einer ganzen Gaußschen Zahl α. Wäre α eine Einheit, so wäre p zu π assoziiert und es würde auch gelten

$$p \mid z + i \text{ oder } p \mid z - i.$$

was offensichtlich nicht richtig ist, denn dann wäre $\frac{1}{p}z + \frac{1}{p}i$ bzw. $\frac{1}{p}z - \frac{1}{p}i$ eine ganze Gaußsche Zahl. Wir wissen also α ist genau wie π eine Nicheinheit. Aus der Zerlegung $p = \pi \cdot \alpha$ erhalten wir

$$p^2 = N(p) = N(\pi) \cdot N(\alpha),$$

wobei die beiden Faktoren rechts von 1 verschiedene nicht-negative ganze Zahlen sind. Es folgt

$$N(\pi) = N(\alpha) = p.$$

Schreiben wir π in der Gestalt

$$\pi = x + y \cdot i$$

mit ganzen Zahlen $x, y \in \mathbb{Z}$. Dann gilt

$$p = N(\pi) = x^2 + y^2,$$

d.h.es tritt der Fall (iii) ein.

Umgekehrt ist jede ganze Gaußsche Zahl $\pi = x + y \cdot i$ mit

$$x^2 + y^2 = p$$

ein Primelement: es gilt dann $\pi \cdot \overline{\pi} = p$, d.h. π und $\overline{\pi}$ sind Nicht-Einheiten[5]. Durch Anwenden von N erhalten wir

---

[5] Wenn eine der beiden Zahlen Einheiten wären, so wäre es auch die anderen, denn sie gehen durch Konjugation ineinander über.

$$N(\pi)\bullet N(\overline{\pi}) = N(p) = p^2,$$

also $N(\pi) = N(\overline{\pi}) = p$, d.h. π und $\overline{\pi}$ sind Primelemente.

Wir haben außerdem gezeigt, für jeden Primteiler π in Γ einer Primzahl $p \equiv 1 \pmod 4$ gilt

$$p = N(\pi) = \pi\bullet\overline{\pi}\ ,$$

d.h. p zerfällt in das Produkt von zwei Primelementen

$$\pi = x + y\bullet i \text{ und } \overline{\pi} = x - y\bullet i$$

Die beiden Primfaktoren sind nicht assoziiert (man multiplizieren mit den Einheiten 1, -1, i, -i und beachte, x und y sind betragsmäßig verschieden, weil p ungerade Primzahl ist).

QED.

Bemerkung

Zusammenfassend kann man sagen, in der Situation

$$\begin{array}{ccc} \mathbb{Q} & \subseteq & \mathbb{Q}(i) \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & \Gamma \end{array}$$

spielen die ganzen Gaußschen Zahlen für den Körper

$$\mathbb{Q}(i) = \mathbb{Q}+\mathbb{Q}\bullet i = Q(\Gamma)$$

dieselbe Rolle, wie die ganzen Zahlen $\mathbb{Z}$ für den Körper $\mathbb{Q}$. Aus dem obigen Beweis kann man außerdem einiges zum Verhalten der Primzahlen beim Übergang von $\mathbb{Z}$ nach Γ ablesen:

1. Es kann passieren, daß sie Primelemente bleiben (wie die Primzahlen $p \equiv -1 \pmod 4$).
2. Es kann passieren, daß sie in Produkte nicht-assoziierter Primelemente zerfallen (wie die Primzahlen $p \equiv +1 \pmod 4$).
3. Es kann passieren, daß sie assoziiert sind zur Protenz einer Primzahl (wie die Primzahl $2 = (1+ i)(1 - i) =(-i)\bullet (1+i)^2$).

Es ist deshalb naheliegend zu fragen, ob die beschriebene Sitution auch für andere Körpererweiterungen von $K/\mathbb{Q}$ auftritt. In der Zahlentheorie interessiert man sich besonders für die endlichen Körpererweiterungen von $\mathbb{Q}$,

$$[K: \mathbb{Q}] < \infty,$$

die wir im folgenden einfach Zahlenkörper nennen wollen. Wie sie aus der Grundvorlesung Algebra wissen, treten dabei einige Probleme auf.

1.2 Der Ring $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \sqrt{-5}\bullet\mathbb{Z}$

Dieser Ring hat den Quotientenkörper $\mathbb{Q}(\sqrt{-5})$. Trotzdem ist die Situation für das Diagramm

$$\begin{array}{ccc} \mathbb{Q} & \subseteq & \mathbb{Q}(\sqrt{-5}) \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & \mathbb{Z}[\sqrt{-5}] \end{array}$$

grundlegend anders als im Fall der ganzen Gaußschen Zahlen. Der Grund dafür ist die Identität

$$2\bullet 3 = 1 + (\sqrt{-5})^2 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Wir die bezeichnen mit

$$N: \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}$$

wie im Fall der ganzen Gaußschen Zahlen die Normabbildung, d.h.

$$N(x + y\bullet \sqrt{-5}) = x^2 + 5\bullet y^2$$
$$N(\alpha) = \alpha\bullet\overline{\alpha}$$
$$N(\alpha\bullet\beta) = N(\alpha)\bullet N(\beta).$$

1.2.1 Die Einheiten von $\mathbb{Z}[\sqrt{-5}]$

Für jedes $u \in \mathbb{Z}[\sqrt{-5}]$ sind folgende Aussagen äquivalent.

(i) u ist eine Einheit von $\mathbb{Z}[\sqrt{-5}]$.
(ii) $N(u) = 1$.
(iii) $u \in \{+1, -1\}$

Beweis. (i) $\Rightarrow$ (ii). Nach Voraussetzung gibt es ein $v \in \mathbb{Z}[\sqrt{-5}]$ mit

$$u\bullet v = 1.$$

Es folgt

$$N(u) \bullet N(v) = 1.$$

Da N(u) und N(v) nicht-negative ganze Zahlen sind, muß dann aber gelten

$$N(u) = N(v) = 1.$$

(ii) $\Rightarrow$ (iii).

Wir schreiben u in der Gestalt $u = x + y\bullet \sqrt{-5}$ mit ganzen Zahlen x und y. Dann gilt

$$x^2 + 5\bullet y^2 = 1,$$

also $y = 0$ und $x^2 = \pm 1$.

(iii) $\Rightarrow$ (i). trivial.

QED.

Bemerkung

Im weiteren müssen wir anders vorgehen als im Fall der ganzen Gaußschen Zahlen, denn wir wissen nicht, ob $\mathbb{Z}[\sqrt{-5}]$ ein ZPE-Ring ist. Die Teilbarkeitsargumente von 1.1.3 sind deshalb nicht anwendbar.

1.2.2 Die Unzerlegbarkeit einiger Elemente von $\mathbb{Z}[\sqrt{-5}]$

Die Elemente 2, 3, $1 + \sqrt{-5}$ und $1 - \sqrt{-5}$ sind im Ring $\mathbb{Z}[\sqrt{-5}]$ unzerlegbar.

Beweis. Angenommen, 2 wäre zerlegbar. Dann gibt es Nicht-Einheiten $u, v \in \mathbb{Z}[\sqrt{-5}]$ mit

$$2 = u\bullet v,$$

also mit

$$4 = N(2) = N(u)\bullet N(v).$$

Weil u und v keine Einheiten sind, müssen die beiden Faktoren rechts > 1 sein. Es folgt

$$N(u) = N(v) = 2.$$

Schreiben wir u in der Gestalt

$$u = x + y\bullet \sqrt{-5}$$

mit ganzen Zahlen x und y. Es folgt

$$x^2 + 5\bullet y^2 = 2.$$

Das ist nur möglich, wenn y = 0 ist (andernfalls wäre die linke Seite > 2), also $x^2 = 2$, was nicht möglich ist. Wir haben gezeigt, 2 ist unzerlegbart.
Dieselbe Argumentation mit 3, $1 + \sqrt{-5}$ und $1 - \sqrt{-5}$ zeigt auch die Unzerlegbarkeit dieser Elemente:

$$3 = u \cdot v \Rightarrow 9 = N(u) \cdot N(v) \Rightarrow 3 = N(u) = x^2 + 5 \cdot y^2 \Rightarrow 3 = x^2 \text{ Widerspruch}$$

bzw.

$$1 \pm \sqrt{-5} = u \cdot v \Rightarrow 6 = N(u) \cdot N(v) \Rightarrow 2 \text{ oder } 3 = N(u) = x^2 + 5 \cdot y^2$$
$$\Rightarrow 2 \text{ oder } 3 = x^2 \text{ Widerspruch}$$

QED.

1.2.3 Folgerung

$\mathbb{Z}[\sqrt{-5}]$ ist kein ZPE-Ring.

Beweis. Wäre $\mathbb{Z}[\sqrt{-5}]$ ein ZPE-Ring, so wären nach 1.2.2 die Zahlen

$$2,\ 3,\ 1 + \sqrt{-5} \text{ und } 1 - \sqrt{-5}$$

Primelemente dieses Rings. Wegen

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

würde

$$2 \mid 1 + \sqrt{-5} \text{ oder } 2 \mid 1 - \sqrt{-5}$$

gelten. Beides ist nicht der Fall, denn

$$\frac{1}{2} + \frac{1}{2}\sqrt{-5} \text{ und } \frac{1}{2} - \frac{1}{2}\sqrt{-5}$$

sind keine Elemente von $\mathbb{Z}[\sqrt{-5}]$.
QED.

Bemerkung

Die obigen Ergebnisse zeigen, für den Ring $\mathbb{Z}[\sqrt{-5}]$ kann mit Aussagen, wie wir sie für $\mathbb{Z}$ und Γ kennen, nicht erwarten. Ein Grund dafür könnte sein, daß $\mathbb{Z}[\sqrt{-5}]$ der falsche Teilring von $\mathbb{Q}(\sqrt{-5})$ ist. Es stellt sich also die Frage, gibt es einen Teilring

$$R \subseteq \mathbb{Q}(\sqrt{-5}) \text{ mit } Q(R) = \mathbb{Q}(\sqrt{-5}) \text{ und } \mathbb{Z} \subseteq Q(R),$$

welcher ZPE-Ring ist, d.h. gibt es ein Diagramm

$$\begin{array}{ccc} \mathbb{Q} & \subseteq & \mathbb{Q}(\sqrt{-5}) \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & R \end{array}$$

dessen obere Zeile gerade aus den Quotientenkörpern der unteren Zeile besteht mit

$$R \text{ ZPE-Ring.}$$

Die Antwort lautet ja: $R = \mathbb{Q}(\sqrt{-5})$ ist ein solcher Ring. Das ist natürlich nicht die Antwort, die wir suchen. Der Ring R sollte kein Körper sein, er sollte dem Ring $\mathbb{Z}$ möglichst nahe stehen. Eine Forderung, die man zusätzlich stellen könnnte wäre zum Beispiel die Bedingung, daß

$$R \text{ endlich erzeugter } \mathbb{Z}\text{-Modul}$$

sein soll. Es stellt sich heraus, daß diese zusätzliche Forderung eine Möglichkeit bietet, den Ring R,, falls es ihn gibt, zu bestimmen. Der Ring R ist dann nämlich gerade die sogenannte ganze Abschließung von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$ (welche eindeutig bestimmt ist und sich

berechnen läßt). Wir müssen uns deshalb zunächst mit ganzen Erweiterungen von Ringen und ganzen Abschließungen beschäftigen.

1.3 Ganze Erweiterungen

1.3.1 Definition

Sei $h:R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen mit 1. Ein Element

$$\alpha \in S$$

heißt ganz über R (bezüglich h), wenn es ein Polynom

$$f \in R[x]-\{0\}$$

mit dem höchsten Koeffizienten 1 gibt mit

$$f^h(\alpha) = 0.$$

Dabei bezeichne $f^h \in S[x]$ das Polynom, welches man aus f erhält, wenn man auf alle Koeffizienten den Homomoprhismus h anwendet. Das Polynom f heißt in dieser Situation auch Ganzhzeitspolynom für α.

Der Homomorphismus $h: R \longrightarrow S$ heißt ganz, wenn jedes Element von S ganz ist über R bezüglich h.

Bemerkungen

(i) Der Homomorphismus $h: R \longrightarrow S$ ist genau dann ganz, wenn die natürliche Einbettung

$$h(R) \hookrightarrow S$$

ein ganzer Homomorphismus ist. Bei der Untersuchung von Ganzheitsfragen kann man sich deshalb meist auf den Fall beschränken, daß R ein Teilring von S und h die natürliche Einbettung ist. In dieser Situatin spricht man dann davon, daß S ganz ist über dem Teilring R.

(ii) In der obigen Situation besitzt S in natürlicher Weise die Struktur eines Moduls über R. Die Modul-Multiplikation ist dabei gegeben durch die Abbildung

$$R \times S \longrightarrow S,\ (r, s) \mapsto h(r)\bullet s.$$

Wir werden im folgenden, oft vereinfachend

$$r\bullet s := h(r)\bullet s$$

schreiben, wenn klar ist, welches der Homomoprhismus h sein soll.

1.3.2 Kriterium für die Ganzheit eines Elements

Seien $h:R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen mit 1 und $\alpha \in S$ ein Element. Dann sind folgende Aussagen äquivalent.

(i) α ist ganz über R bezüglich h.

(ii) Der Ring $h(R)[\alpha]$ ist ein endlich erzeugter R-Teilmodul von S.

(iii) Es gibt einen endlich erzeugten R-Teilmodul $M \subseteq S$ mit

$$\alpha M \subseteq M \text{ und } 1 \in M.$$

Beweis. (i) $\Rightarrow$ (ii). Nach Voraussetzung besteht eine Relation der Gestalt

(1) $$\alpha^n + h(a_1)\alpha^{n-1} + ... + h(a_n) = 0 \text{ mit } a_i \in R.$$

Sei

$$M := R\bullet \alpha^0 + R\bullet \alpha + R\bullet \alpha^2 + ... + R\bullet \alpha^{n-1}$$

Dann ist M ein endlich erzeugter R-Modul mit

$$h(R)\bigcup\{\alpha\} \subseteq M \subseteq h(R)[\alpha].$$

Es reicht zu zeigen, rechts gilt das Gleichheitszeichen. Der Ring

$$h(R)[\alpha]$$

ist der kleinste Teilring von S, der h(R) und α enthält. Deshalb reicht es zu zeigen,

$$M \text{ ist ein Teilring von } S.$$

Offensichtlich ist M eine additive Untergruppe von S. Es reicht also zu zeigen, das Produkt von zwei Elementen aus M liegt wieder in M. Da M ein R-Modul ist, reicht es zu zeigen, das Produkt von je zwei der Erzeugenden α^i liegt wieder in M,

$$\alpha^i\bullet\alpha^j \in M \text{ für } i,j = 0,...,n-1.$$

Zum Beweis kann man annehmen, i = 1. Dann ist die Aussage aber für j=0,..., n-2 trivial:

$$\alpha\bullet \alpha^j = \alpha^{j+1} \in M.$$

Sei also h = n-1. Wir haben zu zeigen $\alpha^n \in M$. Das gilt aber wegen (1).

(ii) $\Rightarrow$ (iii). trivial: $M = h(R)[\alpha]$ ist ein solcher Modul.

(iii) $\Rightarrow$ (i). (vgl. den Beweis der Cramerschen Regel). Sei

$$M = Rm_1 + ... + Rm_s$$

ein Teilmodul von S mit $\alpha M \subseteq M$ und $1\in M$. Wegen $\alpha M \subseteq M$ gilt

$$\alpha m_i = \sum_{j=1}^{s} a_{ij} m_j \text{ mit } a_{ij} \in R,$$

d.h.

$$0 = \sum_{j=1}^{s} (\alpha\delta_{ij} - a_{ij}) m_j \text{ für } i = 1,...,s,$$

wobei δ_{ij} das Kronecker-Symbol bezeichne. Wir fixieren jetzt einen Index ℓ und betrachten die s×s- Matrix

$$(\alpha\delta_{ij} - a_{ij}).$$

Wir multiplizieren die i-te Gleichung mit der adjungierten Unterdeterminante $A_{i\ell}$ und bilden die alternierende Summe. Nach dem Entwicklungssatz für Determinanten erhalten wir

$$0 = \det(\alpha\delta_{ij} - a_{ij})\bullet m_\ell.$$

Diese Relation gilt für jedes m_ℓ und, da die m_ℓ den Modul M erzeugen, für jedes Element von m,

$$\det(\alpha\delta_{ij} - a_{ij})\bullet m = 0 \text{ für jedes } m\in M.$$

Wegen $1\in M$ ist damit auch

$$\det(\alpha\bullet h(\delta_{ij}) - h(a_{ij})) = 0.$$

Nun ist

$$f(x) = \det(\delta_{ij}\bullet x - a_{ij}) \in R[x]$$

ein Polynom vom Grad s mit dem höchsten Koeffizienten 1 und es gilt

$$f^h(\alpha) = \det(\alpha\bullet h(\delta_{ij}) - h(a_{ij})) = 0.$$

Mit anderen Worten α ist ganz über R.
QED.

1.3.3 Beispiele

(i) Der Ring der ganzen Gaußschen Zahlen ist ganz über $\mathbb{Z}$ (weil er als $\mathbb{Z}$-Modul endlich erzeugt ist).

(ii) Ist S ein kommutativer Ring mit 1,

$$R \subseteq S$$

ein Teilring mit 1 und $x \in S$ ein über R ganzes Element, so ist

$$R[x] \text{ ganz über } S.$$

Denn R[x] ist dann ein endlich erzeugter R-Modul der das Einselement enthält und jedes Element y von R[x] hat die Eigenschaft

$$y \bullet R[x] \subseteq R[x]$$

(ii) Die Ringe $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\sqrt[3]{2}]$, ...sind ganz über $\mathbb{Z}$ weil die Elemente $\sqrt{-5}$, $\sqrt[3]{2}$ sind über dem Ring $\mathbb{Z}$::;

$$(\sqrt{-5})^2 + 5 = 0,\ (\sqrt[3]{2})^2 - 2 = 0,\ \ldots$$

1.3.4 Die ganze Abschließung

Sei $h: R \longrightarrow S$ ein Homomorphismus von Ringen mit 1. Dann ist die Menge

$$\overline{R} := \{ x \in S \mid x \text{ ist ganz über R bezüglich h} \}$$

ein Teilring von S. Er heißt <u>ganze Abschließung</u> von R in S.

Ist R ein Teilring von S und h die natürliche Einbettung $R \longrightarrow S$, so sagt man, R ist <u>ganz abgeschlossen</u> in S, falls $R = \overline{R}$ gilt. Ein Integritätsbereich, der ganz abgeschlossen ist in seimen Quotientenkörper, heiß <u>normal</u>.

Beweis. Wir können R durch $h(R) \subseteq S$ ersetzen und deshalb annehmen,

$$R \subseteq S$$

(und h ist die natürliche Einbettung). Wir haben zu zeigen, mit je zwei Elementen

$$x,y \in \overline{R}$$

liegt auch das Produkt und die Summe in $\overline{R}$. Weil x ganz ist über R, ist R[x] ein endlich erzeugter R-Modul,

$$R[x] = R\omega_1 + \ldots + R\omega_s$$

Weil das Element y ganz ist über R, ist es auch ganz über R[x], d.h.
R[x,y] ist ein endlich erzeugter R[x]-Modul,

$$R[x, y] = R[x]\eta_1 + \ldots + R[x]\eta_s.$$

Zusammen erhalten wir, daß R[x,y] als Modul über R von den endlich vielen Produkten

$$\omega_i.\eta_j$$

erzeugt wird. Deshalb ist jedes Element von R[x,y] ganz über R, inbesondere also auch xy und x+y.
QED.

1.3.5 Beispiel für einen normalen Integritätsbereich

Sei R ein ZPE-Ring mit dem Quotientenkörper K. Dann ist R ganz abgeschlossen in K, also normal.

Beweis. Sei $x \in K$ ganz über K. Wir haben zu zeigen,

$$x \in R.$$

Wir schreiben x in der Gestalt

$$x = a/b \text{ mit } a,b \in R \text{ und } a,b \text{ teilerfremd.}$$

Nach Voraussetzung gilt für x eine Identität der Gestalt

$$x^n + a_1 x^{n-1} + ... + a_n = 0 \text{ mit } a_i \in R.$$

Wir multiplizieren diese Identität mit b^n und erhalten

$$a^n + a_1 a^{n-1} b + a_2 a^{n-2} b^2 + ... + a_n b^n = 0.$$

Dies ist eine Identität in R. Es gilt also

$$b \text{ teilt } a^n.$$

Das ist aber nur möglich, wenn b eine Einheit ist, denn a und b sind nach Wahl teilerfremd. Also ist x = a/b ein Element von R.

QED.

Bemerkung

Kehren wir zur Situation zurück, wie wir sie in 1.2.3 betrachtet haben:

$$\begin{array}{ccc} \mathbb{Q} & \subseteq & \mathbb{Q}(\sqrt{-5}) \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & R \end{array}$$

mit einem Ring R, der als $\mathbb{Z}$-Modul endich erzeugt ist und den Quotientenkörper $\mathbb{Q}(\sqrt{-5})$ besitzt. Dann ist R ganz über $\mathbb{Z}$. Ist R außerdem ein ZPE-Ring, so ist R nach dem eben bewiesenen Ergebnis ganz abgeschlossen in $\mathbb{Q}(\sqrt{-5})$. Mit anderen Worten, der von uns gesuchte Ring ist gerade die ganze Abschließung von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$,

$$R = \text{ganze Abschließung von } \mathbb{Z} \text{ in } \mathbb{Q}(\sqrt{-5}).$$

Das nachfolgende Ergebnis besagt leider, daß wir damit nicht weitergekommen sind, den die gesuchte ganze Abschließung ist danach gerade der Ring

$$\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z} \bullet \sqrt{-5},$$

von dem wir bereits wissen, daß es kein ZPE-Ring ist. Es besagt aber auch, daß es keinen ZPE-Ring gibt, we wir ihn suchen: wir werden uns etwas anderes einfallen lassen müssen.

1.3.6 Beispiel für eine ganze Abschließung: $\mathbb{Z}[\sqrt{-5}]$

Die ganze Abschließung von $\mathbb{Z}$ im Zahlenkörper $\mathbb{Q}(\sqrt{-5})$ ist der Ring $\mathbb{Z}[\sqrt{-5}]$.

Beweis. Weil

$$\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z} \bullet \sqrt{-5},$$

als Modul über $\mathbb{Z}$ endlich erzeugt ist, ist $\mathbb{Z}[\sqrt{-5}]$ ganz über über $\mathbb{Z}$. Wir haben noch zu zeigen, jedes über $\mathbb{Z}$ ganze Element von $\mathbb{Q}(\sqrt{-5})$ liegt in diesem Ring. Sei also

$$\alpha = a + b \bullet \sqrt{-5} \in \mathbb{Q}(\sqrt{-5})$$

ganz über $\mathbb{Z}$. Dann ist aber auch

$$\overline{\alpha} = a - b\bullet\sqrt{-5}$$

ganz über $\mathbb{Z}$ (dann das Ganzheitspolynom für α besitzt auch $\overline{\alpha}$ als Nullstelle). Dann sich abert auch die rationalen Zahlen

$$\alpha+\overline{\alpha} = 2a$$

und

$$\alpha\bullet\overline{\alpha} = a^2 + 5\bullet b^2$$

ganz über $\mathbb{Z}$. Nun ist $\mathbb{Z}$ ein ZPE-Ring, also ganz abgeschlossen in $\mathbb{Q}$, d.h. es gilt[6]

$$2a \in \mathbb{Z} \text{ und } a^2 + 5\bullet b^2 \in \mathbb{Z}. \qquad (1)$$

Wir schreiben

$$a = \frac{1}{2}a' \text{ mit } a' \in \mathbb{Z}.$$

Es folgt $\frac{1}{4}\bullet a'^2 + 5\bullet b^2 \in \mathbb{Z}$, also $a'^2 + 20\bullet b^2 \in \mathbb{Z}$, also $20\bullet b^2 \in \mathbb{Z}$. Damit läßt sich b in der folgenden Gestalt schreiben:

$$b = \frac{u}{v} \text{ mit u, v} \in \mathbb{Z}, \text{ u, v teilerfremd, } v^2 \mid 20 = 2^2\bullet 5.$$

Daraus ergibt sich $v \mid 2$ und wir können schreiben

$$b = \frac{1}{2}b' \text{ mit } b' \in \mathbb{Z}.$$

Durch Einsetzen in den rechten Ausdruck von (1) erhalten wir

$$a'^2 + 5\bullet b'^2 \in 4\mathbb{Z},$$

d.h.

$$a'^2 + b'^2 \equiv 0 \bmod 4.$$

Da das Quadrat einer ganzen Zahl nur kongruent 0 oder 1 modulo 4 sein kann, folgt

$$a'^2 \equiv b'^2 \equiv 0 \bmod 4,$$

d.h. a' und b' sind gerade und a und b sind ganz:

$$a, b \in \mathbb{Z},$$

d.h. $\alpha = a + b\bullet\sqrt{-5} \in \mathbb{Z}[-5]$.

Wir haben gezeigt, $\mathbb{Z}[-5]$ ist die ganze Abschließung von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$.
QED.

Bemerkungen

(i) Ist R ein ZPE-Ring und

$$x = (p_1)^{n1}\bullet\ldots\bullet(p_s)^{ns} \qquad (2)$$

so besteht für die von x und den p_i erzeugten Ideale

$$I := xR \text{ und } \wp_i := p_iR$$

die Relation

$$I = (\wp_1)^{n1}\bullet\ldots\bullet(\wp_s)^{ns} \qquad (3)$$

und diese Relation ist äquivalent zu (2). Der Satz über die eindeutige Zerlegung in Primfaktoren läßt sich also auch in der folgenden Weise formulieren:
Jedes von 0 und R verschiedene Ideal I eines ZPE-Rings läß sich in eine Produkt von Primidealpotenzen zerlegen. Die Exponenten in dieser Zerlegung sind eindeutig bestimmt.

---

[6] Man beachte, aus den beiden nachfolgenden Relationen folgt auch umgekehrt, daß α ganz ist über $\mathbb{Z}$, denn α ist Nullstelle des Polynoms

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})\bullet x + \alpha\bullet\overline{\alpha}\ .$$

(ii) Wie sich herausstellt, läßt sich die Aussage in der Gestalt (3) auf den Fall verallgemeinern, daß R ein normaler Integritätsbereich ist, in welchem jedes von 0 verschiedene Primideal maximal ist. Solche Ringe heißen Dedekind-Ringe.

Wir werden später sehen, die ganze Abschließung

$$\mathcal{O}_K$$

von $\mathbb{Z}$ in einer endlichen Körpererweiterung K von $\mathbb{Q}$ ist ein Dedekind-Ring. Diese Ringe spielen deshalb dieselbe Rolle für den Körper K, wie es die ganzen Zahlen für den Körper der rationalen Zahlen spielen. Der Ring $\mathcal{O}_K$ heißt deshalb auch Ring der ganzen Zahlen von K. Um diese ganzen Zahlen von den gewöhnlichen ganzen Zahlen von $\mathbb{Z}$ zu unterscheiden, werden wir letzter auch ganze rationale Zahlen nennen.

(iii) Bevor wir die Dedekind-Ringe etwas genauer beschreiben und den Zerlegungssatz beweisen können, benötigen wir einige elementare Eigenschaften der sogenannten diskreten Bewertungsringe.

1.4 Gebrochene Ideale und diskrete Bewertungsringe

1.4.1 Operationen mit Idealen

Seien R ein Integritätsbereich mit dem Quotientenkörper

$$K = Q(R)$$

und

$$I', I'' \subseteq K$$

R-Teilmoduln von K. Dann sind[7]

$$I' + I'',\ I' \bigcap I'',\ I' \bullet I''$$

ebenfalls R-Teilmoduln von K. Weiter sind für jeden R-Teilmodul

$$I \subseteq K$$

die beiden folgenden Mengen wieder R-Teilmoduln von K.

$$I^{-1} := \{ x \in K \mid xI \subseteq R \},$$

$$R(I) := \{ x \in K \mid xI \subseteq I \}.$$

1.4.2 Eigenschaften von Ideal-Operationen

(i) Addition, Multiplikation und Durchschnitt von R-Teilmoduln von K sind assoziative und kommutative Operationen.

(ii) $I \bullet (I' + I'') = I \bullet I' + I \bullet I''$.

(iii) $R(I) \supseteq R \supseteq I \bullet I^{-1}$.

(iv) $I' \subseteq I'' \longrightarrow I''^{-1} \subseteq I'^{-1}$.

1.4.3 Begriff des gebrochenen Ideals

Sei R ein Integritätsbereich mit dem Quotientenkörper

$$K = Q(R).$$

---

[7] Nach Definition ist

$$I' + I'' := \{x' + x'' \mid x' \in I' \text{ und } x'' \in I''\}$$

und

$$I' \bullet I''$$

ist der von den Produkten $x' \bullet x''$ mit $x' \in I'$ und $x'' \in I''$ erzeugte R-Modul.

Ein gebrochenes Ideal von R ist ein R-Teilmodul

$$I \subseteq K$$

von K mit $I \neq 0$ und mit der Eigenschaft, daß es ein Element $a \in K - \{0\}$ gibt mit

$$aI \subseteq R.$$

Bemerkungen

(i) Das Element a kann man in der beschriebenen Situation aus $R - \{0\}$ wählen.
(ii) aI ist ein Ideal von R.

1.4.4 Eigenschaften von gebrochenen Idealen

Seien R ein Integritätsbereich und I', I" und I gebrochene Ideale von R. Dann sind auch die folgenden Mengen gebrochene Ideale.

$$I' + I'',\ I' \bigcap I'',\ I' \bullet I'',\ I^{-1},\ R(I).$$

Beweis. Für die ersten drei Mengen ist das offensichtlich. Für die letzten beiden betrachten wir die Menge

$$J := \{ x \in K \mid xI'' \subseteq I' \}.$$

Für $I' = R$ und $I'' = I$ ist $J = I^{-1}$. Für $I' = I'' = I$ ist $J = R(I)$. Es reicht also zu zeigen, daß J ein gebrochenes Ideal ist.

Die Menge J ist $\neq 0$: wählen wir von Null verschiedene Elemente a, b mit

$$aI'' \subseteq R \text{ und } b \in I' \bigcap R.$$

Dann ist ab ein von Null verschiedenes Element mit

$$ab \in J.$$

Es gibt ein von Null verschiedenes Element c mit $cJ \subseteq R$: wir wählen von Null verschiedene Elemente e, f mit

$$eI' \subseteq R \text{ und } f \in I''.$$

Dann gilt $efJ \subseteq R$.

QED.

1.4.5 Kriterium für gebrochene Ideale im Fall noetherscher Ringe

Seien R ein noetherscher Integritätbereich mit dem Quotientenkörper K und

$$I \subseteq K$$

ein von Null verschiedener R-Teilmodul von K. Dann sind folgende Aussagen äquivalent.

(i) I ist ein gebrochenes Ideal von R.
(ii) I ist als R-Modul endlich erzeugt.

Beweis. (i) $\Rightarrow$ (ii). Sei $a \in K - \{0\}$ ein Element mit $aI \subseteq R$. Weil R noethersch ist, besitzt das Ideal aI ein eindliches Erzeugenden System, sagen wir

$$aI = Ra_1 + ... + Ra_n.$$

Dann gilt aber

$$I = R \bullet \frac{a_1}{a} + ... + R \bullet \frac{a_n}{a},$$

d.h. der R-Modul I ist endlich erzeugt.

(ii) $\Rightarrow$ (i). Sei $a_1, ..., a_n \in K$ ein endliches Erzeugendensystem des R-Moduls I,

$$I = R \bullet a_1 + ... + R \bullet a_n.$$

Jedes a_i können wir in der Gestalt $a_i = \frac{b_i}{c_i}$ schreiben mit $b_i, c_i \in R$, $c_i \neq 0$. Wir setzen

$$c = c_1 \bullet \ldots \bullet c_n.$$

Dann gilt $c \bullet a_i \in R$ für jedes i, also

$$c \bullet I = R \bullet ca_1 + \ldots + R \bullet ca_n \subseteq R.$$

QED.

1.4.6 Begriff der diskreten Bewertung

Sei K ein Körper. Eine diskrete Bewertung von K ist ein surjektiver Gruppenhomomorphismus

$$v: K^* \longrightarrow \mathbb{Z}$$

der multiplikativen Gruppe des Körpers K auf die additive Gruppe der ganzen rationalen Zahlen. Dabei soll nach Vereinbarung

$$v(0) = \infty$$

sein und für je zwei Elemente $x, y \in K$ soll gelten

$$\min \{ v(x), v(y) \} \leq v(x + y)$$

1.4.7 Beispiel: formale Laurent-Reihen

Seien F ein Körper, t eine Unbestimmte und

$$K := F((t))$$

der Körper der formalen Laurent-Reihen, d.h. der formalen Summen der Gestalt

$$f := \sum_{n >> -\infty}^{\infty} a_n t^n \text{ mit } a_n \in F \text{ für alle n.} \qquad (1)$$

Dabei soll $n >> -\infty$ bedeuten, daß es nur endlich viele von Null verschiedene a_n mit negagiven n geben soll. In dieser Situation ist durch

$$v(f) := \inf \{ n \mid a_n \neq 0\}$$

eine diskrete Bewertung gegegen. Mit anderen Worten v(f) ist die Nullstellen-Polstellen-Ordung von f an der Stelle t = 0.
Um einzusehen, daß K tatsächlich ein Körper ist, betrachtet man zunächst den formalen Potenzreihen ring

$$F[[t]]$$

d.h. die Menge der formalen Summen den Gestalt

$$f := \sum_{n = 0}^{\infty} a_n t^n \text{ mit } a_n \in F \text{ für alle n.} \qquad (2)$$

Man sieht sofort, daß man solche Summen addieren kann (indem man die Koeffizienten a_n addiert). Die Formel für die Multiplikation von Polynomen aus F[t] definiert auch für solche formalen Summen eine Multiplikation und versieht F[[t]] mit der Struktur eines kommutativen Rings mit 1. In diesem Ring ist das Element 1 - t umkehrbar, und es gilt

$$\frac{1}{1-t} = 1 + t + t^2 + t^3 + \ldots = \sum_{n = 0}^{\infty} t^n$$

(wie man durch Multiplizieren von 1 - t mit der Reihe auf der rechten Seite sieht). Für jede Reihe (2) mit dem Absolutglied

$$f(0) = a_0 = 1$$

sieht man, indem man in der obigen Formel für t die Reihe

$$f - f(0) = \sum_{n=1}^{\infty} a_n t^n$$

einsetzt, daß auch die Reihe (2) umkehrbar ist. Insgesamt ergibt sich:

$$f \in F[[t]] \text{ ist umkehrbar} \Leftrightarrow f(0) \neq 0.$$

Insbesondere sehen wir, der Potenzreihenring F[[t]] ist ein lokaler Ring mit dem einzigen maximalen Ideal

$$t \bullet F[[t]].$$

Mit anderen Worten, jedes Element $f \in F[[t]] - \{0\}$ hat die Gestalt

$$f = t^n \bullet u \tag{3}$$

mit einer eindeutig bestimmten Potenzreihe u, deren Absolutglied $\neq 0$ ist, die also eine Einheit von F[[t]] ist. Mit der oben definierten Funktion v gilt

$$v(f \bullet g) = v(f) + v(g) \text{ für } f, g \in F[[t]] - \{0\}$$

(weil sich die Anfangsterme der Potenzreihen multiplizieren, wenn man die Potenzreihen multpliziert). Insbesondere ist mit f und g auch f•g von Null verschieden, d.h.

$$F[[t]] \text{ ist ein Integritätsbereich.}$$

Auf Grund der Beschreibung (3) der von Null verschiedenen Elemente von (3) sehen wir, die von Null verschiedenen Elemente des Quotientenkörpers haben die Gestalt

$$f = t^n \bullet u,\ n \in \mathbb{Z} \text{ und u Einheit von } F[[t]].$$

Mit anderen Worten, es gilt

$$Q(F[[t]]) = F((t)).$$

1.4.8 Eigenschaften diskreter Bewertungen

(i) Für jede diskrete Bewertung $v: K^* \longrightarrow \mathbb{Z}$ und Elemente x, y mit $v(x) \neq v(y)$ gilt

$$v(x + y) = \min\{ v(x), v(y) \}.$$

(ii) Für jede diskrete Bewertung $v: K^* \longrightarrow \mathbb{Z}$ ist die Menge

$$R_v := \{x \in K \mid v(x) \geq 0\}$$

ein kommutativer Integritätsbereich mit 1, der genau ein maximales Ideal besitzt. Dieses maximale Ideal wird von nur einem Element erzeugt. Jedes Element $x \in K$ mit $v(x) = 1$ erzeugt dieses Ideal. Der Ring R_v hei0t Bewertungsring von v, dessen maximales Ideal Bewertungsideal von v.

Jedes Element $y \in K^*$ läßt sich auf genau eine Weise in der Gestalt

$$y = u \bullet x^n$$

schreiben mit einer ganzen Zahl n und einer Einheit u von R_v. Jedes von Null verschiedene Ideal von R_v hat die Gestalt

$$x^n R,\ n \in \mathbb{Z},\ n \geq 0.$$

Insbesondere ist xR das einzige von Null verschiedene Primideal und es gilt

$$\bigcap x^n R = 0$$

(Krullscher Durchschnittssatz).

(iii) Sei R ein kommutativer Integritätsbereich mit 1 mit genau einem von Null verschiedenen Primideal[8]. Dieses Ideal werde von nur einem Element erzeugt. Dann ist R Bewertungsring einer diskreten Bewertung des Quotientenkörpers von R.

Beweis. Zu (ii). Weil $v: K^* \longrightarrow \mathbb{Z}$ ein Homomorphismus ist, gilt

$$x, y \in R_v - \{0\} \Rightarrow v(xy) = v(x) + v(y) \geq 0 \Rightarrow xy \in R_v.$$

Weiter gilt

$$x, y \in R_v \Rightarrow v(x + y) \geq \min \{v(x), v(y)\} \geq 0 \Rightarrow x + y \in R_v.$$

Wegen

$$v(1) = v(1 \bullet 1) = v(1) + v(1)$$

gilt $v(1) = 0$, also

$$1 \in R_v.$$

Weiter ist

$$0 = v(1) = v((-1) \bullet (-1)) = v(-1) + v(-1) = 2 \bullet v(-1),$$

also $v(-1) = 0$, d.h.

$$-1 \in R_v.$$

Zusammen sehen wir, daß R ein kommutativer Ring mit 1 ist. Wegen $R_v \subseteq K$ ist R_v ein Integritätsbereich. Weil die Abbildung

$$v: K^* \longrightarrow \mathbb{Z}$$

surjektiv ist, gibt es ein Element

$$\pi \in K^* \text{ mit } v(\pi) = 1.$$

Insbesondere ist

$$\pi \in R_v.$$

Ist $y \in K^*$ ein beliebiges weiteres Element und bezeichnet $n := v(y) \in \mathbb{Z}$ dessen Wert, so gilt

$$v(y/\pi^n) = v(y) - n \bullet v(\pi) = n - n = 0$$

d.h.

$$u = y/\pi^n$$

ist ein Element von R_v mit dem Wert 0, d.h. auch u^{-1} liegt in R_v. Wir haben gezeigt, jedes Element von K^* hat die Gestalt

$$y = u \bullet \pi^n \text{ mit einer Einheit } u \in R_v^*.$$

Dabei sind u und n durch y eindeutig festgelegt, denn es ist

$$v(y) = v(u \bullet \pi^n) = v(u) + n \bullet v(\pi) = 0 + n \bullet 1 = n,$$

d.h. n ist eindeutig bestimmt (und damit auch u). Weiter gilt

$$y \in R_v \Leftrightarrow n \geq 0$$

und

$$y \in \pi R_v \Leftrightarrow v(y) \geq 1.$$

---

[8] Im Fall noetherscher Ringe reicht es zu fordern, daß es genau ein von Null verschiedenes maximales Ideal gibt. Nach dem Krullschen Durchschnittssatz für nullteilerfreie lokale Ringe gibt es dann auch nur ein von Null verschiedens Primideal.

Insbesondere ist jedes Element von R_v, welches nicht in πR_v liegt, eine Einheit. Mit anderen Worten,

$$\pi R_v = \{y \in K \mid v(y) \geq 1\}$$

ist das einzeige maximale Ideal von R_v. Letztere Identität gilt für jedes Element $\pi \in K^*$ mit $v(\pi) = 1$.

Sei jetzt J ein von Null verschiedenes Ideal von R_v. Wir fixieren ein

$$\text{Erzeugendensystem } \{a_i\}_{i \in I},$$

d.h. eine Familie von Elementen a_i aus J mit der Eigenschaft, daß jedes Element von J eine R-Linearkombination der a_i ist. Wir schreiben die a_i in der Gestalt

$$a_i = u_i \pi^{n_i} \text{ mit } u_i \in R_v^*, \; n_i \in \mathbb{Z}, \; n_i \geq 0,$$

und setzen

$$n := \min \{n_i\}.$$

Dann gibt es ein i mit $n = n_i$.. Alle Erzeuger sind damit Vielfache des zugehörigen a_i und es gilt

$$I = a_i R_v = \pi^n R_v$$

Zu (iii). Sei

$$m = \pi \bullet R, \; \pi \in R,$$

das einzige von Null verschiedene Primideal von R. Dann ist m auch das einzige maximale Ideal von R. Für jedes $x \in R$ setzen wir

$$\begin{aligned} v(x) &:= \sup \{ n \in \mathbb{Z} \mid n \geq 0, \, x \in m^n\} \\ &:= \sup \{ n \in \mathbb{Z} \mid n \geq 0, \, \pi^n \mid x\} \end{aligned}$$

Dann gilt für $x, y \in R$

$$v(xy) \geq v(x) + v(y).$$

Angenommen, es gibt Elemente $x, y \in R - \{0\}$ mit

$$v(xy) > v(x) + v(y),$$

Dann sind die Summanden v(x) und v(y) auf der rechten Seite endlich,

$$x = u \bullet \pi^a, \; y = v \bullet x^b, \; a = v(x), \; b = v(y), \; u, v \in R.$$

Die Elemente u und v können dann nicht in m liegen, d.h. sie sind Einheiten,

$$u, v \in R^*.$$

Wegen der obigen echten Ungleichung besteht aber auch eine Relation

$$xy = w \bullet \pi^{a+b+1} \text{ mit } w \in R.$$

d.h.

$$uv \bullet \pi^{a+b} = w \bullet \pi^{a+b+1}.$$

Weil R ein Integritätsbereich ist, folgt

$$uv = w \bullet \pi \in m,$$

Das Produkt uv der Einheiten u und v ist eine Nicht-Einheit. Das ist offensichtlich nicht möglich. Wir haben damit gezeigt

$$v(xy) = v(x) + v(y) \text{ für beliebige Element } x, y \in R. \qquad (1)$$

Als maximales Ideal ist m echt enthalten in R,

$$m \subset R.$$

Weil R ein Integritätsbereich ist, ist die Multiplikation mit π eine injektive Abbildung. Aus der obigen echten Inklusion erhält man also durch Multiplikation mit π^n die echte Inklusion

$$m^{n+1} \subset m^n.$$

Insbesondere gibt es ein Element

$$x \in m - m^2.$$

Weil x ein Vielfaches des Erzeugers π von m ist, folgt

$$\pi \in m - m^2,$$

d.h.

$$v(\pi) = 1,$$

also

$$v(u\pi^n) = n \text{ für jede Einheit } u \in R^* \text{ und für n nicht-negativ ganz.}$$

Sei

$$J = \{x \in R \mid v(x) = \infty\}$$

die Menge der Elemente von R, die durch jede Potenz von π teilbar sind. Diese Menge ist ein Ideal von R, und es gilt

$$J = \bigcap_{n=1}^{\infty} m^n.$$

Für $xy \in J$ gilt wegen (1):

$$v(x) + v(y) = v(xy) = \infty,$$

also $v(x) = \infty$ oder $v(y) = \infty$. Mit anderen Worten,

J ist ein Primideal.

Wegen $J \subseteq m^2 \subset m$ muß dann aber $J = 0$ gelten, d.h. es gilt der Krullsche Durchschnittssatz[9]

$$\bigcap_{n=1}^{\infty} m^n. = 0. \qquad (2)$$

Mit anderen Worten nur für $x = 0$ gilt $v(x) = 0$,

$$v(x) < \infty \text{ für jedes } x \in R - \{0\}.$$

Insbesondere läßt sich jedes Element $x \in R - \{0\}$ in der Gestalt

---

[9] Der Durchschnittssatz von Krull besagt, daß für jedes echte Ideal I in einem noetherschen Integritätsbereichz gilt

$$\bigcap I^n = 0$$

(es gibt weitere Varianten dieses Satzes - vgl. Matsumura [1], Th. 8.10). Falls R nothersch ist, ist also (2) automatisch erfüllt. Wir müssen dann nur annehmen, das einzige maximale Ideal von R wird von einem Element erzeugt.

$$x = u \bullet \pi^n \text{ mit } n \in \mathbb{Z},\ n \geq 0\ ,\ u \text{ Einheit in } R$$

schreiben (man wähle für n die größte nicht-negative ganze Zahl mit $x \in m^n$, dann muß u eine Einheit sein). Die von Null verschiedenen Elemente des Quotientenkörpers

$$K = Q(R)$$

haben damit die Gestalt

$$x = u \bullet \pi^n \text{ mit } u \in R^*.$$

Wir können so die Abbildung v zu einem Homomorphismus

$$v: K^* \longrightarrow \mathbb{Z}$$

fortsetzen, indem wir setzen

$$v(u \bullet \pi^n) = n.$$

Dieser Homomorphismus ist surjektiv wegen $v(\pi) = 1$. Weiter gilt für $u, u' \in R^*$ und $n \leq n'$:

$$\begin{aligned} v(u \bullet \pi^n + u' \bullet \pi^{n'}) &= v((u + u' \bullet \pi^{n'-n}) \bullet \pi^n) \\ &= v(u + u' \bullet \pi^{n'-n}) + v(\pi^n) \\ &\geq v(\pi^n) \qquad (3) \\ &= n \\ &= \min\{n, n'\} \\ &= \min\{ v(u \bullet \pi^n) + v(u' \bullet \pi^{n'})\} \end{aligned}$$

d.h. für $x, y \in K$ gilt

$$v(x + y) \leq \min\{v(x), v(y)\}$$

Wir haben gezeigt, v ist ein diskrete Bewertung von K. Der zugehörige diskrete Bewertungsring ist

$$\{x \in K \mid v(x) \geq 0\} \quad = \{u \bullet \pi^n \mid n \geq 0\} = R.$$

Zu (i). In der gerade durchgeführten Rechnung gilt im Fall $n < n'$ in (3) das Gleichheitszeichen, denn das Element

$$u + u' \bullet \pi^{n'-n}$$

ist in dieser Situation eine Einheit, d.h. es gilt $v(u + u' \bullet \pi^{n'-n}) = 0$.

QED.

1.4.9 Definition: diskreter Bewertungsring

Ein diskreter Bewertungsring ist ein Hauptidealring[10] mit genau einem von Null verschiedenen Primideal.

1.4.10 Charakterisierung der diskreten Bewertungsringe

Sei R ein Integritätsbereich mit dem Quotientenkörper

$$K = Q(R).$$

Dann sind folgende Aussagen äquivalent.

(i) R ist ein Bewertungsring.
(ii) R ist Bewertungsring einer diskreten Bewertung von K.
(iii) R besitzt genau ein von Null verschiedenes Primideal, welches Hauptideal ist.
(iv) R ist noethersch, normal und besitzt genau ein von Null verschiedenes Primideal.

Beweis. (iii) $\Rightarrow$ (ii). Dies ist gerade die Aussage von 1.4.7 (iii).

---

[10] Ein Hauptidealring ist ein Integritätbereich mit der Eigenschaft, daß jedes Ideal ein Hauptideal ist, d.h. von nur einem Element erzeugt wird.

(ii) $\Rightarrow$ (i). Dies ist ein Teil der Aussage von 1.4.7 (ii).

(i) $\Rightarrow$ (iii). Gilt trivialerweise.

Wir haben gezeigt, die Aussagen (i), (ii) und (iii) sind äquivalent.

(i) $\Rightarrow$ (iv). Nach Voraussetzung ist R ein Hauptidealring, also insbesondere noethersch. Als Hauptidealring ist R ein ZPE-Ring, also normal (nach 1.3.5). Die letzte Bedingung von (iv) ist erfüllt auf Grund der Defintion des Begriffs "diskreter Bewertungsring" (vgl. 1.4.8).

(iv) $\Rightarrow$ (i). Es reicht zu zeigen, jedes Ideal von R ist ein Hauptideal.
Sei I ein beliebiges gebrochenes Ideal von R. Betrachten wir das gebrochene Ideal

$$R(I) := \{x \in K \mid xI \subseteq I\}$$

(vgl. 1.4.1 und 1.4.3).

1. Schritt: R(I) = R.

Aus der Definition von R(I) liest man ab, daß

R(I) kommutativer Ring mit 1

ist und daß die Inklusionen

$$R \subseteq R(I) \subseteq K$$

bestehen. Für jedes $\alpha \in R(I)$ gilt

$$R[\alpha] \subseteq R(I).$$

Weil R noethersch ist, ist das gebrochene Ideal R(I) als R-Modul endlich erzeugt (nach 1.4.4), also noethersch. Insbesondere ist $R[\alpha]$ als R-Modul endlich erzeugt, d.h. α ist ganz über R (nach 1.3.2). Weil R nach Voraussetzung normal ist, folgt $x \in R$. Wir haben gezeigt,

$$R(I) = R. \tag{1}$$

Bezeichne m das einzige von Null verschiedene Primideal von R. Wegen $m \subseteq R$ gilt

$$R = R(R) = R^{-1} \subseteq m^{-1} \tag{2}$$

Das erste Gleicheitszeichen ergibt sich aus (1), dann R ist ein gebrochenes Ideal über sich selbst. Das zweiter Gleichheitszeichen folgt direkt aus den Definitionen in 1.4.1 und die Inklusion rechts ergibt sich aus 1.4.2.

2. Schritt. $m^{-1} \neq R$.
Zumindest gibt es ein von Null verschiedenes Ideal I,

$$0 \neq I \subseteq R$$

mit

$$I^{-1} \neq R.$$

(zum Beispiel ist für $I = aR$ mit $a \in m - \{0\}$, das Ideal $I^{-1} \supseteq \frac{1}{a} R \supset R$ echt größer als R). Weil R noethersch ist, gibt es unter den Idealen I ein maximales. Sei

J

ein solches Ideal. Es reicht zu zeigen, J ist ein Primideal (denn dann gilt J = m).
Seien $x, y \in R$ Elemente mit

$$xy \in J \text{ und } x \notin J.$$

Es reicht zu zeigen, $y \in J$. Zum Beweis fixieren wir ein Element

$$z \in J^{-1} - R.$$

Es gilt

$$zy(xR + J) = zyxR + zyJ \subseteq zJ \subseteq R$$

also

$$zy \in (xR + J)^{-1}$$

Wegen $x \notin R$ und der Maximalität von J ist das Inverse von $xR + J$ gleich R, d.h. es ist

$$zy \in R,$$

also

$$z(yR + J) \subseteq R,$$

also

$$z \in (yR + J)^{-1}$$

Weil z nicht in R liegt, folgt

$$(yR + J)^{-1} \neq R.$$

Wegen der Maximalität von J kann das Ideal $yR + J$ nicht echt größer sein als J, d.h. es gilt

$$y \in J.$$

3. Schritt. $m \bullet m^{-1} = R$.
Es gilt

$$R \supseteq m \bullet m^{-1} \supseteq m.$$

Die linke Inklusion ergibt sich dabei aus der Definition von m^{-1}, die rechte aus $m^{-1} \supseteq R$ (vgl. (2)). Da das Ideal m maximal in R ist,, folgt

$$m \bullet m^{-1} = R \text{ oder } m \bullet m^{-1} = m.$$

Es reicht zu zeigen, die zweite Identität ist falsch. Angenommen, es wäre

$$m \bullet m^{-1} = m.$$

Nach Definition von R(m) ist dann

$$m^{-1} \subseteq R(m).$$

Nach dem ersten Schritt steht auf der rechten Seite aber R,, und diese Inklusion wiederspricht der Aussage des zweiten Schritts (zusammen mit (2)).

4. Schritt. $\bigcap_{n=1}^{\infty} m^n = 0$.
Wir setzen

$$D := \bigcap_{n=1}^{\infty} m^n$$

Auf Grund des dritten Schritts gilt

$$m^{-1} \bullet m^n \subseteq m^{n-1}$$

also

$$m^{-1} \bullet D \subseteq D,$$

also

$$m^{-1} \subseteq R(D).$$

Weil R noethersch ist, ist das Ideal D endlich erzeugt, also ein gebrochenes Ideal von R oder gleich Null (nach 1.4.4). Nach dem ersten Schritt wäre im ersten Fall die rechte Seite der Inklusion gleich R, im Widerspruch zum zweiten Schritt. Also gilt

$$D = 0.$$

5. Schritt. Es gibt ein Element $\pi \in m - m^2$.

Wäre $m = m^2$, so wäre $m^n = m$ für n = 1,2,3,..., also

$$m = \bigcap_{n=1}^{\infty} m^n = 0.$$

Nach Voraussetzung soll aber m das von Null verschiedene Primideal von R sein.

6. Schritt. Es gilt $m = \pi R$.

Aus $\pi \in m$, d.h. $\pi R \subseteq m$ erhalten wir durch Multiplikation mit m^{-1}

$$\pi \bullet m^{-1} \subseteq m \bullet m^{-1} \subseteq R .$$

Die Inklusion rechts besteht nach Definition von m^{-1}. Die Inklusion

$$\pi \bullet m^{-1} \subseteq m$$

kann jedoch nicht bestehen, denn durch Multiplikation mit m würde sich daraus

$$\pi R =^{11} \pi \bullet m^{-1} \bullet m \subseteq m^2$$

ergeben im Widerspruch zur Wahl von π im 5. Schritt. Wir sehen so, $\pi \bullet m^{-1}$ ist ein Ideal von R, welches nicht ganz im maximalen Ideal von R enthalten ist, d.h.

$$\pi \bullet m^{-1} = R.$$

Wir multiplizieren mit m und erhalten auf Grund des 3. Schritts

$$\pi R = m.$$

7. Schritt. Jedes Element $\alpha \in R - \{0\}$ läßt sich in der Gestalt

$$\alpha = u \bullet \pi^n$$

schreiben mit $u \in R^*$ und n nicht-negativ ganz.

Wegen $\alpha \neq 0$ und dem 4. Schritt gibt es eine nicht-negative ganze Zahl n mit

$$\alpha \in m^n - m^{n+1},$$

d.h. α hat nach dem 6. Schritt die Gestalt

$$\alpha = u \bullet \pi^n \text{ mit } u \in R.$$

Wegen $\alpha \notin m^{n+1}$ kann u nicht in m liegen. Nun ist aber m das einzige maximale Ideal von R, d.h. u ist eine Einheit.

7. Schritt. Jedes Ideal J von R ist ein Hauptideal.

Wir können annehmen, $J \neq 0$. Dann gibt es ein Erzeugendensystem $\{a_i\}_{i \in I}$ von J aus von Null verschiedenen Elementen

$$a_i \in J - \{0\}$$

(d.h. jedes Element von J ist eine endliche R-Linearkombination der a_i). Wir schreiben die a_i in der Gestalt

$$a_i = u_i \bullet \pi^{n_i} \text{ mit } u_i \in R^* \text{ und } n_i \text{ nicht-negativ ganz}$$

und setzen

$$n := \min \{n_i\}.$$

Dann gibt es ein i mit $n_i = n$. Das zugehörige a_i teilt alle anderen a_j, d.h. es gilt

$$J = a_i R.$$

Wir haben gezeigt, J ist ein Hauptideal.

QED.

---

[11] vgl. den 3. Schritt.

1.4.11 Die Topologie zu einer diskreten Bewertung

Seien K ein Körper, $v: K^* \longrightarrow \mathbb{Z}$ eine diskrete Bewertung und

$$\rho \in (0, 1) \subseteq \mathbb{R}$$

eine fest gewählte reelle Zahl im offenen Einheitsintervall. Wir setzen

$$|x|_v := \rho^{v(x)} \text{ für } x \in K.$$

Dann gilt

(i) $|x|_v \geq 0$ für alle x und $|x|_v = 0 \Leftrightarrow x = 0$.

(ii) $|x \bullet y|_v = |x|_v \bullet |y|_v$

(iii) $|x + y|_v \leq |x|_v + |y|_v$

Mit anderen Worten, $|x|_v$ hat die Eigenschaften einer Norm, und die Abstandsfunktion

$$d(x, y) := |x - y|_v ,$$

welche durch diese Norm definier wird, versieht den Körper K mit der Struktur eines metrischen Raumes. Dabei sind die folgenden Abbildungen stetig.

$\alpha: K \times K \longrightarrow K, (x, y) \mapsto x + y,$

$\nu: K \longrightarrow K, x \mapsto -x,$

$\mu: K \times K \longrightarrow K, (x, y) \mapsto xy,$

$\iota: K^* \longrightarrow K^*, x \mapsto x^{-1}$

d.h. (K, +), (K*, •) sind topologische Gruppen und K ist ein topologischer Körper. Der zugehörige Bewertungsring

$$R := R_v = \{ x \in K \mid v(x) \geq 0 \} = \{x \in K \mid |x|_v \leq 1\}$$

und das zugehörige Bewertungsideal

$$p := p_v = \{ x \in K \mid v(x) > 0 \} = \{x \in K \mid |x|_v < 1\}$$

sind offene und gleichzeitig abgeschlossene Teilmengen von K. Eine Abbildung

$$K \longrightarrow \mathbb{R}, x \mapsto |x|_v,$$

welche den obigen Bedingungen (i) - (iii) genügt, heißt auch (die zu v gehörige) multiplikative Bewertung.[12] Um den Gegensatz zu dieser Art von Bewertung zu betonen werden wir gelegentlich von additiven Bewertungen sprechen, wenn wir die diskreten Bewertungen im Auge haben.

Bemerkungen

(i) Wir werden später sehen, daß die Topologie der eben beschriebenen metrischen Räume nicht von der speziellen Wahl der Zahl ρ abhängt.

(ii) Für die von uns betrachteten Körper wird der Restklassenkörper $\kappa = R/p$ fast immer endlich sein. Wir setzen dann

$$\rho = 1/ \# k.$$

(iii) Wie der nachfolgende Beweis zeigt, gilt sogar eine verschärfte Variante der Dreiecksungleichung:

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

---

[12] Dies ist eine vorläufige Definition des Begriffs der multiplikativen Bewertung eines Körpers, die wir später noch etwas modifizieren werden.

Man nennt multiplikative Bewertungen, die dieser zusätzlichen Bedingung genügen auch archmedische Bewertungen. Solche für die dies nicht gilt, heißen archimedisch.[13]

Beweis. Für $x \in K$ gilt

$$|x|_v = 0 \Leftrightarrow \rho^{v(x)} = 0 \Leftrightarrow v(x) = \infty \Leftrightarrow x = 0.$$

Weiter erhalten wir für $x, y \in K$:

$$|x \bullet y|_v = \rho^{v(x \bullet y)} = \rho^{v(x)+v(y)} = \rho^{v(x)} \bullet \rho^{v(y)} = |x|_v \bullet |y|_v$$

und

$$|x + y|_v \le \rho^{v(x+y)} \le \rho^{\min\{v(x),\, v(y)\}} \le \max\{\rho^{v(x)}, \rho^{v(y)}\} = \max\{|x|_v, |y|_v\}$$
$$\le |x|_v + |y|_v$$

Damit sind (i), (ii) und (iii) bewiesen. Die Eigenschaften der zugehörigen Abstandsfunktion d ergeben sich daraus:

$$d(x, y) = 0 \Leftrightarrow |x - y|_v = 0 \Leftrightarrow x - y = 0 \Leftrightarrow x = y.$$

$$d(x, y) = |x - y|_v = |-1|_v \bullet |y - x|_v = \rho^{v(-1)} \bullet d(y, x) = \rho^0 \bullet d(y, x) = d(y, x).$$

$$d(x, y) + d(y, z) = |x - y|_v + |y - z|_v \ge |(x-y) + (y-z)|_v = |x-z|_v = d(x, z).$$

Auf Grund der Definitionen sieht man sofort, daß R abgeschlossen ist in K und p offen. Da die multiplikative Bewertung $|?|_v$ außer Null nur Werte annimmt, die Potenzen von ρ sind, kann man R und p aber auch wie folgt beschreiben.

$$R = \{x \in K \mid |x|_v < 1/\rho\}$$

$$p = \{x \in K \mid |x|_v \le \rho\}.$$

Mit anderen Worten, R ist auch offen und p ist auch abgeschlossen.[14] Im weiten Beweis schreiben wir einfach $|?|$ anstelle von $|?|_v$.

Stetigkeit der Abbildung $\alpha: K \times K \longrightarrow K,\ (x, y) \mapsto x + y$.

Es reicht zu zeigen, das vollständige Urbild jeder ε-Umgebung ist offen, d.h. es reicht zu zeigen,

$$\alpha(U_{\varepsilon/2}(x) \times U_{\varepsilon/2}(y)) \subseteq U_\varepsilon(\alpha(x, y))$$

für jedes $x \in K$, jedes $y \in K$ und jedes $\varepsilon > 0$. Für $x' \in U_{\varepsilon/2}(x)$ und $y' \in U_{\varepsilon/2}(y)$ gilt

$$|x - x'| < \varepsilon/2 \text{ und } |y - y'| < \varepsilon/2$$

also

$$|\alpha(x,y) - \alpha(x', y')| = |x-x' + y - y'| \le |x-x'| + |y - y'| \le \varepsilon/2 + \varepsilon/2 = \varepsilon,$$

$$\alpha(x', y') \in U_\varepsilon(\alpha(x, y)).$$

Stetigkeit der Abbildung $\nu: K \longrightarrow K,\ x \mapsto -x,$.

Es reicht zu zeigen, das vollständige Urbild jeder ε-Umgebung ist offen. Es gilt

---

[13] Die angegebenen Definitionen für archimedisch und nicht-archimedisch sind als vorläufing zu betrachten. Die allgemein üblischen Definitionen folgen später.

[14] Daß R und p beide sowohl abgeschlossen als auch offen sind, hängt mit der allgemeinen Tatsache zusammen, daß offene Untergruppen einer topologischen Gruppen auch abgeschlossen sind.

$$x' \in U_\varepsilon(x) \Leftrightarrow |x-x'| < \varepsilon \Leftrightarrow |\nu(x) - \nu(x')| < \varepsilon \Leftrightarrow \nu(x') \in U_\varepsilon(\nu(x)),$$

also

$$\nu^{-1}(U_\varepsilon(\nu(x)) = U_\varepsilon(x).$$

Stetigkeit der Abbildung $\mu: K\times K \longrightarrow K,\ (x, y) \mapsto xy$.
Sei

$$(x, y) \in \mu^{-1}(U_\varepsilon(z)).$$

Wir haben zu zeigen, es gibt eine offene Umgebung von (x, y), die ganz im vollständigen Urbild auf der rechten Seite liegt. Indem wir $U_\varepsilon(z)$ durch eine offene ε'-Umgebung von xy ersetzen mit hinreichend kleinem ε', reduzieren wir den Beweis Behauptung auf den Spezialfall

$$z = xy.$$

1. Fall: $x \neq 0$ und $y \neq 0$.
Wir setzen

$$\delta' := \min\{\frac{\varepsilon}{2\bullet|y|}, |x|\} \text{ und } \delta'' := \frac{\varepsilon}{4\bullet|x|}$$

Es reicht zu zeigen,

$$\mu(U_{\delta'}(x)\times U_{\delta''}(y)) \subseteq U_\varepsilon(xy).$$

Für $x' \in U_{\delta'}(x)$ und $y' \in U_{\delta''}(y)$ gilt

$$\begin{aligned} |\mu(x',y') - xy| = |x'y' - xy| &= |x'(y'-y) + (x'-x)y| \\ &\leq |x'|\bullet|y'-y| + |x'-x|\bullet|y| \\ &< |x'|\bullet\delta'' + \delta'\bullet|y| \\ &\leq |x'|\bullet\delta'' + \frac{\varepsilon}{2} \end{aligned}$$

Wegen $|x'| = |x'-x + x| \leq |x'-x| + |x| \leq \delta' + |x| \leq 2\bullet|x|$ folgt

$$|\mu(x',y') - xy| < 2\bullet|x|\bullet\delta'' + \frac{\varepsilon}{2} = \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

d.h. es ist $\mu(x',y') \in U_\varepsilon(xy)$.

2. Fall: $x \neq 0$ und $y = 0$.
Wir setzen

$$\delta' := |x| \text{ und } \delta'' := \frac{\varepsilon}{2\bullet|x|}$$

Es reicht zu zeigen,

$$\mu(U_{\delta'}(x)\times U_{\delta''}(0)) \subseteq U_\varepsilon(0).$$

Für $x' \in U_{\delta'}(x)$ und $y' \in U_{\delta''}(0)$ gilt

$$|\mu(x',y') - 0| = |x'y'| = |x'|\bullet|y'| \leq |x'|\bullet\ \delta'' = |x'|\bullet\frac{\varepsilon}{2\bullet|x|}$$

Wegen $|x'| = |x'-x + x| \leq |x'-x| + |x| \leq \delta' + |x| = 2\bullet|x|$ folgt

$$|\mu(x',y') - 0| \leq \varepsilon,$$

d.h. es ist $\mu(x',y') \in U_\varepsilon(0)$.

3. Fall: $x = y = 0$.

Wir setzen

$$\delta' := \sqrt{\varepsilon} \text{ und } \delta'' := \sqrt{\varepsilon}$$

Es reicht zu zeigen,

$$\mu(U_{\delta'}(0) \times U_{\delta''}(0)) \subseteq U_{\varepsilon}(0).$$

Für $x' \in U_{\delta'}(0)$ und $y' \in U_{\delta''}(0)$ gilt

$$|\mu(x',y') - 0| = |x'y'| < \sqrt{\varepsilon} \bullet \sqrt{\varepsilon} = \varepsilon,$$

d.h. es ist $\mu(x',y') \in U_{\varepsilon}(0)$.

Die Stetigkeit der Abbildung $\iota: K^* \longrightarrow K^*$, $x \mapsto x^{-1}$.
Sei

$$y \in \iota^{-1}(U_{\varepsilon}(x)).$$

Es reicht zu zeigen, des gibt ein δ-Umgebung von y, die ganz im vollständigen Urbild auf der rechten Seite liegt. Indem wir $U_{\varepsilon}(x)$ durch eine ε'-Umgebung von i(y) ersetzen mit hinreichend kleinem ε' reduzieren wir den Beweis der Behauptung auf den Spezialfall

$$x = \iota(y).$$

Wir setzen

$$\delta = \min \{\frac{\varepsilon \bullet |y|^2}{2}, \frac{|y|}{2}\}.$$

Es reicht zu zeigen,

$$\iota(U_{\delta}(y)) \subseteq U_{\varepsilon}(\iota(y).$$

Sei $y' \in U_{\delta}(y)$. Dann gilt

$$|\iota(y') - \iota(y)| = |\frac{1}{y'} - \frac{1}{y}| = \frac{|y - y'|}{|y| \bullet |y'|} < \frac{\delta}{|y| \bullet |y'|}$$

Wegen

$$|y| = |y - y' + y'| \leq |y-y'| + |y'| \leq \delta + |y'| \leq \frac{|y|}{2} + |y'|$$

gilt $\frac{|y|}{2} \leq |y'|$ also $\frac{1}{|y'|} \leq \frac{2}{|y|}$. Damit erhalten wir aus der obigen Abschätzung

$$|\iota(y') - \iota(y)| < \frac{2\delta}{|y|^2} \leq \varepsilon,$$

d.h. es ist $\iota(y') \in U_{\varepsilon}(\iota(y)$.

QED.

Im verbleibenden Teil dieses Abschnitts beschreiben wir einige später benötigte Eigenschaften verschiedener Untergruppen von R.

1.4.12 Die Potenzen des Bewertungsideals und der Restklassenkörper

Sei R ein Bewertungsring mit dem Parameter π, dem Bewertungsideal $p = \pi R$ und dem Restklassenkörper $\kappa = R/p$. Dann besteht für jede nicht-negative ganze Zahl n ein Isomorphismus von k-Moduln

$$\kappa \xrightarrow{\cong} p^n/p^{n+1},\ c \bmod p \mapsto c \bullet \pi^n \bmod p^{n+1}.$$

Beweis. Betrachten wir die Zusammensetzung

$$R \xrightarrow{\pi^n} p^n \longrightarrow p^n/p^{n+1},\ r \mapsto r\bullet\pi^n \bmod p^{n+1}$$

der Multplikation mit π^n mit der natürlichen Abbildung auf den Faktormodul. Dies ist eine R-lineare Abbildung. Da jede der beiden Teilabbildungen surjektiv ist, gilt dies auch für die Zusammensetzung. Ein Element $r \in R$ liegt genau dann im Kern der Zusammensetzung, wenn gilt

$$r\bullet\pi^n \in p^{n+1} = \pi^{n+1}R,$$

d.h. genau dann, wenn r in $\pi P = p$ liegt. Die Zusammensetzung induziert also eine R-lineare Bijektion

$$\kappa = R/p \longrightarrow p^n/p^{n+1},\ r \bmod p \mapsto r\bullet\pi^n \bmod p^{n+1}.$$

QED.

1.4.13 Eine exakte Sequenz für die Einheiten einer diskreten Bewertung

Sei K ein Körper mit der diskreten Bewerung $v: K^* \longrightarrow \mathbb{Z}$, dem Bewertungsring R und der Gruppe

$$U := U_v := R^*$$

der Einheiten von v. Dann ist die folgende Sequenz von abelschen Gruppen exakt.

$$1 \longrightarrow U \longrightarrow K^* \xrightarrow{v} \mathbb{Z} \longrightarrow 0.$$

Beweis. Das folgt unmittelbar aus der Definition einer diskreten Bewertung und des zugehörigen Bewertungsrings.
QED.

1.4.14 Die Gruppe der n-Einheiten

Sei K ein Körper mit der diskreten Bewerung $v: K^* \longrightarrow \mathbb{Z}$, dem Bewertungsring R und dem Bewertungsideal p. Dann ist für jede natürlichen Zahl n die Menge

$$U_n = 1 + p^n$$

eine offene (und abgeschlossene) Untergruppe der Einheitengruppe $U = R^*$. Sie heißt Gruppe der n-Einheiten.[15] Weiter gilt:

(i) Die Untergruppen U_n bilden eine Umgebungsbasis der 1 der topologischen Räume K und U.

(ii) $\bigcap U_n = \{1\}$.

Beweis. Die Menge U_n ist eine Teilmenge von U, welche multplikativ abgeschlossen ist: für $x, y \in p^n$ gilt

$$(1 + x)(1+y) = 1 + (x + y + xy) \text{ und } x + y + xy \in p^n.$$

Speziell für $y := -(1+x)^{-1}x \in p^n$ erhält man

$$(1 + x)(1 + y) = 1,$$

d.h. mit jedem Element von U_n liegt auch dessen Inverses in U_n. Damit ist U_n eine Untergruppe von U.
Wir haben noch die Offenheit von U_n zu zeigen. Es gilt

---

[15] Genauer, die Gruppe der Einheiten, welche in der n-ten infinitesiamalen Umgebung des Einselements liegen.

$$\begin{aligned} U_n &= \{x \in R \mid x - 1 \in p^n\} \\ &= \{x \in R \mid v(x - 1) \geq n \} \\ &= \{x \in R \mid v(x - 1) > n-1 \} \\ &= \{x \in R \mid \rho^{v(x-1)} < \rho^{n-1} \} \\ &= \{x \in R \mid d(x, 1) < \rho^{n-1} \}, \end{aligned}$$

d.h. U_n ist eine offene Menge. Eine leichte Modifikation der obigen Rechnung zeigt,

$$U_n = \{x \in R \mid d(x, 1) \leq \rho^n \},$$

d.h. U_n ist eine eine abgeschlossene Menge.

Zu (i). Es reicht zu zeigen, jede ε-Umgebung von 1 enthält ein U_n. Wir wählen $n \in \mathbb{N}$ derart, daß gilt

$$n > \log_\rho(\varepsilon).$$

Für $x \in U_n$ gilt dann $x - 1 \in p^n$, also

$$v(x - 1) \geq n > \log_\rho(\varepsilon),$$

also

$$| x - 1 | = \rho^{v(x-1)} < \rho^{\log_\rho(\varepsilon)} = \varepsilon.$$

Wir haben gezeigt, ,$U_n \subseteq U_\varepsilon(1)$.

Zu (ii). Es gilt

$$\bigcap U_n = \bigcap (1 + p^n) = 1 + \bigcap p^n = 1 + \{0\} = \{1\}.$$

QED.

Bemerkung

Die erste Aussage bedeutet, die offenen Teilmengen von K* sind gerade die Vereinigungen der Mengen der Gestalt

$$x \bullet U_n \text{ mit } x \in K^* \text{ und } n \in \mathbb{N}$$

(d.h. die Mengen der Gestalt $x \bullet U_n$ bilden eine Topologie-Basis für K*). Man beachte, für jede nicht-leere offene Teilmenge

$$W \subseteq K^*$$

und jeden Punkt

$$x \in W$$

ist

$$x^{-1}W$$

eine offene Umgebung von 1 (weil die Multiplikationen mit x und x^{-1} zueinander inverse stetige Abbildungen sind). Also gibt es ein n mit

$$U_n \subseteq x^{-1}W,$$

d.h. mit

$$x \in x \bullet U_n \subseteq W.$$

1.4.15 Faktorgruppen von Einheitengruppen

Sei K ein Körper mit der diskreten Bewertung v: $K^* \longrightarrow \mathbb{Z}$, dem Bewertungsring R, dem Bewertungsideal p, dem Restklassenkörper κ, der Einheitengruppe U und der Gruppe der n-Einheiten U_n. Dann gilt:

(i) Die natürliche Abbildung $R \longrightarrow \kappa$ induziert einen Isomorphismus von Gruppen

$$U/U_1 \longrightarrow \kappa^*.$$

(ii) Für jede natürliche Zahl n gibt es einen Isomorphismus

$$U_n/U_{n+1} \longrightarrow p^n/p^{n+1},\ u \bmod U \mapsto u\text{-}1 \bmod p^{n+1}$$

der multiplikativen Gruppe links mit der additiven Gruppe rechts.

Beweis. Zu (i). Wir betrachten den natürlichen Homomorphismus

$$R \longrightarrow R/p = \kappa.$$

Das vollständige Urbild von $0 \in \kappa$ ist gerade p. Das vollständige Urbild des Komplementes $\kappa^* = \kappa - \{0\}$ ist gerade R - p = U. Die natürliche Abbildung definiert somit eine Surjektion

$$U \twoheadrightarrow \kappa^*,\ u \mapsto u \bmod p.$$

Der Kern dieser Surjektion besteht aus allen Einheiten $u \in U$ mit

$$u \equiv 1 \bmod p,$$

d.h. mit $u - 1 \in p$, d.h. mit $u \in 1 + p$. Der Kern ist gleich $1 + p = U_1$.

Zu (ii). Nach Definition von U_n ist die Abbildung

$$U_n \longrightarrow p^n,\ u \mapsto u - 1,$$

surjektiv. Ihre Zusammensetzung α mit der natürlichen Surjektion $p^n \twoheadrightarrow p^n/p^{n+1}$ ist somit auch surjektiv:

$$\alpha: U_n \twoheadrightarrow p^n/p^{n+1}.$$

Für $x, y \in p^n$, d.h. $1+x, 1+y \in U_n$ gilt

$$\alpha((1+x)(1+y)) = \alpha(1 + x + y + xy)$$
$$= x + y + xy \bmod p^{n+1}$$

Wegen $n \geq 1$ ist aber $xy \in p^{n+n} \subseteq p^{n+1}$. Damit ist

$$\alpha((1+x)(1+y)) = x + y \bmod p^{n+1}$$
$$= \alpha(1+x) + \alpha(1+y).$$

Wir haben gezeigt, α ist ein (surjektiver) Homomorphismus der multiplikativen Gruppe U_n/U_{n+1} mit Werten in der additiven Gruppe p^n/p^{n+1}. Berechnen wir den Kern von α. Es gilt

$$1 + x \in \mathrm{Ker}(\alpha) \Leftrightarrow x \bmod p^{n+1} = \mathrm{Null} \Leftrightarrow x \in p^{n+1} \Leftrightarrow 1 + x \in U_{n+1}.$$

Die Behauptung folgt jetzt aus dem Homomorphiesatz.
QED.

1.4.16 Folgerung: die additive Gruppe des Restklassenkörpers als Faktorgruppe von Einheiten

Sei K ein Körper mit der diskreten Bewertung v: $K^* \longrightarrow \mathbb{Z}$, dem Bewertungsring R, dem Paramter π, dem Bewertungsideal p, dem Restklassenkörper κ und der Gruppe der n-Einheiten U_n. Dann besteht für jede natürliche Zahl ein Isomorphismus

$$\kappa^+ \overset{\cong}{\longrightarrow} U_n/U_{n+1} \text{ , } u \bmod p \mapsto 1+ u\pi^n \bmod U_{n+1}$$

der additiven Gruppe des Restklassenkörpers mit der multiplikativen Gruppe U_n/U_{n+1}.

Beweis. Man setze die Isomorphismen von 1.4.12 und 1.4. 15 zusammen.
QED.

1.4.17 Einige Automorphismen der n-Einheitengruppen

Sei K ein Körper mit der diskreten Bewertung v: $K^* \longrightarrow \mathbb{Z}$, dem Bewertungsring R, dem Paramter π, dem Bewertungsideal p, dem Restklassenkörper κ und der Gruppe der n-Einheiten U_n. Dann gilt:

(i) Ist κ ein Körper mit Charakteristik $p > 0$, so gilt für jede natürliche Zahl n:

$$(U_n)^p \subseteq U_{n+1} .$$

(ii) Sei K vollständig bezüglich der gegebenen Bewertung, und sei m eine zur Charakteristik von κ teilerfremde natürliche Zahl,

$$ggt(m, char(\kappa)) = 1.$$

Dann ist für jede natürliche Zahl n die Abbildung

$$U_n \longrightarrow U_n, u \mapsto u^m,$$

ein Automorphismus der Gruppe U_n.

Beweis.Zu (i). Nach Definition der Charakteristik wird der Restklassenkörper κ von p annulliert. Wegen 1.4.16 erhatlen wir, daß dasselbe für U_n/U_{n+1} gilt. Weil U_n ein multiplikative Gruppe ist, folgt die Behauptung.
Zu (ii). Bezeichne p die Charakteristik des Restklassenkörper κ. Im Fall $p > 1$ gibt es nach Wahl von m ganze Zahlen p' und m' mit

$$p \bullet p' + m \bullet m' = 1.$$

Die Multiplikation mit m induziert also auf κ eine Abbildung, die invers ist zu der durch m' induzierten. Insbesondere induziert die Multiplikation mit m eine Bijektion auf κ. Letzteres gilt auf für den Fall $p = 0$ (denn dann gilt $\mathbb{Z} \subseteq \kappa$, also $\mathbb{Q} \subseteq \kappa$).

Auf Grund des Isomorphismus 1.4.16 induziert der Gruppen-Homomorphismus

$$\alpha: U_n \longrightarrow U_n, u \mapsto u^m,$$

für jedes $q \geq n$ auf U_q/U_{q+1} eine Bijektion. Damit gilt

$$Ker(\alpha) \subseteq U_q \text{ für jedes } q \geq n,$$

also nach 1.4.14(ii) sogar

$$Ker(\alpha) = 1.$$

Wir haben gezeigt, α ist injektiv.

Weil α auf U_n/U_{n+1} eine Bijektion induziert, gibt es für jedes

$$u_0 \in U_n$$

Elemente $v_0 \in U_n$ und $u_1 \in U_{n+1}$ mit

$$u_0 = v_0^m u_1.$$

Durch Wiederholen dieser Argumentation finden wir für i = 1, 2, 3, ... Elemente
Elemente $v_i \in U_{n+i}$ und $u_{i+1} \in U_{n+i+1}$ mit

$$u_i = v_i^m u_{i+1}.$$

Es folgt

$$u_0 = (v_0 \bullet \ldots \bullet v_i)^m \bullet u_{i+1} \qquad (1)$$

Wegen $u_i \in U_{n+1}$ konvergiert die Folge der u_i gegen 1,

$$u_i \longrightarrow 1.$$

Betrachten wir die Folge der Produkte

$$p_i := v_0 \bullet \ldots \bullet v_i$$

Für i > j gilt

$$p_i/p_j = v_{j+1} \bullet \ldots \bullet v_i \in U_{n+j+1} \bullet U_{n+j+2} \bullet \ldots \bullet U_{n+i} \subseteq U_{n+j+1}.$$

Mit anderen Worten, p_i/p_j liegt für i und j hinreichend groß in jeder ε-Umgebung von 1: für jedes ε > 0 gibt es ein N(ε) mit

$$| p_i/p_j - 1| < \frac{1}{2}\varepsilon \text{ für } i, j \geq N(\varepsilon),$$

d.h.

$$| p_i - p_j |_v < \frac{1}{2}\varepsilon \bullet |p_j|_v$$

Alle Glieder der Folge liegen in

$$U_n = 1 + p^n = \{ x \in K \mid v(x - 1) \geq n \} = \{x \in K \mid |x - 1| \leq \rho^n\}$$

$$\subseteq {}^{16}\{x \in K \mid |x| \leq \rho^n + 1\} \subseteq {}^{17}\{x \in K \mid |x| \leq 2\}.$$

Wir erhalten

$$| p_i - p_j |_v < \varepsilon \text{ für } i, j \geq N(\varepsilon),$$

d.h. die p_i bilden eine Cauchy-Folge. Weil K vollständig ist, besitzt diese Cauchy-Folge einen Limes in K,

$$p_i \longrightarrow p.$$

Weil U_n abgeschlossen ist in K, liegt dieser Limes in U_n,

$$p \in U_n.$$

Aus (1) und der Definition von p_i erhalten wir

---

[16] Mit $|x - 1| \leq \rho^n$ gilt $|x| = |x-1 + 1| \leq |x-1| + |1| \leq \rho^n + 1$.
[17] n ist eine natürliche Zahl und ρ liegt im Einheitsinterval.

$$u_0 = (p_i)^m \bullet u_{i+1} ,$$

also für $i \longrightarrow \infty$

$$u_0 = p^m = \alpha(p)$$

Wir haben gezeigt, jedes $u_0 \in U_n$ liegt im Bild von α, d.h. α ist surjektiv.

QED.

Bemerkung

Bevor wir nun zur Beschreibung der Dedekind-Ringe übergehen, erinnern wir noch einige Eigenschaften von Quotientenringen.

1.4.18 Lokalisierungen nach einem Primideal

Seien R ein Integritätsbereich mit dem Quotientenkörper K und $p \subseteq R$ ein Primideal von R. Dann heißt der Quotientenring

$$R_p := \{ \frac{a}{b} \in K \mid a \in R, b \in R - p\}$$

Lokalisierung von R in p. Nach Konstruktion ist jedes Element von R_p, welches nicht im Ideal

$$pR_p = \{ \frac{a}{b} \in K \mid a \in p, b \in R - p\}$$

(welches von p erzeugt wird) liegt, eine Einheit, d.h.

R_p

ist ein lokaler Ring mit dem maximalen Ideal pR_p. Es gilt:

(i) $p = pR_p \bigcap R$.

(ii) $J = (J \bigcap R) \bullet R_p$ für jedes Ideal J von R_p.[18]

Beweis. Zu (i). Nach Definition gilt

$$p \subseteq pR_p \bigcap R.$$

Beweisen wir die umgekehrt Inklusion. Jedes Element aus dem Durchschnitt auf der rechten Seite hat die Gestalt

$$r = \frac{a}{b} \text{ mit } a \in p \text{ und } b \notin p.$$

Insbesondere ist $b \bullet r \in p$. Weil b und r in R liegen und p ein Primideal von R ist, folgt

$$b \in p \text{ oder } r \in p.$$

Das erste ist aber nach Wahl von b nicht der Fall. Also gilt $r \in p$.

Zu (ii). Der Durchschnitt $J \bigcap R$ ist eine Teilmenge von J. Als liegt das von dieser Teilmenge erzeugt Ideal ebenfalls in J,

$$(J \bigcap R) \bullet R_p \subseteq J.$$

Beweisen wir, es besteht auch die umgekehrte Inklusion. Jedes Element von J hat die Gestalt

$$x := \frac{a}{b} \in J \text{ mit } a \in R, b \in R - p.$$

Insbesondere ist $b \bullet x = a$ ein Element von $J \bigcap R$. Wegen $b \in R\text{-}p$ ist $\frac{1}{b} \in R_p$. Es folgt

---

[18] Die Identität bleibt richtig für Quotientenringe bezüglich beliebiger multiplikativ abgeschlossener Mengen Der Beweis ist derselbe.

$$x = (b \bullet x) \bullet \frac{1}{b} \in (J \bigcap R) \bullet R_p$$

QED.

1.5 Dedekind-Ringe

1.5.1 Eine Charakterisierung der Dedekind-Ringe

Sei R eine Integritätsbereich. Dann sind folgende Aussagen äquivalent.

(i) R ist noethersch und normal, und jedes von Null verschiedene Primideal ist maximal.

(ii) R ist noethersch und für jedes von Null verschiedene Primideal $p \subseteq R$ ist R_p ein diskreter Bewertungsring.

(iii) Jedes gebrochene Ideal I von R ist umkehrbar, d.h. es gilt $I \bullet I^{-1} = R$.

Ein Integritätsbereich R, der eine dieser äquivalenten Bedingungen erfüllt, heißt Dedekind-Ring.

Beispiele

(i) Jeder Hauptidealring ist ein Dedekind-Ring (weil Bedingung (i) erfüllt ist). Insbesondere gilt dies für $\mathbb{Z}$.

(ii) Wir werden später sehen, für jeden Dedekind-Ring R mit dem Quotientenkörper K und jede endliche (separable)[19] Körpererweiterung

$$L/K$$

ist die ganze Abschließung S von R in L ein Dedekind-Ring.

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \cup & & \cup \\ R & \hookrightarrow & S \end{array}$$

Speziell im Fall $R = \mathbb{Z}$ und $K = \mathbb{Q}$ bedeutet dies, die von uns als Ersatz für die ganzen Zahlen ins Auge gefaßten Ringe S sind sämtlich Dedekind-Ringe.

(iii) Jeder diskrete Bewertungsring ist ein Dedekind-Ring.

Das ergibt sich aus der obigen Aussage (ii) der Behauptung und der Charakterisierung der diskreten Bewertungsringe 1.4.10 (iv) (oder auch einfach aus der Tatsache, daß diskrete Bewertungsringe Hauptidealringe sind).

Beweis der Äquivalenz der drei Bedingungen.

(i) $\Rightarrow$ (ii). Wir haben zu zeigen, für jedes von Null verschiedene Primideal $p \subseteq R$ ist R_p ein diskreter Bewertungsring. Zum Beweis verwenden wir das Kriterium 1.4.10. (iv): es reicht zu zeigen,

1. R_p ist noethersch.
2. R_p ist normal.
3. R_p besitzt genau ein von Null verschiedenes Primideal.

Zu 1. Sei J ein Ideal von R_p. Nach 1.4.18 (ii) gibt es ein Ideal $I \subseteq R$ mit

$$J = I \bullet R_p$$

[19] Die Aussage gilt ohne die Voraussetzung der Separabilität. Wir werden jedoch nur den separablen Fall behandeln.

(man setze $I = J \cap R$). Weil R noethersch ist, besitzt I ein endliches Erzeugendensystem über R. Dieses Erzeugendensystem ist aber auch ein Erzeugendensystem von J über R_p, d.h. J ist als Ideal von R_p endlich erzeugt.

Zu 2. Sei $\alpha \in K := Q(R_p)$ ein Element des Quotientenkörpers von R_p, welches ganz ist über R_p. Wir haben zu zeigen, α liegt in R_p. Nach Voraussetzung besteht in K eine Identität der Gestalt

$$\alpha^n + r_{n-1}\alpha^{n-1} + ... + r_0 = 0 \text{ mit } r_i \in R_p \text{ für jedes i.} \qquad (1)$$

Die r_i sind Quotienten von Elementen aus R, wobei der Nenner nicht p liegt. Bezeichne

$$b \in R - p$$

das Produkt dieser Nenner. Dann kann man jedes der r_i in der Gestalt

$$r_i = \frac{a_i}{b} \text{ mit } a_i \in R.$$

Wir multiplizieren (1) mit b^n und erhalten eine Identitüät

$$(b\alpha)^n + a_{n-1}b\bullet(b\alpha)^{n-1} + a_{n-2}b^2\bullet(b\alpha)^{n-2}+...+a_0b^n = 0.$$

Diese Identität zeigt, daß $b\alpha \in K = Q(R_p) = Q(R)$ ganz ist über R. Weil R nach Voraussetzung normal ist, folgt

$$b\alpha \in R.$$

Wegen $b \in R - p$ erhalten wir

$$\alpha = \frac{b\alpha}{b} \in R_p.$$

Zu 3. Sei q ein von Null verschiedenes Primideal von R_p. Es reicht zu zeigen, $q = pR_p$. Weil jedes Element von $R_p - pR_p$ eine Einheit ist, gilt

$$q \subseteq pR_p.$$

Wir haben zu zeigen, es gilt das Gleichheitszeichen. Wir schneiden mit R und erhalten

$$q \cap R \subseteq pR_p \cap R = p \qquad (2)$$

Das Gleichheitszeichen rechts gilt nach 1.4.18 (i). Weil q ein Primideal von R_p ist, ist der Durchschnitt links ein Primideal von R. Weil $q \neq 0$ ist, gilt auch

$$0 \neq q \cap R$$

(weil nach 1.4.18. (ii) der Durchschnitt $q \cap R$ das Ideal q in R_p erzeugt). Nun sind nach Voraussetzung alle von Null verschiedenen Primideale von R maximal. Insbesondere ist $q \cap R$ maximal. Mit (2) gilt also sogar

$$q \cap R = p.$$

Wir gehen zu den in R_p erzeugten Idealen über und erhalten

$$q = (q \cap R)\bullet R_p = p\bullet R_p.$$

Das Gleichheitszeichen links gilt dabei nach 1.4.18 (ii).

(ii) $\Rightarrow$ (iii). Wir haben zu zeigen, jedes gebrochende Ideal I ist umkehrbar, d.h. es gilt

$$I \bullet I^{-1} = R.$$

Weil R noethersch ist, besitzt I ein endliches Erzeugendensystem (nach 1.4.5), sagen wir

$$I = Ra_1 + ... + Ra_n \text{ mit } a_i \in K := Q(R).$$

Für jedes von Null verschiedene Primideal $p \subseteq R$ bezeichnen wir mit

$$v_p : K^* \longrightarrow \mathbb{Z}$$

die Bewertung zum Bewertungsring R_p. Für jedes fest gewählte p gibt es ein i mit

$$v_p(a_i) = \min \{v_p(a_1), \ldots, v_p(a_n)\}.$$

Jedes a_j ist dann ein Vielfaches von a_i

$$IR_p = R_p a_1 + ... + R_p a_n = R_p \bullet a_i,$$

d.h. für j = 1, ... , n ist a_j in R_p ein Vielfaches von a_i,

$$\frac{a_j}{a_i} = \frac{x_j}{y_j} \text{ mit } x_j \in R, \text{ und } y_j \in R - p.$$

Indem wir die Brüche auf der rechten Seite geeignet erweitern (und jedes y_j durch das Produkt der y_j ersetzen) erreichen wir

$$y_1 = y_2 = ... = y_n = y \in R\text{-}p.$$

Dann ist

$$y \bullet \frac{a_j}{a_i} \in R \text{ für jedes j,}$$

also $\frac{y}{a_i} \bullet I \subseteq R$, also

$$\frac{y}{a_i} \in I^{-1}$$

Multiplikation mit a_i liefert

$$y \in a_i I^{-1} \subseteq I \bullet I^{-1}.$$

Wir haben gezeigt, für jedes von Null verschiedene Primideal p von R gibt es ein Elemetn $y \in R\text{-}p$, welches im Ideal $I \bullet I^{-1}$ von R liegt. Mit anderen Worten, $I \bullet I^{-1}$ ist in keinem Primideal von R enthalten (also auch in keinem maximalen Ideal). Es muß deshalb

$$I \bullet I^{-1} = R$$

gelten.

<u>(iii) $\Rightarrow$ (i)</u>. Wir haben zu zeigen:

1. R ist noethersch.
2. R ist normal.
3. Jedes von Null verschiedene Primideal ist maximal.

<u>Zu 1</u>. Sei I ein von Null verschiedenes Ideal. Nach Voraussetzung gilt dann

$$I \bullet I^{-1} = R.$$

Insbesondere ist $1 \in I \bullet I^{-1}$, d.h. es gibt Elemente $a_1, ..., a_n \in I$ und $b_1, ..., b_n \in I^{-1}$ mit

$$\sum_{i=1}^{n} a_i b_i = 1.$$

Für jedes $x \in I$ erhalten wir

$$\sum_{i=1}^{n} a_i(b_i x) = x$$

mit $b_i x \in I^{-1} \bullet I = R$, d.h. x ist R-Linearkombination der a_i. Wir haben gezeigt,

$$I = (a_1,...,a_n)R.$$

Da dies für jedes Ideal $I \neq 0$ gilt, ist R noethersch.

Zu 2. Sei $x \in K := Q(R)$ ein über R ganzes Element. Dann ist

$$S := R[x] \ (\subseteq K)$$

ein endlich erzeugter R-Modul (nach 1.3.2 (ii)), also ein gebrochenes Ideal von R (nach 1.4.5). Außerdem ist S ein Ring mit 1, d.h. es gilt

$$S \bullet S = S,$$

also

$$\begin{aligned} S &= SR && \text{(wegen } 1 \in R \subseteq S\text{)} \\ &= SSS^{-1} && \text{(wegen } SS^{-1} = R \text{ nach Voraussetzung)} \\ &= SS^{-1} && \text{(wegen } SS = S\text{, siehe oben)} \\ &= R && \text{(wegen } SS^{-1} = R \text{ nach Voraussetzung)} \end{aligned}$$

Insbesondere gilt $x \in S = R$. Wir haben gezeigt, R ist ganz abgeschlossen in K, d.h. normal).

Zu 3. Sei I ein von Null verschiedenes Primideal und p ein maximalen Ideal von R, welches I enthält.

$$0 \neq I \subseteq p, \text{ I Primideal, p maximal.}$$

Dann gilt

$$I \bullet p^{-1} \subseteq p \bullet p^{-1} = R,$$

d.h. $I \bullet p^{-1}$ ist ein Ideal von R, und es gilt

$$(I \bullet p^{-1}) \bullet p = I \bullet (p^{-1} p) = I \bullet R = I$$

Weil I ein Primideal von R ist, folgt

$$I \bullet p^{-1} \subseteq I \text{ oder } p \subseteq I. \qquad (3)$$

Falls die linke Inklusion besteht, erhalten wir durch Multiplikation von I^{-1}

$$p^{-1} \subseteq I^{-1} \bullet I = R,$$

und durch Multiplikation mit p,

$$R = p \bullet p^{-1} \subseteq p,$$

also p = R im Widerspruch zur Wahl des maximalen Ideals p. Die erste Inklusion in (3) ist somit nicht möglich. Es besteht die zweite Inklusion. Wegen der Maximalität von p folgt dann aber

$$I = p,$$

d.h. I ist maximal.
QED.

1.5.2 Bezeichnungen

Sei R ein Dedekind-Ring mit dem Quotientenkörper K. Für jedes von Null verschiedene Primideal p von R bezeichne dann

$$v_p : K^* \longrightarrow \mathbb{Z}$$

die diskrete Bewertung von K mit dem Bewertungsring R_p.Für jede nicht-leere Teilmenge $I \subseteq K$ setzen wir

$$v_p(I) := \inf \{ v_p(x) \mid x \in I\}.$$

Man beachte, $v_p(I)$ kann den Wert $-\infty$ haben,

$$v_p(\varnothing) = -\infty.$$

1.5.3 Satz von der Zerlegung in Primfaktoren

Sei R ein Dedekind-Ring. Dann bilden die gebrochenen Ideale von R eine abelsche Gruppe

$$\mathbf{F}(R)$$

bezüglich der Multiplikation. Die maximalen Ideale von R bilden ein <u>freies</u> (d.h. $\mathbb{Z}$-linear unabhängiges) Erzeugendensystem dieser Gruppe.

Mit anderen Worten, jedes gebrochene Ideal I von R läßt sich in der Gestalt

$$I = (p_1)^{n_1} \bullet \ldots \bullet (p_r)^{n_r} \tag{1}$$

mit (bis auf die Reihenfolge) eindeutig bestimmten maximalen Idealen

$$p_1, \ldots, p_r$$

von R und eindeutig bestimmen ganzen Zahlen

$$n_1, \ldots, n_r \in \mathbb{Z} - \{0\}.$$

Genauer: es gilt

$$n_i = v_{p_i}(I).$$

Läßt man in (1) für die Exponenten auch den Wert 0 zu, so bekommt die Formel die Gestalt

$$I = \prod_p p^{v_p(I)}, \tag{2}$$

wobei das Produkt über alle maximalen Ideale p des Rings R zu erstrecken ist.

Außerdem gilt für jedes maximale Ideal p von R

$$IR_p = (pR_p)^{v_p(I)} \tag{3}$$

Beweis. <u>1. Schritt</u>. Die gebrochenen Ideale bilden eine abelsche Gruppe.
Nach 1.4.4 ist das Produkt gebrochender Ideale eine wohldefinierte Abbildung

$$F(R) \times F(R) \longrightarrow F(R),\ (I', I'') \mapsto I' \bullet I''.$$

Dieses Produkt ist nach 1.4.2 assoziativ. Nach Definition des Produkts von Idealen spielt dabei das gebrochene Ideal R die Rolle des Einselement. Nach 1.5.1 (iii) gibt es für jedes $I \in F(R)$ ein inverses Element (nämlich I^{-1}). Zusammen sehen wir, F(R) hat die Struktur einer Gruppe (welches offensichtlich abelsch ist).
<u>2. Schritt</u>. Die maximalen Ideale von R erzeugen die Gruppe F(R).
Wir haben zu zeigen, jedes gebrochene Ideal I von R ist Produkt von maximalen Idealen.

Sei $a \in R - \{0\}$ ein Element mit

$$aI \subseteq R.$$

Wenn sich aR und aI als Produkt maximaler Ideale schreiben lassen, so gilt dasselbe für

$$(aI) \bullet (aR)^{-1} = (aR) \bullet I \bullet (aR)^{-1} = I.$$

Es reicht also zu zeigen, jedes von Null verschiedene Ideal

$$I \subseteq R$$

läßt sich als Produkt maximaler Ideale schreiben.

Angenommen, diese Aussage ist falsch. Dann gibt es in der Menge der Ideale I, für welche diese Aussage falsch ist, ein maximales bezüglich der Relation "$\subseteq$" maximales Element. Sei I ein solches Element. Dann ist I echtes Ideal von R,

$$I \subset R,$$

denn I = R ist Produkt von maximalen Idealen (wobei die Anzahl der Faktoren gleich Null ist).

Es gibt somit ein maximales Ideal p von R mit

$$I \subseteq p.$$

Es folgt

$$I \subseteq Ip^{-1} \subseteq pp^{-1} = R. \qquad (4)$$

Die Gleichheit rechts besteht dabei wegen 1.5.1 (iii). Die Inklusion in der Mitte erhält man aus $I \subseteq p$ durch Multiplikation mit p^{-1} und die Inklusion links ergibt sich wie folgt: wegen $p \subseteq R$ gilt $R = R^{-1} \subseteq p^{-1}$. Durch Multiplikation mit I erhält man die gesuchte Inklusion.

Man beachte, die linke Inklusion in (4) ist echt, denn andernfalls würde wegen der Gruppeneigenschaft von F(R) gelten $p^{-1} = R$, d.h. $p = R^{-1} = R$ im Widerspruch dazu, daß p ein maximales Ideal sein soll.

$$I \subset Ip^{-1} \subseteq R.$$

Wir schreiben jetzt

$$I = p\bullet(Ip^{-1}) \qquad (5)$$

Weil I echt enthalten ist in Ip^{-1} und auf Grund der Maximalität von I, läßt sich Ip^{-1} als Produkt von maximalen Idealen schreiben. Wegen (5) gilt dann aber dasselbe auch für I.

3. Schritt. Für jedes maximale Ideal $p \subset R$ hat die Abbildung

$$f_p: \mathbf{F}(R) \longrightarrow \mathbf{F}(R_p),\ I \mapsto IR_p,$$

die folgenden Eigenschaften.

1. f_p ist ein surjetiver Gruppen-Homomorphismus.
2. Die Einschränkung auf die von p erzeugte Untergruppe ist ein Isomorphismus.
3. $\mathrm{Ker}(f_p)$ wird erzeugt von den maximalen Idealen $\neq p$.

Zu 1. Mit I ist auch IR_p ungleich Null. Mit $aI \subseteq R$ gilt $aIR_p \subseteq R_p$. Mit anderen Worten IR_p ist ein gebrochenes Ideal von R_p und f_p ist eine wohldefinierte Abbildung mit Werten in der Gruppe $F(R_p)$ der gebrochenen Ideale von R_p. Es gilt

$$f_p(I'\bullet I'') = I'\bullet I''\bullet R_p = I'R_p \bullet I''R_p = f_p(I')\bullet f_p(I''),$$

d.h. f_p ist ein Gruppen-Homomorphismus.

Nach dem 2. Schritt wird $F(R_p)$ vom einzigen maximalen Ideal von R_p erzeugt, d.h. von

$$pR_p = f_p(p). \qquad (6)$$

Da dieser Erzeuger im Bild von f_p liegt, ist f_p surjektiv.

Zu 2. Wie gerade erwähnt besteht $F(R_p)$ aus den Potenzen von (6). Bezeichnet

$$\pi \in pR_p$$

einen Parameter, so lassen sich diese Potenzen in der Gestalt

$$\pi^n R_p \ , \ n \in \mathbb{Z},$$

schreiben. Da π keine Einheit in R_p ist (und der Ring nullteilerfrei ist) sind diese Potenzen paarweise verschieden[20], d.h. der Homomorphismus

$$\mathbb{Z} \longrightarrow F(R_p), \ n \mapsto (pR_p)^n \ ,$$

ist bijektiv und $F(R_p)$ ist eine freie zyklische Gruppe. Der surjektive Homomorphismus

$$f_p|_{<p>} : <p> = \{p^n \mid n \in \mathbb{Z}\} \longrightarrow F(R_p), \ p^n \longrightarrow (pR_p)^n,$$

muß deshalb injektiv sein (andern falls wäre das Bild endlich).

Zu 3. Sei q ein von p verschiedenes maximales Ideal von R. Dann gibt es ein Element

$$a \in q - p.$$

Dieses Element ist in R_p eine Einheit. Es gilt also

$$qR_p = R_p,$$

d.h. $f_p(q) = 1$, d.h.

$$q \in \mathrm{Ker}(f_p).$$

Der Kern enthält also die von den $q \neq p$ erzeugte Untergruppe. Sei umgekehrt I ein Element aus dem Kern. Wir denken uns I als Produkt von Potenzen von maximalen Idealen geschrieben, sagen wir

$$I = p^n \cdot (\text{Produkt von maximalen Idealen } q \neq p).$$

Alle maximalen Ideale $q \neq p$ gehen bei f_p ins neutrale Element über. Durch Anwenden von f_p erhalten wir somit

$$1 = f_p(I) = f_p(p^n).$$

Wegen der Injektivitätsaussage von 2. folgt $n = 0$, d.h. I liegt in der von den $q \neq p$ erzeugten Untergruppe.

4. Schritt. Das Erzeugendensystem der maximalen Ideale ist linear unabhängig.

Seien $p_1, \ldots, p_r$ paarweise verschiedene maximale Ideale und $n_1, \ldots, n_r$ ganze Zahlen mit

$$(p_1)^{n_1} \cdot \ldots \cdot (p_r)^{n_r} = R.$$

Wir haben zu zeigen, alle n_i sind gleich Null. Zum Beweis wenden wir den Homomorphismus f_{p_i}. Aus der Beschreibung des Kerns von f_{p_i} im 3. Schritt ergibt sich

---

[20] $\pi^a R_p = \pi^b R_p \Leftrightarrow \pi^{a-b} R_p = R_p \Leftrightarrow \pi^{a-b}$ liegt in R_p und ist eine Einheit $\Leftrightarrow a = b$.

$$f_{p_i}((p_i)^{n_i} = 1.$$

Und aus der Injektivitätsaussage des 3. Schritts folgt

$$n_i = 0.$$

5. Schritt. Berechnung der Exponenten einer Zerlegung mit Hilfe der v_p.

Wir haben zu zeigen, für

$$I = (p_1)^{n1} \bullet \ldots \bullet (p_r)^{n_r}$$

gilt

$$n_i = v_{p_i}(I).$$

Wegen

$$IR_p = \{ \frac{a}{b} \mid a \in I, b \in R\text{-}p\}$$

gilt

$$\begin{aligned} v_p(IR_p) &= \inf \{v_p(\tfrac{a}{b}) \mid a \in I, b \in R\text{-}p\} \\ &= \inf \{ v_p(a) \mid a \in I \} \qquad \text{(wegen } v_p(b) = 0) \\ &= v_p(I). \end{aligned}$$

Es reicht also zu zeigen

$$n_i = v_{p_i}(IR_{p_i}).$$

Wir wenden auf I die Abbildung f_{p_i} an. Aus der Beschreibung des Kerns von f_{p_i} im 3. Schritt erhalten wir

$$IR_{p_i} = f_{p_i}(I) = f_{p_i}((p_i)^{n_i}) = (p_i R_{p_i})^{n_i}$$

Es reicht zu zeigen,

$$v_p(p^n R_p) = n$$

für jedes maximale Ideal p von R und jede ganze Zahl n. Sei π ein Parameter vom v_p. Dann gilt

$$\begin{aligned} v_p(p^n R_p) &= v_p(\pi^n R_p) \\ &= \inf \{ v_p(\pi^n r) \mid r \in R_p\} \\ &= \inf \{ n + v_p(r) \mid r \in R_p \} \\ &= n + \inf \{v_p(r) \mid r \in R_p\} \\ &= n. \end{aligned}$$

Es bleibt noch die zusätzliche Identität (3) zu beweisen.

6. Schritt. Es gilt $IR_p = (pR_p)^{v_p(I)}$

Wir wenden den Homomorphismus f_p auf die Zerlegung

$$I = (p_1)^{n1} \bullet \ldots \bullet (p_r)^{n_r} \qquad (7)$$

an, wobei wir annehmen, daß p im Produkt auf der rechten Seite mit dem Exponenten

$$n = v_p(I)$$

vorkommt (welcher gleich Null sein kann). Wegen der Aussage zum Kern von f_p im 3. Schritt erhalten wir aus (7) die Identität

$$IR_p = (pR_p)^n.$$

Dies ist aber gerade die gesuchte Identität.
QED.

1.5.4 Folgerung: Der Wert eines Elements für verschiedene p

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und

$$a \in K^*.$$

Dann gilt für fast alle[21] maximalen Ideale p von R

$$v_p(a) = 0.$$

Beweis. In der Primfaktorzerlegung von aR kommen nur endlich viele Faktoren mit einem von 0 verschiedenen Exponenten vor. Für alle anderen p gilt

$$0 = v_p(aR) = \inf \{v_p(a) + v_p(r) \mid r \in R\} = v_p(a).$$

QED.

1.5.5 Folgerung: direkte Summenzerlegung von F(R)

Für jeden Dedekind-Ring besteht ein Gruppen-Isomorphismus

$$F(R) \xrightarrow{\cong} \oplus''_p F(R_p),\ I \mapsto (f_p(I))_p\ . \qquad (1)$$

Dabei durchlaufe p auf der rechten Seite alle maximalen Ideale von R und f_p bezeichne den Gruppen-Homomorphismus im Beweis des Zerlegungssatzes 1.5.3,

$$F(R) \longrightarrow F(R_p),\ I \mapsto IR_p.$$

Beweis. Wie im 3. Schritt des Beweises von 1.5.3 gezeigt, liegt pR_p im Bild von f_p. Also liegt $F(R_p)$ im Bild von (1). Da dies für jedes p gilt, ist (1) surjektiv.

Liegt

$$I = (p_1)^{n_1} \bullet \ldots \bullet (p_r)^{n_r}$$

im Kern von f_{p_i} so muß

$$n_i = 0$$

gelten (nach dem 3.Schritt im Beweis vn 1.5.3). Liegt I im Kern von (1), so liegt I im Kern jedes f_p. Also mut $n_i = 0$ für jedes i gelten, d.h. I = R.
QED.

1.5.6 Folgerung: Rechenregeln für $v_p(I)$

Seien R ein Dedekind-Ring mit dem Quotientenkörper K, $p \subseteq R$ ein maximales Ideal von R und I, I', I'' gebrochene Ideale. Dann gilt

(i) $v_p(I'I'') = v_p(I') + v_p(I'')$.

(ii) $v_p(I^{-1}) = - v_p(I)$.

---

[21] d.h. für alle mit eventueller Ausnahme von endliche vielen.

(iii) $v_p(I' + I'') = \inf \{v_p(I'), v_p(I'')\}$

(iv) $v_p(I' \bigcap I'') = \sup \{ v_p(I'), v_p(I'') \}$

Beweis. Zu (i) und (ii).Für jedes gebrochene Ideal I ist $v_p(I)$ der Exponent von p im der Primfaktorzerlegung von I von R. Aussage (i) übersetzt sich damit in die Aussage, daß sich beim Multiplizieren der Ideale, die Exponenten addieren (was offensichtlich richtig ist). Analog übersetzt sich Aussage (ii) in die Aussage, daß die Exponenten der Primfaktorzerlegung eines Ideals beim Invertieren in ihr Negatives übergehen, was ebenfalls richtig ist.
Zu (iii) und (iv). Für jedes gebrochene Ideal I von R ist $v_p(I)$ gerade der Exponent n in der Darstellung

$$IR_p = (pR_p)^n$$

von IR_p als Potenz des maximalen Ideals von R_p. Aussage (iii) übersetzt sich damit in die Aussage, daß der Exponent zu einer Summe von Idealen gleich dem Mininimum der Exponenten der Ausgangsideale ist. Bezeichne π einen Parameter von v_p. Dann gilt

$$\pi^a R_p + \pi^b R_p = \pi^a(R_p + \pi^{b-a}R_p) = \pi^a R_p \qquad \text{(O.B.d.A. } a \le b\text{)}$$
$$= \pi^{\min\{a, b\}} R_p.$$

Analog ergibt sich Aussage (iv) aus

$$\pi^a R_p \bigcap \pi^b R_p = \pi^b R_p \qquad \text{(O.B.d.A. } a \le b\text{)}$$
$$= \pi^{\max\{a, b\}} R_p.$$

QED.

1.6 Moduln über Dedekind-Ringen (und Bilinearformen)

1.6.1 Vorbemerkung

Unser nächstes Ziel ist der Beweis der Aussage, daß die ganze Abschließung eines Dedekind-Rings in einer endlichen (separablen) Erweiterung des Quotientenkörpers wieder ein Dedekind-Ring ist.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

R	Dedekind-Ring mit K:=Q(R)
L/K	endliche Körper-Erweiterung
S	ganze Abschließung von R in L

Außerdem wollen wir bei dieser Gelegenheit einige wichtige zahlentheoretische Begriffe wie den der Differente und den der Diskriminante einführen.

Zu diesem Zweck müssen wir einige Vorbetrachtungen durchführen, für welche die Tatsache, daß L ein Körper ist, keine Rolle spielt: wir werden lediglich verwenden, daß L ein endlich-dimensionaler K-Vektorraum ist. Wir betrachten also zunächst eine etwas allgemeinere Situation und drücken dies wie folgt auch durch die Wahl unserer Bezeichnungen aus.

1.6.2 Die Situation

$$\begin{array}{cc} K & U \\ \cup & \cup \\ R & T \end{array}$$

In diesem Abschnitt 1.6 seien

K	ein Körper
U	ein endlich-dimensionaler K-Vektorraum
R	ein Dedekind-Ring mit dem Quotientenkörper K = Q(R).
T	ein R-Teilmodul von U
L,M,N	Gitter[22] in U über R, d.h. endlich erzeugte R-Teilmoduln von U, die eine Basis von U über K enthalten.

1.6.3 Ein Durchschnittssatz

Seien K, R und T wie in 1.6.2. Dann gilt

$$\bigcap T_p = T$$

wenn p die Menge maximalen Ideale von R durchläuft und

$$T_p = T \bullet R_p := \{\frac{t}{b} \mid t \in T,\ b \in R - p\} \ (\subseteq U)$$

die Lokalisierung[23] von T nach dem Primideal p bezeichnet.

Die Aussagea gilt auch ohne die Annahme, daß R ein Dedekind-Ring ist.

Beweis. Trivialerweise gilt

$$T \subseteq \bigcap T_p.$$

Wir haben die umgekehrte Inklusion zu beweisen. Sei

$$u \in \bigcap T_p.$$

Wir betrachten die Menge

$$J_u := \{x \in R \mid xu \in T\}.$$

Dies ist ein Ideal von R. Es reicht zu zeigen, $J_u = R$, d.h. es reicht zu zeigen,

J_u liegt in keinem maximalen Ideal von R.

Sei p ein vorgegebenes maximales Ideal. Dann hat u nach Voraussetzung die Gestalt

$$u = \frac{w}{x} \text{ mit } w \in T \text{ und } x \in R - p.$$

Wegen $x \bullet u = w \in T$ gilt $x \in J_u$. Wegen $x \in R - p$ ist J_u nicht ganz in p enthalten.

QED.

1.6.4 Vergleichslemma für Gitter

(i) Seien R ein Integritätsbereich, U ein endlich-dimensionaler Vektorraum über

$$K = Q(R)$$

und

$$M, N \subseteq U$$

zwei Gitter von U. Dann gibt es ein Element

$$a \in R - \{0\}$$

mit

---

[22] genauer: Gitter vom maximalen Rang. Zum Beispiel ist $\mathbb{Z}^n \subseteq \mathbb{R}^n$ ein Gitter vom maximalen Rang über $\mathbb{Z}$ im $\mathbb{R}$-Vektorraum $\mathbb{R}^n$.

[23] d.h. $T_p = T \otimes_R R_p$

$$aM \subseteq N.$$

(ii) Ist R außerdem ein Dedekind-Ring, so gilt

$$M_p = N_p$$

für fast alle maximalen Ideale p von R.

Beweis. Zu (i). Seien

$$n_1, \dots, n_r \in N$$

die Elemente einer Basis von U und

$$m_1, \dots, m_s \in M$$

ein Erzeugendensystem von M über R. Es reicht die Existenz eines $a \in K - \{0\}$ zu beweisen mit

$$am_i \in N.$$

Da die n_j eine Basis von U über K bilden, können wir die $m_i \in M \subseteq U$ in der Gestalt

$$m_i = \sum_{j=1}^{s} c_{ij} \cdot n_j \text{ mit } c_{ij} \in K$$

schreiben. Wegen K = Q(R) haben die Koeffizienten c_{ij} die Gestalt

$$c_{ij} = \frac{r_{ij}}{s_{ij}} \text{ mit } r_{ij}, s_{ij} \in R \text{ und } s_{ij} \neq 0.$$

Wir können für a das Produkt der s_{ij} wählen, denn dann gilt $ac_{ij} \in R$ für alle i und j, also

$$am_i = \sum_{j=1}^{s} (ac_{ij}) \cdot n_j \in N$$

für alle i.

Zu (ii). Wegen (i) können wir Elemente $a, b \in K - \{0\}$ wählen mit[24]

$$aM \subseteq N \subseteq bM. \qquad (1)$$

Nach 1.5.4 gibt es nur endlich viele maximale Ideale p mit

$$v_p(a) \neq 0 \text{ oder } v_p(b) \neq 0.$$

Für alle übrigen p sind a und b Einheiten von R_p, d.h. mit (1) gilt

$$M \cdot R_p \subseteq N \cdot R_p \subseteq M \cdot R_p,$$

d.h. $M_p = N_p$.

QED.

1.6.5 Konstruktion: der Index zweier Gitter

Seien R, K und U wie in 1.6.2 und

$$M, N \subseteq U$$

zwei Gitter von U über R. Wir betrachten zunächst den Spezialfall. M und N sind frei[25].

Dann existiert ein K-linearer Automorphismus

---

[24] man wähle b derart, daß $\frac{1}{b} N \subseteq M$ gilt.

[25] d.h. die Moduln besitzen R-linear unabhängige Erzeugendensystem. Diese sind automatisch auch linear unabhänging über K, also Vektorraumbasen von U über K.

$$f: U \longrightarrow U$$

mit

$$f(M) = N.$$

Man kann f zum Beispiel so wählen, daß ein vorgegebenes freies Erzeugendensystem von M in ein vorgegebenes freies Erzeugendensystem von N abgebildet wird. Ist

$$g: U \longrightarrow U$$

ein weiterer Automorphismus mit

$$g(M) = N,$$

so gilt

$$g^{-1}f(M) = M \text{ und } f^{-1}g(N) = N,$$

d.h. $g^{-1}f$ ist ein Automorphismus von U, welcher die Elemente einer Basis von M in R-linearkombinationen dieser Basiselemente überführt. Insbesondere gilt

$$\det(f)/\det(g) = \det(g^{-1}f) \in R.$$

Analog folgt

$$\det(g)/\det(f) = \det(f^{-1}g) \in R.$$

Wir haben gezeigt, $e = \det(f)/\det(g)$ ist eine Einheit von R, d.h.

$$\det(f)R = e \bullet \det(g)R = \det(g)R.$$

ist ein von der speziellen Wahl des Automorphismus f unabhängiges gebrochenes Ideal. Es wird mit

$$(M:N) := \det(f)R$$

bezeichnet und heißt Index des Gitters N im Gitter M.

Bemerkungen

(i) Die obige Situation liegt vor, wenn R ein diskreter Bewertungsring ist. Es gilt die folgende Aussage.

(ii) Jedes Gitter M über einem diskreten Bewertungsring R besitzt ein R-linear unabhängiges Erzeugendensystem. Genauer gilt:

(iii) Jedes minimale Erzeugendensystem [26] eines Gitters über einem diskreten Bewertungsring R ist R-linear unabhängig.

Beweis der Bemerkugnen.

Es reicht, die letzte Aussage zu beweisen. Sei $m_1, \ldots, m_r$ ein minimales Erzeugendensystem des Gitters M über dem diskreten Bewertungsring R mit dem Parameter π. Angenommen es besteht eine lineare Abhängigkeit, sagen wir

$$a_1 m_1 + \ldots + a_r m_r = 0,$$

wobei nicht alle Koeffizienten $a_i \in R$ gleich Null sind. Falls alle a_i Nicht-Einheiten sind, kann man eine Potenz von π ausklammern und wegen $M \subseteq U$ kürzen.[27] Wir können also annehmen, eines der a_i ist eine Einheit von R. Dann ist aber m_i eine R-Linearkombination der übrigen Erzeuger im Widerspruch zur Minimalität des gewählten Erzeugendensystems. Dieser Widerspruch zeigt, die obigen Bemerkungen sind richtig.
QED (Bemerkungen)

Wir behandeln jetzt den allgemeinen Fall von Gittern über einem Dedekind-Ring die nicht notwendig frei sein müssen.

---

[26] Ein Erzeugendensystem heißt minimal, wenn die Eigenschaft, Erzeugendensystem zu sein, beim Streichen eines beliebigen Elements verlorengeht.

[27] Der Nullvektor von U läßt sich mit $1/\pi$ multiplizieren und das Produkt ist gleich dem Nullvektor.

Der Fall beliebiger Gitter M und N.

Für jedes maximale Ideal p von R betrachten wir das gebrochene Ideal

$$(M_p : N_p) \text{ von } R_p.$$

Wegen $M_p = N_p$ für fast alle p gilt

$$(M_p : N_p) = R_p \text{ für fast alle maximalen Ideale p.}$$

Es gibt deshalb ein eindeutig bestimmtes gebrochenes Ideal I von R mit

$$I \bullet R_p = (M_p : N_p).$$

Dieses gebrochene Ideal heißt Index von N in M und wird mit

$$(M: N)$$

bezeichnet.

Bemerkungen

(iv) Wir verwenden hier den Satz von der Primfaktorzerlegung 1.5.3: jedes gebrochene Ideal I von R hat die Gestalt

$$I = \prod_{p \text{ maximal}} p^{n_p}$$

mit eindeutig bestimmten ganzen Zahlen

$$n_p := v_p(I) = v_p(IR_p).$$

Umgekehrt kann man die ganzen Zahlen n_p beliebig vorgeben, vorausgesetzt, nur endlich viele von ihnen sind ungleich Null.

(v) Die obige Definition hat als Formel die Gestalt

$$(M : N) = \prod_{p \text{ maximal}} p^{v_p((M_p:N_p))}$$

(vi) (M:N) ist das eindeutig bestimmte gebrochene Ideal von R mit[28]

$$(M: N)R_p = (M_p : N_p).$$

(vii) Im Fall freier R-Moduln M und N stimmt die Definition im Spezialfall mit der für den allgemeinen Fall gegebenen überein: ist $f: U \longrightarrow U$ ein Automorphismus mit

$$f(M) = N,$$

so gilt für jedes maximale Ideal p auch

$$f(M_p) = N_p,$$

d.h. es ist

$$(M_p : N_p) = \det(f) \bullet R_p$$

Das eindeutig bestimmte gebrochene Ideal I mit $I \bullet R_p = (M_p : N_p)$ für jedes p ist somit gleich $I = \det(f)R$.

(viii) Im Fall $R = \mathbb{Z}$ und $M \supseteq N$ ist

$$(M:N)$$

gerade das Ideal von R, welches vom Index der Untergruppe N von M erzeugt wird.

Als $\mathbb{Z}$-Teilmoduln von U sind M und N nämlich torsionsfrei und damit endlich erzeugte abelsche Gruppen, d.h.

$$M \cong \mathbb{Z}^n.$$

---

[28] Die Vorgabe des Ideals $I \bullet R_p$ ist äquivalent zur Vorgabe der ganzen Zahle $v_p(I \bullet R_p)$: im ersten Fall gibt man $\pi^n R_p$ vor und im zweiten die ganze Zahle n.

Bezeichne $e_i \in \mathbb{Z}^n$ das n-Tupel mit der n-ten Koordinate 1 und allen anderen Koordinaten gleich 0, sodaß wir

$$M = \mathbb{Z}e_1 + ... + \mathbb{Z}e_n$$

schreiben können. Nach dem Elementarteilersatz können wir dabei das $\mathbb{Z}$-linear unabhängige Erzeugendensystgem der e_i noch so wählen, daß sich der Teilmodul N in der Gestalt

$$N = d_1\mathbb{Z}e_1 + ... + d_n\mathbb{Z}e_n$$

schreiben läßt mit den Elementarteilern $d_i \in \mathbb{N}$. Der Index von N in M im Gruppentheoretischen Sinne ist dann gerade

$$d = d_1 \bullet ... \bullet d_n.$$

Zur Berechnung von (M:N) betrachten wir den $\mathbb{Q}$-linearen Automorphismus

$$f: \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$$

mit der Matrix

$$M(f) = \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_n \end{pmatrix}$$

bezüglich der e_i. Dann gilt

$$f(M) = N,$$

also

$$(M:N) = \det(f)\bullet\mathbb{Z} = d\bullet\mathbb{Z},$$

wie behauptet.

1.6.6 Eigenschaften des Index

Seien R, K und U wie in 1.6.2 und M, N, L Gitter in U über R. Dann gilt:

(i) $(M: M) = R$.

(ii) $(L: M)\bullet(M:N) = (L:N)$.

(iii) Im Fall $M \supseteq N$ ist (M:N) ein ganzes Ideal, d.h.

$$(M: N) \subseteq R,$$

und im Fall $(M:N) = R$ gilt $M = N$.

Beweis. Nach dem Satz von der Primfaktorzerlegung 1.5.3 sind zwei gebrochene Ideale I, J genau dann gleich, wenn zu ihnen dieselben Exponenten in der Primfaktorzerlegung gehören. Das gilt sowohl für R als auch für alle Lokalisierungen R_p. Beim Beweis der obigen Relationen können wir also alle gebrochenen Ideale durch deren zugehörige Ideal in den Lokalisierungen R_p von R ersetzen:

$$I = J \text{ in } R \Leftrightarrow I\bullet R_p = J\bullet R_p \text{ für jedes maximale Ideal p von R.}$$

Zu (i). Es reicht zu zeigen

$$(M_p:M_p) = R_p$$

für jedes maximale Ideal p von R. Zur Berechnund des Index auf der linken Seite können wir die identische Abbildung $id: U \longrightarrow U$ verwenden. Wir erhalten

$$(M_p:M_p) = \det(id)R_p = 1\bullet R_p = R_p.$$

Zu (ii). Es reicht zu zeigen

$$(L_p : M_p)\bullet(M_p : N_p) = (L_p : N_p).$$

Seien $f: U \longrightarrow U$ und $g: U \longrightarrow U$ Automorphismen mit

$$f(L_p) = M_p \text{ und } g(M_p) = N_p.$$

Dann gilt $(g\circ f)(L_p) = N_p$, also

$$(L_p : N_p) = \det(g\circ f)R_p = \det(g)\bullet\det(f)R_p = (M_p : N_p)\bullet(L_p : M_p).$$

Zu (iii). Mit $M \supseteq N$ gilt $M_p \supseteq N_p$. Sei $f: U \longrightarrow U$ ein Automorphismus mit

$$f(M_p) = N_p. \tag{1}$$

Die Bilder bei f eines freien Erzeugendensystems von M_p liegen somit in $N_p \subseteq M_p$, können also als R_p-Linearkombinationen dieses Erzeugendensystems geschrieben werden. Also gilt $\det(f) \in R_p$, d.h.

$$(M_p : N_p) \subseteq R_p \text{ für jedes maximale Ideal p von R.}$$

Die Exponenten der Primfaktorzerlung von (M:N) sind somit sämtlich ≥ 0. Also gilt

$$(M: N) \subseteq R.$$

Sei jetzt (M:N) = R. Dann gilt

$$(M_p : N_p) = R_p$$

für jedes maximale Ideal p von R. Der oben für festes p gewählte Automorphismus f hat also als Determinante eine Einheit von R_p,

$$\det(f) \in R_p^*$$

Das bedeutet, die Matrix von f bezüglich eines freien Erzeugendensystems von M_p besitzt eine Umkehrung mit Koeffizienten in R_p. Insbesondere induziert f^{-1} eine Abbildung

$$M_p \xrightarrow{f^{-1}} M_p \tag{2}$$

Nun ist aber die Zusammensetzung

$$M_p \xrightarrow{f} N_p \subseteq M_p \xrightarrow{f^{-1}} M_p$$

gerade die identische Abbildung, also surjektiv. Also ist (2) surjektiv. Zusammen mit (1) erhalten wir, daß die identische Abbildung

$$M_p \xrightarrow{f^{-1}} M_p \xrightarrow{f} N_p$$

surjektiv ist, d.h. es ist $M_p \subseteq N_p$.

Jedes Element von M ist somit R_p-Linearkombination von Element aus N. Mit anderen Worten,

$$\text{für jedes } m \in M \text{ gibt es ein } a \in R - p \text{ mit } am \in N.$$

Weil M endlich erzeugt ist, gibt es dann aber auch ein gemeinsames a für alle Elemente aus M: für jedes maximale Ideal p von R gibt es ein $a \in R - p$ mit $aM \subseteq N$, d.h. die Menge

$$\{a \in R \mid aM \subseteq N\}$$

liegt in keinem maximalen Ideal von R. Nun ist diese Menge ein Ideal von R, d.h. diese Menge ist gleich R, d.h. 1 liegt in dieser Menge, d.h. es gilt

$$M \subseteq N.$$

Wir haben gezeigt, im Fall $M \supseteq N$, $(M:N) = R$ gilt $M = N$.

QED.

1.6.7 Invarianz des Index bei Automorphismen

Seien R, K und U wie 1.6.2 und seien M, N Gitter in U über R. Dann gilt

$$(M:N) = (f(M):f(N))$$

für jeden K-linearen Automorphismus $f: U \longrightarrow U$.

Beweis. Auf Grund des Satzes von der Zerlegung in Primfaktoren 1.5.3 reicht es zu zeigen

$$(M_p:N_p) = (f(M_p):f(N_p))$$

für jedes maximale Ideal p von R, d.h. wir können annehmen, R ist ein diskreter Bewertungsring und M und N sind freie R-Moduln. Sei

$$g: U \longrightarrow U$$

ein K-linearer Automorphismus mit

$$g(M) = N. \tag{1}$$

Dann gilt

$$(f \circ g \circ f^{-1})(f(M)) = f(N). \tag{2}$$

Aus (1) und (2) erhalten wir damit nach Definition des Index

$$(M:N) = \det(g) \bullet R$$

bzw.

$$\begin{aligned}(f(M):f(N)) &= \det(f \circ g \circ f^{-1}) \bullet R \\ &= \det(f) \bullet \det(g) \bullet \det(f)^{-1} \bullet R \\ &= \det(g) \bullet R \\ &= (M:N).\end{aligned}$$

QED.

Bemerkung

Wie bereits erwähnt wollen wir im nächsten Abschnitt endliche separable Körpererweiteungen L/K unseren Grundkörpers K betrachten. Mit Hilfe einer solchen Körpererweiterung (genauer mit Hilfe der Spur einer solchen Erweiterung) kann man eine nicht-entartete symmetrische K-bilineare Abbildung

$$L \times L \longrightarrow K, (x, y) \mapsto \mathrm{tr}(xy),$$

konstruieren. Die weiteren Definitionen und Sätze dieses Abschnitts hängen von der Wahl einer solchen Bilinearform ab. Wir wollen deshalb im folgenden eine solche Bilinearform als vorgegeben ansehen. Die Konstruktion dieser Bilinearform verschieben wir auf den nächsten Abschnitt 1.7.

1.6.8 Die Situation (Wahl einer Bilinearform)

$$\begin{array}{cc} K & U \\ \cup & \cup \\ R & T \end{array}$$

In diesem Abschnitt 1.6 seien

K	ein Körper
U	ein endlich-dimensionaler K-Vektorraum

$B: U\times U \longrightarrow K$	nicht-entartete symmetrische Bilnearform über K.
R	ein Dedekind-Ring mit dem Quotientenkörper K = Q(R).
T	ein R-Teilmodul von U
L,M,N	Gitter in U über R (vgl. 1.6.2).

Das Vorhandensein der fest gewählten Bilinearform B werden wir gelegentlich auch dadurch betonen, daß wir sagen, U sei ein euklidischer K-Vektorraum mit dem Skalarprodukt B.

1.6.9 Das Dual eines Moduls

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und U ein euklidischer K-Vektorraum (vgl. 1.6.8) Weiter sei

$$T \subseteq U$$

ein R-Teilmodul von U, welcher eine Basis des K-Vektorraums U enthält. Dann heißt

$$D(T) := D_R(T) := \{ u \in U \mid B(u, T) \subseteq R\}$$

Dual von T über R.

1.6.10 Das Dual eines freien Gitters

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und U ein euklidischer K-Vektorraum (vgl. 1.6.8) Weiter sei

$$M$$

ein freies Gitter in U über R mit dem R-linear unabhängigen Erzeugendensystem

$$u_1, \ldots, u_n. \tag{1}$$

Dann gilt.

(i) D(M) ist ein freies Gitter. Die zu (1) duale Basis[29]

$$\breve{u}_1, \ldots \breve{u}_n.$$

ist ein R-linear unabhängiges Erzeugendensystem von D(M).

(ii) D(D(M)) = M.

Beweis. Es genügt, (i) zu beweisen. Wir schreiben u∈U als Linearkombination der $\breve{u}_i$'

$$u = \sum_i c_i \breve{u}_i .$$

Dann gilt

$$\begin{aligned} u\in D(M) &\Leftrightarrow B(u,M)\subseteq R \\ &\Leftrightarrow B(u,u_j) \in R \text{ für alle } j \\ &\Leftrightarrow \sum_i c_i B(\breve{u}_i,u_j) \in R \text{ für alle } j \\ &\Leftrightarrow c_j \in R \text{ für alle } j, \end{aligned}$$

d.h. $D(M) = R\bullet\breve{u}_1 + \ldots + R\bullet \breve{u}_n$.

QED.

---

[29] d.h. die Basis von U über K mit $B(u_i, \breve{u}_j) = \delta_{ij}$ (Kronecker-Symbol) für alle i und j.

1.6.11 Eigenschaften des Duals

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und U ein euklidischer K-Vektorraum (vgl. 1.6.8) Weiter seien

$$M, N \subseteq U$$

Gitter in U über R und p ein maximales Ideal von R. Dann gilt

(i) D(M) ist ein Gitter von U.

(ii) $D(M)R_p = D_{R_p}(M_p)$.

(iii) $D(M) = \cap D_{R_p}(M_p)$,

wobei der Durchschnitt über alle maximalen Ideale p von R erstreckt wird.

(iv) D(D(M)) = M.

(v) (D(M):D(N)) = (N:M).

Beweis. Zu (i). Weil M ein Gitter ist, enthält M eine Basis von U über K, also ein freies Gitter

$$N \subseteq M \text{ , } N \text{ freies Gitter.}$$

Außerdem gibt es ein $c \in K^*$ mit

$$N \subseteq M \subseteq c \bullet N$$

(nach dem Vergleichslemma für Gitter 1.6.4). Man beachte, mit N ist auch c•N ein freies Gitter. Nach Definition des Duals folgt

$$D(c \bullet N) \subseteq D(M) \subseteq D(N).$$

Nun sind D(c•N) und D(N) freie Gitter (nach 1.6.10). Insbesondere ist D(M) als R-Teilmodul des endlich erzeugten R-Moduls D(N) endlich erzeugt. Außerdem enthält mit D(c•N) auch D(M) eine Basis von U über K. Wir haben gezeigt, D(M) ist ein Gitter in U über R.

Zu (ii). Wir fixieren ein endliches Erzeugendensystem von M über R, sagen wir

$$M = R \bullet w_1 + ... + R \bullet w_n.$$

Beweis von "$\supseteq$": Sei $v \in D_{R_p}(M_p)$. Dann gilt

$$B(v, M) \subseteq B(v, M_p) \subseteq R_p$$

also

$$B(v, w_i) = \frac{a_i}{b_i} \text{ mit } a_i \in R, b_i \in R - p.$$

Durch Erweitern der endlich vielen Brüche erreichen wir,

$$b_1 = ... = b_n = b.$$

Dann gilt $b \bullet B(v, w_i) = a_i \in R$, also

$$b \bullet B(v, M) \subseteq R,$$

also

$$B(bv, M) \subseteq R,$$

also

$$bv \in D(M),$$

also $v \in D(M) \bullet \frac{1}{b} \subseteq D(M) \bullet R_p$.

Beweis von "$\subseteq$". Es reicht zu zeigen,

$$D(M) \subseteq D_{R_p}(M_p)$$

(weil die Menge rechts ein R_p-Modul ist), d.h. zu zeigen ist

$$B(v, M_p) \subseteq R_p \text{ für jecdes } v \in D(M).$$

Weil B bilinear ist über K, gilt $B(v, M_p) = B(v, M \bullet R_p) = B(v, M) \bullet R_p$. Es reicht also zu zeigen

$$B(v, M) \subseteq R_p.$$

Wegen $v \in D(M)$ gilt aber sogar $B(v, M) \subseteq R$.

Zu (iii). Es gilt

$$\cap D_{R_p}(M_p) = \cap D(M)R_p \qquad \text{(wegen (ii))}$$

$$= D(M) \qquad \text{(nach 1.6.3).}$$

Zu (iv). Nach (ii) gilt

$$D(D(M)) \subseteq D(D(M)) \bullet R_p = D_{R_p}(D_{R_p}(M_p))$$

Als endlich erzeugter R_p-Modul ist M_p frei über R_p (nach Bemerkung 1.6.5), d.h. wir können 1.6.10 (ii) auf die rechte Seite anwenden. Es folgt

$$D(D(M)) \subseteq M_p$$

für jedes maximale Ideal p, d.h.

$$D(D(M)) \subseteq \bigcap M_p = M$$

(nach 1.6.3). Wir haben die umgekehrte Inklusion zu beweisen. Sei $v \in M$. Nach Definition von D(M) gilt

$$B(v, w) \subseteq R \text{ für jedes } w \in D(M),$$

d.h. es ist

$$B(v, D(M)) \subseteq R,$$

also

$$v \in D(D(M)).$$

Zu (v). Nach Definition des Index reicht es zu zeigen,

$$(D(M):D(N)) \bullet R_p = (N:M) \bullet R_p$$

für jedes maximale Ideal p von R.[30] Wegen (ii) ist letzteres äquivalent zu

$$(D_{R_p}(M_p):D_{R_p}(N_p)) = (N_p:M_p)$$

Der Beweis der Behauptung ist damit auf den Fall $R = R_p$ zurückgeführt, d.h. wir können annehmen,

R ist ein diskreter Bewertungsring und M und N sind freie Gitter über R.

Wir fixieren ein freies Erzeugendensystem von M über R, sagen wir

$$M = R \bullet u_1 + \ldots + R \bullet u_n$$

und bezeichnen die zu den u_i duale Basis mit $v_1, \ldots, v_n$,

$$D(M) = R \bullet v_1 + \ldots + R \bullet v_n \text{ und } B(u_i, v_j) = \delta_{ij}.$$

---

[30] Der Index zweier Gitter ist ein Ideal, welches durch die Ideale definiert ist, die es in den Lokalisierungen von R bezüglich der maximalen Ideale von R erzeugt.

Nun besitzt auch N ein freies Erzeugendensystem über R, und dieses ist eine Basis von U über K. Es gibt also einen K-linearen Automorphismus

$$f: U \longrightarrow U,$$

welcher die u_i in dieses freie Erzeugendensystem von N abbildet. Insbesondere gilt

$$f(M) = N, \tag{1}$$

und dieses freie Erzeugendensystem besteht aus den Vektoren $f(u_i)$,

$$N = R \bullet f(u_1) + ... + R \bullet f(u_n).$$

Bezeichne

$$f^*: U \longrightarrow U$$

die zu f bezüglich B duale Abbildung, d.h. f* sei der K-Automorphismus von U mit

$$B(f(u'), u'') = B(u', f^*(u'')) \text{ für alle } u', u'' \in U.$$

Insbesondere ist dann

$$B((f^*)^{-1}(v_i), f(u_j)) = B(f^*((f^*)^{-1}(v_i)), u_j) = B(v_i, u_j) = \delta_{ij},$$

d.h. die $(f^*)^{-1}(v_i)$ bilden gerade die zu den $f(u_j)$ duale Basis. Es folgt (nach 1.6.10)

$$D(N) = R \bullet (f^*)^{-1}(v_1) + ... + R \bullet (f^*)^{-1}(v_n),$$

d.h.

$$(f^*)^{-1}(D(M)) = D(N),$$

d.h.

$$f^*(D(N)) = D(M). \tag{2}$$

Aus (2) und (1) erhalten wir, weil alle beteiligten Moduln frei sind,

$$(D(N):D(M)) = \det(f^*) \bullet R$$
$$(M:N) = \det(f) \bullet R$$

Es reicht also zu zeigen

$$\det(f^*) = \det(f).$$

Das ist aber der Fall, weil die Matrix von f* bezüglich der dualen Basis der v_i gerade transponiert ist zur Matrix von f bezüglich der Basis der u_i.

QED.

1.6.12 Die Diskriminante eines Gitters

Seien R ein Dedekind-Ring mit dem Quotientenkörper K, U ein endlich-dimensionaler K-Vektorraum mit Skalarprodukt[31]

$$B: U \times U \longrightarrow K$$

und M ein R-Gitter in U. Dann heißt

$$\delta(M) := \delta(M/R) := (D_R(M) : M)$$

Diskriminante von M über R.

1.6.13 Eigenschaften der Diskriminante

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und U ein endlich-dimensionaler K-Vektorraum mit Skalarprodukt. Für beliebige R-Gitter

$$M, N \subseteq U$$

in U gilt dann:

---

[31] d.h. mit nicht-entarteter symmetricher Bilinearform.

(i) $\delta(N) = \delta(M)\bullet(M:N)^2$.

(ii) $\delta(M_p/R_p) = \delta(M/R)\bullet R_p$ für jedes maximale Ideal p von R.

(iii) $\delta(M) = \det B(u_i, u_j)\bullet R$

falls M das freie Erzeugendensystem $u_1, \dots, u_n$ besitzt,

$M = R\bullet u_1+\dots+R\bullet u_n$, $n := \dim_K U$.

(iv) Im Fall $M \supseteq N$ gilt

$\delta(M) \mid \delta(N)$ (d.h. $\delta(M) \supseteq \delta(N)$).

Außerdem ist dann

$\delta(M) = \delta(N) \Leftrightarrow M = N$.

Beweis. Zu (i). Es gilt

$\delta(N)$	$= (D(N) : N)$	(nach Definition)
	$= (M:N)\bullet (D(N):M)$	(nach 1.6.6 (ii))
	$= (M:N)\bullet (D(N):D(M))\bullet(D(M):M)$	(nach 1.6.6 (ii))
	$= (M:N)^2\bullet (D(M):M)$	(nach 1.6.11 (v))
	$= \delta(M)\bullet (M:N)^2$	(nach Definition)

Zu (ii). Für jedes maximale Ideal p von R gilt

$\delta(M/R)\bullet R_p$	$= (D_R(M) : M)\bullet R_p$	(nach Definition)
	$= (D_R(M) \bullet R_p : M\bullet R_p)$	(Bemerkung 1.6.5 (vi))
	$= (D_{R_p}(M_p):M_p)$	(nach 1.6.11)
	$= \delta(M_p/R_p)$	(nach Definition).

Zu (iii). Seien $v_1, \dots, v_n$ die zu den u_i duale Basis und

$$f: U \longrightarrow U$$

der K-lineare Automorphismus mit

$$f(v_i) = u_i \text{ für } i = 1, \dots, n.$$

Dann wird D(M) von den v_i erzeugt, d.h. es gilt f(D(M)) = M, also

$$\delta(M) = (D(M):M) = \det(f)R.$$

Außerdem ist

$$\det B(u_i, u_j) = \det B(u_i, f(v_j)) =^{32} \det(f)\bullet\det B(u_i, v_j) =^{33} \det(f).$$

---

[32] Links steht die Determinante der Zusammensetzung der Abbilung

$$K^n \longrightarrow U, e_i \mapsto f(v_i)$$

mit der Abbildung

$$U \longrightarrow K^n, x \mapsto (B(u_1, x), \dots, B(u_n, x).$$

Identifiziert man U mit Hilfe der Basis der v_j mit K^n, so bekommt die erste Abbildung die Determinante det(f) und die zweite die Determinante $\det B(u_i, v_j)$.

[33] $B(u_i, v_j)$ ist nach Definition der v_j die Einheitsmatrix.

Zu (iv). Im Fall $M \supseteq N$ ist (M:N) ein Ideal von R (nach 1.6.6 (iii)). Der erste Teil der Behauptung folgt damit aus (i).
Ebenfalls nach (i) ist

$$\delta(M) = \delta(N) \Leftrightarrow (M:N) = R .$$

Nach 1.6.6 (iii) ist aber die Identität rechts äquivalent zu M = N.
QED.

1.6.14 Verhalten bei direkten Summen

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und U ein endlich-dimensionaler K-Vektorraum mit Skalarprodukt. Weiter sei

$$U = U_1 \oplus U_2$$

eine Zerlegung in orthogonale K-lineare Unterräume. Für beliebige R-Gitter

$M_i , N_i \subseteq U_i$ (i = 1,2)

sind dann

$$M := M_1 \oplus M_2 \text{ und } N := N_1 \oplus N_2$$

R-Gitter von U mit

(i) $(M:N) = (M_1:N_1)\bullet(M_2:N_2)$

(ii) $D(M) = D(M_1)+D(M_2)$

(iii) $\delta(M) = \delta(M_1)\bullet\delta(M_2)$.

Aussage (i) gilt auch ohne die Annahme der Orthogonalität der Zerlegung von U.
Beweis. Zu (i). Wir können annehmen, R ist ein diskreter Bewertungsring und die auftretenden Gitter sind sind frei. Wir wählen Automorphismen

$$f_i: U_i \longrightarrow U_i$$

mit

$$f_i(M_i) = N_i \text{ für } i = 1, 2.$$

Für den Automorphismus f: U $\longrightarrow$ U mit den Koordinatenfunktionen f_1, f_2 gilt dann

$$\det(f) = \det(f_1)\bullet\det(f_2),$$

also ist

$$(M:N) = \det(f)R = \det(f_1)R\bullet\det(f_2)R = (M_1:N_1)\bullet(M_2:N_2).$$

Zu (ii). Sei B_i die Einschränkung der Bilinearform B auf U_i. Für

$$u = (u_1, u_2), v = (v_1, v_2) \in U_1 \oplus U_2 = U$$

gilt dann wegen der Orthogonalität der Zerlegung von U:

$$B(u, v) = B(u_1, v_1) + B(u_2, v_2)$$

also

$$B(u, M) = B(u_1, M_1) + B(u_2, M_2).$$

Es folgt

$$B(u, M) \subseteq R \Leftrightarrow = B(u_1, M_1) \subseteq R \text{ und } B(u_2, M_2) \subseteq R,$$

d.h.

$$u \in D(M) \Leftrightarrow u_1 \in D(M_1) \text{ und } u_2 \in D(M_2).$$

Zu (iii).

$$\begin{aligned} \delta(M) &= (D(M):M) \\ &= (D(M_1) + D(M_2) : M_1 + M_2) \qquad \text{(nach (ii))} \end{aligned}$$

$$= (D(M_1):M_1) \bullet (D(M_2):M_2) \qquad \text{(nach (i))}$$
$$= \delta(M_1)\bullet\delta(M_2)$$

QED.

1.6.15 Verhalten bei Erweiterungen

Seien $R \subseteq R'$ ineinanderliegende Dedekind-Ringe mit den Quotientenkörpern

$$K = Q(R) \text{ und } K' = Q(R').$$

Weiter sei U ein endlich-dimensionaler K-Vektorraum und

$$U' := U \otimes_K K'.$$

(i) Für beliebige R-Gitter $M, N \subseteq U$ sind MR' $NR' \subseteq U'$ Gitter über R' mit

$$(MR' : NR') = (M:N)R'.$$

Sei weiter $B: U \times U \longrightarrow K$ ein Skalarprodukt und $B': U'\times U' \longrightarrow K'$ dessen bilineare Fortsetzung auf U'. Dann gilt

(ii) $D_{R'}(MR') = D_R(M)R'$.

(iii) $\delta(MR'/R') = \delta(M/R)R'$.

Beweis. Es genügt, die Identitäten lokal in den maximalen Idealen p' von R' zu überprüfen. Ist $p'\cap R$ maximal in R, so reduziert dies die Behauptung auf den Fall, daß R und R' diskrete Bewertungsringe und M,N freie R-Moduln sind. Ist $p := p'\cap R$ nicht maximal, so ist R_p ein Körper, also $MR_p = NR_p = U$ und die zu beweisenden lokalen Identitäten sind trivial:

- In (i) steht auf beiden Seiten R'.
- In (ii) steht auf beiden Seiten UR'
- In (iii) steht auf beiden Seiten (UR':UR') = R'.

Damit genügt es, die Behauptung für freie Moduln M und N über einem diskreten Bewertungsring R zu beweisen. In diesem Fall ergeben sich aber die Identitäten aus der jeweiligen expliziten Beschreibung der beteiligten Moduln:

- In (i) steht auf beiden Seiten das gebrochene Ideal von R', welches von der Determinante eines Automorphismus $f: U \longrightarrow U$ mit $f(M) = N$ erzeugt wird.
- In (ii) steht auf beiden Seiten der (freie) R'-Modul, welcher von der dualen Basis eines freien Erzeugendensystems von M über R erzeugt wird.
- In (iii) steht auf beiden Seiten das Ideal von R', welches von der Determinante eines Automorphismus $f: U \longrightarrow U$ erzeugt wird, welcher die duale Basis eines freien Erzeugendensystem in dieses Erzeugendensystem abbildet.

QED.

1.7 Norm und Spur

1.7.1 Der Endomorphismenring eines freien Moduls

Seien R ein kommutativer Ring mit Eins und M ein freier R-Modul mit dem linear unabhängigen Erzeugendensystem $\omega_1,\ldots,\omega_n$. Die Menge der R-linearen Endomorphismen von M, d.h. der R-linearen Abbildungen $M\to M$ bezeichnen wir mit

$$\mathrm{End}_R(M).$$

Dies ist ein im allgemeinen nicht mehr kommutativer Ring, welcher isomorph ist zum Ring der n×n-Matrizen

$$R^{n\times n}$$

mit Einträgen aus R, und zwar gehört zu jeder Basis von M über R ein Isomorphismus.

$$R^{n\times n} \to \mathrm{End}_R(M),\ (r_{ij}) \mapsto (\omega_i \mapsto \sum_{j=1}^{n} r_{ij}\omega_j).$$

Der Ring R läßt sich als Teilring von $\mathrm{End}_R(M)$ auffassen vermittels der Abbildung

$$R \to \mathrm{End}_R(M),\ r \mapsto (m \mapsto rm).$$

1.7.2 Definition von Spur und Norm eines Endomorphismus

Seien R ein kommutativer Ring mit Eins und M ein freier R-Modul. Für jedes

$$A\in\mathrm{End}_R(M)$$

betrachten wir das charakteristische Polynom von A,

$$\chi(A, x) := \det(x\cdot Id - A).^{34}$$

Wir schreiben

$$\chi(A, x) = x^n - \mathrm{Tr}(A)\cdot x^{n-1} \pm \ldots + (-1)^n N(A).$$

Die Koeffizienten Tr(A) und N(A) heißen Spur bzw. von Norm von A.

Bemerkung

Identifiziert man den Endomorphismus A mit der zugehörigen n×n-Matrix bezüglich irgendeines freien Erzeugendensystems von M über R, sagen wir

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \text{ mit } a_{ij} \in R,$$

so gilt

$$\begin{aligned} N(A) &= (-1)^n \chi(A, 0) = (-1)^n \det(-A) \\ &= \det(A) \end{aligned}$$

und

$$\begin{aligned} \mathrm{Tr}(A) &= \text{negativer Koeffizient von } x^{n-1} \text{ in } \det\begin{pmatrix} x-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x-a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n1} & -a_{n2} & \cdots & x-a_{nn} \end{pmatrix} \\ &= a_{11} + \ldots + a_{nn} \end{aligned}$$

1.7.3 Eigenschaften von Spur und Norm

Seien R ein kommutativer Ring mit Eins und M ein freier R-Modul. Dann gilt:

(i) $N(AB) = N(A)N(B)$ für $A,B\in\mathrm{End}_R(M)$.

---

[34] Wir ziehen hier diese Definition der Variante

$$\chi(A, x) = \det(A - x\cdot Id)$$

vor, weil auf diese Weise $\chi(A, x)$ ein normiertes Polynom in x wird. Dadurch fallen in einigen Formeln sonst nötige Vorzeichenfaktoren weg.

(ii) $\mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$ für $A,B \in \mathrm{End}_R(M)$.

(iii) $N(r) = r^n$ für $r \in R$.

(iv) $\mathrm{Tr}(r) = n \cdot r$ für $r \in R$.

(v) $\mathrm{Tr}(rA) = r \cdot \mathrm{Tr}(A)$ für $r \in R$ und $A \in \mathrm{End}_R(M)$.

Beweis. Zu (i). $N(AB) = \det(AB) = \det(A) \cdot \det(B) = N(A) \cdot N(B)$.

Zu (ii) und (v). Sei (a_{ij}) die Matrix von A bezüglich der Basis $\omega_1, ..., \omega_n$. Dann gilt

$$\mathrm{Tr}(A) = a_{11} + ... + a_{nn}.$$

Dieser Ausdruck ist offensichtlich R-linear in A.

Zu (iii) und (iv). Mit den Bezeichnungen von (ii) erhalten wir im Fall $A = r \in R$ für die zugehörigen Matrix

$$(a_{ij}) = \begin{pmatrix} r & 0 & \dots & 0 \\ 0 & r & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & r \end{pmatrix},$$

also $\mathrm{Tr}(r) = n \cdot r$ und $N(r) = r^n$.

QED.

1.7.4 Satz von Hamilton-Cayley

Seien R ein kommutativer Ring mit Eins und M ein freier R-Modul. Dann gilt

$$\chi(A,A) = 0 \text{ für jedes } A \in \mathrm{End}_R(M).$$

Beweis. Sei (a_{ij}) die Matrix von A bezüglich der Basis $\omega_1, ..., \omega_n$. Dann gilt

$$A\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

also

$$(*) \qquad 0 = \sum_{j=1}^{n} (\delta_{ij}A - a_{ij})\omega_j$$

Dabei fassen wir die Ausdrücke $\delta_{ij}A - a_{ij}$ als Elemente des Rings $\mathrm{End}_R(M)$ auf. Genauer liegen diese Ausdrücke sogar in dem kommutativen Teilring

$$R[A] \subseteq \mathrm{End}_R(M).$$

Wir betrachten die Matrix der $b_{ij} = \delta_{ij}A - a_{ij}$ im Ring der n×n-Matrizen über R[A]. Bezeichne B_{ij} die adjungierte Unterdeterminante von (b_{ij}) zur Position (i,j). Wir multiplizieren die i-te Gleichung von (*) mit B_{ij_0} und bilden die Summe der entstehenden Gleichungen. Wegen

$$\sum_{i=1}^{n} B_{ij_0} b_{ij} = \begin{cases} \det(b_{ij}) \text{ für } j = j_0 \\ 0 \quad \text{sonst} \end{cases}$$

erhalten wir aus (*):

$$0 = \det(\delta_{ij}A - a_{ij})\omega_{j_0}.$$

Da j_0 beliebig war, ist die Multplikation mit $\det(\delta_{ij}A- a_{ij})$ die Nullabbildung des Endomorphismenrings $End_R(M)$, mit anderen Worten, es gilt

$$0=\det(\delta_{ij}A- a_{ij}) = \chi(A,A).$$

QED.

1.7.5 Das Charakteristische Polynom als Norm

Seien R ein kommutativer Ring mit Eins und M ein freier R-Modul. Weiter sei

$$x$$

ein über dem Ring R transzendentes Element. Dann definieren die n×n-Matrizen mit Einträgen aus R[x] lineare Endomorphismen von $M\otimes_R R[x]$, so daß für solche Endomorphismen die Norm definiert ist. Es gilt

$$(-1)^n\cdot N(x-A) = \chi(A,x)$$

für jedes $A\in End_R(M)$.

Beweis. Die Elemente $\omega_1, ..., \omega_n$ bilden eine linear unabhängiges Erzeugendensystem von $M\otimes_R R[x]$ über R[x]. Es gilt

$$A\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

also

$$(x-A)\omega_i = \sum_{j=1}^{n} (\delta_{ij}x-a_{ij})\omega_j$$

also

$$N(x-A) = \det(\delta_{ij}x-a_{ij}) = (-1)^n\chi(A,x).$$

QED.

Bemerkung

Die eben bewiesene Identität bleibt gültig, wenn man für t ein Element von R einsetzt.

1.7.6 Die Norm eines Polynoms mit Koeffizienten aus End(M)

Seien $A_1,...,A_\ell\in End_R(M)$ und x ein über R transzendentes Element. Dann gilt

$$N(x^\ell+A_1x^{\ell-1}+...+A_\ell) = x^{n\ell} + r_1\cdot x^{n\ell-1}+...+r_{n\ell}$$

mit gewissen Elementen $r_i\in R$. Insbesondere ist

$$r_1=Tr(A_1) \text{ und } r_{n\ell} = N(A_\ell).$$

Beweis. Die Beweisidee ist dieselbe wie bei der vorhergehenden Aussage. Für $\nu=1,...,\ell$ haben wir Identitäten

$$A_\nu\omega_i = \sum_{j=1}^{n} a_{\nu ij}\omega_j .$$

Also ist

$$(x^\ell+A_1x^{\ell-1}+...+A_\ell)\omega_i = \sum_{j=1}^{n} (\delta_{ij}x^\ell+a_{1ij}x^{\ell-1}+...+a_{\ell ij})\omega_j ,$$

also

$$N(t^{\ell}+A_1t^{\ell-1}+...+A_{\ell}) = \det(\delta_{ij}t^{\ell}+a_{1ij}t^{\ell-1}+...+a_{\ell ij}).$$

Daraus ergibt sich die erste Identität. Die letzte Idenität erhält man daraus, indem man x = 0 setzt.
Zum Beweis der verbleibenden Identiät beachte man, die Summanden, die Beiträge zum Koeffizienten r_1 liefern, sind Produkte aus einem Faktor des Grades ℓ - 1 und lauter Faktoren des Grades ℓ. Die Faktoren des Grades ℓ kommen von Einträgen der Hauptdiagonalen (nur dort befinden sich Polynome des Grades ℓ). Der einzige Faktor des Grades ℓ - 1 muß dann aber auch aus der Hauptdiagonalen kommen.
QED.

1.7.7 Komposition von Spuren und von Normen

Seien R und S kommutative Ringe mit Eins und

$$M$$

ein freier S-Modul endlichen Rangs. Weiter sei

$$R \subseteq S$$

und S sei als R-Modul ebenfalls frei und vom endlichem Rang. Für jedes $A \in End_S(M) \subseteq End_R(M)$ gilt dann

$$Tr_{M/R}(A) = Tr_{S/R}(Tr_{M/S}(A))$$
$$N_{M/R}(A) = N_{S/R}(N_{M/S}(A))$$

Außerdem ist

$$\chi_R(A, t) = N_{S/R}(\chi_S(A, t))$$

wobei $\chi_R(A, t)$ und $\chi_S(A, t)$ die charakteristischen Polynome von A bezeichnen sollen, wobei man einmal A als Element von $End_R(M)$ und einmal als Element von $End_S(M)$ auffaßt.

Bemerkung
Die ersten beiden Identitäten besagen, daß folgende Diagramme kommutativ sind.

$$\begin{array}{ccc} End_S(M) & \xrightarrow{Tr_{M/S}} & S \\ \| & & \downarrow Tr_{S/R} \\ End_S(M) & \xrightarrow{Tr_{M/R}} & R \end{array} \qquad \begin{array}{ccc} End_S(M) & \xrightarrow{N_{M/S}} & S \\ \| & & \downarrow N_{S/R} \\ End_S(M) & \xrightarrow{N_{M/R}} & R \end{array}$$

Beweis von 1.7.7. 1. Schritt. Beweis der Formel für die Norm.
Wir führen den Beweis durch Induktion nach der Anzahl der linear unabhängigen Erzeugenden des freien S-Moduls M. Im Fall eines Erzeugendensystems der Länge 1 gilt $M \cong S$, $Tr_{M/S}=N_{M/S}=$ Id und die Behauptung ist trivial. Sei jetzt n>1 und $\omega_1,...,\omega_n$ ein linear unabhängiges Erzeugendensystem von M über S,

$$M = S\bullet\omega_1+...+S\bullet\omega_n \qquad \text{(freies Erzeugendensystem)}.$$

Für vorgegebenes $A \in End_S(M)$ schreiben wir

$$A\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j \text{ mit } a_{ij} \in S.$$

Wir betrachten das Element $B \in End_S(M)$ mit

$$B\omega_1 := \omega_1 - \sum_{j=2}^{n} a_{1j}\omega_j$$
$$B\omega_i := a_{11}\omega_i \quad , \tag{1}$$

d.h.

$$B = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ * & a_{11} & 0 & \dots & 0 \\ * & 0 & a_{11} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ * & 0 & 0 & \dots & a_{11} \end{pmatrix}$$

Bei der Zusammensetzung C := BA werden die Basiselemente von M wie folgt abgebildet.

$$\omega_1 \mapsto \sum_{j=1}^{n} a_{1j}\omega_j \mapsto a_{11}(\omega_1 - \sum_{j=2}^{n} a_{1j}\omega_j) + \sum_{j=2}^{n} a_{1j}\, a_{11}\omega_j = a_{11}\omega_1$$
$$\omega_i \mapsto \sum_{j=1}^{n} a_{ij}\omega_j \mapsto a_{i1}(\omega_1 - \sum_{j=2}^{n} a_{1j}\omega_j) + \sum_{j=2}^{n} a_{ij}\, a_{11}\omega_j = a_{i1}\omega_1 + \sum_{j=2}^{n} c_{ij}\,\omega_j$$

mit $c_{ij} = a_{ij}\, a_{11} - a_{i1}\, a_{1j}$. Mit anderen Worten, es gilt

$$C\omega_1 = a_{11}\omega_1$$
$$C\omega_i = a_{i1}\omega_1 + \sum_{j=1}^{n} c_{ij}\omega_j \quad (\text{für } i>1) \tag{2}$$

d.h.

$$C = \begin{pmatrix} a_{11} & * & * & \dots & * \\ 0 & * & * & \dots & * \\ \dots & \dots & \dots & \dots & \dots \\ 0 & * & * & \dots & * \end{pmatrix}$$

Die Matrix dieser Abbildung hat in der ersten Spalte als einzigen eventuell von Null verschiedenen Eintrag das Element a_{11} in der ersten Position. Deshalb gilt nach dem Entwicklungssatz

$$N_{M/S}(C) = a_{11} N_{M'/S}(C').$$

Dabei sei $M' := S\omega_2 + \dots S\omega_n$ und C' bezeichne die S-lineare Abbildung

$$C': M' \to M',\ \omega_i \mapsto \sum_{j=2}^{n} c_{ij}\,\omega_j \quad (i = 2,\dots,n).$$

Damit gilt

$$N_{S/R}(N_{M/S}(C)) = N_{S/R}(a_{11}) \cdot N_{S/R}(N_{M'/S}(C')).$$

Den Ausdruck ganz rechts können wir jetzt nach Induktionsvoraussetzung berechnen. Es folgt

$$N_{S/R}(N_{M/S}(C)) = N_{S/R}(a_{11}) \cdot N_{M'/R}(C'). \tag{3}$$

Sei jetzt $s_1,...,s_m$ ein R-linearer unabhängiges Erzeugendensystem des R-Moduls S,

$$S = R\bullet s_1 +...+ R\bullet s_m \qquad \text{(freies Erzeugendensystem).}$$

Dann bilden die Produkte $s_i\omega_j$ eine lineare unabhängiges Erzeugendensystem des R-Moduls M und die Matrizen der Abbildungen B und C bezüglich der $s_i\omega_j$ lassen sich aus (1) und (2) gewinnen, indem man diese Identitäten auf alle möglichen Weisen mit einem s_i multipliziert. Die entstehenden Matrizen zerfallen in Blöcke, wobei für jedes Paar (i,j) der zugehörige Block zu den $s_\mu\omega_i$ und $s_\nu\omega_j$ (mit festem i und j und ν, μ = 1,..., m) gehört.

Da in der Matrix von C über R nach (2) in der linken oberen Ecke der Block zur Multiplikation mit a_{11} steht und unter diesem Block lauter Nullen stehen, folgt nach dem Entwicklungssatz

$$N_{M/R}(C) \quad = N_{S/R}(a_{11})\cdot N_{M'/R}(C')$$

also mit (3):

$$N_{M/R}(C) \quad = N_{S/R}(N_{M/S}(C)). \tag{4}$$

Dies ist die gesuchte Formel für die Norm nur mit C = BA anstelle von A. Auf Grund der sehr speziellen Gestalt der Matrizen von B über R bzw. S (vgl. Formel (1)) erhalten wir in analoger Weise die entsprechende Formel für B,

$$\begin{array}{c} N_{M/R}(B) \quad = N_{S/R}(N_{M/S}(B)) \\ \| \\ N_{S/R}(a_{11})^{n-1} \\ \| \\ N_{S/R}(a_{11}^{n-1}) \end{array} \tag{5}$$

Da die Norm multiplikativ ist, ergibt sich daraus die Behauptung zumindest in dem Fall, daß $N_{S/R}(a_{11}^{n-1})$ eine Einheit ist. Im allgemeinen Fall müssen wir einen etwas künstlich wirkenden Trick anwenden.

Sei t ein über S transzendentes Element (eine Unbestimmte). Wir bezeichnen mit A_t, B_t und C_t die Matrizen, welche man aus A, B und C erhält, indem man das Element a_{11} durch $a_{11}+t$ ersetzt. Die obigen Betrachtungen sind dann natürlich auch für A_t, B_t und C_t anstelle von A, B und C gültig (mit S[t] anstelle von S). Die Identität (4) mit

$$C_t = B_tA_t$$

anstelle von C kann man dann in der folgenden Gestalt schreiben.

$$N_{S/R}(a_{11}+t)^{n-1}\, N_{M/R}(A_t) = N_{S/R}(a_{11}+t)^{n-1}\cdot N_{S/R}(N_{M/S}(A_t))$$

(wegen (5)). Dies ist eine Identität von Polynomen aus R[t]. Der höchste Koeffizient des Polynoms $N_{S/R}(a_{11}+t)$ ist Eins (z.B. nach 1.7.5). Deshalb ist dieses Polynom in R[t] kein Nullteiler[35], d.h. es gilt

$$N_{M/R}(A_t) = N_{S/R}(N_{M/S}(A_t))$$

Wir setzen t=0 und erhalten die Behauptung des ersten Schritts.

2. Schritt. Beweis der beiden anderen Formeln.
Nach Lemma 1.7.5 gilt

$$\chi_{M/S}(A,t) = (-1)^n \cdot N_{M/S}(t-A) \text{ mit } n := rk_S(M)$$
$$= N_{M/S}(A-t)$$

und analog

$$\chi_{M/R}(A,t) = (-1)^{nm} \cdot N_{M/R}(t-A) \text{ mit } m := rk_R(S)$$
$$= N_{M/R}(A - t)$$

Aus der eben bewiesenen Formel für die Norm ergibt sich damit

$$\chi_{M/R}(A,t) = N_{M/R}(A-t)$$
$$= N_{S/R}(N_{M/S}(A-t))$$
$$= N_{S/R}(\chi_S(A, t))$$

Die noch verbleibende Formel für die Spur ergibt sich jetzt durch Koeffizientenvergleich: der negative Koeffizient von t^{mn-1} in $\chi_{M/R}(A,t)$ ist gerade

$$Tr_{M/R}(A)$$

(nach Definition der Spurt) und derselbe negative Koeffizient auf der rechten Seite ist

$$Tr_{S/R}(Tr_{M/S}(A))$$

(nach Lemma 1.7.6 angewandt auf das Polynom $\chi_S(A, t)$ und mit $r_1 = Tr_{M/S}(A)$).
QED.

1.7.8 Der Fall einer endlichen Körpererweiterung

Seien K/k eine endliche Körpererweiterung und $\alpha \in K$ ein Element mit dem Minimalpolynom f(x) über k. Dann gilt

(i) deg f(x) | [K:k]

(ii) $\chi(\alpha, x) = f(x)^{\ell}$ mit $\ell := \frac{[K:k]}{\deg f(x)}$.

(iii) $Tr_{K/k}(\alpha) = \ell \cdot (\alpha_1 + ... + \alpha_m)$

(iv) $N_{K/k}(\alpha) = (\alpha_1 \cdot ... \cdot \alpha_m)^{\ell}$

Dabei seien n = [K:k], m= deg f und $\alpha_1, ..., \alpha_m$ die (mit ihren algebraischen Vielfachheiten aufgelisteten) Nullstellen von f in irgendeiner Erweiterung von K.
Beweis. Betrachten wir zunächst den Fall

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

Wegen $\chi(\alpha, \alpha)=0$ gilt $f|\chi$ und wegen [K:k] = deg f muß dann sogar $\chi(\alpha, x) = f(x)$ sein. Damit gilt (ii) (mit $\ell = 1$) und insbesondere (i).

---

[35] Man betrachte den höchsten Koeffizienten des Produkts.

Wir schreiben

$$\chi(\alpha, x) = f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_m),$$

Wir führen die Multiplikationen auf der rechten Seite aus und erhalten

$$\chi(\alpha, x) = x^m - (\alpha_1+\ldots+\alpha_m)\bullet x^{m-1} \pm \ldots + (-1)^m(\alpha_1\cdot\ldots\cdot\alpha_m).$$

Nach Definiton von Spur und Norm gelten damit auch die Aussagen (iii) und (iv) (mit ℓ = 1). Damit sind die Behauptungen im Fall K = k(α) bewiesen.

Im allgemeinen Fall betrachten wie den Körperturm

$$k \subseteq k(\alpha) \subseteq K$$

und wenden 1.7.7 an.
QED.

1.8 Separabilität

1.8.1 Die Zahl der Einbettungen eines Erweiterungskörpers

Seien K/k und L/k endliche Körpererweiterungen. Dann gibt es höchstens [K:k] Einbettungen

$$K \rightarrow L,$$

welche den Körper k elementsweise festlassen.

Beweis. Im Fall K=k(α) ist das trivial, da Nullstellen des Minimalpolynoms von α in Nullstellen des Minimalpolynoms übergehen müssen. Im allgemeinen Fall betrachtet man einen Körperturm

$$k=K_0 \subset K_1 \subset \ldots \subset K_j = K$$

aus einfachen Erweiterungen $K_i = K_{i-1}(\alpha_i)$ und führt den Beweis durch Induktion nach j.
QED.

1.8.2 Definition der Separabilität

Eine endliche Körpererweiterung K/k heißt <u>separabel</u>, wenn es eine endliche Erweiterung L/k gibt mit der Eigenschaft, daß die Zahl der verschiedenen Einbettungen

$$K \rightarrow L,$$

welche k elementeweise festlassen, gleich [K:k] ist.

1.8.3 Separabilität von Teilerweiterungen

Seien K/k und L/K endliche Körpererweiterungen. Dann besteht folgende Implikation.

$$L/k \text{ separabel} \Rightarrow K/k \text{ und } L/K \text{ separabel.}$$

Beweis. Nach 1.8.1 gibt es höchstens [K:k] verschiedene Einbettungen

$$K \rightarrow M$$

in irgendeine endiche Erweiterung M/k. Nach demselben Lemma läßt sich jede von diesen Einbettungen auf höchstens [L:K] verschiedene Weisen fortsetzen zu einer Einbettung

$$L \rightarrow M.$$

Wenn man also insgesamt [L:k] = [L:K]·[K:k] Einbettungen L→M erhält, so muß in jedem Teilschritt bereits die maximal erreichbare Anzahl von Einbettungen möglich sein.
QED.

1.8.4 Separabilität und das Fehlen mehrfacher Nullstellen

Seien K/k eine endliche separable Erweiterung vom Grad n und

$$\sigma_i: K \to M$$

die n verschiedenen k-Einbettungen in einer (hinreichend großen) endlichen Erweiterung M/k. Weiter seien $\alpha \in K$ ein Element und $\alpha_1,...,\alpha_m \in M$ die paarweise verschiedenen Nullstellen des Minimalpolynoms f(x) von α über k in M. Dann gilt

(i) $f(x) = (x-\alpha_1)\cdot...\cdot(x-\alpha_m)$

(ii) $\{\alpha_1,...,\alpha_m\}=\{\sigma_1(\alpha),...,\sigma_n(\alpha)\}$, wobei in der Folge $\sigma_i(\alpha)$ jedes der α_j genau $\frac{n}{m}$ mal angenommen wird.

Beweis. Jede der Nullstellen α_j definiert eine k-Einbettung

$$k(\alpha) \to M.\ \alpha \mapsto \alpha_i\ .$$

Die Zahl dieser Einbettungen ist nach 1.8.3 gleich $m = [k(\alpha):k] = \deg(f)$, d.h. es gilt (i). Jede dieser Einbettungen läßt sich auf $[K:k(\alpha)] = \frac{n}{m}$ verschiedene Weisen fortsetzen zu einem der σ_i. Also kommt jedes der α_j in $\frac{n}{m}$ - facher Weise in der Gestalt $\sigma_i(\alpha)$ vor.
QED.

1.8.5 Die Spurabbildung

Seien K/k eine endliche separable Erweiterung vom Grad n und

$$\sigma_i: K \to M$$

die n verschiedenen k-Einbettungen in eine endliche Erweiterung M/k. Dann gilt

$$Tr_{K/k}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$

für jedes $\alpha \in K$.
Beweis. Dies folgt aus 1.8.4 und 1.7.8.
QED.

1.8.6 Zusammensetzung separabler Erweiterungen

Seien K/k und L/K endliche separable Körpererweiterungen. Dann ist auch L/k separabel.
Beweis. Nach Voraussetzung gibt es paarweise verschiedene k-Einbettungen

$$\sigma_i: K \to U,\ i=1,...,[K:k]$$

und paarweise verschiedene K-Einbettungen

$$\tau_i: L \to V,\ i=1,...,[L:K].$$

Durch geeignetes Vergrößern von U können wir erreichen, daß die σ_i sich zu k-Einbettungen

$$\sigma_i: L \to U$$

fortsetzen lassen. Ohne Beschränkung der Allgemeinheit können wir annehmen $L \subseteq V$ (man identifiziere L mit seinem Bild bei einem der τ_i). Wir setzen die σ_i zu k-Einbettungen

$$\sigma_i: V \to U$$

fort (bei eventueller Vergrößerung von U). Nach Konstruktion sind die Einschränkungen der $\sigma_i\tau_j$ auf L paarweise verschieden:

$$\sigma_i\tau_j = \sigma_{i'}\tau_{j'} \text{ auf } L \quad \Rightarrow \sigma_i = \sigma_{i'} \text{ auf K (da die } \tau \text{ K-Einbettungen sind)}$$
$$\Rightarrow i=i'$$
$$\Rightarrow \tau_j = \tau_{j'} \text{ auf L (da die } \sigma \text{ injektiv sind)}$$
$$\Rightarrow j=j'.$$

Die Anzahl der $\sigma_i\tau_j|_L$ ist gleich $[L:K]\cdot[K:k] = [L:k]$

QED.

1.8.7 Separabilität in der Charakteristik Null

Jede endliche Erweiterung K/k eines Körpers der Charakteristik Null ist separabel.
Beweis. Auf Grund von 1.8.6 genügt es, den Fall einer einfachen Körpererweiterung zu betrachten,

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

Sei

$$f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_m)$$

das Minimalpolynom von α, wobei die α_i einer geeigneten endlichen Erweiterung M von K entnommen seien. Es reicht zu zeigen, daß es m verschiedene k-Einbettungen $K\rightarrow M$ gibt. Dazu wiederum genügt es zu zeigen, die Nullstellen von f sind paarweise verschieden. Hätte f eine mehrfache Nullstelle, so hätte der größte gemeinsame Teiler

$$g = GCD(f, f')$$

von f und der Ableitung von f einen positiven Grad. Mit anderen Worten f hätte einen echten Teiler, im Widerspruch zur Wahl von f.
QED.
Bemerkungen

(i) Wir benutzen beim Beweis den Tatsache, daß in der Charakteristik Null die Ableitung eines von Null verschiedenen Polynoms ungleich Null ist.
(ii) Die obige Argumentation zeigt, ein irreduzibles Polynom f(x) hat genau dann mehrfache Nullstellen, wenn $f'(x)=0$ gilt.
(iii) Wir zeigen jetzt, daß jede endliche separable Erweitungen einfach ist. Die umgekehrte Aussage gilt natürlich nicht.

1.8.8 Separabilität und mehrfache Nullstellen

Eine eine einfache algebraischen Erweiterung $K=k(\alpha)$ ist genau dann separabel, wenn das Minimalpolynom $f\in k(x)$ von α keine mehrfachen Nullstellen besitzt (d.h. wenn f separabel ist bzw. wenn α über k separabel ist).
Beweis. Besitze f keine mehrfache Nullstellen. Jede Nullstelle von f liefert dann eine andere Einbettung von K in eine hinreichend große Erweiterung von k, d.h. die Erweiterung K/k ist separabel. Die umgekehrte Implikation ergibt sich aus 1.8.4.
QED.

1.8.9 Satz vom primitiven Element

Jede endliche separable Erweiterung K/k ist einfach.
Beweisskitze. 1. Fall: k ist endlich.
Dann ist auch K endlich, d.h. die Einheitengruppe K* ist zyklisch. Sei ξ ein erzeugendes Element dieser Einheitengruppe. Dann enthält $k(\zeta)$ alle von Null verschiedenen Elemente von K, d.h. es ist $K=k(\zeta)$.

2. Fall: k ist unendlich und K=k(α,β).
Seien

$$\sigma_i: K \to M,\ i=1,...,n := [K,k]$$

die paarweise verschiedenen k-Einbettungen von K in eine geeignete endliche Körpererweiterung M von k. Dann gilt für je zwei i,j∈{1,...,n} jeweils eine der beiden Ungleichungen

$$\sigma_i(\alpha) \neq \sigma_j(\alpha) \text{ oder } \sigma_i(\beta) \neq \sigma_j(\beta).$$

Weil k unendlich ist, gibt es Elemente a,b∈k mit[36]

$$a\cdot(\sigma_i(\alpha) - \sigma_j(\alpha)) + b\cdot(\sigma_i(\beta) - \sigma_j(\beta)) \neq 0$$

für beliebige i,j∈{1,...,n} mit i≠j. Wir setzen $\gamma := a\cdot\alpha + b\cdot\beta$. Dann gilt

$$\sigma_i(\gamma) - \sigma_j(\gamma) \neq 0.$$

Insbesondere sind die k-Einbettungen $\sigma_i|_{k(\gamma)}: k(\gamma) \to M$ paarweise verschieden. Nach 1.b.1 gilt deshalb

$$[k(\gamma):k] \geq n = [K:k].$$

Wegen k(γ)⊆K muß dann aber K=k(γ) gelten, d.h. K/k ist einfach.
3. Fall: k ist unendlich und K/k beliebig.

$$\text{Es gilt } K=k(\alpha_1,...,\alpha_n).$$

Nach dem zweiten Fall kann man n solange verkleinern bis n=1 gilt.
QED.

1.8.10 Separabilität und das Nichtentarten der Killingform

Sei K/k eine endliche separable Erweiterung. Dann ist die Abbildung

$$Tr: K\times K \to k,\ (a,b) \mapsto Tr(a,b) := Tr_{K/k}(ab).$$

eine nicht-entartete symmetrische Bilinearform über k.
Beweis. Lediglich die Aussage, daß die Form nicht-entartet ist, bedarf eines Beweises. Wir wählen ein primitiven Element γ∈K, d.h. ein Element mit

$$K = k(\gamma).$$

Wir betrachten die Vektorraumbasis

$$\omega_1=1,\ \omega_2 = \gamma,\ ...,\ \omega_n = \gamma^{n-1}\ ,\ n := [K:k]$$

von K über k und die Determinante

$$D := \det(Tr(\omega_i\omega_j)).$$

Wir haben zu zeigen D ≠ 0. Dazu wählen wir n paarweise verschiedene Einbettungen

$$\sigma_\ell: K \to M,\ \ell=1,...,n,$$

in einen geeigneten Oberkörper M von K und betrachten wir die (Vandermondesche) Determinante

$$\Delta := \det(\sigma_\ell\omega_i) = \det(\sigma_\ell\gamma^{i-1}) = \prod_{i<j}(\sigma_j\gamma - \sigma_i\gamma)\ (\neq 0).$$

Es gilt

---

[36] Man setze a = 1 und betrachte b als Unbestimmte. Man erhält so endlich viele lienare Polynome in b, von denen keines das Nullpolynom ist. Nun wähle man für b ein Element, welches von den endlich vielen Nullstellen dieser endlich vielen Polynome verschieden ist.

$$
\begin{aligned}
0 \neq \Delta^2 &= \det(\sigma_\ell \omega_i)\cdot\det(\sigma_\ell \omega_j)^T \\
&= \det\Big(\sum_{\ell=1}^{n} \sigma_\ell \omega_i \sigma_\ell \omega_j\Big) \\
&= \det\Big(\sum_{\ell=1}^{n} \sigma_\ell (\omega_i \omega_j)\Big) \\
&= \det(\mathrm{Tr}(\omega_i \omega_j)) \qquad \text{(vgl. 1.8.5)} \\
&= D.
\end{aligned}
$$

QED.

1.8.11 Erhaltung der Separabilität bei Basiswechsel

Seien K/k eine beliebige und k(α)/k eine endliche separable Körpererweiterung. Dann ist K(α)/K separabel.

Beweis. Nach Voraussetzung hat das Minimalpolynom f von α über k keine mehrfachen Nullstellen. Das Minimalpolynom F von α über K ist aber ein Teiler von f.
QED.

1.8.12 Separabilität von Erweiterungen und von Elementen

Sei K/k eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent.

(i) K/k ist separabel.

(ii) Jedes Element $\alpha \in K$ ist separabel über k (d.h. das Minimalpolynom von α über k hat keine mehrfachen Nullstellen).

Beweis. (i) ⇒ (ii). Nach 1.8.3 ist k(α)/k für jedes $\alpha \in K$ separabel, also ist α nach 1.8.8 separabel über k.

(ii) ⇒ (i). Wir zerlegen die Erweiterung K/k in eine endliche Folge einfacher Erweiterungen

$$k = K_0 \subset K_1 \subset \ldots \subseteq K_t = K.$$

Nach 1.8.6 reicht es zu zeigen, jede der Erweiterungen K_i/K_{i-1} ist separabel. Jedes $\alpha \in K_i$ ist nach Voraussetzung separabel über k, also erst recht über K_{i-1}. Da die Erweiterung

$$K_i/K_{i-1}$$

einfach ist, ist sie damit nach 1.8.8 separabel.
QED.

1.8.13 Das Entarten der Killingform im inseparablen Fall

Sei K/k eine endliche inseparable Körpererweitung. Dann gilt

$$\mathrm{Tr}_{K/k}(\alpha) = 0$$

für jedes $\alpha \in K$.

Beweis. 1. Fall: K=k(α) mit α{k, $\alpha^p \in k$, p:= char(k)>0.
Wir betrachten die folgende Vektorraumbasis von K über k.

$$\omega_1 = 1, \omega_2 = \alpha, \omega_3 = \alpha^2, \ldots, \omega_p = \alpha^{p-1}$$

Für $\beta = b_1 + b_2\alpha + \ldots + b_p\alpha^{p-1}$ mit $b_i \in k$ schreiben wir

$$\beta\cdot\omega_i = \sum_{j=1}^{p} b_{ij}\omega_j \text{ mit } b_{ij}\in k.$$

Mit $b:= \alpha^p \in k$ erhalten wir

$$\begin{aligned}\beta = \beta\cdot\omega_1 &= b_1 + b_2\alpha + ... + b_p\alpha^{p-1}\\ \beta\cdot\omega_2 &= b\cdot b_p + b_1\alpha + ... + b_{p-1}\alpha^{p-1}\\ &\dots\end{aligned}$$

Koeffizientenvergleich für i=1,...,p liefert

$$b_{ii} = b_1,$$

d.h. es gilt $Tr_{K/k}(\beta) = p\cdot b_1 = 0$.

2.Fall: K/k beliebig.
Bezeichne p die Charakteristik von k. Nach 1.8.7 gilt p>0. Nach 1.8.12 gibt es ein Element $\beta\in K$, welches nicht separabel über k ist. Sei

$$f(x) = a_0 + a_1x + a_2x^2 + ... + a_{n-1}x^{n-1} + x^n \in k[x]$$

das Minimalpolynom von β über k. Dann gilt nach Bemerkung (ii) von 1.8.7

$$0 = f'(x) = a_1 + 2a_2x + ... + (n-1)a_{n-1}x^{n-2} + nx^{n-1},$$

d.h. $i\cdot a_i = 0$ für alle i, d.h. $p \nmid i$ oder $a_i=0$. Mit anderen Worten, man kann f in der Gestalt

$$f(x) = g(x^{p^s}) \text{ mit } g\in k[x] \text{ und } s\geq 1$$

schreiben. Indem man s so groß wie mögliche wählt, erreicht man, daß das Polynom g eine von Null verschiedene Ableitung besitzt. Die Erweiterung $k\subset k(\beta)$ zerfällt damit in eine Folge

$$k \subseteq k' := k(\beta^{p^s}) \subseteq k(\beta)$$

von Erweiterungen. Das Minimalpolynom h von β^{p^s} über k ist ein Teiler von g. Wegen

$$[k(\beta):k] = \deg f = \deg g\cdot p^s \geq \deg h\cdot p^s \geq [k':k]\cdot[k(\beta):k']$$ [37]

muß sogar h=g gelten. Die Erweiterung k'/k ist linkd somit separabel. Also ist die Erweiterung rechts echt (und inseparabel). Insbesondere gilt

$$\beta^{p^0} = \beta \notin k'.$$

Sei t die kleinste natürliche Zahl mit $(\beta^{p^t})^p = \beta^{p^{t+1}} \in k'$. Wir setzen $\alpha := \beta^{p^t}$. Dann ist die Erweiterung $k''=k'(\alpha)$ von k' von der im 1.Fall betrachteten Gestalt, d.h. es gilt $Tr_{k''/k'} = 0$. Aus dem Körperturm

$$k\subseteq k'\subset k''\subset K$$

und den Formeln von 1.7.7 ergibt sich $Tr_{K/k} = 0$.

QED.
Bemerkung

---

[37] Es gilt $p^s \geq [k(\beta):k']$ weil β Nullstelle des Polynoms $x^{p^s} - \beta^{p^s} \in k'[x]$ ist.

Wir kehren jetzt zu dem Problem zurück, welches uns eigentlich interessierte: wir wollen zeigen, daß die ganze Abschließung von $\mathbb{Z}$ in einer endlichen Erweiterungen von $\mathbb{Q}$ ein Dedekind-Ring ist.

1.9 Ganze Abschließungen in endlichen Körpererweiterungen

1.9.1 Die Situation

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

R	Dedekind-Ring mit K:=Q(R)
L/K	endliche separable Körper-Erweiterung
S	ganze Abschließung von R in L

Dabei denken wir uns den K-Vektorraum L mit der nicht-entarteten symmetrischen Bilinearform

$$B: L \times L \longrightarrow K, (x, y) \mapsto Tr_{L/K}(xy),$$

versehen, d.h. L wird als euklidischer K-Vektorraum im Sinne von 1.6.8 angesehen (vgl. 1.8.10).

Bemerkungen

(i) Wir wollen in diesem Abschnitt zeigen, daß in dieser Situation S ein Dedekind-Ring mit dem Quotientenkörper L ist.

(ii) Die Forderung der Separabilität ist dafür eigentlich nicht notwendig (siehe Zaristki und Samuel [1], Kapitel V, Theorem 19 oder Serre [1], Kapitel II, Proposition 3). Da in der uns interessierenden Situation keine inseparablen Erweiterungen L/K auftreten und der Beweis in der allgemeinen Situation etwas technisch ist, beschränken wir uns hier auf den angegebenen Spezialfall.

(iii) Wir beginnen mit einer vorbereitenden Aussage, nach welcher die beschriebene Situation mit Lokalisierungen verträglich ist.

1.9.2 Verträglichkeit mit Lokalisierungen

In der Situation von 1.9.1 ist für jedes Primideal p von R der R_p-Teilmodul

$$S \bullet R_p$$

von L gerade die ganze Abschließung von R_p in L.

Beweis. Jedes Element von $S \bullet R_p$ hat die Gestalt

$$s_1 \bullet r_1 + ... + s_n \bullet r_n \text{ mit } s_i \in S \text{ und } r_i \in R_p.$$

Insbesondere sind die s_i ganz über R also auch über R_p, d.h. sie liegen in der ganzen Abschließung

$$\overline{R}_p$$

von R_p in L. Da $\overline{R}_p$ ein Ring ist (vgl. 1.3.4), folgt

$$S \bullet R_p \subseteq \overline{R}_p .$$

Sei jetzt umgekehrt ein Element $x \in \overline{R}_p$, d.h. x liege in L und sei ganz über R_p, d.h. es besteht eine Ganzheitsgleichung

$$x^n + r_1 \bullet x^{n-1} + ... + r_n = 0 \text{ mit } r_i = \frac{a_i}{b_i} \in R_p, \ a_i \in R, \ b_i \in R - p.$$

Wir können annehmen

$$b_1 = ... = b_n =: b.$$

Wir multiplizieren die Ganzheitsgleichung mit b^n und sehen so, daß $bx \in L$ ganz ist über R, d.h. es gilt

$$bx \in S,$$

also

$$x \in S \bullet \frac{1}{b} \subseteq S \bullet R_p.$$

QED.

1.9.3 Die ganze Abschließung von Dedekind-Ringen in endlichen separablen Erweiterungen

Seien R ein Dedekind-Ring mit dem Quotientenkörper K = Q(R), L/K eine endliche separable Körpererweiterung und S die ganze Abschließung von R in L.

$$\begin{array}{ccc} K & \subseteq & L \\ \cup & & \cup \\ R & \subseteq & S \end{array}$$

Dann gilt:

(i) S ist als R-Modul endlich erzeugt.

(ii) Der von S über K erzeugte Vektorraum ist gleich L,

$$L = S \bullet K.$$

(iii) S ist ein Dedekind-Ring.

(iv) Jedes maximale Ideal q von S liegt über einem maximalen Ideal $q \cap R$ von R.

(v) Jedes maximale Ideal p von R liegt in einem maximalen Ideal q von S.

Beweis. Zu (ii). Trivialerweise gilt

$$S \bullet K \subseteq L.$$

Beweisen wir die umgekehrte Inklusion. Jedes Element $\alpha \in L$ ist nach Voraussetzung algebraisch über K, d.h. es besteht eine Identität

$$\alpha^n + c_1\alpha^{n-1} + ... + c_n = 0 \text{ mit } c_i = \frac{a_i}{b_i} \in K,\ a_i \in R\ ,\ b_i \in R - \{0\}.$$

Wir können dabei annehmen, $b_1 = b_2 = ... = b_n =: b$. Wir multiplizieren diese Identität mit b^n und erhalten auf diese Weise eine Ganzheitsgleichung für $b\alpha$ über R. Insbesondere gilt

$$b\alpha \in S,$$

also

$$\alpha \in S \bullet \frac{1}{b} \subseteq S \bullet K.$$

Zu (i). Wegen S•K = L gibt es eine Basis von L über K aus Elementen, die ganz in S liegen, d.h. S enthält ein freies R-Gitter

$$M \subseteq S.$$

Wir gehen zum dualen R-Moduln (vgl. 1.6.9) über und erhalten

$$D(S) := \{x \in L \mid B(x, S) \subseteq R\} \subseteq D(M)$$

Es reicht zu zeigen,

$$S \subseteq D(S), \qquad (1)$$

denn dann liegt S im Gitter D(M) und ist damit als Teilmodul eines endlich erzeugten R-Moduls selbst endlich erzeugt über R.

Zum Beweis von (1) müssen wir zeigen, für jedes Element $\alpha \in S$ gilt

$$B(\alpha, S) \subseteq R,$$

d.h. für je zwei Elemente $\alpha, \beta \in S$ gilt

$$Tr_{L/K}(\alpha \bullet \beta) = B(\alpha, \beta) \in R.$$

Mit $\alpha, \beta \in S$ gilt auch $\alpha \bullet \beta \in S$. Es reicht also zu zeigen,

$$Tr_{L/K}(\alpha) \in R \text{ für jedes } \alpha \in S.$$

Wegen $Tr_{L/K}(\alpha) \in K$ reicht es zu zeigen,

$$Tr_{L/K}(\alpha) \text{ ist ganz über R für jedes } \alpha \in S.$$

Nun ist $Tr_{L/K}(\alpha)$ nach 1.7.8 (iii) gerade eine Summe von Konjugierten von α. Diese Summe ist zu bilden in irgendeiner endlichen Erweiterung von K, zum Beispiel im Zerfällungskörper E des Minimalpolynoms von α über K, sagen wir

$$E := \text{Zerfällungskörper des Minimalpolynoms von } \alpha \text{ über K.}$$

Da die Summe ganzer Elemente ganz ist, reicht es zu zeigen, die Konjugierten von $\alpha \in S$ sind ganz über K. Sei

$$\alpha_i \in E$$

ein über K zu α konjugiertes Element. Weil E/K ein Galois-Erweiterung ist, gibt es einen K-Automorphismus

$$\sigma: E \longrightarrow E \text{ mit } \sigma(\alpha) = \alpha_i.$$

Wir wenden σ auf eine Ganzheitsgleichung von $\alpha \in S$ über R an, sagen wir auf

$$\alpha^n + r_1\alpha^{n-1} + \ldots + r_n = 0 \text{ mit } r_i \in R.$$

Weil σ die Elemente von $R \subseteq K$ invariant läßt, erhalten wir

$$\alpha_i^n + r_1\alpha_i^{n-1} + \ldots + r_n = 0.$$

Dies ist eine Ganzheitsgleichung für α_i über R. Insbesondere ist α_i ganz über R.

Zu (iii). Als endlich erzeugter R-Modul über dem noetherschen Ring R ist S selbst noethersch. Nach Konstruktion ist S ganz abgeschlossen in L und nach (ii) ist L der Quotientenkörper von S:

$$L = S \bullet K \subseteq Q(S) \subseteq Q(L) = L.$$

Mit anderen Worten S ist normal. Es reicht also zu zeigen (vgl. 1.5.1):

$$\text{Jedes von Null verschiedene Primideal q von S ist maximal.} \qquad (2)$$

Nach Voraussetzung gibt es ein Element $\alpha \in q - \{0\}$. Wir betrachten eine Ganzheitgleichung von α über R, sagen wir

$$\alpha^n + r_1\alpha^{n-1} + \ldots + r_n = 0 \text{ mit } r_i \in R.$$

Weil $S \subseteq L$ ein Integritätsbereich ist, können wir annehmen,

$$r_n \neq 0$$

(andernfalls ließe sich eine Potenz von α wegkürzen). Wegen $\alpha \in q$ gilt

$$r_n \in p := q \bigcap R.$$

Insbesondere ist p ein von Null verschiedenes Primideal, also maximal (weil R ein Dedekind-Ring ist).

Bemerkung: wir haben damit Aussage (iv) der Behauptung bewiesen.

Nach Wahl von p gilt $q \supseteq pS$. Also wird der R-Modul

$$S/q$$

von p annulliert und ist somit ein Modul über R/p, d.h. ein Vektorraum über R/p. Weil S als R-Modul endlich erzeugt ist, gilt dasselbe für S/q über R/p, d.h.

$$\dim_{R/p} S/q < \infty.$$

Weil q ein Primideal ist, ist S/q außer dem eine nullteilerfreie R/p-Algebra, also ein Körper. Wir haben gezeigt, q ist ein maximales Ideal.
Zu (iv). siehe den obigen Beweis von (iii).
Zu (v). Sei p ein von Null verschiedenes Primideal von R. Angenommen die Behauptung ist falsch. Dann gilt

$$pS = S,$$

also

$$p^{-1}S = p^{-1}(pS) = (p^{-1}p)S = R \bullet S = S,$$

also

$$p^{-1} \subseteq S \bigcap K =^{38} R,$$

also

$$p \supseteq R^{-1} = R,$$

was im Widerspruch dazu steht, daß p ein Primideal sein soll.
QED.
Bemerkung
Aus dem Beweis von (i) ergibt sich insbesondere,

$$Tr_{L/K}(S) \subseteq R.$$

1.9.4 Folgerung: die gebrochenen Ideale von R und S

Seien R ein Dedekind-Ring mit dem Quotientenkörper K = Q(R), L/K eine endliche separable Körpererweiterung und S die ganze Abschließung von R in L.

$$\begin{array}{ccc} K & \subseteq & L \\ \bigcup & & \bigcup \\ R & \subseteq & S \end{array}$$

Dann ist die Abbildung

$$F(R) \longrightarrow F(S),\ I \mapsto IS,$$

ein injektiver Gruppen-Homomorphismus.
Beweis. Die Abbildung ist offensichtlich ein Gruppen-Homomorphismus:

$$I' \bullet I'' S = I'S \bullet I''S.$$

Sei $I \in F(R)$ im Kern dieses Homomorphismus, d.h.

$$IS = S.$$

Wir haben zu zeigen I = R. Wir schreiben I in der Gestalt

$$I = I' \bullet I''^{-1}$$

mit ganzen Idealen I', $I'' \subseteq R$. Wir können dabei annehmen, daß es keine maximales Ideal gibt, welches in der Faktorzerlegung beider Ideale wirklich vorkommt.[39]

---

[38] Alle über R ganzen Elemente von K liegen in R.

Mit anderen Worten, es gibt kein maximales Ideal p von R mit

$$I' \subseteq p \text{ und } I'' \subseteq p.$$

Dann gilt aber#

$$I' + I'' = R,$$

also

$$I'S + I''S = S.$$

Es gibt deshalb kein maximales Ideal von S, welches in den Faktorzerlegungen der beider ganzer Ideale I'S und I"S von S wirklich vorkommt. Nun ist aber

$S = IS = I'S \bullet I''^{-1}S$,

d.h. multiplikation mit I" ergibt

$$I''S = I'S \bullet (I'' \bullet I''^{-1})S = I'S \bullet (RS) = I'R.$$

Mit andern Worten, die beiden ganzen Ideale I'S und I" sind gleich, besitzen aber keinen gemeinsamen Primfaktor. Das ist nur möglich im Fall

$$I'S = I''S = S.$$

Dann können aber I' und I" keine echten Ideale von R sind (wegen 1.9.3(v)). Also gilt

$$I' = I'' = R.$$

Dann ist aber auch

$$I = I' \bullet I''^{-1} = R.$$

QED.

1.9.5 Bemerkung zum weiteren Verlauf der Vorlesung

Damit ist die grundlegende Aussage, daß für die ganzen Abschließungen S von $\mathbb{Z}$ in den endlichen Erweiterungen K von $\mathbb{Q}$ der Satz von der Primfaktorzerlegung gilt.

$$\begin{array}{ccc} \mathbb{Q} & \subseteq & K \\ \cup & & \cup \\ \mathbb{Z} & \subseteq & S \end{array} \qquad [K:\mathbb{Q}] < \infty$$

Wir setzen

$$\mathcal{O}_K := S = \text{ganze Abschließung von } \mathbb{Z} \text{ in } K$$

und nennen $\mathcal{O}_K$ den Ring der ganzen Zahlen von K.

Wir wissen, über jedem maximalen Ideal $p\mathbb{Z}$ liegt mindestesns ein maxmales Ideal q von $\mathcal{O}_K$ und dieses kommt damit in der Primfaktorzerlegung von $p\mathcal{O}_K$ vor.

Das bedeudet aber, es gibt höchstens endlich viele solche maximalen Ideale, sagen wir

$$q_1, \ldots, q_r \subseteq \mathcal{O}_K \text{ maximal mit } p\mathbb{Z} \subseteq q_i,$$

und es ist

$$p\,\mathcal{O}_K = q_1^{e_1} \bullet \ldots \bullet q_r^{e_r} \text{ mit } e_i \geq 1,$$

Die nächste naheliegende Frage wäre nun, herauszufinden wie groß die Anzahl r dieser Ideale q_i ist und mit welchen Exponenten diese vorkommen können (und wie die Zahlen r und e_i zu berechnen sind).

Um dieser Frage nachgehen zu können, brauchen wir Aussagen über die Fortsetzbarkeit diskreter Bewertunen. Diese Aussagen lassen sich am besten mit Hilfe der zugehörigen multiplikativen Bewertungen beweisen (durch topologische Argumente). Wir wenden

---

[39] Wir betrachten die Faktorzerlegung von I und sammeln in I' die Primidealpotenzen mit positiven und in I" die Primidealpotenzen mit negativen Exponenten.

uns deshalb zunächst einer allgemeinen Untersuchung von multiplikativen Bewertungen zu.

2. Multiplikative Bewertungen

2.1 Definition und Beispiele

Wir beschränken uns hier auf den Fall sogenannter Bewertungen des Ranges 1. Der Begriff (multiplikative) Bewertung soll also stets (multiplikative) "Bewertung des Ranges 1" bedeuten.

2.1.1 Definition

Sei k ein Körper. Eine multiplikative Bewertung von k ist eine Abbildung

$$|?|: k \longrightarrow \mathbb{R}, \alpha \mapsto |\alpha|,$$

mit folgenden Eigenschaften.

1. $|\alpha| \geq 0$ und $|\alpha| = 0 \Leftrightarrow \alpha = 0$ für $\alpha \in k$.
2. $|\alpha\beta| = |\alpha| \cdot |\beta|$ für $\alpha, \beta \in k$.
3. Es gibt eine reelle Zahl C mit $|\alpha+1| \leq C$ für jedes $\alpha \in k$ mit $|\alpha| \leq 1$.

Bemerkungen

(i) Anstelle der dritten Bedingung würde man normalerweise die aus der Analysis gewohnte Dreieckungleichung erwarten. Wir werden bald sehen, daß diese Bedingung im wesentlichen äquivalent zur Dreiecksungleichung ist. Die hat den Vorteil, etwas besser an die im vorigen Abschnitt auftretenden Beispiele der Gestalt

$$|?| = \rho^{v(?)}$$

angepasst zu sein.

(ii) Die multiplikative Bewertung mit

$$|\alpha| = 1 \text{ für alle } \alpha \in k$$

heißt triviale Bewertung von k. Die trivialen Bewertungen werden wir oft aus unseren Betrachtungen ausschließen.

2.1.2 Erste Eigenschaften

Seien k ein Körper und $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung. Dann gilt:

(i) $|1| = 1$

(ii) $|\alpha| = 1$ für jedes $\alpha \in k$ mit $\alpha^n = 1$ für ein $n \in \mathbb{N}$.

(iii) $|-\alpha| = |\alpha|$ für jedes $\alpha \in k$.

(iv) Für jede reelle Zahl $c > 0$ ist auch

$$|?|^c: k \longrightarrow \mathbb{R}, \alpha \mapsto |\alpha|^c,$$

eine multiplikative Bewertung von k.

Beweis. Zu (i). Nach Axiom 2 gilt

$$|1| \cdot |1| = |1|$$

und nach Axiom 1 ist $|1| \neq 0$. Division durch die reelle Zahl $|1|$ liefert die Behauptung.
Zu (ii). Nach Axiom 2 gilt

$$|\alpha|^n = 1.$$

Die einzige nicht-negative reelle Zahl, die dieser Bedingung genügt, ist $|\alpha| = 1$.
Zu (iii). Nach Axiom 2 gilt

$$|-\alpha| = |-1| \cdot |\alpha|,$$

und wegen $(-1)^2 = 1$ und Aussage (ii) gilt $|-1| = 1$.

Zu (iv). Die Axiome 1 und 2 sind offensichtlich auch für $|?|^c$ erfüllt. Betrachten wir Axiom 3. Sei $|\alpha|^c \leq 1$. Dann gilt auch $|\alpha| \leq 1$[40], also nach Axiom 3 $| \alpha + 1 | \leq C$, wobei C eine positive reelle Zahl ist, welche nicht von der speziellen Wahl von α abhängt. Dann ist aber

$$| \alpha + 1 |^c \leq C^c$$

für jedes $\alpha \in k$ mit $|\alpha| \leq 1$.
QED.

2.1.3 Äquivalenz von Bewertungen

Zwei multiplikative Bewertungen $|?|_1, |?|_2: k \longrightarrow \mathbb{R}$ eines Körpers k heißen äquivalent, wenn es eine reelle Zahl $c > 0$ gibt mit

$$| \alpha |_2 = | \alpha |_1^c$$

für jedes $\alpha \in k$.

2.1.4 Äquivalenz und Dreiecksungleichung

Sei k ein Köper. Dann gelten folgende Aussagen.

(i) Jede Bewertung von k ist äquivalent zu einer Bewertung, für welche die reelle Zahl C in Axiom 3 gleich 2 ist.

(ii) Für jede multiplikative Bewertung $|?|: k \longrightarrow \mathbb{R}$ mit C = 2 in Axiom 3 gilt die Dreiecksungleichung:

$$| \alpha + \beta | \leq |\alpha| + |\beta| \text{ für beliebige } \alpha, \beta \in k.$$

(iii) Für jede multiplikative Bewertung $|?|: k \longrightarrow \mathbb{R}$ mit C = 2 in Axiom 3 gilt

$$| |\alpha| - |\beta| | \leq | \alpha - \beta | \text{ für beliebige } \alpha, \beta \in k.$$

Beweis. Zu (i). Seien $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung und C wie in Axiom 3 von 2.1.1, d.h. es gelte

$$| 1 + \alpha | \leq C \text{ für jedes } \alpha \in k \text{ mit } |\alpha| \leq 1.$$

Für jede positive reelle Zahl c gilt dann

$$| 1 + \alpha |^c \leq C^c \text{ für jedes } \alpha \in k \text{ mit } |\alpha| \leq 1.$$

Für $c \longrightarrow 0$ gilt $C^c \longrightarrow 1$, d.h. für hinreichend kleines c ist $C^c < 2$. Dann gilt also

$$| 1 + \alpha |^c \leq 2 \text{ für jedes } \alpha \in k \text{ mit } |\alpha| \leq 1.$$

Zu (ii). 1. Schritt. $| \alpha + \beta | \leq 2 \bullet \max \{ |\alpha| , |\beta| \}$
Zum Beweis können wir annehmen,

$$|\alpha| \geq |\beta| > 0.$$

Wir setzen $\gamma := \beta/\alpha$. Dann gilt $|\gamma| = |\beta| / |\alpha| \leq 1$, also

$$\left| \frac{\beta}{\alpha} + 1 \right| = | \gamma + 1 | \leq C = 2.$$

Wir multiplizieren mit $|\alpha|$ und erhalten

---

[40] Wegen $c > 0$ läßt sich c durch Quotienten natürlicher Zahlen approximieren. Die Aussage folgt aus der Tatsache, daß das Erheben in eine Potenz (mit einer natürlichen Zahl als Exponenten) eine monotone Operation ist.

$$|\alpha + \beta| \le 2 \cdot |\alpha| = 2 \cdot \max\{|\alpha|, |\beta|\}.$$

2. Schritt. $|\sum_{j=1}^{2^r} \alpha_j| \le 2^r \cdot \max\{\alpha_1, \dots, \alpha_{2^r}\}$

Der Fall r = 1 ist gerade die Aussage des ersten Schritts. Der allgemeine Fall ergibt sich durch Induktion nach r :

$$\sum_{j=1}^{2^r} \alpha_j = \left(\sum_{j=1}^{2^{r-1}} \alpha_j\right) + \left(\sum_{j=2^{r-1}+1}^{2^r} \alpha_j\right)$$

$$= \left(\sum_{j=1}^{2^{r-1}} \alpha_j\right) + \left(\sum_{j=1}^{2^{r-1}} \alpha_{j+2^{r-1}}\right)$$

3. Schritt. $|\sum_{j=1}^{n} \alpha_j| \le 2n \cdot \max\{\alpha_1, \dots, \alpha_n\}$ für jede natürliche Zahl n.

Sei r die eindeutig bestimmte natürliche Zahl mit

$$2^{r-1} < n \le 2^r.$$

Wir fügen zu den $\alpha_1, \dots, \alpha_n$ noch $2^r - n$ Summanden hinzu, die alle gleich Null sind. Dann gilt auf Grund der Ungleichung des zweiten Schritts

$$|\sum_{j=1}^{n} \alpha_j| \le 2^r \cdot \max\{\alpha_1, \dots, \alpha_n\}$$

Wegen $2^{r-1} < n \le 2^r$ ist außerdem $2^r < 2n$, d.h. es gilt die Behauptung des 3. Schritts.

4. Schritt. Beweis der Aussage von (ii).
Wir setzen in der Ungleichung des dritten Schritts alle Summanden gleich 1 und erhalten

$$|n| \le 2n \cdot |1| \text{ für jedes } n \in \mathbb{N}.$$

Damit ist

$$\begin{aligned} |\alpha + \beta|^n &= |\sum_{j=0}^{n} \binom{n}{j} \alpha^j \beta^{n-j}| \\ &\le 2(n+1) \cdot \max\{|\binom{n}{j} \alpha^j \beta^{n-j}| : j = 0, \dots, n\} \text{ nach dem 3. Schritt.} \\ &= 2(n+1) \cdot \max\{\binom{n}{j} |\alpha|^j |\beta|^{n-j} : j = 0, \dots, n\} \\ &\le 2(n+1) \cdot \sum_{j=0}^{n} \binom{n}{j} |\alpha|^j |\beta|^{n-j} \qquad \text{(alle Summanden sind } \ge 0) \\ &= 4(n+1) \cdot (|\alpha| + |\beta|)^n \end{aligned}$$

Wir ziehen die n-te Wurzel und erhalten

$$\begin{aligned} |\alpha + \beta| &\le \sqrt[n]{4(n+1)} \cdot (|\alpha| + |\beta|) \\ &= \sqrt[n]{4}\, \sqrt[n]{n} \cdot \sqrt[n]{(n+1)/n} \cdot (|\alpha| + |\beta|) \end{aligned}$$

Für $n \longrightarrow \infty$ erhalten wir die Behauptung von (ii).

Zu (iii). Nach (ii) gilt

$$|\alpha| = |\alpha - \beta + \beta| \le |\alpha - \beta| + |\beta|$$

also

$$|\alpha| - |\beta| \leq |\alpha - \beta|.$$

Dasselbe Argument mit α und β vertauscht liefert

$$|\beta| - |\alpha| \leq |\beta - \alpha| = |\alpha - \beta|.$$

Zusammen erhalten wir die Behauptung von (iii).
QED.

2.1.5 Diskrete Bewertungen

Eine multiplikative Bewertung $|?|: k \longrightarrow \mathbb{R}$ des Körpers k heißt diskret, wenn es eine reelle Zahl

$$\delta > 0$$

gibt mit der Eigenschaft, daß für jedes $\alpha \in k$ mit

$$1 - \delta < |\alpha| < 1 + \delta$$

gilt $|\alpha| = 1$.

Bemerkungen

(i) Mit anderen Worten, die Bewertung ist genau dann diskret, wenn die Menge

$$\{|c| : c \in k\}$$

ihrer Werte eine diskrete Untergruppe der multiplikativen Gruppe der von Null verschiedenen reellen Zahlen ist.

(ii) Ist $|?|: k \longrightarrow \mathbb{R}$ eine diskrete nicht-triviale Bewertung, so besteht die Menge der von Null verschiedenen Werte von $|?|$ aus den ganzzahligen Potenzen einer eindeutig bestimmten reellen Zahl $c < 1$,

$$\{|x| : x \in k^*\} = \{c^n \mid n \in \mathbb{Z}\}$$

(iii) In der Situation von (ii) schreibt man

$$ord(\alpha) = m$$

für ein Element $\alpha \in k - \{0\}$, falls $|\alpha| = c^m$ gilt und nennt m die Ordnung von α bezüglich der gegebenen diskreten Bewertung $|?|$. Außerdem setzt man

$$ord(0) = \infty.$$

Nach Definition gilt

1. $ord(\alpha) \in \mathbb{Z}$ und $ord(\alpha) = \infty \Leftrightarrow \alpha = 0$.
2. $ord(\alpha\beta) = ord(\alpha) + ord(\beta)$ für $\alpha, \beta \in k^*$.

Beweis. Zu (i). Es gilt die folgende allgemeinere Aussage.

Lemma

Seien G eine topologische Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind folgende Ausagen äquivalent.

(i) H ist eine diskrete Untergruppe, d.h. für jedes $x \in H$ gibt es eine offene Umgebung U mit

$$H \bigcap U = \{x\}.$$

(ii) Es gibt eine offene Umgebung U von $e \in H$ mit $H \bigcap U = \{e\}$.

Beweis des Lemmas. (i) $\Rightarrow$ (ii). trivial.

(ii) $\Rightarrow$ (i). Sei U eine offene Umgebung wie in (ii). Die Multiplikation mit x ist ein Homöomorphismus

$$G \longrightarrow G,\ g \mapsto xg.$$

Also ist xU eine offene Umgebung von x, und es gilt

$$g \in H \bigcap xU \Leftrightarrow x^{-1}g \in x^{-1}H \bigcap x^{-1}xU$$
$$\Leftrightarrow x^{-1}g \in H \bigcap U \qquad \text{(wegen } x \in H\text{)}.$$
$$\Leftrightarrow x^{-1}g \in \{e\} \qquad \text{(nach Wahl von U)}$$
$$\Leftrightarrow g = x.$$

Es gilt also $H \bigcap xU = \{x\}$.
QED (Lemma).

Zu (ii). Da die Bewertung nicht-trivial sein soll, gibt es einen von 0 und 1 verschiedenen Wert. Da die Werte eine Untergruppe der multiplikativen Gruppe $\mathbb{R}^*$ bilden (d.h. mit jeder reellen Zahl ist auch deren inverses ein Wert), gibt es einen von Null verschiedenen Wert < 1. Insbesondere ist die Menge

$$\{x \in \mathbb{R} \mid 0 < x < 1,\ x = |\alpha| \text{ für ein } \alpha \in k^*\}$$

nicht leer. Wir setzen

$$c := \sup \{x \in \mathbb{R} \mid 0 < x < 1,\ x = |\alpha| \text{ für ein } \alpha \in k^*\}.$$

Nach Konstruktion gilt

$$0 < c \leq 1.$$

Wäre c kein Wert von |?|, so würde es nach Definition des Supremums ein $\alpha \in k^*$ geben mit $0 < |\alpha| < 1$ und $|\alpha|$ beliebig nahe bei c, sagen wir

$$c - |\alpha| < \delta.$$

Dabei können wir für δ die positive reelle Zahl mit

$$U_\delta(1) \bigcap \text{Im } |?| = \{1\}$$

wählen. Wegen $c \leq 1$ und $|\alpha| < 1$ folgt $0 < 1 - |\alpha| < \delta$, also

$$|\alpha| \in U_\delta(1) \bigcap \text{Im } |?| = \{1\}$$

also $|\alpha| = 1$ im Widerspruch zu $|\alpha| < 1$. Dieser Widerspruch zeigt, es gibt ein α, dessen Wert gleich c ist,

$$c = |\alpha| \text{ für ein } \alpha \in k \text{ mit } 0 < |\alpha| < 1.$$

Insbesondere ist $c < 1$.

Für jedes $\beta \in k^*$ gibt es somit eine ganze Zahl m mit

$$0 < |\beta| \cdot c^m < 1$$

Ebenfalls wegen $c < 1$ gilt $|\beta| \cdot c^m c^{-n} \longrightarrow \infty$ für $n \longrightarrow \infty$. Wir können deshalb die ganze Zahl m außerdem noch so wählen, daß gilt

$$1 \leq |\beta| \cdot c^{m-1}$$

Zusammen ist

$$0 < |\beta\alpha^m| < 1 \leq |\beta\alpha^{m-1}|$$

Nach Wahl von $c = |\alpha|$ ist außerdem

$$0 < |\beta\alpha^m| \leq |\alpha| < 1 \leq |\beta\alpha^{m-1}|$$

Aus der zweiten Ungleichung erhalten wir durch Multiplikation mit $|\alpha|^{-1}$ die Ungleichung $|\beta\alpha^{m-1}| \leq 1$, zusammen mit der Ungleichung rechts also

$$|\beta\alpha^{m-1}| = 1,$$

also

$$|\beta| = |\alpha|^{1-m} = c^{1-m}$$

Wir haben gezeigt, der Wert jedes $\beta \in k^*$ ist eine ganzzahlige Potenz von c.
Zu (iii). Die Aussagen folgen direkt aus den Definitionen.
QED.

2.1.6 Archimedische und nicht-archimedishe Bewertungen

Seien k ein Körper und $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung von k. Diese Bewertung heiß nicht-archimedisch, wenn Axiom 3 von 2.1.1 mit C = 1 gilt. Andernfalls heißt die Bewertung archimedisch.

Bemerkungen

(i) Eine Bewertung ist genau dann nicht-archimedisch, wenn eine (bzw. alle) zur ihr äquivalente Bewertung(en) nicht-archimedisch sind.

(ii) Eine Bewertung $|?|$ des Körpers ist genau dann nicht-archimedisch, wenn gilt

$$| \alpha + \beta | \leq \max \{| \alpha | , | \beta | \} \text{ für beliebige } \alpha, \beta \in k.$$

Beweis. Zu (i). Wenn für $|?|$ das dritte Axiom mit C = 1 gilt,

$$|\alpha + 1| \leq 1 \text{ für } |\alpha| \leq 1,$$

so ist das auch der Fall für $|?|^c$ mit $c > 0$.

Zu (ii). Falls die Ungleichung besteht, so gilt insbesondere

$$| \alpha + 1| \leq \max \{ |\alpha|, 1 \} \leq 1 \text{ für } |\alpha| \leq 1,$$

d.h. die Bewertung ist nicht-archimedisch. Sei umgekehrt $|?|$ nicht-archimedisch. Wir haben zu zeigen

$$| \alpha + \beta | \leq \max \{| \alpha | , | \beta | \}.$$

Zum Beweis können wir annehmen $|\alpha| \leq |\beta|$. Dann gilt $|\alpha/\beta| \leq 1$, also - da $|?|$ nicht-archimedisch ist,

$$| \alpha/\beta + 1 | \leq 1.$$

Durch Multiplikation mit $|\beta|$ erhalten wir

$$| \alpha + \beta | \leq | \beta | = \max \{| \alpha | , | \beta | \}.$$

QED.

2.1.7 Eigenschaften nicht-archimedischer Bewertungen

Seien k ein Körper und $|?|: k \longrightarrow \mathbb{R}$ eine nicht-archimedische Bewertung. Dann gelten folgende Aussagen.

(i) Nicht-archimedische Dreiecksungleichung.Für beliebige $\alpha, \beta \in k$ gilt

$$| \alpha + \beta | \leq \max \{| \alpha | , | \beta | \},$$

wobei im Fall $| \alpha | \neq | \beta |$ sogar das Gleichheitszeichen gilt.

(ii) Die Menge

$$\mathcal{O} := \{\alpha \in k \mid | \alpha | \leq 1\}$$

ist ein Teilring von k. Dieser heißt Ring der ganzen Elemente von k bezüglich $|?|$.

(iii) Seien $|?|_1$ und $|?|_2$ zwei nicht-archimedische Bewertungen des Körpers k. Dann sind folgenden Aussagen äquivalent.

1. $|?|_1$ und $|?|_2$ sind äquivalent.
2. Für beliebige $\alpha, \beta \in k$ gilt $|\alpha|_1 < |\beta|_1 \Leftrightarrow |\alpha|_2 < |\beta|_2$.
3. Die zu $|?|_1$ und $|?|_2$ gehörigen Ringe der ganzen Elemente sind gleich.

(iv) Die Menge

$$\wp := \{\alpha \in k \mid |\alpha| < 1\}$$

ist das einzige maximale Ideal des Rings $\mathcal{O}$ der ganzen Elemente. Es besteht gerade aus den Nicht-Einheiten von $\mathcal{O}$.

(v) Die Bewertung $|?|$ ist genau dann diskret, wenn $\wp$ ein Hauptideal ist.

Beweis. Zu (i). Die Ungleichung besteht auf Grund der Bemerkung v on 2.1.6. Seien jetzt die beiden Werte von α und β verschieden, sagen wir

$$|\alpha| < |\beta|. \tag{1}$$

Dann gilt

$$|\beta| = |(\alpha+\beta) - \alpha| \leq \max \{|\alpha+\beta|, |\alpha|\}|.$$

Wegen (1) kann das Maximum rechts nicht gleich $|\alpha|$ sein, also ist es gleich $|\alpha+\beta|$,

$$|\beta| \leq |\alpha+\beta|.$$

Die linke Seite ist wegen (1) gleich $\max \{|\alpha|, |\beta|\}$,

$$\max \{|\alpha|, |\beta|\} \leq |\alpha+\beta|.$$

Zusammen mit Bemerkung 2.1.6 ist das gerade die Behauptung von (i).
Zu (ii). Nach (i) ist die Summe zweier Elemente von $\mathcal{O}$ wieder in $\mathcal{O}$. Für das Produkt ist dies ohnehin der Fall. Man beachte, wegen $|-1| = |1| = 1$ gilt

$$\pm 1 \in \mathcal{O}.$$

Zu (iii). 1 $\Rightarrow$ 2. Wegen $|?|_2 = |?|_1^c$ für ein $c > 0$ ist die Bedingung 2 trivialerweise erfüllt.

2 $\Rightarrow$ 3. Aus der Bedingung ergibt sich, daß auch die unechten Ungleichungen für die beiden Bewertungten äquivalent sind.

$$|\alpha|_1 \leq |\beta|_1 \Leftrightarrow |\alpha|_2 \leq |\beta|_2.$$

Speziell mit $\beta = 1$ ergibt sich

$$|\alpha|_1 \leq 1 \Leftrightarrow |\alpha|_2 \leq 1.$$

Also stimmen die beiden Ringe der ganzen Elemente überein.

3 $\Rightarrow$ 2. Wegen

$$|\alpha|_i \leq |\beta|_i \Leftrightarrow |\alpha\beta^{-1}|_i \leq 1 \Leftrightarrow \alpha\beta^{-1} \in \mathcal{O}$$

gilt

$$|\alpha|_1 \leq |\beta|_1 \Leftrightarrow |\alpha|_2 \leq |\beta|_2.$$

Damit gilt aber auch links das Gleichheitszeichen, wenn es rechts gilt, d.h. es ist

$$|\alpha|_1 < |\beta|_1 \Leftrightarrow |\alpha|_2 < |\beta|_2.$$

2 $\Rightarrow$ 1. Sei $\gamma := \alpha^m\beta^n$. Nach Voraussetzung gilt $|\gamma|_1 \geq 1 \Leftrightarrow |\gamma|_2 \geq 1$. Wir gehen zu den Logarithmen über und erhalten

$$m \cdot \log |\alpha|_1 + n \cdot \log |\beta|_1 \geq 0 \Leftrightarrow m \cdot \log |\alpha|_2 + n \cdot \log |\beta|_2 \geq 0.$$

Das Skalarprodukt aller Vektoren

$$\begin{pmatrix} m \\ n \end{pmatrix} \tag{2}$$

mit ganzzahligen Koordinaten mit den beiden Vektoren

$$\begin{pmatrix} \log |\alpha|_1 \\ \log |\beta|_1 \end{pmatrix} \text{ und } \begin{pmatrix} \log |\alpha|_2 \\ \log |\beta|_2 \end{pmatrix} \tag{3}$$

hat stets dasselbe Vorzeichen, d.h. die Vektoren (2) liegen stets in derselben durch (2) definierten Halbebene. Das ist nur möglich, wenn die beiden Vektoren dieselben Richtung haben, d.h. es gilt

$$\log |\alpha|_1 / \log |\alpha|_2 = \log |\beta|_1 / \log |\beta|_2 .$$

Wir haben gezeigt,

$$c := \log |\alpha|_1 / \log |\alpha|_2 \in \mathbb{R}$$

ist unabhängig von der speziellen Wahl von $\alpha \in k$. Damit gilt

$$|\alpha|_2 = e^{\log |\alpha|_2} = e^{c \cdot \log |\alpha|_1} = |\alpha|_1^c \text{ für jedes } \alpha \in k,$$

d.h. die beiden Bewertungen sind äquivalent.

Zu (iv). Wegen $|\alpha\beta| = |\alpha| \cdot |\beta|$ und $|\alpha+\beta| \leq \max \{|\alpha|, |\beta|\}$ ist $\wp$ ein Ideal von $\mathcal{O}$. Es gilt

$$\alpha \in \mathcal{O}\text{-}\wp \Leftrightarrow |\alpha| = 1 \Leftrightarrow \alpha \text{ ist Einheit von } \mathcal{O}.$$

Also ist $\wp$ das einzige maximale Ideal von $\mathcal{O}$.

Zu (v). Sei $\wp$ ein Hauptideal, sagen wir

$$\wp = \pi\mathcal{O}.$$

Dann hat jedes Element von $\mathcal{O}$ die Gestalt

$$\alpha = u \cdot \pi^n$$

mit einer Einheit u von $\mathcal{O}$ und einer nicht-negativen ganzen Zahl n. Für die Elemente α aus k - $\mathcal{O}$ gilt $|\alpha| > 1$, also $|\alpha^{-1}| < 1$, also $\alpha^{-1} \in \mathcal{O}$. Damit hat jedes Element von k die Gestalt

$$\alpha = u \cdot \pi^n \text{ mit } n \in \mathbb{Z}.$$

Die Werte dieser Elemente sind damit Potenzen von $|\pi|$, d.h.die Bewertung ist diskret. Sei jetzt umgekehrt |?| eine nicht-triviale diskrete Bewertung. Nach Bemerkung 2.1.5 (ii) sind besteht die Menge der von Null verschiedenen Werte von |?| aus den Potenzen einer reellen Zahl $c < 1$. Sei $\pi \in k$ ein Element mit

$$|\pi| = c.$$

Dann gibt es für jedes Element $\alpha \in k^*$ eine ganze Zahl n mit

$$|\alpha| = |\pi|^n.$$

Es gilt dann $|\alpha/\pi^n| = 1$, d.h. $u := \alpha/\pi^n$ ist eine Einheit von $\mathcal{O}$. Jedes Element von k^* hat die Gestalt

$$\alpha = u \cdot \pi^n$$

mit einer Einheit u von $\mathcal{O}$ und einer ganzen Zahl n. Dieses Element liegt genau dann in $\mathcal{O}$ wenn $n \geq 0$ ist und genau dann in $\wp$ wenn $n > 0$ ist. Insbesondere ist

$$\wp = \pi\mathcal{O}$$

ein Hauptideal.

QED.

2.1.8 Kriterium für nicht-archimedische Bewertungen

Seien k ein Körper und $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung. Dann sind folgende Aussagen äquivalent.

(i) |?| ist nicht-archimedisch.

(ii) $| n \bullet 1_k | \leq 1$ für jede ganze Zahl n.

Beweis. (i) $\Rightarrow$ (ii). Nach Voraussetzung gilt

$$| n \bullet 1_k | \leq | 1_k | = 1$$

für jedes $n \in \mathbb{Z}$.

(ii) $\Rightarrow$ (i). Wir können |?| durch eine äquivalente Bewertung ersetzten und auf Grund von 2.1.4 annehmen, für |?| gilt die Dreiecksungleichung. Für $|\alpha| \leq 1$ gilt dann

$$\begin{aligned} | \alpha + 1 |^n = |(\alpha + 1)^n| &\leq \sum_{j=0}^{n} | \binom{n}{j} \alpha^j | \quad \text{(Dreiecksungleichung)} \\ &\leq \sum_{j=0}^{n} |\alpha^j| \quad \text{(wegen Bedingung (ii))} \\ &\leq \sum_{j=0}^{n} 1 \quad \text{(wegen } |\alpha| \leq 1) \\ &= n \end{aligned}$$

Wir gehen zu den n-ten Wurzeln über und erhalten

$$| \alpha + 1 | \leq \sqrt[n]{n} .$$

Für $n \longrightarrow \infty$ erhalten wir

$$| \alpha + 1 | \leq 1$$

für beliebige α mit $|\alpha| \leq 1$. Mit anderen Worten, die Bewertung ist nicht-archimedisch. **QED**.

2.1.9 Kriterium für archimedische Bewertungen

Seien k ein Körper und $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung. Dann sind folgende Aussagen äquivalent.

(i) |?| ist archimedisch.

(ii) Für jede reelle Zahl $B \in \mathbb{R}$ gibt es eine natürliche Zahl n mit

$$B \leq |n \bullet 1_k|.$$

Beweis. (ii) $\Rightarrow$ (i). Nach Voraussetzung gibt es ein n mit $2 \leq |n \bullet 1_k|$. Auf Grund von 2.1.8 muß |?| archimedisch sein.

(i) $\Rightarrow$ (ii). Nach 2.1.8 gibt es ein $m \in \mathbb{N}$ mit

$$1 < |m \bullet 1_k|.$$

Die Folge $\{ |m \bullet 1_k|^i \}_{i=1,2,..}$ geht dann gegen Unendlich. Insbesondere gibt es ein i mit

$$B \leq |m \bullet 1_k|^i = | m^i \bullet 1_k$$

Die geforderte Bedingung ist somit für $n = m^i$ erfüllt.

QED.

2.1.10 Folgerung: der Fall positiver Charakteristik

Sei k ein Körper der Charakteristik > 0. Dann ist jede Bewertung von k nicht-archimedisch.

Beweis. Der Primkörper F von k ist dann endlich. Sei q die Anzahl seiner Elemente. F* ist dann eine multiplikative Gruppe der Ordnung q-1. Für jedes Element $\alpha \in F$ ist dann

$$\alpha^{q-1} = 1.$$

Für jede multiplikative Bewertung |?| ist damit

$$|\alpha| = 1 \text{ für jedes } \alpha \in F^*,$$

also

$$|\alpha| \leq 1 \text{ für jedes } \alpha \in F.$$

Die ganzzahligen Vielfachen von 1_k liegen aber sämtlich in F, d.h. die Bedingung 2.1.8(ii) ist erfüllt, d.h. k ist nicht-archimedisch.

QED.

2.1.11 Beispiel: die komplexen Zahlen

Der Körper der komplexen Zahlen hat bezüglich des gewöhnlichen Absolutbetrags

$$|.|: \mathbb{C} \to \mathbb{R}_{\geq 0}$$

die Struktur eines (archimedisch) bewerteten Körpers. Dasselbe gilt für jeden Teilkörper von $\mathbb{C}$.

Problem: man finde weitere Beispiele für archimedische Bewertungen.

2.1.12 Beispiel: die rationalen Zahlen

Jede Primzahl p definiert wie folgt eine (nicht-archimedische diskrete) Bewertung

$$|?|_p : \mathbb{Q} \longrightarrow \mathbb{R}$$

auf dem Körper $\mathbb{Q}$ der rationalen Zahlen. Seien $r \in \mathbb{Q} - \{0\}$ eine rationale Zahl,

$$r = p_1^{e_1} \bullet \ldots \bullet p_r^{e_r}$$

deren Zerlegung in ein Produkt von paarweise teilerfremden Primzahlpotenzen (mit ganzzahligen Exponenten) und e der Exponent, mit welchem die gegebene Primzahl p in dieser Zerlegung vorkommt (wir setzen e = 0 falls p nicht vorkommt). Dann sei

$$| r |_p := (\frac{1}{p})^e$$

Weiter sei $|0|_p := 0$. Dann ist $|?|_p$ ein nicht-archimedische Bewertung von $\mathbb{Q}$, genauer,

$$|?|_p = (\frac{1}{p})^{v_p(?)}$$

ist die multiplikative Bewertung zur diskreten Bewertung

$$v_p : \mathbb{Q}^* \longrightarrow \mathbb{Z},$$

welche zum Primideal $p\mathbb{Z}$ des Dedekind-Rings $\mathbb{Z}$ gehört (vgl. 1.5.2).

Problem: Man finde weitere nicht-archimedische Bewertungen von $\mathbb{Q}$.

2.1.13 Beispiel: die rationalen Funktionenkörper

Seien k ein Körper, t eine Unbestimmte über k, K:= k(t), $p(t) \in k[t]$ ein irreduzibles Polynom und ρ eine reelle Zahl mit

$$0 < \rho < 1$$

Zum Beispiel kann man $\rho := 2^{-\deg p}$ setzen oder, falls k endlich ist,

$$\rho := (\#\, k[t]/(p))^{-1}.$$

Jedes Element $f(t) \in K^*$ läßt sich dann in der Gestalt

$$f = p^n.\frac{u}{v}$$

mit zu p(t) teilerfremden Polynomen u und v. Wir setzen.

$$|f(t)|_p := \rho^n$$

Die so definierte Abbildung

$$|.|_p : k(t)^* \to R$$

ist eine multiplikative Bewertung von k(t) und heißt p-adische Bewertung oder auch Bewertung zur Stelle p. Es ist dann

$$|?|_p = \rho^{v_p(?)},$$

d.h. $|?|_p$ ist die multiplikative Bewertung zur diskreten Bewertung

$$v_p : k(t)^* \longrightarrow \mathbb{Z},$$

welche zum Primideal pk[t] des Dedekind-Rings k[t] gehört.

Für beliebige von Null verschiedenen Polynome u,v∈k[t] und

$$f := \frac{u}{v}$$

setzen wir weiter

$$|f|_\infty := c^{\deg(v)-\deg(u)}$$

Auf diese Weise ist ebenfalls eine Bewertung von k(t) definiert. Ersetzt man in der obigen Definition von K=k(t) die Unbestimmte t durch $s := t^{-1}$ so ist dies gerade die Bewertung zur Stelle s. Man nennt diese Bewertung auch die Bewertung zur Stelle t=∞. Wie im endlichen Fall ist

$$|?|_\infty = \rho^{v_\infty(?)}$$

die multiplikative Bewertung zur diskreten Bewertung $v_\infty : k(t) \longrightarrow \mathbb{Z}$, welche zum Primideal sk[s] des Dedekind-Rings k[s] gehört.

2.1.14 Die multiplikativen Bewertungen über einem Dedekind-Ring

Seien R ein Dedekind-Ring mit dem Quotientenkörper K und

$$|\,?\,| : K \longrightarrow \mathbb{R}$$

eine nicht-triviale multiplikative Bewertung mit

$$|r| \le 1 \text{ für jedes } r \in R.$$

Dann gibt es eine reelle Zahl $\rho \in (0, 1) \subseteq \mathbb{R}$ und ein maximales Ideal $p \subseteq R$ mit

$$|x| = \rho^{v_p(x)} \text{ für jedes } x \in K.$$

Beweis. Wegen

$$|r| \le 1 \text{ für jedes } r \in R.$$

muß die Bewertung |?| nicht-archimedisch sein. Es gilt also sogar die verschärfte Dreiecksungleichung

$$|x + y| \le \max\{|x|, |y|\}. \qquad (1)$$

Sei

$$p := \{r \in R \mid |r| < 1\}$$

Dann ist p ein Ideal von R:

$x \in R, y \in p \Rightarrow xy \in p$ (wegen der Multiplikativität von |?|).

$x, y \in p \Rightarrow x \pm y \in p$ (wegen (1))

Dieses Ideal ist echt:

$1 \notin p$ (wegen $|1| = 1$).

Sei jetzt $x \in K - \{0\}$ ein Element mit $|x| \neq 1$. Wir schreiben $x = \frac{a}{b}$ mit $a, b \in R - \{0\}$. Dann haben a und b verschiedene Werte,

$$|a| \neq |b|,$$

die beide $\neq 0$ sind. Es gilt also $|a| \neq 1$ oder $|b| \neq 1$ und wegen $a, b \in R$ sogar

$$|a| < 1 \text{ oder } |b| < 1.$$

Es folgt

$$a \in p \text{ oder } b \in p.$$

Wir haben gezeigt, p ist von Null verschieden,

$$p \neq 0.$$

Weiter ist p ein Primideal: für $x, y \in R$ mit $xy \in p$ gilt

$$|x| \cdot |y| = |xy| < 1 \text{ , } |x| \leq 1, |y| \leq 1.$$

Die Elemente x und y können dann nicht beide den Wert 1 haben, d.h. es gilt $x \in p$ oder $y \in p$. Wir haben gezeigt, p ist ein von Null verschiedenes Primideal.

Insbesondere ist

$$R_p$$

ein diskreter Bewertungsring von K, d.h.

$$R_p = \{x \in K \mid v_p(x) \geq 0\} = \{x \in K \mid |x|_{v_p} \leq 1\}$$

Damit besteht die Implikation

$$x \in K - R_p \Rightarrow x^{-1} \in pR_p. \qquad (2)$$

(für $x \in K - R_p$ ist $v_p(x) < 0$, also $v_p(x^{-1}) = -v_p(x) > 0$).

Jedes Element $x \in R_p$ hat die Gestalt $x = \frac{a}{b}$ mit $a \in R$ und $b \in R - p$, d.h.

$$|x| = |a|/|b| = |a|/1 = |a| \leq 1.$$

Es gilt also

$$R_p \subseteq \{x \in K \mid |x| \leq 1\} =: S.$$

Nach Definition von p ergibt sich damit

$$pR_p \subseteq \{x \in K \mid |x| < 1\}.$$

Wäre $x \in S$ ein Element, welches nicht in R_p liegt, so wäre wegen (2) das Inverse x^{-1} ein Element von pR_p, d.h. $|x^{-1}| < 1$, d.h. $|x| > 1$, was im Widerspruch zur Wahl von x (und der Definition von S) steht. Es gilt also

$$R_p = \{x \in K \mid |x| \leq 1\} \tag{3}$$

Weiter ist

$$pR_p = \{x \in K \mid |x| < 1\} \tag{4}$$

Die Inklusion "$\subseteq$" haben wir oben gerade bewiesen. Beweisen wir die umgekehrte Inklusion. Sei x ein Element aus der Menge auf der rechten Seite. Wegen (3) gilt dann $x \in R_p$. Nun ist aber x wegen $|x| < 1$ keine Einheit von R_p (denn x^{-1} liegt wegen (3) nicht in R_p). Also gilt $x \in pR_p$.

Sei jetzt $\pi \in pR_p$ ein Parameter des Bewertungsrings R_p. Dann ist

$$\rho = |\pi| \in (0, 1) \subseteq \mathbb{R},$$

(wegen $\pi \neq 0$ ist $|\pi| > 0$ und wegen (4) ist $|\pi| < 1$). Außerdem läßt sich jedes Element $x \in K^*$ in der Gestalt

$$x = u \bullet \pi^n \text{ mit } u \in R_P^* \text{ und } n = v_p(x)$$

schreiben. Es folgt

$$|x| = |u| \bullet |\pi|^n = \rho^n = \rho^{v_p(x)}.$$

Für $x = 0$ ist $|x| = 0 = \rho^{\infty} = \rho^{v_p(x)}$.

QED.

2.1.15 Satz von Ostrovskij: die Bewertungen der rationalen Zahlen

Jede nicht-triviale multiplikative Bewertung des Körpers $\mathbb{Q}$ der rationalen Zahlen ist äquivalent zu einer der p-adischen Bewertungen $|?|_p$ oder zum gewöhnlichen Absolutbetrag.

Beweis. Sei |?| eine nicht-triviale Bewertung von $K := \mathbb{Q}$. O.B.d.A. gelte für |?| die Dreiecksungleichung. Sei

$$a \in \mathbb{Z} \text{ und } a > 1.$$

Dann kann man jede nicht-negative ganze $b \in \mathbb{Z}$ im Zahlensystem zur Basis a darstellen, sagen wir

$$b = b_m a^m + b_{m-1} a^{m-1} + \ldots + b_0$$

mit $0 \leq b_j < a$ für jedes j und[41] $m \leq \log(b)/\log(a)$. Die Dreiecksungleichung liefert[42]

$$|b| \leq M \cdot \left(\frac{\log(b)}{\log(a)} + 1\right) \cdot \max(1, |a|^{\log(b)/\log(a)})$$

mit

$$M := \max\{|d| : d = 0, \ldots, a-1\}$$

Speziell für $b = c^n$ und durch Ziehen der n-ten Wurzel erhalten wir[43]

---

[41] Die nachfolgende Ungleichung gilt, weil m die größte ganze Zahl ist mit $a^m \leq |b|$.

[42] Der erste Faktor rechts schätzt die Werte der Koeffizienten b_i ab, der zweite die Anzahl der Summanden und der dritte die Werten der Potenzen von a.

[43] Wir ziehen den n-te Wurzel aus dem Maximum rechts, indem wir aus jedem Glied unter dem Maximum die Wurzel ziehen.

$$|c| \leq \sqrt[n]{M} \cdot \sqrt[n]{n} \cdot \sqrt[n]{\frac{\log(c)}{\log(a)}} \cdot \max\{1, |a|^{\log(c)/\log(a)}\}.$$

Für $n \to \infty$ folgt

$$|c| \leq \max\{1, |a|^{\log(c)/\log(a)}\} \qquad (1)$$

1.Fall: Es gibt ein $c \in \mathbb{Z}$ mit $|c|>1$.
Dann gilt $c \neq 0, +1, -1$. O.B.d.A. sei $c > 1$. Dann gilt (1) für dieses c und jedes $a > 1$ (denn $a \in \mathbb{Z}$ war beliebig gewählt mit $a > 1$).
Bedingung (1) bekommt für $|c| > 1$ die Gestalt

$$|c|^{1/\log(c)} \leq |a|^{1/\log(a)}.$$

Aus Symmetriegründen muß sogar das Gleichheitszeichen gelten,

$$|c|^{1/\log(c)} = |a|^{1/\log(a)}.$$

Durch Auflösen nach $|a|$ sehen wir, $|a|$ ist bis auf Äquivalenz der gewöhnliche Absolutbetrag:

$$|a| = |c|^{\log(a)/\log(c)}.$$

2. Fall: Es gilt $|c| \leq 1$ für jedes $c \in \mathbb{Z}$.
Nach dem Kriterium für nicht-archimedische Bewertungen 2.1.8 ist $|?|$ eine nicht-archimedische Bewertung. Da sie nach Voraussetzung nicht-trivial ist, gibt es ganze Zahlen $a \in \mathbb{Z}$ mit $|a|<1$ und die Menge dieser ganzen Zahlen ist ein Ideal. Wegen $|ab| = |a| \cdot |b|$ ist dieses Ideal ein Primideal, welches von einer Primzahl p erzeugt wird. Nach 2.1.14 ist $|?|$ gerade die zur p-adischen Bewertung gehörige multiplikative Bewertung.
QED.

2.1.16 Die Bewertungen eines rationalen Funktionenkörpers

Seien k in Körper und t eine Unbestimmte. Dann ist jede nicht-triviale Bewertung von k(t), welche auf k trivial ist, äquivalent zu einer p(t)-adischen Bewertung oder einer solchen zur Stelle $t=\infty$. (vgl. 2.1.13).
Beweis. Wegen der Trivialität auf k ist die Bewertung nicht-archimedisch. Wie im letzten Teil des Beweises von 2.1.15 (2. Fall) wende man 2.1.14 an.
QED.

2.2 Archimedisch bewertete Körper

Die Ergebnisse dieses Abschnitts stellen eigentlich eine Ablenkung von unseren zahlentheoretischen Zielstellungen dar. Sie sind aber interessant genug für die Einordnung unserer Ergebnisse in einen allgemeineren Zusammenhang, sodaß wir diese Ablenkung in Kauf nehmen. Wir wollen uns hier eine Vorstellung von den archimedisch bewerteten Körpern verschaffen.

Zunächsts benötigen wir einen vorbereitenten Satz.

2.2.1 Die topologische Gruppenstruktur zu einer reellen Norm

Seien A eine $\mathbb{C}$-Algebra[44],

$$|.|: A \to \mathbb{R}$$

eine reelle Norm[45] des $\mathbb{C}$-Vektorraums A und $G := A^*$ die Gruppe der Einheiten der Algebra A. Es gelte

---

[44] Eine Algebra über einem kommutativen Ring R mit 1 ist ein kommutativer Ring A mit 1 zusammen mit einem Homomorphismus $R \longrightarrow A$, dessen Bild im Zentrum von A liegt. Ist R ein Körper wie im vorliegend Fall, so ist dieser Homomorphismus injektiv, so daß man R mit einem Teilring von A identifizieren kann.

$$|xy| \le |x|\cdot|y| \text{ für } x,y\in A$$

und die Algebra A sei vollständig bezüglich der Norm |.| .
Dann ist G eine topologische Gruppe, d.h. die Multiplikation und der Übergang zum Inversen definieren stetige Abbildungen

$$G\times G \to G,\ (x,y) \mapsto xy,$$

$$G\to G,\ x \mapsto x^{-1}.$$

Beweis. Die Stetigkeit der Multiplikation ergibt sich aus der folgenden Abschätzung.

$$|xy - ab| = |x(y-b)+(x-a)b| \le |x|\cdot|y-b| + |x-a|\cdot|b|.$$

Zum Beweis der Stetigkeit der zweiten Abbildung müssen wir den Ausdruck

$$\left|\frac{1}{x} - \frac{1}{a}\right|$$

(mit x,a∈G und x nahe bei a) abschätzen. Dazu betrachten wir das Element

$$u := \frac{1}{a}(x-a).$$

Es gilt

(1) $$|u| \le \left|\frac{1}{a}\right|\cdot|x-a| < 1$$

falls x in einer geeigneten Umgebung von a liegt (nämlich falls $|x-a| < \left|\frac{1}{a}\right|$ gilt). Dann ist aber die Reihe

(2) $$\sum_{n=0}^{\infty} (-u)^n$$

absolut konvergent gegen das Inverse von 1+u. Insbesondere ist 1+u eine Einheit von A und es gilt

(3) $$\frac{1}{x} = \frac{1}{a(1+u)} = \frac{1}{a}\sum_{n=0}^{\infty}(-u)^n = \frac{1}{a} + \frac{1}{a}\sum_{n=1}^{\infty}(-u)^n$$

Die Reihe (2) läßt sich wie folgt betragmäßig abschätzen.

$$\left|\sum_{n=0}^{\infty}(-u)^n\right| \le \sum_{n=0}^{\infty}|u|^n = \frac{1}{1-|u|}$$

(4) $$\le \frac{1}{1-\left|\frac{1}{a}\right|\cdot|x-a|} \qquad \text{(nach Definition von u).}$$

Insbesondere bleibt die Reihe beschränkt, wenn x gegen a konvergiert.
Es gilt

$$\left|\frac{1}{x} - \frac{1}{a}\right| = \left|\frac{1}{a}\sum_{n=1}^{\infty}(-u)^n\right| \qquad \text{(nach (3))}$$

$$\le \left|\frac{1}{a}\right|\cdot|u|\cdot\left|\sum_{n=0}^{\infty}(-u)^n\right|$$

---

[45] d.h. es gilt

1. $|x| \ge 0$ und $|x| = 0 \Leftrightarrow x = 0$.
2. $|\lambda x| = |\lambda|\bullet|x|$ für $x \in A$ und $\lambda\in\mathbb{C}$.
3. $|x + y| \le |x| + |y|$ für $x, y \in A$.

Ist A nur eine $\mathbb{R}$-Algebra, so fordert man die Gültigkeit von Bedingung 2 nur für $\lambda\in\mathbb{R}$.

$$\leq |\frac{1}{a}|^2 \cdot |x-a| \cdot |\sum_{n=0}^{\infty} (-u)^n| \qquad \text{(nach (1))}.$$

Der Beweis der Behauptung ist damit zurückgeführt auf die Beschränktheit (4) des letzten Faktors.
QED.

2.2.2 Satz von Gelfand-Mazur

Sei A eine $\mathbb{R}$-Algebra mit folgenden Eigenschaften.

1. Es gibt ein $j \in \mathbb{R}$ mit $j^2=-1$.
2. Es gibt eine reelle Norm $|?|:A \to \mathbb{R}$ auf A mit $|xy| \leq |x| \cdot |y|$.
3. A ist ein Schiefkörper.

Dann gilt $A = \mathbb{R} \cdot 1 + \mathbb{R} \cdot j$. Insbesondere ist A sogar ein Körper.
Beweis. Wir setzen

$$\mathbb{C} := \mathbb{R} \cdot 1 + \mathbb{R} \cdot j.$$

Die Ungleichung $|xy| \leq |x| \cdot |y|$ impliziert,daß die Multiplikation von A eine stetige Abbildung ist. Wir können die Algebra A durch ihre Vervollständigung bezüglich der gegebenen Norm |?| ersetzen und deshalb annehmen, daß A eine Banachalgebra[46] ist. Nach 2.2.1 ist dann auch die Umkehrung

$$A-\{0\} \to A-\{0\},\ x \mapsto x^{-1},$$

eine stetige Abbildung.

Angenommen, es gibt ein Element $c \in A-\mathbb{C}$. Dann ist die Abbildung

$$f: \mathbb{C} \to A,\ z \mapsto \frac{1}{c-z},$$

wohldefiniert und stetig. Für $z \neq 0$ gilt

$$f(z) = \frac{1}{z} \cdot \frac{1}{\frac{c}{z} - 1},$$

d.h. für $z \to \infty$ geht f gegen Null. Insbesondere ist

$$|f|: \mathbb{C} \to \mathbb{R}_{\geq 0},\ z \mapsto |\frac{1}{c-z}|$$

eine stetige Abbildung, welche außerhalb einer hinreichend großen Kreisscheibe sehr kleine Werte annimmt. Insbesondere nimmt |f| einen Maximalwert M an. Sei

$$D := \{x \in \mathbb{C} \mid |f|(x) = M\}$$

Die Menge D ist abgeschlossen, nicht-leer und beschränkt. Zum Nachweis des gewünschten Widerspruchs genügt es zu zeigen, daß D offen ist.[47]
Sei

$$a \in D.$$

Durch Ausführen einer Verschiebung können wir erreichen, daß

$$a=0$$

gilt. Zeigen wir, für $r>0$ klein, liegt die r-Umgebung von 0 ganz in D,

---

[46] d.h. die $\mathbb{R}$-Algebra ist mit einer reellen Norm $|?|: A \longrightarrow \mathbb{R}$ versehen. Zusätzlich wird gefordert, daß die Ungleichung

$$|xy| \leq |x| \cdot |y|$$

besteht und der Vektorraum A bezüglich der durch die Norm definierten Metrik vollständig ist.

.

[47] Weil $\mathbb{C}$ zusammenhängend ist, ist jede nicht-leere Teilmenge von $\mathbb{C}$, die gleichzeitig offen und abgeschlossen ist, gleich der ganzen komplexen Ebene, kann also nicht beschränkt sein.

$$U_r(0) \subseteq D.$$

Dazu betrachten wir die Summe

$$S(n) := \frac{1}{n} \cdot \sum_{k=1}^{n} \frac{1}{c - w^k \bullet r},$$

wobei w eine primitive n-te Einheitswurzel bezeichne (d.h. die Summe wird über alle n-ten Einheitswurzeln erstreckt). Durch Bilden der logarithmischen Ableitung des Polynoms

$$X^n - r^n = \prod_{k=1}^{n} (X - w^k \bullet r)$$

sehen wir, es gilt

$$\frac{nX^{n-1}}{X^n - r^n} = \sum_{k=1}^{n} \frac{1}{X - w^k \bullet r}$$

also

$$S(n) = \frac{c^{n-1}}{c^n - r^n} = \frac{1}{c - r \cdot (\frac{r}{c})^{n-1}}.$$

Für r klein (z.B. für r<|c|) erhalten wir

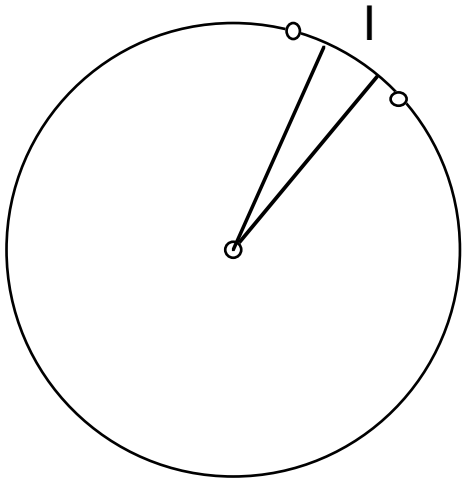
$$\lim_{n \to \infty} |S(n)| = |\frac{1}{c}| = |f|(0) = M \qquad (1)$$

Falls in jeder Umgebung von a=0 Elemente aus dem Komplement von D liegen, kann man ein r<|c| wählen und eine komplexe Zahl b vom Betrag 1 mit

$$M > |f(rb)| = |\frac{1}{c - rb}|$$

In der Nähe von b gibt es dann auf dem Einheitskreis ein Intervall I und ein ε>0 mit

$$M - \varepsilon > |\frac{1}{c - r\zeta}|$$



für alle Einheitswurzeln ζ∈I. Sei b(n) die Anzahl der n-ten Einheitswurzeln, welche in I liegen. Dann ist $\frac{2\pi}{n} \bullet b(n)$ annähernd gleich die Länge[48] des Intervalls I. Insbesondere strebt $\frac{b(n)}{n}$ für $n \to \infty$ gegen einen von Null verschiedenen Grenzwert. Wir schreiben jetzt |S(n)| in der Gestalt

---

[48] $\frac{2\pi}{n}$ ist die Länge des Intervalls zwischen zwei benachbarten Einheitswurzeln.

$$S(n) = \frac{1}{n}\ (\Sigma_I \frac{1}{c\text{-}w^k{}_{\bullet r}}\ +\ \Sigma_{II} \frac{1}{c\text{-}w^k{}_{\bullet r}}),$$

wobei die erste Summe über alle n-ten Einheitswurzeln aus I und die zweite Summe über den Rest erstreckt wird. Die Summanden der ersten Summe haben einen Betrag ≤ M-ε und die der zweiten Summe einen Betrag ≤ M. Also gilt

$$|S(n)| \le \frac{1}{n}(b(n)(M-\varepsilon) + (n-b(n))M) = M - \frac{b(n)}{n} \cdot \varepsilon .$$

Für $n\to\infty$ liefert dies den gewünschten Widerspruch (vgl. (1)).
QED.

2.2.3 Die archimedisch bewerteten Erweiterungen von $\mathbb{R}$

Sei K eine archimedisch bewertete Körpererweiterung von $\mathbb{R}$. Dann ist K isomorph[49] zu $\mathbb{R}$ oder $\mathbb{C}$,

$$K \cong \mathbb{R} \text{ oder } K \cong \mathbb{C}$$

Beweis. Falls $\mathbb{C} \subseteq K$ gilt, so ist nach dem Satz von Gelfand-Mazur 2.2.2 sogar[50]

$$\mathbb{C} = K.$$

Sei jetzt $\mathbb{C}$ nicht in K enthalten. Wir setzen

$$L := K(j) \text{ mit } j^2=-1.$$

Wir versehen den $\mathbb{R}$-Vektorraum L mit der Norm

$$|x+yj| := |x| + |y|.$$

Diese Norm hat die in 2.2.2 geforderte Eigenschaft: mit z=x+yj und z'= x'+y'j gilt nämlich

$$\begin{aligned} |zz'| &= |xx'-yy'| + |xy'+x'y| \\ &\le |x|\cdot|x'|+|y|\cdot|y'| + |x|\cdot|y'|+|x'|\cdot|y| \\ &= (|x|+|y|)\cdot(|x'|+|y'|) \\ &= |z|\cdot|z'| \end{aligned}$$

Nach 2.2.2 erhalten wir L=$\mathbb{C}$. Wegen $\mathbb{R}\subseteq K$ gilt damit

$$1 = \dim_{\mathbb{R}}\mathbb{R} \le \dim_{\mathbb{R}} K = \frac{1}{2}\dim_{\mathbb{R}} L = \frac{1}{2}\dim_{\mathbb{R}} \mathbb{C} = 1.$$

Es gilt also überall das Gleichheitszeichen, d.h.

$$\mathbb{R} = K.$$

QED.

2.2.4 Satz von Gelfand-Tornheim

Jeder archimedisch bewertete Körper k ist isomorph (als bewerteter Körper) zu einem Teilkörper des Körpers der komplexen Zahlen (versehen mit dem gewöhnlichen Absolutbetrag).
Beweis. 1. Schritt. Es gilt char(k) = 0.
Angenommen, die Charakteristik von k ist eine Primzahl p>0. Dann liegt jedes von Null verschiedene $z = n\cdot 1_k$ mit $n\in\mathbb{Z}$ im Primkörper von k, d.h. es gilt nach dem kleinen Fermatschen Satz

$$z^{p-1}=1,$$

also $|z|^{p-1} = 1$, also |z| = 1. Wir haben gezeigt, es gilt

---

[49] Zunächst sind dies nur Körper-Isomorphien. Später werden wir sehen, es sind Isomorphien bewerteter Körper.
[50] Gleichheit als bewertete Körper, wegen der Eindeutigkeit der Fortsetzung auf endliche Erweiterungen, falls die der Grundkörper vollständig ist.

$$|n\cdot 1_k| \leq 1 \text{ für } n=1,2,3,...$$

Nach dem Kriterium für nicht-archimedische Bewertungen 2.1.8 ist |.| nicht-archimedisch im Widerspruch zu unseren Voraussetzungen.
2. Schritt. Abschluß des Beweises.
Wir wissen nach dem ersten Schritt, daß k die Charakteristik Null hat, d.h. es gilt

$$\mathbb{Q} \subseteq k.$$

Die Einschränkung der Bewertung von k auf $\mathbb{Q}$ ist eine archimedische Bewertung von $\mathbb{Q}$, also nach dem Satz von Ostrovskij 2.1.15 äquivivalent zum gewöhnlichen Absolutbetrag. Wir können annehmen, |?| ist auf $\mathbb{Q}$ gleich dem gewöhnlichen Absolutbetrag. Wir können k durch seine Vervollständigung bezüglich |.| ersetzen und deshalb ohne Beschränkung der Allgemeinheit annehmen, k ist vollständig. Dann gilt aber mit $\mathbb{Q}\subseteq k$ sogar $\mathbb{R}\subseteq k$. Nach 2.2.3 erhalten wir $k = \mathbb{C}$ oder $k = \mathbb{R}$.

Nach Konstruktion ist |?| auf $\mathbb{R}$ äquivalent zum gewöhnlichen Absolutbetrag. Wir haben noch zu zeigen, das is dann auch auf $\mathbb{R}$ bzw. $\mathbb{C}$ der Fall. Zum Beweis reicht es, die folgende Aussage über die Eindeutigkeit von Fortsetzungen zu beweisen.
QED.

2.2.5 Eindeutigkeitssatz für die Fortsetzung von Bewertungen

Seien K/k eine endliche Körpererweiterung und

$|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung.

Wir nehmen weiter an,

k ist vollständig

bezüglich der gegebenen Bewertung. Dann sind je zwei multiplikative Bewertungen von K, welche beide die gegebene Bewertung |?| von k fortsetzen, äquivalent.

Diese Aussage wird sich als direkte Folgerung einer allgemeineren Aussage des nachfolgenden Abschnitts ergeben.

2.3 Die Topologie zu einer multiplikativen Bewertung

2.3.1 Umgebungsbasen

Eine Umgebungsbasis eines topologischen Raumes X ist eine Familie von offenen Mengen von X mit der Eigenschaft, daß jede offene Menge Vereinigung von Mengen der Familie ist.

Bemerkungen

(i) Sei $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung. Dann bilden die Mengen der Gestalt

$$U_\varepsilon(\alpha) := \{ x \in k : |x - \alpha| < \varepsilon\} \text{ mit } \alpha\in k \text{ und } 0 < \varepsilon \in \mathbb{R},$$

welche ε-Umgebungen der Bewertung heißten, eine Umgebungsbasis für die durch diese Bewertung definierte Topologie.

(ii) Ersetzt man die gegebene Bewertung |?| von k durch eine äquivalente, so bleibt die zugehörige Menge der ε-Umgebungen unverändert, und damit auch die Topologie.

(iii) Wählt man in der Äquivalenzklasse von |?| eine (stets existierende) Bewertung aus, für welche die Dreiecksungleichung gilt, so sind die oben beschriebenen ε-Umgebungen gerade die ε-Umgebungen der zugehörigen Metrik.

2.3.2 Erste Eigenschaften der Topologie zu einer multiplikativen Bewertung

(i) Sei $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung des Körpers k. Dann ist k bezüglich der durch |?| definierten Topologie ein topologischer Körper, d.h. die Abbildungen

$$k \times k \longrightarrow k, (x, y) \mapsto x + y,$$

$$k \times k \longrightarrow k, (x, y) \mapsto x \bullet y,$$

$$k^* \longrightarrow k^*, x \mapsto \frac{1}{x},$$

sind stetig bezüglich dieser Topologie.

(ii) Zwei multiplikative Bewertungen $|?|_1$ und $|?|_2$ sind genau dann äquivalent, wenn die zugehörigen Topologien übereinstimmen, d.h.eine Menge ist bezüglich der einen Bewertung genau dann offen, wenn sie es bezüglich der anderen Bewertung ist.

Beweis. Zu (i). Siehe den Beweis von 1.4.11.
Zu (ii) (vgl. den Beweis von 2.1.7 (iii)). Falls die beiden Bewertungen äquivalent sind, so gehören zu ihnen dieselben offenen Mengen, d.h. die beiden Topologien stimmen überein.
Seien jetzt umgekehrt die beiden Topologien zu $|?|_1$ und $|?|_2$ gleich. Dann bestehen für

jedes Element $\alpha \in k$ die folgenden Implikationen:

$$|\alpha|_1 < 1 \quad \Rightarrow |\alpha^n - 0|_1 = |\alpha|_1^n \longrightarrow 0 \text{ (für n gegen } \infty)$$

$$\Rightarrow \alpha^n \longrightarrow 0 \text{ bezüglich der Topologie zu } |?|_1$$

$$\Rightarrow \alpha^n \longrightarrow 0 \text{ bezüglich der Topologie zu } |?|_2$$

$$\Rightarrow |\alpha^n - 0|_2 \longrightarrow 0$$

$$\Rightarrow |\alpha|_2^n = |\alpha^n|_2 \longrightarrow 0$$

$$\Rightarrow |\alpha|_2 < 1$$

Wir haben gezeigt, für jedes $\alpha \in k$ besteht die Implikation

$$|\alpha|_1 < 1 \Rightarrow |\alpha|_2 < 1.$$

Aus Symmetriegründen muß dann aber auch

$$|\alpha|_1 < 1 \Leftrightarrow |\alpha|_2 < 1.$$

gelten.

Damit gilt aber auch

$$|\alpha|_1 \geq 1 \Leftrightarrow |\alpha|_2 \geq 1$$

Wie beim Beweis der Implikation $x \Rightarrow y$ von 2.1.7 (iii) sehen wir jetzt , daß die beiden Bewertungen äquivalent sind:

Sei $\gamma := \alpha^m \beta^n$. Dann gilt

$$|\gamma|_1 \geq 1 \Leftrightarrow |\gamma|_2 \geq 1.$$

Wir gehen zu den Logarithmen über und erhalten

$$m \cdot \log |\alpha|_1 + n \cdot \log |\beta|_1 \geq 0 \Leftrightarrow m \cdot \log |\alpha|_2 + n \cdot \log |\beta|_2 \geq 0.$$

Das Skalarprodukt aller Vektoren

$$\begin{pmatrix} m \\ n \end{pmatrix} \tag{2}$$

mit ganzzahligen Koordinaten mit den beiden Vektoren

$$\begin{pmatrix} \log |\alpha|_1 \\ \log |\beta|_1 \end{pmatrix} \text{ und } \begin{pmatrix} \log |\alpha|_2 \\ \log |\beta|_2 \end{pmatrix} \tag{3}$$

hat stets dasselbe Vorzeichen, d.h. die Vektoren (2) liegen stets in derselben durch (2) definierten Halbebene. Das ist nur möglich, wenn die beiden Vektoren dieselben Richtung haben, d.h. es gilt

$$\log |\alpha|_1 / \log |\alpha|_2 = \log |\beta|_1 / \log |\beta|_2 .$$

Wir haben gezeigt,

$$c := \log |\alpha|_1 / \log |\alpha|_2 \in \mathbb{R}$$

ist unabhängig von der speziellen Wahl von $\alpha \in k$. Damit gilt

$$|\alpha|_2 = e^{\log |\alpha|_2} = e^{c \cdot \log |\alpha|_1} = |\alpha|_1^c \text{ für jedes } \alpha \in k,$$

d.h. die beiden Bewertungen sind äquivalent.
QED.

2.3.3 Die Vervollständigung eines bewerteten Körpers

(i) Sei $|?|: k \longrightarrow \mathbb{R}$ eine multiplikative Bewertung. Dann ist k Teilkörper eines vollständigen bewerteten Körpers $\overline{k}$,

$$k \subseteq \overline{k}$$

mit folgenden Eigenschaften.

1. Die gegebene Bewertung von k ist die Einschränkung der Bewertung von $\overline{k}$.
2. Der Körper k liegt dicht in $\overline{k}$.

Der Körper $\overline{k}$ ist durch diese beiden Bedingungen bis auf natürliche k-Isomorphie eindeutig bestimmt. Er heißt Vervollständigung von k bezüglich der gegebenen Bewertung.

(ii) Jede Einbettung eines bewerteten Körpers k in einen vollständigen bewerteten Körper, welche die Bewertungen respektiert, faktorisiert sich auf genau eine Weise über dessen Vervollständigung $\overline{k}$.

(iii) Die Bewertung des Körper k von (i) ist genau dann nicht-archimedisch, wenn es die von $\overline{k}$ ist. Die Menge der Werte dieser beiden Bewertungen stimmen in diesem (nicht-archimedischen) Fall überein.

Beweis. Zu (i). Existenz von $\overline{k}$.

Sei $\overline{k}$ die Vervollständigung des metrischen Raums k zu einer Bewertung von k, die äquivalent ist zu |?| und der Dreiecksungleichung genügt. Da Additiion, Multiplikation und Übergang zum Inversen stetige Abbildungen

$$k \times k \longrightarrow k \longrightarrow \overline{k}$$

bzw.

$$k^* \longrightarrow k^* \longrightarrow \overline{k}^*$$

sind, besitzen sie eindeutig bestimmte stetige Fortsetzungen zu stetigen Abbildungen

$$\overline{k} \times \overline{k} \longrightarrow \overline{k}$$

bzw.

$$\overline{k}^* \longrightarrow \overline{k}^*$$

Diese Fortsetzungen definieren auf $\overline{k}$ die Struktur eines Körpers. Weil $\mathbb{R}$ vollständig ist, besitzt auch

$$|?|: k \longrightarrow \mathbb{R}$$

eine eindeutig bestimmte Fortsetzung auf $\overline{k}$. Diese Fortsetzung ist eine multiplikative Bewertung von $\overline{k}$. Daraus ergibt sich die Existenzausage von (i).
Zum Beweis der Eindeutigkeitsaussage, reicht es (ii) zu beweisen, denn für je zwei Einbettungen

$$i': k \longrightarrow \overline{k}' \text{ und } i'': k \longrightarrow \overline{k}''$$

wie oben gibt es dann eindeutig bestimmte Fortsetzungen

$$\overline{k}' \longrightarrow \overline{k}'' \text{ und } \overline{k}'' \longrightarrow \overline{k}'$$

deren beide Zusammensetzungen gleich der identischen Abbildung sind.
Zu (ii). Sei

$$k \longrightarrow K$$

eine Einbettung bewerteter Körper, welche die Bewertungen respektiert, wobei K vollständig ist. Dann ist dies eine stetige Abbildung bezüglich der zugehörigen Topologien.

Weil K vollständig ist, gibt es dann eine stetige Fortsetzung auf $\overline{k}$. Wegen der Stetigkeit von Addition und Multiplikation ist diese stetige Fortsetzung ein Homomorphismus von Ringen mit 1.

Weil k dicht liegt in $\overline{k}$, ist die Fortsetzung eindeutig.

Zu (iii). Da das Einselement von k auch das Einselement von $\overline{k}$ ist, folgt der erste Teil der Behauptung aus der Charakterisierung der nicht-archimedischen Bewertungen in 2.1.8: die Ungleichungen

$$|n \cdot 1_k| \leq 1 \text{ für jedes } n \in \mathbb{N}$$

bestehen genau dann in k, wenn sie in $\overline{k}$ bestehen.

Beweisen wir den zweiten Teil. Seien die Bewertungen von k und $\overline{k}$ nicht-archimedisch und sei $x \in \overline{k}$. Wir haben ein $y \in k$ zu finden mit $|x| = |y|$. Dabei können wir annehmen, daß $x \neq 0$, also

$$|x| > 0$$

ist. Weil k dicht liegt in $\overline{k}$, gibt es ein $y \in k$ mit

(1) $$|x-y| < |x|.$$

Außerdem kann man y so wählen, daß der Wert von x-y beliebig nahe bei Null und der von y beliebig nahe bei |x| liegt. Insbesondere kann man

(2) $$|x-y| < |y|.$$

erreichen.
Es reicht zu zeigen, aus (1) und (2) folgt $|x|=|y|$. Aus (1) ergibt sich, da die Bewertung nicht-archimedisch ist,

$$|y| = |(y-x)+x| \leq \max\{|x-y|, |x|\} = |x|.$$

Analog folgt aus (2)

$$|x| = |(x-y) + y| \leq \max\{|x-y|, |y|\} = |y|$$

Zusammen folgt $|x| = |y|$.
QED.

2.3.4 Schwacher Approximationssatz

Seien k ein Körper und

$$|?|_1 , \ldots , |?|_N$$

paarweise nicht-äquivalente Bewertungen von k. Bezeichne

$$\overline{k}_i$$

die Vervollständigung von k bezüglich der i-ten Bewertung $|?|_i$ und

$$\Delta \subseteq \Pi := \prod_{i=1}^{n} \overline{k}_i$$

das Bild von k bei der Diagonaleinbettung

$$k \longrightarrow \prod_{i=1}^{n} \overline{k}_i , \; x \mapsto (x, \ldots , x).$$

Dann liegt Δ dicht im Raum Π.

Bemerkungen

(i) Die obige Aussage läßt sich etwas weniger theoretisch wie folgt formulieren:

Für jede Wahl von N Elementen

$$\alpha_1 \in \overline{k}_1 , \ldots , \alpha_N \in \overline{k}_N$$

und jedes reelle $\varepsilon>0$ gibt es ein $\xi \in k$ mit

$$| \alpha_i - \xi |_i < \varepsilon \text{ für } i = 1, \ldots , N.$$

(ii) Ist $k = \mathbb{Q}$ und sind die $|?|_i$ p-adische Bewertungen, so verwandelt sich die obige Aussage gerade in den chinesichen Restesatz. Letzterer besitzt jedoch noch eine bessere Verallgemeinerung: den starken Approximationssatz.

Beweis von 2.3.4. Da k dicht liegt in jedem der $\overline{k}_i$, d.h. jedes α_i läßt sich beliebig genau durch ein Element aus k, können wir annehmen,

$$\alpha_i \in k \text{ für } i = 1, \ldots , N.$$

1. Schritt: Es reicht zu zeigen, daß es Elemente $\theta_i \in k$ gibt mit

$$| \theta_i |_i > 1 \text{ für alle } i$$

und

$$| \theta_i |_j < 1 \text{ für } i \neq j.$$

Dann gilt nämlich

$$\eta_{i,n} := \frac{\theta_i^n}{1+\theta_i^n} = \frac{1}{1+\theta_i^{-n}} \longrightarrow \begin{cases} 1 \text{ bzgl. der Topologie zu } |?|_i \\ 0 \text{ bzgl. der Topologie zu } |?|_j \text{ mit } j \neq i \end{cases}$$

für $n \longrightarrow \infty$. Für hinreichen größ gewähltes n ist dann aber

$$\xi = \sum_{i=1}^{N} \eta_{i,n} \bullet \alpha_i$$

ein Element der gesuchten Art.

2. Schritt. Existenzbeweis für die θ_i.

Aus Symmetriegründen reicht es die Existenz eines $\theta = \theta_1$ zu beweisen mit

$$|\theta|_1 > 1 \text{ und } |\theta|_i < 1 \text{ für } i = 2, \ldots, N.$$

Wir führen den Beweis durch Induktion nach N. Im Fall N = 2 gibt es, weil $|?|_1$ und $|?|_2$ nicht äquivalent sein sollen ein $\alpha \in k$ mit

$$|\alpha|_1 < 1 \text{ und } |\alpha|_2 \geq 1$$

und analog ein $\beta \in k$ mit

$$|\beta|_1 \geq 1 \text{ und } |\beta|_2 < 1.$$

Dann ist aber $\theta = \beta\alpha^{-1}$ ein Element der gesuchten Art.

Sei jetzt N > 2. Nach Induktionsvoraussetzung gibt es ein $\phi \in k$ mit

$$|\phi|_1 > 1 \text{ und } |\phi|_i < 1 \text{ für } i = 2, \ldots, N\text{-}1.$$

Außerdem ergibt sich aus dem Beweis des Induktionsanfangs die Existenz eines $\psi \in k$ mit

$$|\psi|_1 > 1 \text{ und } |\psi|_N < 1.$$

Wir setzen

$$\theta := \begin{cases} \phi & \text{falls } |\phi|_N < 1 \\ \phi^n\psi & \text{falls } |\phi|_N = 1 \\ \phi^n\psi/(1+\phi^n) & \text{falls } |\phi|_N > 1 \end{cases}$$

Für n hinreichend groß ist dann θ ein Element der gesuchten Art. Man beachte, für $n \longrightarrow \infty$ gilt im letzten Fall bezüglich der i-ten Topologie

$$\frac{\phi^n\psi}{1+\phi^n} \longrightarrow 0 \text{ für } i = 2, \ldots, N\text{-}1$$

und

$$\frac{\phi^n\psi}{1+\phi^n} = \frac{\psi}{1+\phi^{-n}} \longrightarrow \psi \text{ für } i = 1 \text{ und } i = N.$$

QED.

2.3.5 Normierte Vektorräume über bewerteten Körpern

Seien k ein Körper mit der multiplikativen Bewertung

$$|?|: k \longrightarrow \mathbb{R}.$$

und V ein k-Vektorraum. Für die Bewertung gelte die Dreiecksungleichung. Eine Norm auf V ist eine Abbildung

$$\| ? \|: V \longrightarrow \mathbb{R}$$

mit folgenden Eigenschaften.

(i) $\| v \| \geq 0$ für jedes $v \in V$ und $\| v \| = 0 \Leftrightarrow v = 0$.

(ii) $\| v' + v'' \| \leq \|v'\| + \|v''\|$ für $v', v'' \in V$.

(iii) $\|\alpha \bullet v\| = |\alpha| \bullet \|v\|$ für $\alpha \in k$ und $v \in V$.

Zwei Normen $\|?\|_1$ und $\|?\|_2$ auf V heißen äquivivalent, wenn es reelle Konstanten c', c'' gibt mit

$$\|v\|_1 \leq c' \bullet \|v\|_2 \text{ und } \|v\|_2 \leq c'' \bullet \|v\|_1$$

für jedes $v \in V$.

2.3.6 Normierte Vektorräume über vollständigen Körpern

Seien k ein Körper, welcher vollständig ist bezüglich einer multiplikativen Bewertung

$$|?|: k \longrightarrow \mathbb{R},$$

für welche die Dreiecksungleichung gilt, und V ein endlich-dimensionaler k-Vektorraum,

$$\dim_k V < \infty.$$

Dann sind je zwei Normen auf V äquivalent.

Bemerkung

Wir werden später sehen, daß die Forderung der Vollständigkeit wesentlich ist für diese Aussage.

Beweis. Zum Beweis können wir annehmen, daß die Bewertung |?| von k der Dreiecksungleichung genügt. Wir fixieren eine Basis von V, sagen wir $\omega_1, \ldots, \omega_n$,

$$V = k \bullet \omega_1 + \ldots + k \bullet \omega_n.$$

Wir setzen

$$\| \sum_{i=1}^{n} \xi_i \omega_i \|_0 := \max \{ |\xi_i| : i = 1, \ldots, n \}.$$

Auf diese Weise ist auf V eine Norm definiert. Es reicht zu zeigen, jede Norm ||?|| von V ist äquivalent zu dieser Norm. Wir führen den Beweis durch Induktion nach

$$n := \dim_k V.$$

Für n = 1 ist die Aussage trivial: auf Grund des dritten Axioms sind je zwei Normen auf einem 1-dimensionalen Vektorraum proportional. Sei also

$$n > 1.$$

Dann gilt

$$\| \sum_{i=1}^{n} \xi_i \omega_i \| \leq \sum_{i=1}^{n} \| \xi_i \omega_i \| = \sum_{i=1}^{n} |\xi_i| \bullet \|\omega_i\| \leq c' \bullet \| \sum_{i=1}^{n} \xi_i \omega_i \|_0 \qquad (1)$$

mit $c' := \max \|\omega_i\|$.

Nehmen wir an, es gibt kein c'' mit

$$\|v\|_0 \leq c'' \bullet \|v\|.$$

Für jedes reelle $\varepsilon > 0$ gibt es dann ein $v = \sum_{i=1}^{n} \xi_i \omega_i$ mit

$$0 < \| \sum_{i=1}^{n} \xi_i \omega_i \| < \varepsilon \bullet \max \{ |\xi_i| : i = 1, \ldots, n \}$$

(andernfalls könnte man $c'' = 1/\varepsilon$ setzen). Weil die Situation symmetrisch in den Koordinaten ξ_i ist, können wir annehmen,

$$\max \{ |\xi_i| : i = 1, \dots, n \} = |\xi_n|.$$

Indem wir die obige Abschätzung mit $1/|\xi_n|$ multiplizieren, erreichen wir

$$\xi_n = 1.$$

Indem wir ε eine Nullfolge durchlaufen lassen finden wir Elemente $\xi_{i,m} \in k$ mit

$$0 < \| \sum_{i=1}^{n-1} \xi_{i,m} \omega_i + \omega_n \| \longrightarrow 0 \text{ für } m \longrightarrow \infty, \tag{2}$$

also auch

$$0 < \| \sum_{i=1}^{n-1} (\xi_{i,m} - \xi_{i,\ell}) \omega_i \| \longrightarrow 0 \text{ für } m, \ell \longrightarrow \infty,$$

Wir können jetzt die Induktionsvoraussetzung auf den (n-1)-dimensionalen Teilvektorraum

$$k \bullet \omega_1 + \dots + k \bullet \omega_{n-1}$$

anwenden und erhalten

$$|\xi_{i,m} - \xi_{i,\ell}| \longrightarrow 0 \text{ für } m, \ell \longrightarrow \infty.$$

Für i = 1, ... , n-1 bilden also die $\xi_{i,m}$ eine Cauchy-Folge in k. Weil k vollständig ist, gibt es Elemente

$$\xi_i^* \in k$$

mit

$$|\xi_{i,m} - \xi_i^*| \longrightarrow 0 \text{ für } m, \ell \longrightarrow \infty.$$

Wegen (2) und (1) gilt dann

$$\| \sum_{i=1}^{n-1} \xi_i^* \omega_i + \omega_n \| \le \| \sum_{i=1}^{n-1} \xi_{i,m} \omega_i + \omega_n \| + \| \sum_{i=1}^{n-1} (\xi_i^* - \xi_{i,m}) \omega_i \| \longrightarrow 0$$

für $m \longrightarrow \infty$, d.h. es ist

$$\| \sum_{i=1}^{n-1} \xi_i^* \omega_i + \omega_n \| = 0$$

im Widerspruch zum ersten Norm-Axiom.

QED.

2.3.7 Fortsetzung von Bewertungen

Seien K/k eine Körpererweiterung, |?| eine multiplikative Bewertung auf k und ||?|| eine multiplikative Bewertung auf K. Dann heißt ||?|| Fortsetzung von |?|, wenn gilt

$$\|x\| = |x| \text{ für jedes } x \in k.$$

2.3.8 Existenz und Eindeutigkeit der Fortsetzung im vollständigen Fall

Seien k ein Körper, welcher vollständig ist bezüglich einer multiplikativen Bewertung |?| und

$$K/k$$

eine endliche Körpererweiterung des Grades

$$[K:k] = n < \infty.$$

Dann gibt es genau eine Fortsetung ||?|| von |?| auf K. Diese ist gegeben durch

$$\|x\| = \sqrt[n]{N_{K/k}(x)}.$$

Dabei bezeichne $N_{K/k}: K \longrightarrow k$ die Norm der Körpererweiterung K/k.

Beweis. 1. Schritt: Eindeutigkeit.
Zum Beweis können wir annehmen, für |?| gilt die Dreiecksungleichung. Wir betrachten K als endich-dimensionalen k-Vektorraum. Jede Fortsetzung ||?|| der Bewertung von k ist dann eine Norm dieses Vektorraums im Sinne von 2.3.5. Weil k vollständing ist, sind je zwei Fortsetzungen $\|?\|_1$ und $\|?\|_2$ der Bewertung von k als Normen äquivalent (nach 2.3.6). Insbesondere induzieren die beiden Fortsetzungen auf K dieselbe Topologie. Nach 2.3.2 sind sie dann aber äquivalent, d.h.

$$\|?\|_2 = \|?\|_1^c$$

Da die beiden Bewertungen dieselbe Bewertung |?| von k fortsetzen, gilt

$$\|\alpha\|_2 = \|\alpha\|_1$$

für jedes $\alpha \in k$. Deshalb ist c = 1 (es sei denn beide Bewertungen sind trivial, so daß man c = 1 annehmen kann).

Bemerkung
Die gerade bewiesene Eindeutigkeitsaussage ist gerade die Aussage von 2.2.5. Damit ist die Lücke im Beweis des Satzes 2.2.4 von Gelfand-Tornheim hinsichtlich des Vergleichs der Bewertungen geschlossen.

2. Schritt: Existenz.
1. Fall: die Bewertung |?| von k ist nicht-archimedisch.

Wir beschränken uns hier auf den Fall, daß die Bewertung

$$|?|: k \longrightarrow \mathbb{R}$$

diskret ist.[51] Den Beweis des allgemeinen Falls[52] findet man in

> E. Artin: Theory of algebraic numbers, Striker, Göttingen 1956
> N. Bourbaki: Algèbre Commutative, Chapitre 6. Valuations, Hermann, Paris 1964

Sei also |?| eine diskrete nicht-archimedische Bewertung. Dann ist

$$\mathcal{O} := \{x \in k : |x| \leq 1\}$$

ein diskreter Bewertungsring mit dem Bewertungsideal

$$\wp := \{x \in k: |x| < 1\},$$

welches ein Hauptideal ist,

$$\wp = \pi\mathcal{O}$$

(nach 2.17). Bezeichne

$$v: k^* \twoheadrightarrow \mathbb{Z}$$

die zugehörige additive Bewertung. Dann gilt nach 2.1.14:

$$|x| = \rho^{v(x)} \text{ für jedes } x \in k$$

---

[51] Wir brauchen die Aussage, daß die ganze Abschließung in K eines Dedekind-Rings R mit dem Quotientenkörper k ein Dedekind-Ring S mit dem Quotientenkörper K ist, d.h. wir müssen noch annehmen, daß die Erweiterung K/k separabel ist (siehe 1.9.3 und Bemerkung 1.9.1(ii)).
[52] Man muß allgemeinere multiplikative Bewertungen betrachten, deren Werte nicht notwendig in $\mathbb{R}$ liegen bzw. Bewertungsringe, die nicht-notwendig noethersch sind.

mit $\rho := |\pi|$ (< 1). Sei

$$S \subseteq K$$

die ganze Abschließung von $\mathcal{O}$ in K. Dann ist S ein Dedekind-Ring (vgl. 1.9.3 bzw. Bemerkung 1.9.1 (ii)). Sei

$$q \subseteq S$$

ein maximales über $\mathfrak{p}$ liegendes Ideal von S. Dann ist

$$\mathcal{O}_K := S_q$$

ein diskreter Bewertungsring. Für die zugehörige additive Bewertung

$$v_K K^* \twoheadrightarrow \mathbb{Z}$$

gilt

$$v_K(x) = e \bullet v(x) \text{ für jedes } x \in k,$$

wenn e den Verzweigungsindex von v_K über v bezeichnet (d.h. wenn sich der Paramter π von v in der Gestalt

$$\pi = u \bullet \pi_K^e$$

schreiben läßt mit einer Einheit u von $\mathcal{O}_K$ und einem Parameter π_K von v_K. Wir betrachten die folgende multiplikative Bewertung von K.

$$\|x\| := \rho^{\frac{1}{e} v_K(x)} = \sqrt[e]{\rho}^{v_K(x)}.$$

Für jedes $x \in k$ gilt

$$\|x\| = \rho^{\frac{1}{e} v_K(x)} = \rho^{v(x)} = |x|,$$

d.h. ||?|| ist die gesuchte Fortsetzung von |?|.

2. Fall: die Bewertung |?| ist archimedisch.
Nach dem Satz von Gelfand-Tornheim 2.2.4 ist k ein Teilkörper von $\mathbb{C}$,

$$k \subseteq \mathbb{C}$$

und |?| ist die Einschränkung des Absolutbetrags auf k. Weil $\mathbb{C}$ algebraisch abgeschlossen ist, können wir K mit einem Teilkörper von $\mathbb{C}$ identifizieren (als Körper über k),

$$k \subseteq K \subseteq \mathbb{C}.$$

Die Einschränkung des Absolutbetrags von $\mathbb{C}$ auf K liefert dann die gesuchte Fortsetzung von |?|.
3. Schritt: Beweis der Formel für die Fortsetzung.
Sei L/k eine normale Körpererweiterung von k, welche den Körper K als Teilkörper enthält und seien

$$\sigma_i : K \longrightarrow L,\ i = 1, \ldots, n := [K:k],$$

die k-Einbettungen von K in L (mit geeigneten Vielfachheiten gezählt). Dann gilt

$$N_{K/k}(x) = \sigma_1(x) \bullet \ldots \bullet \sigma_n(x),$$

Für die Fortsetzung |||?||| von ||?|| gilt dann

$$| N_{K/k}(x) | = ||| N_{K/k}(x) ||| = ||| \sigma_1(x) ||| \bullet \ldots \bullet |||\sigma_{[K:k]}(x)|||.$$

Weil L/k normal ist, lassen sich die Einbettungen σ_i auf L fortsetzen und damit als k-Automorphismen von L aufffassen. Die Komposition von σ_i mit |||?||| ist eine

multiplikative Bewertung von L, welche |?| fortsetzt. Wegen der obigen Eindeutigkeitsaussage stimmt diese Komposition mit |||?||| überein. Insbesondere gilt

$$||| \sigma_i (x) ||| = ||| x ||| \text{ für jedes } x \in L.$$

Einsetzen in die obige Identität liefert

$$| N_{K/k}(x) | = ||| x |||^n = ||x||^n,$$

also

$$||x|| = \sqrt[n]{N_{K/k}(x)}$$

QED.

2.3.9 Folgerung: Vergleich mit der Maximum-Bewertung

Seien K/k eine endliche Körpererweiterung und |?| eine Bewertung von K. Der Körper k sei vollständig bezüglich der Einschränkung von |?| auf k. Weiter sei

$$\omega_1 , \dots , \omega_n \in K$$

eine Vektorraumbasis von K über k.

Dann gibt es nicht-negative reelle Konstanten

$$c', c''$$

mit

$$c' \le \frac{| \sum_{i=1}^{n} \alpha_i \omega_i |}{\max \{|\alpha_i|: i=1,\dots,n\}} \le c''$$

für beliebige $\alpha_i \in k$, die nicht sämtlich gleich Null sind.

Beweis. Durch

$$| \sum_{i=1}^{n} \alpha_i \omega_i | \text{ und } \max \{|\alpha_i| : i = 1, \dots , n\}$$

sind zwei Normen des k-Vektorraums K gegeben. Weil k vollständig ist, sind diese beiden Normen äquivalent (nach 2.3.6).
QED.

2.3.10 Folgerung: Vollständigkeit der Erweiterung

Seien k ein vollständiger bewerteter Körper und K/k eine endliche Körpererweiterung. Dann ist K vollständig bezüglich der eindeutig bestimmten Bewertung, welche die von k fortsetzt.
Beweis. Auf Grund der vorangehenden Aussage 2.3.9 besitzt K die Topologie eines endlich-dimensionalen Vektorraums über k , d.h. Konvergenz bedeutet koodinatenweise Konvergenz.
QED.

Bemerkung

Wir haben damit die Frage nach der Fortsetzbarkeit multiplikativer Bewertungen im Fall vollständiger Bewertungen abgehandelt. Im Rest dieses Abschnitts wollen wir uns mit der Frage beschäftigen, wie die Situation im Fall nicht notwendig vollständiger Körper ist, d.h. wir betrachten eine endliche separable Körpererweiterung K/k eines bewerteten Körpers k und fragen nach den Fortsetzung der Bewertung auf K. Zur Beantwortung der Frage führen wir die Vervollständigung $\overline{k}$ von k ein und müssen zunächst das Tensorprodukt

$$K \otimes_k \overline{k}$$

betrachten.

2.3.11 Das Tensorprodukt von Körpererweiterungen

Seien K/k eine endliche separable und L/k eine beliebige Körpererweiterung. Dann ist das Tensorprodukt

$$K\otimes_k L$$

ein kommutativer Ring mit 1, welcher in ein direktes Produkt von endlichen Körpererweiterungen von L zerfällt, sagen wir[53]

$$K\otimes_k L \cong L_1\times\ldots\times L_r\ .$$

Als Körper über k und L sind die L_i paarweise isomorph und gleich dem Kompositum von K und L ,

$$L_i \cong K\bullet L.$$

Für $\alpha\in K$ bezeichne

$$\chi_\alpha \in k[x]\ ,\ \chi_{i,\alpha} \in L_i[x]$$

das Charakteristische Polynom[54] von α bezüglich K/k bzw. L_i/L. Dann gilt

$$\chi_\alpha = \chi_{1,\alpha}\bullet\ldots\bullet\ \chi_{r,\alpha}.$$

Insbesondere gilt für Norm und Spur

$$N_{K/k}(\alpha) = \prod_{i=1}^{r} N_{L_i/L}(\alpha)$$

und

$$Tr_{K/k}(\alpha) = \sum_{i=1}^{r} Tr_{L_i/L}(\alpha)$$

Beweis. Nach dem Satz vom primitiven Element ist K/k als separable Körpererweiterung einfach, d.h. es gilt

$$K = k(\beta)$$

für ein $\beta\in K$. Sei

$$f \in k[x],\ f(\beta) = 0,$$

das Minimalpolynom von α über k. Wir betrachten die Zerlegung von f in irreduzible Faktoren über L , sagen wir

$$f = (g_1)^{e_1}\bullet\ldots\bullet(g_r)^{e_r} \text{ mit } g_i \in L[x] \text{ normiert und irreduzibel.}$$

Man beachte, weil der höchste Koeffizient von f gleich 1 ist, können wir dasselbe auch von den g_i annehmen. Weil K/k nach Voraussetzung separabel ist, d.h. f besitzt keine mehrfachen Nullstellen, erhalten wir

$$e_1 = \ldots = e_r = 1.$$

Weil die g_i nach Konstruktion teilerfremd sind, gilt

$$K\otimes_k L \cong k[x]/(f)\otimes_k L \qquad \text{(nach Definition von } \alpha \text{ und f)}$$

---

[53] Auf der rechten Seite stehe die direkte Summe der L-Moduln L_i , welche mit der koordinatenweisen Multiplikation versehen sei. Die Anzahl der direkten Summanden muß endlich sein, weil auf der linken Seite ein endlich-dimensionaler L-Vektorraum steht.

[54] d.h. das charakteristische Polynom der Multiplikation mit α bezüglich der Vektorräume K bzw. L_i über k bzw. L.

$$\cong L[x]/(f) \qquad (\otimes \text{ kommutiert mit } \oplus)$$
$$= L[x]/(g_1 \bullet ... \bullet g_r)$$
$$\cong L[x]/(g_1) \times ... \times L[x]/(g_r) \quad \text{(Chinesischer Restesatz)}$$
$$= L_1 \times ... \times L_r$$

mit $L_i := L[x]/(g_i)$. Dies ist ein Isomorphismus von L-Algebren, wenn man L als Teilkörper der Tensorprodukts bezüglich der natürlichen Einbettung

$$L \longrightarrow K \otimes_k L \,,\ c \mapsto 1 \otimes c,$$

auffaßt[55]. Analog können wir auch K bezüglich der Einbettung

$$K \longrightarrow K \otimes_k L,\ c \mapsto c \otimes 1,$$

als Teilkörper des Tensorprodukts auffassen. Entsprechend sind die L_i auch Körpererweiterungen von K.

Bezeichne

$$\beta_i \in L_i \,,\ g_i(\beta_i) = 0,$$

die Restklasse von x in L_i. Dann ist der obige Isomorphismus von L-Algebren gegeben durch

$$K \otimes_k L \cong \overline{k}[x]/(f) \longrightarrow L_1 \times ... \times L_r$$
$$\beta = \beta \otimes 1 \mapsto x \bmod (f) \mapsto (x \bmod g_1, \ ... \ , x \bmod g_r) = (\beta_1 \ , ... \ , \beta_r).$$

Man beachte, als Algebra über L wird das Tensorprodukt von $\beta = \beta \otimes 1$ erzeugt. Die Abbildung ist somit durch das Bild von α bereits festgelegt. Die Zusammensetzung

$$K \otimes_k L \longrightarrow L_i$$

mit der Projektion auf den i-ten Faktor ist bis auf Isomorphie gerade die natürliche Abbildung $L[x]/(f) \twoheadrightarrow L[x]/(g_i)$ und ist als solche surjektiv. Damit ist

$$L_i = \text{Bild von } K \otimes_k L$$
$$= \{ \text{ Bild von } \sum_i c_i \otimes d_i \mid c_i \in K \,,\ d_i \in L \}$$
$$= \{ \text{ Bild von } \sum_i c_i d_i \mid c_i \in K \,,\ d_i \in L \}$$
$$`= K \bullet L \qquad \text{(Kompositum von K und L)}$$

Es bleibt noch die Aussage hinsichtlich der charakteristischen Polynome von $\alpha \in K$ zu beweisen. Dazu fixieren wir eine Basis von K über k, sagen wir

$$K = k \bullet \omega_1 + ... + k \bullet \omega_n \quad , n = \dim_k K.$$

Mit

$$\alpha \bullet \omega_i = \sum_{j=1}^{n} a_{ij} \omega_j$$

gilt dann

---

[55] Dies ist ein Homomorphismus von kommutativen Ringen mit 1. Weil L ein Körper ist, ist dieser injektiv.

$$\chi_\alpha = \det(x \bullet \delta_{ij} - a_{ij})$$

(vgl. 1.7.2). Nun bilden die $\omega_i \otimes 1$ aber auch eine Basis von $K \otimes_k L$ über L und es ist

$$\alpha \bullet \omega_i \otimes 1 = \sum_{j=1}^{n} a_{ij} \omega_j \otimes 1,$$

d.h. χ_α ist auch das charakteristische Polynom von α bezüglich des L-Vektorraums $K \otimes_k L$. Wir betrachten K als Teilkörper von $K \otimes L = L_1 \times ... \times L_r$ und schreiben

$$\alpha = (\alpha_1, ..., \alpha_r) \text{ mit } \alpha_i \in L_i$$

Die Multiplikation mit α stimmt für Elemente von L_i mit der Multiplikation von α_i überein, d.h.

$$\chi_{i,\alpha} = \chi_{\alpha_i}.$$

Die Matrix $M(\alpha)$ der Multiplikation mit α auf $L_1 \times ... \times L_r$ hat somit die Gestalt

$$M(\alpha) = \begin{pmatrix} M(\alpha_1) & 0 & .. & 0 \\ 0 & M(\alpha_2) & .. & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & M(\alpha_r) \end{pmatrix}$$

bezüglich einer Basis, die mit der Zerlegung $K \otimes L = L_1 \times ... \times L_r$ verträglich ist. Damit gilt

$$\chi_\alpha = \det(x \bullet Id - M(\alpha)) = \prod_{i=1}^{r} \det(x \bullet Id - M(\alpha_i)) = \prod_{i=1}^{r} \chi_{\alpha_i} = \prod_{i=1}^{r} \chi_{i,\alpha} .$$

QED.

2.3.12 Die Fortsetzung von Bewertungen auf endliche separable Erweiterungen

Sei K/k eine endliche separable Körpererweiterung des (nicht notwendig vollständigen) bewerteten Körpers k des Grades

$$n := [K:k].$$

Dann gibt es (mindestens eine und) höchstens n Fortsetzungen der Bewertung |?| von k auf K, sagen wir

$$\|?\|_1 , ... , \|?\|_r : K \longrightarrow \mathbb{R} \quad (r \le n).$$

Seien

$$\overline{k} , \overline{K}_1 , ... , \overline{K}_r$$

die Vervollständigungen von k und K bezüglich |?| bzw. $\|?\|_1 , ... , \|?\|_r$. Dann besteht ein Isomorphismus

$$K \otimes_k \overline{k} \cong \overline{K}_1 \times ... \times \overline{K}_r ,$$

welcher sowohl ein Isomorphismus im allgebraischen Sinne[56] ist als auch einer im topologischen Sinne[57].

---

[56] d.h. ein Isomorphismus von kommutativen Ringen mit 1.

Beweis. Wir bezeichnen die eindeutig bestimmte Fortsetzung der Bewertung |?| von k auf die Vervollständigung $\overline{k}$ ebenfalls mit |?|,

$$|?|: \overline{k} \longrightarrow \mathbb{R}.$$

Nach 2.3.11 wissen wir, es gilt

$$K\otimes_k \overline{k} \cong L_1\times\ldots\times L_r \qquad (1)$$

mit endlichen Körpererweiterungen L_i von $\overline{k}$. Weil $\overline{k}$ vollständig ist, gibt es für jedes i genau eine Bewertung

$$\|?\|_i: L_i \longrightarrow \mathbb{R} \qquad (2)$$

welche die gegebene Bewertung |?| von $\overline{k}$ fortsetzt. Nun können wir wegen (1) den Körper K mit einem Teilkörper von L_i identifizieren. Die Einschränkung von (2) auf K liefert eine Bewertung von K, welche wir ebenfalls mit $\|?\|_i$ bezeichnen,

$$\|?\|_i: K \longrightarrow \mathbb{R} \qquad (3)$$

Weil k dicht liegt in $\overline{k}$, liegt auch $K = K\otimes_k k$ dicht in $K\otimes_k \overline{k} = L_1\times\ldots\times L_r$, also liegt K erst recht dicht in L_i (für jedes i). Mit anderen Worten,

$$L_i = \overline{K}_i$$

ist gerade die Vervollständigung von K bezüglich der Bewertung $\|?\|_i$ von K. Wir haben noch zu zeigen, daß die Bewertungen $\|?\|_i$ paarweise verschieden sind und daß sie die einzigen Fortsetzungen von |?| auf K sind.[58]

Sei

$$\|?\|: K \longrightarrow \mathbb{R} \qquad (4)$$

irgendeine Fortsetzung der Bewertung |?| von k auf K. Wir können annehmen, daß für sie die Dreiecksungleichung gilt.[59]

Weil $K = K\otimes_k k$ dicht liegt in $K\otimes_k \overline{k}$ können wir die stetige Funktion (4) auf genau eine Weise fortsetzen zu einer stetigen Funktion auf $K\otimes_k \overline{k}$. Wir bezeichnen diese Fortsetzung ebenfalls mit ||?||,

$$\|?\|: K\otimes_k \overline{k} \longrightarrow \mathbb{Z}.$$

Für diese Fortsetzung gilt dann

$$\| x + y \| \leq \| x \| + \| y \| \text{ für } x, y \in K\otimes_k \overline{k}$$

$$\| x\bullet y \| = \|x\| \bullet \|y\| \text{ für } x, y \in K\otimes_k \overline{k}$$

---

[57] d.h. ein Isomorphismus von topologischen Räumen. Dabei werde das Tensorprodukt links als normierter Vektorraum über dem bewerteten Körper $\overline{k}$ angesehen (mit der zugehörigen und eindeutig bestimmten Topologie, die zum Beispiel von der Maximumsnorm bezüglich irgendeiner Basis kommt). Der Vektorraum rechts werde mit der Produkt-Topologie versehen.

[58] Die Gleichheit der Topologien von $K\otimes_k \overline{k}$ und $L_1\times\ldots\times L_r$ ergibt sich aus der Äquivalenz von je zwei Normen dieser endlich-dimensionalen $\overline{k}$-Vektorräume über dem vollständigen Körper $\overline{k}$ (vgl. 2.3.6).

[59] Durch Ersetzung von |?| und ||?|| durch die c-ten Potenzen für ein geignetes c. Später können wir dann wieder zu den ursprünglicnen Potenzen übergehen.

Wir betrachten die Einschränkung von ||?|| auf einen der Körper L_j. Wie wir gerade bemerkt haben, genügt die Funktion ||?|| auf L_j zweien der drei Axiome für eine multiplikative Bewertung auf L_j (vgl. 2.1.1). Untersuchen wir, wie es sich mit dem verbleibenden Axiom verhält.

Falls es ein $\alpha \in L_j$ gibt mit $\|\alpha\| \neq 0$, so gilt für jedes $\beta \in L_j - \{0\}$

$$\|\alpha\| = \|\alpha\beta^{-1}\| \bullet \|\beta\|,$$

d.h. es ist $\|\beta\| \neq 0$ für jedes von Null verschiedene β aus L_j. Wir haben gezeigt,

$$\| ? \| \text{ ist entweder identisch Null auf } L_j \text{ oder eine Bewertung auf } L_j$$

Nach Konstruktion ist $\| ? \|$ auf mindestens einem L_j nicht identisch Null (weil ||?|| nicht identisch Null ist auf dem Tensorprodukt)[60], also eine Bewertung auf L_j, welche nach Konstruktion die Bewertung |?| fortsetzt. Also ist $\| ? \| = \| ? \|_j$ auf L_j. Wir haben gezeigt, jede Fortsetzung von |?| auf K stimmt mit einem der $\|?\|_j$ überein.

Wir haben nocht zu zeigen, die $\|?\|_j$ sind paarweise verschieden. Man beachte, $\|?\|_j$ ist eine Fortsetzung, die auf L_j nicht identisch Null ist. Es reicht somit zu zeigen, die Fortsetzung ||?|| der eben betrachteten allgemeinen Bewertung kann nicht auf zwei verschiedenen Faktoren L_j ungleich Null sein.[61] Angenommen ||?|| ist auf $L_{j'}$ und $L_{j''}$ nicht identisch Null (mit $j' \neq j''$). Für $\alpha' \in L_{j'} - \{0\}$ und $\alpha'' \in L_{j''} - \{0\}$ gilt dann

$$\begin{aligned} 0 \neq \|\alpha'\| \bullet \|\alpha''\| &= \|\alpha' \bullet \alpha''\| \\ &= \|(0\ldots,0,\alpha',0,\ldots) \bullet (0,\ldots,0,\alpha'',0,\ldots)\| \\ &=^{62} \|(0, \ldots, 0)\| \\ &= 0, \end{aligned}$$

ein Widerspruch.
QED.

---

[60] Wäre ||?|| identisch Null auf jedem L_j, so wäre wegen $\| x + y \| \leq \|x\| + \|y\|$, d.h.

$$\| (x_1, \ldots, x_r) \| \leq \sum_{i=1}^{r} \| (0, \ldots, 0, x_i, 0, \ldots, 0) \|$$

die Funktion ||?|| identisch Null auf dem direkten Produkt der L_j.

[61] Wenn zwei der $\|?\|_j$ auf K übereinstimmen, sagen wir $\|?\|_j$, und $\|?\|_{j''}$, so liefern deren eindeutig bestimmte Fortsetzungen auf das Tensorprodukt eine Funktion, die auf mindestens zwei verschiedenen L_j nicht identisch Null sind. Man beachte durch

$$\| (x_1, \ldots, x_r) \| := \max \{ \|x_j\|_j, \|x_{j''}\|_{j''} \}$$

ist dann eine stetige Funktion gegeben, welche $\|?\|: K \longrightarrow \mathbb{R}$ fortsetzt, auf $L_{j'}$ gleich $\|?\|_j$, und auf $L_{j''}$ gleich $\|?\|_{j''}$ ist, d.h. dies ist die eindeutig bestimmte Fortsetzung.

[62] die beiden von Null verschiedenen Koordinaten befinden sich an unterschiedlichen Positionen. Das Produkt bezüglich der koordinatenweisen Multiplikation liefert somit in allen Positionen die Null.

2.3.13 Ganze Abschließung diskreter Bewertungsringe im vollständigen Fall

Seien R ein vollständiger diskreter Bewertungsring mit dem Quotientenkörper K und L/K eine endliche separable Körpererweiterung. Dann ist die ganze Abschließung S von R in L ein diskreter Bewertungsring (mit dem Quotientenkörper L).

Beweis. Jedenfalls ist S ein Dedekindring (nach 1.9.3). Jedes maximale Ideal von S liegt über dem einzigen maximalen Ideal von R (ebenfalls nach 1.9.3). Je zwei dieser Ideale definieren paarweise verschiedene Fortsetzungen der Bewertung von K auf L. Wegen der Eindeutigkeit der Fortsetzung (nach 2.3.8) besitzt S nur ein maximales Ideal. Dann stimmt aber S mit der Lokalisierung bezüglich dieses maximalen Ideals überein, d.h. S ist ein diskreter Bewertungsring.

QED.

Bemerkung

Wir haben damit die Beweise aller Aussagen, die wir über die Fortsetzung von Bewertungen beweisen wollten, abgeschlossen. Bevor wir uns wieder der Frage nach dem Verhalten einer Primzahl beim Übergang in einen größeren Ring von ganzen Zahlen zuwenden, wollen wir hier noch einen Fall von besonderen Interessen untersuchen, nämlich den Fall von bewerteten Körpern, deren Bewertungsringe einen endlichen Restklassenkörper besitzten. Man beachte, im Fall

$k = \mathbb{Q}$

$|?|$ = p-adische Bewertung (p prim)

ist der Bewertungsring gleich

$\mathbb{Z}_{(p)}$

das Bewertungsideal gleich

$p\,\mathbb{Z}_{(p)}$

und der Restklassenkörper gleich

$\mathbb{Z}_{(p)}/p\,\mathbb{Z}_{(p)} \cong \mathbb{Z}/(p)$,

d.h. letzterer ist endlich. Dasselbe gilt, wenn man $k = \mathbb{Q}$ durch eine endliche Körpererweiterung von $\mathbb{Q}$ ersetzt.

2.4 Bewertete Körper mit endlichem Restklassenkörper

2.4.1. Lokale Kompaktheit im vollständigen Fall

Sei k ein Körper mit einer nicht-archimedischen diskreten Bewertung

$$|?|: k \longrightarrow \mathbb{R}.$$

Weil die Bewertung nicht-archimedisch ist, ist der Ring der ganzen Elemente

$$\mathfrak{O} = \mathfrak{O}_k := \{x \in k : |x| \leq 1\}$$

ein wohldefinierter kommuativer Ring mit 1 (vgl. 2.1.7 (ii)). Sein einziges maximales Ideal ist das Bewertungsideal

$$\mathfrak{p} := \{\alpha \in k \mid |\alpha| < 1\}$$

(vgl. 2.1.7 (iv)). Weil die Bewertung diskret ist, ist diese ein Hauptideal,

$$\mathfrak{p} = \pi\mathfrak{O}$$

(vgl. 2.1.7 (v))[63]. Wir nehmen jetzt zusätzlich an, der Restklassenring

$$\kappa := \mathfrak{O}/\mathfrak{p}$$

ist endlich,

$$\#\,\kappa < \infty.$$

---

[63] d.h. $\mathfrak{O}$ ist ein diskreter Bewertungsring (auf Grund des Krullschen Durchschnittssatzes).

Falls in der beschriebenen Situation der Körper k vollständig ist bezüglich der gegebenen Bewertung, so ist der Ring der ganzen Zahlen

$$\mathcal{O} \text{ kompakt,}$$

d.h. der Körper k ist lokal kompakt.[64]

Beweis.

1. Schritt: Der Ring der ganzen Zahlen $\mathcal{O}$ besteht gerade aus denjenigen Elementen $\alpha \in k$, die sich in der Gestalt

$$\alpha = \sum_{j=0}^{\infty} \alpha_j \pi^j$$

als Reihe darstellen lassen, wobei die α_j in einem vorgegebenen Repräsentantensystem

$$\Sigma \subseteq \mathcal{O}$$

von $\kappa = \mathcal{O}/\wp$ liegen.

Jede der Reihen konvergiert gegen ein Element von $\mathcal{O}$:

Wegen $\sum_{j=n}^{N} \alpha_j \pi^j = \pi^n \cdot \sum_{j=0}^{N} \alpha_{j+n} \pi^j \in \pi^n \mathcal{O}$ lassen sich die Partialsummen für n hinreichend groß beliebig klein machen, d.h. die Reihen der angegebenen Gestalt konvergieren in k. Weil die Partialsummen in $\mathcal{O}$ liegen, d.h. einen Betrag ≤ 1 haben, gilt dasselbe für deren Limites.

Jedes Element von $\mathcal{O}$ ist Limes einer Reihe der angegebenen Gestalt:

Für vorgegebenes $a \in \mathcal{O}$ gibt es genau ein $\alpha_0 \in \Sigma$ mit

$$|a - \alpha_0| < 1.$$

d.h. mit $a - \alpha_0 \in \pi\mathcal{O}$. Es folgt

$$a' := \pi^{-1}(a - \alpha_0) \in \mathcal{O},$$

d.h. es gibt genau ein $\alpha_1 \in \Sigma$ mit

$$|a' - \alpha_1| < 1,$$

d.h. $a' - \alpha_1 \in \pi\mathcal{O}$, d.h.

$$a - \alpha_0 - \alpha_1\pi = (a' - \alpha_1)\cdot\pi \in \pi^2\mathcal{O}.$$

Durch Wiederholen der Argumentation erhalten wir eine Folge von Elementen

$$\alpha_i \in \Sigma$$

mit

$$a - \sum_{i=0}^{n} \alpha_i \pi^i \in \pi^{n+1}\mathcal{O}$$

für jedes n. Für $n \longrightarrow \infty$ erhalten wir $a = \sum_{i=0}^{\infty} \alpha_i \pi^i$.

2. Schritt: $\mathcal{O}$ ist kompakt.

---

[64] d.h. jedes Element $x \in k$ besitzt die relativ kompakte Umgebung $x + \mathcal{O}$.

Sei $\{U_\lambda\}_{\lambda\in\Lambda}$ eine offene Überdeckung von $\mathcal{O}$. Wir müssen zeigen, es gibt eine endliche Teilfamilie, welche $\mathcal{O}$ ebenfalls überdeckt. Angenommen, dies ist nicht der Fall.

Sei

$$\Sigma \subseteq \mathcal{O}$$

ein Repräsentantensystem von $\kappa = \mathcal{O}/\pi\mathcal{O}$. Weil κ nach Voraussetzung endlich ist, ist Σ ebenfalls endlich. Nach Wahl von Σ ist $\mathcal{O}$ Vereinigung der endlich vielen Mengen

$$a + \pi\mathcal{O} \text{ mit } a \in \Sigma. \tag{1}$$

Dann wird mindestens eine dieser Mengen, sagen wir

$$\alpha_0 + \pi\mathcal{O},\ \alpha_0 \in \Sigma, \tag{2}$$

nicht von endlich vielen der U_λ überdeckt. Wir multiplikzieren (1) mit π, addieren α_0 und sehen so[65], die Menge (2) ist Vereinigung der endlich vielen Mengen

$$\alpha_0 + a\pi + \pi^2\mathcal{O} \text{ mit } a \in \Sigma. \tag{3}$$

Mindestens eine von ihnen kann nicht von endlich vielen der U_λ überdeckt werden, sagen wir

$$\alpha_0 + \alpha_1\pi + \pi^2\mathcal{O} \text{ mit } \alpha_1 \in \Sigma.$$

Wir können jetzt (1) mit π^2 multiplizieren und $\alpha_0 + \alpha_1\pi$ addieren. Wiederholen der Argumentation liefert eine eine Folge von ineinanderliegenden Mengen

$$\sum_{i=0}^{n-1} \alpha_i\pi^i + \pi^n\mathcal{O} \text{ mit } \alpha_i \in \Sigma, \tag{4}$$

welche nicht von endlich vielen der U_λ überdeckt werden. Sei

$$\alpha := \sum_{i=0}^{\infty} \alpha_i\pi^i \in \mathcal{O}$$

Dann gilt $\alpha \in U_\lambda$ für mindestens ein λ. Weil U_λ offen ist, gibt es eine ganze ε-Umgebung von α, welche ganz in U_λ liegt, d.h.

$$\alpha + \pi^n\mathcal{O} \subseteq U_\lambda$$

Das steht aber im Widerspruch zu der Tatsache, daß die Menge (4) nach Konstruktion nicht von endlich vielen der U_λ überdeckt werden kann.

QED.

2.4.2 Charatkerisierung der lokal kompakten bewerteten Körper

(i) Die Umkehrung der eben bewiesenen Aussage ist ebenfalls richtig:

Ist k ein lokal kompakter Körper bezüglich einer nicht-archimedischen Bewertung von k, so gilt

1. k ist vollständig.
2. Der Restklassenkörper des Bewertungsrings ist endlich.

---

[65] Die $a + \pi\mathcal{O}$ überdecken $\mathcal{O}$. Also überdecken die $\alpha_0 + a\pi + \pi^2\mathcal{O}$ die Menge $\alpha_0 + \pi\mathcal{O}$.

3. Die Bewertung ist diskret.
4. $\mathcal{O}$ ist kompakt.

(ii) Ist k lokal kompakt bezüglich einer archimedischen Bewertung von k so ist $k = \mathbb{R}$ oder $k = \mathbb{C}$ und $|?|$ ist äquivalent zum Absolutbetrag.

Beweis. Zu (i). Sei $U \subseteq k$ eine relativ kompakte Umgebung der Null. Dann enthält U eine ε-Umgebung der Null. Für ein von Null verschiedenes Element $x \in \wp - \{0\}$ aus dem Bewertungsideal gilt dann

$$x^v\mathcal{O} \subseteq U$$

für hinreichend großes v. Nun ist die Menge

$$x^v\mathcal{O} = \{y \in k : |y/x^v| \leq 1\} = \{y \in k : |y| \leq |x|^v\}$$

abgeschlossen, also als Teilmenge der kompakten Mengen $\overline{U}$ komakt. Also ist

$$\mathcal{O} \text{ kompakt,}$$

d.h. es gilt 4. Weil die Topologie von k von einer Metrik kommt, ist $\mathcal{O}$ insbesondere Folgen-kompakt, d.h. jede Cauchy-Folge in $\mathcal{O}$ ist konvergent.[66]
Sei jetzt $\{x_n\}_{n=1,2,..}$ eine Cauchy-Folge in k. Dann gibt es ein n_0 mit

$$|x_n - x_{n_0}| \leq 1 \text{ für alle } n \geq n_0$$

d.h. $\{ x_n - x_{n_0} \}_{n=n_0,n_0+1,..}$ ist eine Cauchy-Folge in $\mathcal{O}$ und als solch konvergent. Dann ist aber auch $\{x_n\}_{n=1,2,..}$ konvergent. Wir haben gezeigt, k ist vollständig, d.h. es es gilt die Aussage 1.

Sei $\{a_\lambda\}_{\lambda\in\Lambda}$ ein Repräsentantensystem von $\kappa = \mathcal{O}/\wp$ in $\mathcal{O}$. Betrachten wir die Zerlegung

$$\mathcal{O} = \bigcup_{\lambda\in\Lambda} (a_\lambda + \wp) \qquad (1)$$

von $\mathcal{O}$ in die paarweise disjunkten Mengen

$$a_\lambda + \wp = \{x \in k : |x - a_\lambda| < 1\}.$$

Dies ist eine Zerlegung in offene Teilmengen, wobei man keine der Mengen weglassen kann. Weil $\mathcal{O}$ kompakt ist, muß die Zahl der offenen Mengen endlich sein, d.h. die Indexmenge Λ ist endlich, d.h.

$$\#\kappa = \#\Lambda < \infty.$$

Damit ist Aussage 2 bewiesen. Wir haben noch zu zeigen, daß die Bewertung diskret ist.

Wie wir gerade gesehen haben, ist die Zerlegung (1) eine (endliche) Zerlegung in paarweise disjunkte offene Teilmengen. Insbesondere ist das Ideal $\wp$ (welches in dieser Zerlegung vorkommt) das Komplement in $\mathcal{O}$ der Vereinigung von offenen Mengen. Also ist $\wp$ eine abgeschlossene Teilmenge der kompakten Menge $\mathcal{O}$, also ist

$$\wp \text{ kompakt.}$$

Wir setzen

---

[66] Es reicht zu zeigen, jede nicht-stationäre Cauchy-Folge besitzt mindestens einen Häufungspunkt. Sei $\{x_n\}$ eine nicht-stationäre Cauchy-Folge von $\mathcal{O}$ ohne Häufungspunkt. Jeder Punkt $x\in\mathcal{O}$ besitzt dann eine Umgebung $U_x \subseteq \mathcal{O}$, die nur endlich viele x_n enthält. Endlich viele der U_x überdecken $\mathcal{O}$. Also gibt es nur endlich viele paarweise verschiedene x_n. Die Folge ist stationär.

$$S_n := \{x \in k : |x| < 1 - \frac{1}{n}\}.$$

Die Mengen S_n mit n = 2, 3, ... bilden eine offene Überdeckung von $\wp$. Weil $\wp$ kompakt ist, gibt es ein n mit

$$\wp = S_n$$

Für $x \in \mathcal{O}$ mit

$$|x - 1| < \frac{1}{n}$$

gilt also

$$1 - |x| = |1| - |x| \leq |1 - x| < \frac{1}{n}$$

d.h.

$$1 - \frac{1}{n} < |x|$$

d.h. x liegt nicht in $\wp$, d.h. x ist Einheit und es gilt |x| = 1. Wir haben gezeigt, die Bewertung ist diskret (vgl. 2.1.5), d.h. es gilt Aussage 3.

Zu (ii). Nach dem Satz von Gelfand-Tornheim ist k ein Teilkörper von $\mathbb{C}$. Insbesondere ist der Primkörper von k der Körper der rationalen Zahlen,

$$\mathbb{Q} \subseteq k.$$

Weil k vollständig ist, folgt

$$\mathbb{R} \subseteq k.$$

Nach 2.2.3 folgt $k = \mathbb{R}$ oder $k = \mathbb{C}$.
QED.

2.4.3 Normalisierte Bewerungen

Sei k ein Körper mit einer diskreten multiplikativen Bewertung

$$|?|: k \longrightarrow \mathbb{R},$$

wobei der zugehörige Restklasenkörper endlich sei,

$$q := \# \kappa < \infty,$$

$$\kappa = \mathcal{O}/\wp,\ \mathcal{O} := \{x \in k : |x| \leq 1\},\ \wp := \{x \in k : |x| < 1\} = \pi\mathcal{O}.$$

Dann heißt die Bewertung |?| normalisiert, wenn

$$|\pi| = \frac{1}{q}$$

gilt.

2.4.4 Normalisierte Bewertungen und Haarsches Maß

Sei k ein vollständiger Körper bezüglich der normalisierten (diskreten) Bewertung

$$|?|: k \longrightarrow \mathbb{R}.$$

Nach 2.4.1 ist dann k lokal kompakt, besitzt also ein bis auf den Übergang zu Vielfachen eindeutig bestimmtes Haarsches Maß[67]

$$\mu.$$

Wir legen dieses Maß dadurch eindeutig fest, indem wir fordern[68]

---

[67] d.h. ein Maß, welches bei den Translationen

$$k \longrightarrow k,\ x \mapsto x + c,$$

($c \in k$) invariant ist. Ein solches existiert auf jeder lokal kompakten kommutativen Gruppe.

[68] Weil die Bewertung diskret ist, ist die Menge $\mathcal{O} = \{x \in k : |x| \leq 1\}$ nicht nur abgeschlossen, sondern auch offen, also meßbar. Weil $\mathcal{O}$ kompakt ist, ist das Maß von $\mathcal{O}$ endlich.

$$\mu(\mathcal{O}) = 1.$$

Dann gilt für beliebige $\alpha, \beta \in k$

$$\mu(\alpha + \beta\mathcal{O}) = |\beta|.$$

Beweis. Bezeichne π einen Parameter von |?|, d.h. einen Erzeuger des maximalen Ideals $\wp$ des Bewertungsring $\mathcal{O}$ von |?|. Nach Definition von μ ist die Zahl

$$\mu_n := \mu(\alpha + \pi^n\mathcal{O})$$

für jedes n unabhängig von $\alpha \in k$. Sei

$$\Sigma = \{\alpha_1, \ldots, \alpha_q\} \subseteq \mathcal{O}$$

ein Repräsentantensystem von $\kappa = \mathcal{O}/\wp$, d.h.

$$q := \# \Sigma = \# \kappa \ (< \infty).$$

Denn läßt sich $\mathcal{O}$ in q Nebenklassen modulo $\wp$ zerlegen,

$$\mathcal{O} = \bigcup_{j=1,\ldots,q} \alpha_j + \pi\mathcal{O}.$$

Multiplikation mit π^n und Addition von α (beide Operationen sind Homöomorphismen von k) liefert eine Zerlegung

$$\alpha + \pi^n\mathcal{O} = \bigcup_{j=1,\ldots,q} \alpha + \alpha_j \pi^n + \pi^{n+1}\mathcal{O}.$$

Weil μ ein Maß ist, folgt

$$\mu_n = q \bullet \mu_{n+1},$$

d.h. für jedes n gilt

$$\begin{aligned} \mu_n &= (1/q)^n \bullet \mu_0 \\ &= |\pi^n| \bullet \mu_0 && \text{(weil |?| normiert ist)} \\ &= |\pi^n| \bullet \mu(\mathcal{O}) && \text{(Definition von } \mu_0) \\ &= |\pi^n| && \text{(Wahl von } \mu). \end{aligned}$$

Wir haben gezeigt

$$\mu(\alpha + \pi^n\mathcal{O}) = |\pi^n|.$$

Nun läßt sich jedes $\beta \in k - \{0\}$ in der Gestalt $\beta = u \bullet \pi^n$ schreiben mit einer Einheit u und einer ganzen Zahl n. Insbesondere ist dann $\beta\mathcal{O} = \pi^n\mathcal{O}$ und $|\beta| = |\pi^n|$, d.h. die obige Identität läßt sich in der Gestalt

$$\mu(\alpha + \beta\mathcal{O}) = |\beta|$$

schreiben. Für $\beta = 0$ gilt die Identität trivialerweise.
QED.

Bemerkungen

(i) Es ist nicht schwer zu zeigen, daß es genau ein Haarsches Maß μ auf der additiven topologischen Gruppe k^+ gibt mit $\mu(\alpha + \beta\mathcal{O}) = |\beta|$.

(ii) Das obige Ergebnis läßt sich für Haarsche Maße μ auf k^+, die nicht notwendig durch die Bedingung $\mu(\mathcal{O}) = 1$ normalisiert sind, wie folgt formulieren.[69]

---

[69] Bezeichne μ_0 das Haarsche Maß mit $\mu_0(\mathcal{O}) = 1$. Dann sind μ und μ_0 proportional, d.h.

Für jedes $\beta \in k - \{0\}$ ist durch

$$\mu_\beta(E) := \mu(\beta \bullet E),\ E \subseteq k^+ ,$$

ein weiteres Haarsches Maß definiert. Da je zwei Haarsche Maße auf k^+ proportional sind, gibt es eine nur von β abhängige reelle Zahl f_β mit

$$\mu(\beta \bullet E) = \mu_\beta(E) = f_\beta \bullet \mu(E). \qquad (1)$$

Diese Zahl f_β ist gerade der Wert von β bezüglich der normalisierten Bewertung von k,

$$f_\beta = |\beta|.$$

(iii) In der Theorie der lokal kompakten topologischen Gruppen betrachtet man die zu k^+ duale Gruppe (die Gruppe der Charaktere, Fourier-Analyse). Es erweist sich, daß diese isomorph ist zu k^+. Wir benötigen diese Aussage hier nicht, und werden sie deshalb nicht beweisen. Einen Beweis dieser Aussage und Anwendungen findet man in

S. Lang: Algebraic numbers, Addison Wesley 1964.

Verallgemeinerungen dieser Aussage findet man in

A. Weil: Adeles and algebraic groups, Inst. Adv. Studies, Princeton 1961.
R. Godement: Seminaire Bourbaki Exp. 171, 172.

Die Frage nach der Bestimmung der Charaktergruppe von k* ist Gegenstand der Klassenkörpertheorie.

(iv) Wir schließen diesen Abschnitt ab mit einigen Aussagen über Einheitengruppen. Dazu benötigen wir das folgende Henselsche Lemma, welches in der Zahlentheorie die Rolle des Auflösungssatzes spielt (vgl. Kurke, Pfister, Roczen: Henselsche Ringe).

2.4.5 Henselsches Lemma

Seien k ein Körper, welcher vollständig ist bezüglich der nicht-archimedischen Bewertung

$$|?|: k \longrightarrow \mathbb{R}.$$

Bezeichne

$$\mathcal{O} := \{x \in k : |x| \leq 1\}$$

$$\mu = \lambda \bullet \mu_0$$

mit einer reellen Zahl λ. Einsetzen in (1) liefert

$$\lambda \bullet \mu_0(\beta \bullet E) = f_\beta \bullet \lambda \bullet \mu_0(E),$$

also

$$\mu_0(\beta \bullet E) = f_\beta \bullet \mu_0(E).$$

Für $E = \mathcal{O}$ erhalten wir

$$f_\beta = f_\beta \bullet \mu_0(\mathcal{O}) = \mu_0(\beta \bullet \mathcal{O}) = |\beta|.$$

den Ring der ganzen Zahlen von k. Weiter seien

$$f(X) \in \mathcal{O}[X] \tag{1}$$

ein Polynom und

$$\alpha_0 \in \mathcal{O}$$

ein Element mit

$$|f(\alpha_0)| < |f'(\alpha_0)|^2. \tag{2}$$

Dann gibt es ein Element $\alpha \in \mathcal{O}$ mit

$$f(\alpha) = 0 \text{ und } |\alpha - \alpha_0| \leq |f(\alpha_0)|/|f'(\alpha_0)|. \tag{3}$$

Spezialfall:[70] sei $f(X) \in \mathcal{O}[X]$ und $\alpha_0 \in \mathcal{O}$ ein Element mit

$$f(\alpha_0) \bmod \wp = 0 \text{ und } f'(\alpha_0) \bmod \wp \neq 0.$$

Dabei sei $\wp := \{x \in k : |x| < 1\}$ das Bewertungsideal. Dann gibt es ein $\alpha \in \mathcal{O}$ mit

$$f(\alpha) = 0 \text{ und } \alpha \bmod \wp = \alpha_0 \bmod \wp.$$

Spezialfall (des Spezialfalls):
Sei $g(X) \in \mathcal{O}[X]$ ein normiertes Polynom mit der Eigenschaft, daß das zugehörige Polynom

$$\overline{g}(X) \in \kappa[X]$$

separabel ist, und sei $\alpha_0 \in k$ eine Nullstelle von $\overline{g}$. Dann gibt es in $\mathcal{O}$ genau ein Element α mit

$$g(\alpha) = 0 \text{ und } \overline{\alpha} = \alpha_0.$$

Beweis des Henselschen Lemmas.
Wir betrachten die Taylor-Entwicklung

$$f(X+Y) = f(X) + f_1(X)Y + \ldots + f_j(X)Y^j \tag{4}$$

von f an der Stelle X. Man beachte es gilt $f_1(X) = f'(X)$. Das Element $\beta_0 \in \mathcal{O}$ sei so gewählt, daß gilt[71]

$$f(\alpha_0) + f_1(\alpha_0) \cdot \beta_0 = 0. \tag{5}$$

Es reicht zu zeigen, es gilt

---

[70] Es gilt dann, wenn q die Anzahl der Elemente des Restklassenkörpers bezeichnet und π einen Parameter,

$$|f(\alpha_0)| \leq |\pi| = \frac{1}{q} < 1 = |f'(\alpha_0)|^2,$$

d.h. die Bedingung des Lemmas ist erfüllt. Für das auf Grund des Lemmas existierende α gilt also

$$f(\alpha) = 0 \text{ und } |\alpha - \alpha_0| < 1, \text{ d.h. } \alpha - \alpha_0 \in \wp.$$

[71] Wegen (2) ist $f'(\alpha_0) \neq 0$, d.h. Gleichung (5) besitzt eine Lösung β_0. Wegen

$$|\beta_0| = |f(\alpha_0)/f_1(\alpha_0)| \leq |f_1(\alpha_0)| \leq 1$$

liegt diese automatisch in $\mathcal{O}$. Man beachte, die erste Abschätzung besteht wegen (2), die zweite, weil α_0, also auch $f_1(\alpha_0)$, in $\mathcal{O}$ liegt.

(6) $|f(\alpha_0 + \beta_0)| < |f(\alpha_0)|$

(7) $|f_1(\alpha_0 + \beta_0)| = |f_1(\alpha_0)|$

(8) $|\beta_0| \leq |f(\alpha_0)/f_1(\alpha_0)|$

Wegen (6) und (7) ist dann nämlich Bedingung (2) auch mit $\alpha_1 := \alpha_0 + \beta_0$ anstelle von α_0 erfüllt. Man kann deshalb die eben durchgeführte Konstruktion mit α_1 anstelle von α_0 wiederholen und erhält eine Folge

$$\{\alpha_i\}$$

von Elementen aus $\mathcal{O}$ mit[72]

(9) $|\alpha_{i+1} - \alpha_i| \leq |f(\alpha_i)/f_1(\alpha_i)| < |f(\alpha_{i-1})/f_1(\alpha_{i-1})| < \ldots < |f(\alpha_0)/f_1(\alpha_0)|.$

Insbesondere ist diese Folge konvergent[73],

$$\alpha_i \longrightarrow \alpha \text{ in } k.$$

Weil die α_i in $\mathcal{O}$ liegen, gilt dasselbe für α.[74] Wegen (6) ist die Folge der $f(\alpha_i)$ eine Nullfolge, d.h. es gilt

$$f(\alpha) = 0.$$

Die Abschätzung (3) ergibt sich aus (9) (und der verschärften Variante der Dreiecksungleichung).

Beweis von (8). Folgt aus der Definition von β_0 (vgl. (5)). Es gilt sogar das Gleichheitszeichen.

Beweis von (6). Wir setzen in der Taylor-Entwicklung (4) die Werte $X = \alpha_0$ und $Y = \beta_0$ ein. Wegen (5) wird dann die Summe der ersten beiden Glieder rechts gleich Null. Es folgt

$$|f(\alpha_0+\beta_0)| \leq \max \{|f_j(\alpha_0)\beta_0^j| : j\geq 2\}$$
$$\leq \max \{|\beta_0^j| : j\geq 2\}$$

(wegen $f_j(\alpha_0) \in \mathcal{O}$). Die Norm von β_0 ist kleiner als 1,

$$|\beta_0| = |f(\alpha_0)/f_1(\alpha_0)| <^{75} |f_1(\alpha_0)| \leq^{76} 1.$$

---

[72] Die erste Ungleichung ergibt sich aus (8) mit $\beta_i = \alpha_{i+1} - \alpha_i$ anstelle von β_0. Die übrigen Abschätzungen folgten aus (6) und (7): die Zähler werden mit wachsenden i immer kleiner, die Nenner bleiben konstant.

[73] Die zugehörige Folge der additiven Bewerturngen $\log |\alpha_{i+1} - \alpha_i|$ ist echt aufsteigend, geht also gegen ∞, d.h. die Folge der $|\alpha_{i+1} - \alpha_i|$ geht gegen Null. Dann ist aber $\{\alpha_i\}$ eine Cauchy-Folge (wegen der verschärften Variante der der Dreiecksungleichung):

$$|\alpha_{i+n} - \alpha_i| \leq \max (|\alpha_{i+1} - \alpha_i|, \ldots, |\alpha_{i+n} - \alpha_{i+n-1}|)$$

[74] $\mathcal{O} = \{x\in k \mid |x| \leq 1\}$ ist abgeschlossen in k.

[75] wegen (2).

Deshalb ist das Maximum rechts gleich der Norm der niedrigsten Potenz,

$$|f(\alpha_0+\beta_0)| \le |\beta_0|^2 = \frac{|f(\alpha_0)|^2}{|f_1(\alpha_0)|^2}$$
$$< |f(\alpha_0)| \qquad \text{(nach (2))}.$$

Beweis von (7).
Wir verwenden die Tayler-Entwicklung von $f_1 = f'$ anstelle der von f,

$$f_1(X+Y) = f_1(X) + f'_1(X)Y+...+f'_j(X)Y^j .$$

Wie oben setzen wir $X = \alpha_0$ und $Y = \beta_0$ und erhalten

$$f_1(\alpha_0+\beta_0) - f_1(\alpha_0) = f'_1(\alpha_0)\beta_0+...+f'_j(\alpha_0)(\beta_0)^j$$

also wie oben

$$|f_1(\alpha_0+\beta_0) - f_1(\alpha_0)| \le \max\{|f'_j(\alpha_0)\beta_0^j| : j\ge 1\}$$
$$\le |\beta_0|$$
$$= |f(\alpha_0)/f_1(\alpha_0)|$$
$$< |f_1(\alpha_0)| \qquad \text{(nach (2))}.$$

Damit ist aber

$$|f_1(\alpha_0 + \beta_0)| = \max\{|f_1(\alpha_0+\beta_0) - f_1(\alpha_0)|, |f_1(\alpha_0)|\} = |f_1(\alpha_0)|.$$

QED.

2.4.6 Einheitengruppen

Sei k ein Körper mit der normalisierten diskreten Bewertung

$$|?|: k \longrightarrow \mathbb{R}.$$

Wie im Fall additiver Berwertungen kann man dann verschiedene Gruppen von Einheiten definieren (die mit den Gruppen zur zugehörigen additiven Bewertung übereinstimmen). Wir setzen

$U := \{x \in k : |x| = 1\}$ Gruppe der Einheiten von k bezüglich |?|

$U_1 := \{x \in k: |x - 1| < 1\}$ Gruppe der 1-Einheiten von k bezüglich |?|

Bemerkungen

(i) Weil die Bewertung diskret ist, sind die Untergruppen U und U_1 der topologischen Gruppe k* sowohl offen als auch abgeschlossen in k.

(ii) Weil sich jedes Element von k* in der Gestalt $x = u\cdot\pi^n$ schreiben läßt mit einer Einheit u und einem Parameter π, ist die Abbildung

$$k^*/U \longrightarrow \mathbb{Z}^+, \pi^n U \mapsto n,$$

wohldefiniert und ein Isomorphismus mit Werten in der additiven Gruppe $\mathbb{Z}^+$ der ganzen Zahlen. Versieht man die Gruppe links mit der Faktorraum-Topologie[77] und die Gruppe rechts mit der diskreten Topologie, so ist dies ein Isomorphismus topologischer Gruppen.

---

[76] weil α_0, also auch $f_1(\alpha_0)$ in $\mathcal{O}$ liegt.

[77] Dies ist die stärkste Topologie des Faktorraums, für welche die natürliche Abbildung auf den Faktorraum stetig ist.

(iii) Bezeichne $\kappa = \mathcal{O}/\wp$ den Restklassenkörper zur Bewertung |?| von k. Dann besteht wie im Fall additiver Bewertungen ein Isomorphismus

$$U/U_1 \longrightarrow \kappa^*,\ x \bullet U_1 \mapsto x + \wp\ ,$$

mit der multiplikativen Gruppe des Restklassenkörpers. Dies ist ein Isomorphismus topologischer Gruppen, wenn man die linke Gruppe mit der Faktorraum-Topologie und die rechte Gruppe mit der diskreten Topologie versieht.

Für die nachfolgenden drei Aussagen nehmen wir zusätzlich an, der Körper

k ist vollständig.

(iv) Bezeichne q die Ordnung des Restklassenkörpers κ. Dann gilt

$$k^* \cong \mathbb{Z}\times\mathbb{Z}/(q-1)\mathbb{Z}\times U_1$$

Die beiden ersten Faktoren rechts sind dabei mit der diskreten Topolgie zu versehen.

(v) Das Haarsche Maß von k^+ ist invariant bei der Multiplikation mit Elementen aus U_1,[78] induziert also ein Haarsches Maß auf U_1 und damit (wegen (iii)) auf k*.

(vi) Im Fall char(k) = 0 sind die Gruppen k* und k^+ lokal isomorph, denn die Exponentialabbildung

$$\exp: k^+ \longrightarrow k^*,\ \alpha \mapsto \sum_{n=0}^{\infty} \frac{\alpha^n}{n!}$$

ist für hinreichend kleine α definiert, und die Umkehrung

$$\log: k^* \longrightarrow k^+,\ \alpha \mapsto \sum_{n=1}^{\infty} \frac{(-1)^n \bullet (\alpha-1)^m}{n}$$

ist für α nahe genug bei 1 definiert.

Beweis von (iv). Die multiplikative Gruppe κ^* des Restklassenkörpers ist eine zyklische Gruppe der Ordnung q-1,

$$\kappa^* = \{1, \overline{\zeta}, \overline{\zeta}^2, \dots, \overline{\zeta}^{q-1}\}$$

mit einer primitiven (q-1)-ten Einheitswurzel $\overline{\zeta}$ (in der Charakteristik von κ). Nun ist $\overline{\zeta}$ eine Nullstelle von

$$X^{q-1} - 1$$

und keine Nullstelle der Ableitung dieses (separablen) Polynoms. Nach dem Henselschen Lemma gibt es ein Element

$$\zeta \in \mathcal{O}$$

mit der Restklasse $\overline{\zeta}$, dessen (q-1)-te Potenz gleich 1 ist, d.h. die Menge

$$\{1, \zeta, \zeta^2, \dots, \zeta^{q-1}\}$$

ist ein Repräsentantensystem von κ^* in $\mathcal{O}$. Jedes Element $\alpha \in k^*$ läßt sich auf genau eine Weise in der Gestalt

$$\alpha = \pi^n \bullet \zeta^m \bullet u \text{ mit } n \in \mathbb{Z},\ m \in \mathbb{Z}/(q-1)\mathbb{Z},\ u \in U_1$$

---

[78] Nach Bemerkung 2.4.4 (ii) ist

$$\mu(\beta \bullet E) = \mu_\beta(E) = f_\beta \bullet \mu(E) \text{ mit } f_\beta = |\beta|.$$

Für $\beta \in U_1$ ist der Faktor f_β somit gleich $|\beta| = \max\{|\beta-1|, |1|\} = |1| = 1$.

schreiben.

QED.

2.4.7 Zusammenhang

Sei k ein Körper mit der normalisierten diskreten Bewertung

$$|?|: k \longrightarrow \mathbb{R}.$$

Dann sind k^* und k^+ sind vollständig unzusammenhängend, d.h. alle Zusammenhangskomponenten bestehen aus nur einem Punkt.
Beweis. Wir können annehmen, k ist vollständig. Wir haben zu zeigen, je zwei Elemente, sagen wir α und β liegen in verschiedenen Zusammenhangskomponenten. Durch eine Verschiebung um α , welches ein Homöomorphismus ist, erreichen wir

$$\alpha = 0.$$

Durch eine Multiplikation mit einer Potenz eines Parameters, welches ein Homöomorphismus ist, erreichen wir

$$\beta \notin \mathcal{O}.$$

nun ist aber $\mathcal{O}$ eine offene und abgeschlossene Teilmenge von k. Die Zusammenhangskomponente $C(\alpha)$ liegt also ganz in $\mathcal{O}$ und die Zusammenhangskomponente $C(\beta)$ liegt ganz im Komplement von $\mathcal{O}$. Also sind $C(\alpha)$ und $C(\beta)$ disjunkt, d.h. α und β liegen in verschiedenen Zusammenhangskomponenten.
QED.

Index

—1—

1-Einheitengruppe, 127

—A—

additive Bewertung, 32
Algebra, 97
Algebra, 99
algebraische Gruppe, 5
Approximationssatz
  schwacher, 106

—Ä—

äquivivalente Normen von Vektorräumen, 108

—A—

archimedisch, 33
archimedische Bewertung, 89
archmedische Bewertungen, 33
assoziiert, 10

—B—

Banachalgebra, 99
Basis
  duale, 59
bewerteter Körper
  Vervollständigung eines, 104
Bewertung
  additive, 32
  archimedische, 89
  diskrete, 87
  diskrete, Einheiten einer, 36
  multiplikative, 32; 84
  nicht-archimedische, 89
  siehe auch Norm, reelle, 97
  triviale, 84
Bewertung zur Stelle p(t), 94
Bewertungsideal, 24
Bewertungsring
  diskreter, 28
Bewertungsring, 24

—C—

charakteristisches Polynom, 66

—D—

Dedekind-Ring, 21; 42
definiert über einem Körper, 7
diskrete Bewertung, 87
diskreter Bewertungsring, 28
Diskriminante eines Gitters, 62
Dreiecksungleichung
  nicht-archimedische, 89
Dual eines Gitters, 59
duale Basis, 59
Durchschnittssatz von Krull, 27

—E—

Einheit
  Gruppe der n-Einheiten, 36
  n-Einheit, 36
Einheiten einer diskreten Bewertung, 36
Einheitengruppe, 127
Element
  ganzes, Ring der, 89
Erzeugendensystem
  freies, einer abelschen Gruppe, 46
Erzeugendensystem
  minimales, 54
Euklidischer Ring, 9
euklidischer Vektorraum, 59
ε-Umgebung, 102

—F—

fast alle, 50
Fermatscher Satz, großer, 3
freies Erzeugendensystem einer abelschen Gruppe, 46

—G—

ganz abgeschlossen, 18
ganze Abschließung, 18
ganze rationale Zahl, 21
ganze Zahl, 21
ganzes Element
  Ring der, 89
Ganzheit
  eines Elements, 16
  eines Homomorphismus, 16
  über einem Teilring, 16
Ganzhzeitspolynom, 16
Geschlecht, 5
Gitter
  Diskriminante eines, 62
  Dual eines, 59
Gitter, 52
großer Fermatscher Satz, 3
Gruppe
  algebraische, 5
Gruppe der 1-Einheiten, 127
Gruppe der Einheiten, 127
Gruppe der n-Einheiten, 36

—H—

Haarsches Maß, 122
Hauptidealring, 28

—I—

Index
  eines Gitters, 54; 55
Integritätsbereich, 9

—K—

Körper
  bewerteter, Vervollständigung eines, 104
  topologischer, 103
Krullscher Durchschnittssatz, 27

—L—

Lokalisierung
  eines Moduls in einem Primideal, 52
Lokalisierung in einem Primideal, 41

—M—

Maß
  Haarsches, 122
minimales Erzeugendensystem, 54
multiplikative Bewertung, 84
multiplikative Bewertung, 32

—N—

nicht-archimedische Bewertung, 89
nicht-archimedische Dreiecksungleichung, 89
Norm
  Äquivivalenz von, 108
  auf einem Vektorraum, 107
  reelle, 97
normal, 18

—P—

p(t)-adische Bewertung, 94
Polynom
  charakteristisches, 66
  Ganzheitspolynom, 16
projektive Abschließung, 4
projektiver Raum, 4
Punkt
  rationaler, 7

—R—

rationaler Punkt, 7
Raum
  projektiver, 4
reelle Norm, 97
Ring
  Dedekind-Ring, 21
  ZPE, 9
Ring der ganzen Elemente, 89
Ring der ganzen Zahlen, 21
Ring der ganzen Zahlen eines Zahlenkörpers, 83
Ring, euklidischer, 9

—S—

Satz
  großer Fermatscher, 3
separables Element, 77
separables Polynom, 75
Skalarprodukt, 62; 64
Skalarprodukt, 59

—T—

topologischer Körper, 103

triviale Bewertung, 84

—U—

Umgebung
ε-Umgebung, 102
Umgebungsbasis, 102

—V—

Vektorraum
Norm auf, 107
Vektorraum, euklidischer, 59
Vervollständigung eines bewerteten Körpers, 104
Verzweigungsindex, 111

—Z—

Zahl
ganze, 21
ganze rationale, 21
Zahlenkörper
Ring der ganzen Zahlen eines, 83
Zahlenkörper, 13
ZPE-Ring, 9

Inhalt

ZAHLENTHEORIE 1

BEZEICHNUNGEN 1

Einleitung 3

1. DEDEKIND-RINGE 9

1.1 Die ganzen Gaußschen Zahlen 9
1.1.1 Definition und grundlegenden Eigenschaften 9
1.1.2 Die Einheiten von Γ 9
1.1.3 Die Primelemente von Γ 10

1.2 Der Ring $Z[\sqrt{-5}] = Z + \sqrt{-5}:Z$ 13
1.2.1 Die Einheiten von $Z[\sqrt{-5}]$ 14
1.2.2 Die Unzerlegbarkeit einiger Elemente von $Z[\sqrt{-5}]$ 14
1.2.3 Folgerung 15

1.3 Ganze Erweiterungen 16
1.3.1 Definition 16
1.3.2 Kriterium für die Ganzheit eines Elements 16
1.3.3 Beispiele 18
1.3.4 Die ganze Abschließung 18
1.3.5 Beispiel für einen normalen Integritätsbereich 19
1.3.6 Beispiel für eine ganze Abschließung: $Z[\sqrt{-5}]$ 19

1.4 Gebrochene Ideale und diskrete Bewertungsringe 21
1.4.1 Operationen mit Idealen 21
1.4.2 Eigenschaften von Ideal-Operationen 21
1.4.3 Begriff des gebrochenen Ideals 21
1.4.4 Eigenschaften von gebrochenen Idealen 22
1.4.5 Kriterium für gebrochene Ideale im Fall noetherscher Ringe 22
1.4.6 Begriff der diskreten Bewertung 23
1.4.7 Beispiel: formale Laurent-Reihen 23
1.4.8 Eigenschaften diskreter Bewertungen 24
1.4.9 Definition: diskreter Bewertungsring 28
1.4.10 Charakterisierung der diskreten Bewertungsringe 28
1.4.11 Die Topologie zu einer diskreten Bewertung 32

1.4.12 Die Potenzen des Bewertungsideals und der Restklassenkörper 35
1.4.13 Eine exakte Sequenz für die Einheiten einer diskreten Bewertung 36
1.4.14 Die Gruppe der n-Einheiten 36
1.4.15 Faktorgruppen von Einheitengruppen 38
1.4.16 Folgerung: die additive Gruppe des Restklassenkörpers als Faktorgruppe von Einheiten 39
1.4.17 Einige Automorphismen der n-Einheitengruppen 39
1.4.18 Lokalisierungen nach einem Primideal 41

1.5 Dedekind-Ringe 42
1.5.1 Eine Charakterisierung der Dedekind-Ringe 42
1.5.2 Bezeichnungen 45
1.5.3 Satz von der Zerlegung in Primfaktoren 46
1.5.4 Folgerung: Der Wert eines Elements für verschiedene p 50
1.5.5 Folgerung: direkte Summenzerlegung von F(R) 50
1.5.6 Folgerung: Rechenregeln für $v_p(I)$ 50

1.6 Moduln über Dedekind-Ringen (und Bilinearformen) 51
1.6.1 Vorbemerkung 51
1.6.2 Die Situation 51
1.6.3 Ein Durchschnittssatz 52
1.6.4 Vergleichslemma für Gitter 52
1.6.5 Konstruktion: der Index zweier Gitter 53
1.6.6 Eigenschaften des Index 56
1.6.7 Invarianz des Index bei Automorphismen 58
1.6.8 Die Situation (Wahl einer Bilinearform) 58
1.6.9 Das Dual eines Moduls 59
1.6.10 Das Dual eines freien Gitters 59
1.6.11 Eigenschaften des Duals 60
1.6.12 Die Diskriminante eines Gitters 62
1.6.13 Eigenschaften der Diskriminante 62
1.6.14 Verhalten bei direkten Summen 64
1.6.15 Verhalten bei Erweiterungen 65

1.7 Norm und Spur 65
1.7.1 Der Endomorphismenring eines freien Moduls 65
1.7.2 Definition von Spur und Norm eines Endomorphismus 66
1.7.3 Eigenschaften von Spur und Norm 66
1.7.4 Satz von Hamilton-Cayley 67
1.7.5 Das Charakteristische Polynom als Norm 68
1.7.6 Die Norm eines Polynoms mit Koeffizienten aus End(M) 68
1.7.7 Komposition von Spuren und von Normen 69
1.7.8 Der Fall einer endlichen Körpererweiterung 72

1.8 Separabilität 73
1.8.1 Die Zahl der Einbettungen eines Erweiterungskörpers 73
1.8.2 Definition der Separabilität 73
1.8.3 Separabilität von Teilerweiterungen 73
1.8.4 Separabilität und das Fehlen mehrfacher Nullstellen 74
1.8.5 Die Spurabbildung 74
1.8.6 Zusammensetzung separabler Erweiterungen 74
1.8.7 Separabilität in der Charakteristik Null 75
1.8.8 Separabilität und mehrfache Nullstellen 75
1.8.9 Satz vom primitiven Element 75
1.8.10 Separabilität und das Nichtentarten der Killingform 76
1.8.11 Erhaltung der Separabilität bei Basiswechsel 77
1.8.12 Separabilität von Erweiterungen und von Elementen 77
1.8.13 Das Entarten der Killingform im inseparablen Fall 77

1.9 Ganze Abschließungen in endlichen Körpererweiterungen 79
1.9.1 Die Situation 79
1.9.2 Verträglichkeit mit Lokalisierungen 79
1.9.3 Die ganze Abschließung von Dedekind-Ringen in endlichen separablen Erweiterungen 80
1.9.4 Folgerung: die gebrochenen Ideale von R und S 82
1.9.5 Bemerkung zum weiteren Verlauf der Vorlesung 83

2. MULTIPLIKATIVE BEWERTUNGEN 84

2.1 Definition und Beispiele 84
2.1.1 Definition 84
2.1.2 Erste Eigenschaften 84
2.1.3 Äquivalenz von Bewertungen 85
2.1.4 Äquivalenz und Dreiecksungleichung 85
2.1.5 Diskrete Bewertungen 87
Lemma 87
2.1.6 Archimedische und nicht-archimedishe Bewertungen 89
2.1.7 Eigenschaften nicht-archimedischer Bewertungen 89
2.1.8 Kriterium für nicht-archimedische Bewertungen 91
2.1.9 Kriterium für archimedische Bewertungen 92
2.1.10 Folgerung: der Fall positiver Charakteristik 92
2.1.11 Beispiel: die komplexen Zahlen 93
2.1.12 Beispiel: die rationalen Zahlen 93
2.1.13 Beispiel: die rationalen Funktionenkörper 93
2.1.14 Die multiplikativen Bewertungen über einem Dedekind-Ring 94
2.1.15 Satz von Ostrovskij: die Bewertungen der rationalen Zahlen 96
2.1.16 Die Bewertungen eines rationalen Funktionenkörpers 97

2.2 Archimedisch bewertete Körper 97
2.2.1 Die topologische Gruppenstruktur zu einer reellen Norm 97
2.2.2 Satz von Gelfand-Mazur 99
2.2.3 Die archimedisch bewerteten Erweiterungen von R 101
2.2.4 Satz von Gelfand-Tornheim 101
2.2.5 Eindeutigkeitssatz für die Fortsetzung von Bewertungen 102

2.3 Die Topologie zu einer multiplikativen Bewertung 102
2.3.1 Umgebungsbasen 102
2.3.2 Erste Eigenschaften der Topologie zu einer multiplikativen Bewertung 103
2.3.3 Die Vervollständigung eines bewerteten Körpers 104
2.3.4 Schwacher Approximationssatz 106
2.3.5 Normierte Vektorräume über bewerteten Körpern 107
2.3.6 Normierte Vektorräume über vollständigen Körpern 108
2.3.7 Fortsetzung von Bewertungen 109
2.3.8 Existenz und Eindeutigkeit der Fortsetzung im vollständigen Fall 109
2.3.9 Folgerung: Vergleich mit der Maximum-Bewertung 112
2.3.10 Folgerung: Vollständigkeit der Erweiterung 112
2.3.11 Das Tensorprodukt von Körpererweiterungen 113
2.3.12 Die Fortsetzung von Bewertungen auf endliche separable Erweiterungen 115
2.3.13 Ganze Abschließung diskreter Bewertungsringe im vollständigen Fall 118

2.4 Bewertete Körper mit endlichem Restklassenkörper 118
2.4.1. Lokale Kompaktheit im vollständigen Fall 118
2.4.2 Charatkerisierung der lokal kompakten bewerteten Körper 120
2.4.3 Normalisierte Bewerungen 122
2.4.4 Normalisierte Bewertungen und Haarsches Maß 122
2.4.5 Henselsches Lemma 124
2.4.6 Einheitengruppen 127

2.4.7 Zusammenhang 129

INDEX 129

INHALT 131