Grundlagen der algebraische Zahlentheorie

Seminar: Algebraische Zahlentheorie, 8. Vortrag, 07. Juni 2017

Joseph Adams

10. Juni 2017

12 Algebraische Zahlentheorie

12.1 Algebraische Vorbereitungen

Prop.
Sei ξ eine algebraische Zahl in $\mathbb{C}$ vom Grad n. Dann existieren genau n Einbettungen von $F = \mathbb{Q}(\xi) = \mathbb{Q}[\xi]$ in $\mathbb{C}$.

Beweis.
Für das Minimalpolynom von ξ schreiben wir: $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$.

1. Es gibt höchstens n solche Einbettungen. Denn sei σ eine solche Einbettung, dann gilt:

$$\begin{aligned} & a_n\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_0 = 0 \\ \Rightarrow\ & \sigma(a_n\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_0) = \sigma(0) \\ \Rightarrow\ & a_n\sigma(\xi)^n + a_{n-1}\sigma(\xi)^{n-1} + \cdots + a_0 = 0 \end{aligned}$$

   Daher ist $\sigma(\xi)$ auch eine Nullstelle des Minimalpolynoms. Da dieses aber Grad n hat, gibt es höchstens n Nullstellen.

2. Jede Nullstelle ξ_i des Minimalpolynoms definiert auch eine Einbettung. Diese hat die die Gestalt $\sigma_i : F = \mathbb{Q}[\xi] \to \mathbb{C}$ definiert durch $\sigma(\xi) = \xi_i$.

3. Es gibt genau n verschiedene Nullstellen des Minimalpolynoms $f(x)$. Denn angenommen, $f(x)$ habe eine k-fache Nullstelle in α. Dann können wir schreiben $f(x) = (x-\alpha)^k h(x)$, für ein $h(x) \in \mathbb{Q}[x]$. Durch ableiten bekommt man $f'(x) = (x-\alpha)^{k-1}(kh(x) + (x-\alpha)h'(x))$. Wir erkennen in $\mathrm{ggT}(f(x), f'(x)) = (x-\alpha)^{k-1} \cdot q(x)$, dass es ein Polynom kleineren Grades gibt, sodass α auch Nullstelle dieses Polynoms ist. Das ist ein Widerspruch dazu, dass $f(x)$ das Minimalpolynom war.

So folgern wir, dass es genau n Einbettugen von F in $\mathbb{C}$ gibt. $\square$

Wir werden im Folgenden nur Körper der Charakteristik 0 untersuchen.

Definition (Dimension, Norm und Spur)
Sei L/K eine endliche algebraische Körpererweiterung. Die Dimension von L/K bezeichnen wir mit $[L : K]$. Sei $\alpha \in L$ und seien $\sigma_1, \sigma_2, \ldots, \sigma_n$ die verschiedenen Einbettungen von L in einen algebraischen Abschluss von K. Wir bezeichnen $\sigma_j(\alpha)$ durch $\alpha^{(j)}$. Die Elemente $\alpha^{(j)}$ heißen Konjugierte zu α. Hier ist $\alpha^{(1)}$ dann α. Wir definieren die Spur von α als $t(\alpha) = \alpha^{(1)} + \alpha^{(2)} + \cdots + \alpha^{(n)}$ und die Norm von α durch $N(\alpha) = \alpha^{(1)}\alpha^{(2)} \cdots \alpha^{(n)}$. Diese Definitionen erweitern die aus dem Kapitel 11.2.

Im Folgenden heißt die Norm immer $N(\alpha)$ und die Spur immer $t(\alpha)$, da wir jeweils nur eine einzige Körpererweiterung L/K betrachten werden.

Elementare Eigenschaften
Für $\alpha, \beta \in L/K$ und $a \in K$ gilt:

(a) $N(\alpha\beta) = N(\alpha)N(\beta)$

(b) $t(\alpha + \beta) = t(\alpha) + t(\beta)$

(c) $N(a\beta) = a^n N(\beta)$, mit $n = [L : K]$

(d) $t(a\beta) = at(\beta)$

(e) Wenn $\alpha \neq 0$ folgt $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$.
Damit gilt für $N(\alpha^{-1}) = N(\alpha)^{-1}$

(f) $t(\alpha)$ ist nicht die Nullabbildung.

Definition (Diskriminante)
Seien $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. Dann heißt $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) := \det(t(\alpha_i\alpha_j))$ die Diskriminante von $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Prop. 12.1.1
Die Diskriminante $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ ist genau dann ungleich 0, wenn $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Basis von L/K bilden.

Beweis.
Wir beweisen dies durch Kontraposition. Dafür seien $\alpha_1, \alpha_2, \ldots, \alpha_n$ linear abhängig. Dann existieren $a_1, a_2, \ldots, a_n \in K$, wobei nicht alle gleich 0 sind, so dass $\sum_i a_i\alpha_i = 0$. Diesen Ausdruck multiplizieren wir mit α_j und nehmen die Spur:

$$\sum_i a_i t(\alpha_i\alpha_j) = 0 \quad \text{für } j = 1, 2, \ldots, n$$

Das zeigt das die Spalten von $(t(\alpha_i\alpha_j))_{ij}$ linear abhängig sind und somit ist $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$.

Jetzt sei $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Basis und $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. Dann hat das lineare Gleichungssystem

$$\sum_i x_i t(\alpha_i \alpha_j) = 0 \quad \text{für } j = 1, 2, \ldots, n$$

eine nicht-triviale Lösung: $x_i = a_i \in K$, $i = 1, 2, \ldots, n$, denn die Determinate der Spuren verschwindet. Sei $\alpha = \sum_i a_i \alpha_i \neq 0$. Dann, wegen der Linearität der Spur, $t(\alpha \alpha_j) = 0$ für $j = 1, 2, \ldots, n$ und da $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Basis ist, folgt $t(\alpha\beta) = 0$ für alle $\beta \in L$. Daraus folgt $t \equiv 0$, ein Widerspruch. □

Prop. 12.1.2
Seien $\alpha_1, \alpha_2, \ldots, \alpha_n$ und $\beta_1, \beta_2, \ldots, \beta_n$ Basen von L/K. Sei $\alpha_i = \sum_j a_{ij}\beta_j$ mit $a_{ij} \in K$. Dann $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(a_{ij})^2 \Delta(\beta_1, \beta_2, \ldots, \beta_n)$

Beweis.
Man nehme die Spur beider Seiten von:

$$\alpha_i \alpha_k = \sum_j \sum_l a_{ij} a_{kl} \beta_j \beta_l$$

Sei $A = (t(\alpha_i \alpha_j))_{ij}$, $B = (t(\beta_j \beta_l))_{jl}$ und $C = (a_{ij})_{ij}$. Dann findet man das $A = C^T B C$. Betrachtet man die Determinante beider Seiten folgt (wegen $\det(M) = \det(M^T)$):

$$\begin{aligned} \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(A) &= \det(C)^2 \det(B) \\ &= \det(a_{ij})^2 \Delta(\beta_1, \beta_2, \ldots, \beta_n) \end{aligned}$$

□

Prop. 12.1.3
Seien $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. Dann:

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(\alpha_i^{(j)})^2$$

Beweis.
Man bermerke: $t(\alpha_i \alpha_j) = \alpha_i^{(1)} \alpha_j^{(1)} + \alpha_i^{(2)} \alpha_j^{(2)} + \cdots + \alpha_i^{(n)} \alpha_j^{(n)}$. Sei nun $A = (t(\alpha_i \alpha_j))_{ij}$ und $B = (\alpha_i^{(j)})_{ij}$. Dann gilt:

$$\begin{aligned} A = BB^T &\Rightarrow \det(A) = \det(B)^2 \\ &\Rightarrow \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(\alpha_i^{(j)})^2 \end{aligned}$$

□

Prop. 12.1.4
Seien $1, \beta, \beta^2, \ldots, \beta^{n-1} \in L$ linear unabhängig über K und sei $f(x) \in K[x]$ das Minimalpolynom für β über K. Dann gilt:

$$\Delta(1, \beta, \beta^2, \ldots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N(f'(\beta))$$

wobei $f'(x) \in K[x]$ die formale Ableitung von f ist.

Beweis.
Die Matrix $((\beta^{(j)})^i)_{ij}$ hat Vandermonde-Gestalt, also gilt:

$$\det((\beta^{(j)})^i) = \prod_{i<j}(\beta^{(j)} - \beta^{(i)})$$

Damit bekommen wir:

$$\Delta(1, \beta, \beta^2, \ldots, \beta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\beta^{(j)} - \beta^{(i)})$$

Allerding gilt auch: $f(x) = \prod_i (x - \beta^{(i)})$ und somit $f'(x) = \sum_j \prod_{i \neq j}(x - \beta^{(i)})$, womit dann $f'(\beta^{(j)}) = \prod_{i \neq j}(\beta^{(j)} - \beta^{(i)})$. Da $f'(\beta^{(j)}) = (f'(\beta))^{(j)}$ folgt die Behauptung indem man über j das Produkt bildet. □

12.2 Eindeutige Faktorisierung in algebraischen Zahlkörpern

Definition (Algebraischer Zahlkörper)
Ein Unterkörper $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ heißt algebraischer Zahlkörper, falls $[F : \mathbb{Q}]$ endlich ist. Wenn F ein solcher Zahlkörper ist, bildet die Menge der darin enthaltenen ganzalgebraischen Zahlen einen Ring D, den Ring der ganzalgebraischen Zahlen in F.

Zur Erinnerung: Eine ganzalgebraische Zahl (oder wie im zweiten Vortrag: algebraischer Integer) ist Nullstelle eines normierten Polynoms mit Koeffizienten in $\mathbb{Z}$.

Prop. 6.1.2 zeigt, dass ein algebraischer Zahlkörper aus algebraischen Zahlen besteht (man setzte $V = F$ und $\gamma_1, \gamma_2, \ldots, \gamma_n$ als $\mathbb{Q}$-Basis von F). Sei Ω die Menge aller ganzalgebraischen Zahlen, dann haben wir in Prop. 6.1.5 gesehen, dass Ω ein Ring ist. Somit ist $D = \Omega \cap F$ als Schnitt von zwei Ringen ebenfalls ein Ring. (Es stellt sich heraus, dass D im Allgemeinen kein faktorieller Ring ist.)

Definition (Dedekindring)
Sei R ein Integritätsring und sei $0 \neq I \trianglelefteq R$ ein Ideal in R. Wenn sich I eindeutig in ein Produkt von Primidealen zerlegen lässt heißt R Dedekindring.

Beispiel
Diese Definiton ist für uns interessant, da man nicht in jedem Ring, der eine Erweiterung von $\mathbb{Q}$ ist, eindeutig Faktorisieren kann. Hierzu betrachte man $6 \in \mathbb{Q}[\sqrt{-5}]$. Das können wir schreiben als $2 \cdot 3 = 6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$.

Von hier an soll Ideal immer nicht-nullsches Ideal bedeuten.

Lemma 1
Sei $\beta \in F$. Dann existiert $b \in \mathbb{Z} \setminus \{0\}$ mit $b\beta \in D$.

Beweis.
β erfüllt die Gleichung: $a_0\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0$ mit $a_i \in \mathbb{Z}$, $a_0 \neq 0$. Dann:

$$\begin{aligned} & a_0\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0 \\ \iff & (a_0\beta)^n + a_1(a_0\beta)^{n-1} + a_2a_0(a_0\beta)^{n-2} + \cdots + a_na_0^{n-1} = 0 \end{aligned}$$

$\Rightarrow a_0\beta$ ist ganzalgebraische Zahl, da $a_ia_0^{i-1} \in \mathbb{Z}$. □

Prop. 12.2.1
Jedes Ideal $A \trianglelefteq D$ enthält eine $\mathbb{Q}$-Basis von F.

Beweis.
Sei $\beta_1, \beta_2, \ldots, \beta_n$ eine beliebige $\mathbb{Q}$-Basis von F. Wegen Lemma 1 existiert $b \in \mathbb{Z}\backslash\{0\}$ mit $b\beta_1, b\beta_2, \ldots, b\beta_n \in D$. Man wähle ein $\alpha \in A \setminus \{0\}$, dann sind $b\beta_1\alpha, b\beta_2\alpha, \ldots, b\beta_n\alpha \in A$ eine $\mathbb{Q}$-Basis von F. □

Ab jetzt betrachten wir die Begriffe Norm, Spur und Diskriminante für die Erweiterung $F/\mathbb{Q}$.

Behauptung
Sei $\alpha \in D$, dann $N(\alpha), t(\alpha) \in \mathbb{Z}$.

Beweis.
α ist Nullstelle eines Polynoms aus $\mathbb{Z}[x]$ mit Leitkoeffizientem gleich 1, ebenso wie die Konjugierten zu α, da diese Nullstellen des charakteristischen Polynoms der Darstellungs-Matrix zu der von α induzierten linearen Abbildung φ_α ist. Daher sind $N(\alpha)$ und $t(\alpha)$ ganzalgebraische Zahlen, als Produkt und Summe ganzalgebraischer Zahlen. Außerdem liegen sie in $\mathbb{Q}$, also liegen sie nach Prop. 6.1.1 auch in $\mathbb{Z}$. □

Korollar
Sei $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine $\mathbb{Q}$-Basis von F mit $\alpha_i \in D$ für $i = 1, 2, \ldots, n$. Dann ist $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}$, da $t(\alpha) \in \mathbb{Z}$.

Beispiel
Die Menge $\{1, i\}$ ist Basis für $\mathbb{Q}(i)/\mathbb{Q}$. Durch Rechnung erhält man: $\Delta(1, i) = -4$.

Prop. 12.2.2
Sei $A \trianglelefteq D$ ein Ideal und $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ eine Basis für $F/\mathbb{Q}$ mit $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)|$ minimal. Dann $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$.

Beweis.
Weil $|\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)| \in \mathbb{N}$ existiert eine solche Basis überhaupt. Sei $\alpha \in A$ und $\alpha = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n$ mit $\gamma_i \in \mathbb{Q}$ für $i = 1, 2, \ldots, n$.

Zu zeigen: $\gamma_i \in \mathbb{Z}$. Widerspruchs-Annahme: Es gibt ein $\gamma_i \notin \mathbb{Z}$ dann o.B.d.A. $\gamma_1 \notin \mathbb{Z}$. Schreibe $\gamma_1 = m + \theta$ mit $m \in \mathbb{Z}$ und $\theta \in]0, 1[$. Sei $\beta_1 = \alpha - m\alpha_1$ und $\beta_i = \alpha_i$ für

$i = 2, 3, \ldots, n$. Dann ist $\beta_1, \beta_2, \ldots, \beta_n \in A$ eine Basis für $F/\mathbb{Q}$. Weil $\beta_1 = \theta\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n$ ist die Basiswechselmatrix zwischen den Basen der α_i und β_i gegeben durch:

$$\begin{pmatrix} \theta & \gamma_2 & \gamma_3 & \cdots & \gamma_{n-1} & \gamma_n \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ & & & \vdots & & \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Nach Prop. 12.1.2 finden wir $\Delta(\beta_1, \beta_2, \ldots, \beta_n) = \theta^2\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ was im Widerspruch zur Minimalität von $|\Delta(\beta_1, \beta_2, \ldots, \beta_n)|$ steht, denn $\theta \in]0, 1[$. Daraus folgt: $\gamma_i \in \mathbb{Z}$ für $i = 1, 2, \ldots, n$ und $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. □

Definition (Integritätsbasis)
Ist $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ eine $\mathbb{Q}$-Basis von F und $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$, so nennen wir $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Integritätsbasis von A.

Aus Prop 12.1.2 folgt, dass die Diskriminante zweier Integritätsbasen gleich sind, denn wenn wir versuchen von einer Integritätsbasis in eine andere zu wechseln, benutzen wir eine Basiswechselmatrix, die Einträge in $\mathbb{Z}$ hat. Daher ist auch ihre Determinate in $\mathbb{Z}$. Allerdings ist die Rücktransformation dann mittels ihrer Inverse möglich, und ihre Inverse muss nach dem selben Argument auch Determinate aus $\mathbb{Z}$ haben. Daher ist die Determinate 1.

Definition (Diskriminante eines Ideals)
Diesen Wert nennen wir die Diskriminante von A. Wir bezeichnen ihn mit $\Delta(A)$. Außerdem nennen wir die Diskriminante $\Delta(D) = \delta_F$ von D auch die Diskriminante von $F/\mathbb{Q}$.

Lemma 2
Sei $A \trianglelefteq D$ ein Ideal, dann $A \cap \mathbb{Z} \neq \{0\}$.

Beweis.
Sei $\alpha \in A \setminus \{0\}$. Dann existieren $a_i \in \mathbb{Z}$ mit $\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$. Weil wir in einem Körper sind können wir $a_m \neq 0$ annehmen. Dann $0 \neq a_m = -\alpha^m - a_1\alpha^{m-1} - \cdots - a_{m-1}\alpha \in A \cap \mathbb{Z}$. □

Prop. 12.2.3
Für jedes Ideal $A \trianglelefteq D$ ist $|D/A| < \infty$

Beweis.
Wegen Lemma 2 existiert ein $a \in (A \cap \mathbb{Z}) \setminus \{0\}$. Sei (a) das von a erzeugte Hauptideal. Weil $D/(a)$ auf D/A abbildet, genügt es zu zeigen, dass $D/(a)$ endlich ist. Genauer werden wir zeigen, dass $D/(a)$ genau a^n Elemente besitzt. Nach Prop 12.2.2 können wir schreiben: $D = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n$. Sei $S = \{\sum_i \gamma_i\omega_i \mid \gamma_i \in \mathbb{Z},\ 0 \leq \gamma_i < a\}$.

Behauptung: S ist eine Menge von Repräsentanten von Nebenklassen von $D/(a)$.

Sei $\omega = \sum_i m_i\omega_i \in D$ für bestimmte $m_i \in \mathbb{Z}$. Schreiben wir $m_i = q_i a + \gamma_i$ mit $\gamma_i \in \mathbb{Z}$ und $0 \leq \gamma_i < a$. Klar ist: $\omega \equiv \sum_i \gamma_i\omega_i \pmod{a}$. Daher enthält jede Nebenklasse von A ein Element von S.

Wenn $\sum_i \gamma_i\omega_i$ und $\sum_i \gamma_i'\omega_i$ beide in S liegen und in der selben Nebenklasse modulo a, dann folgt aus der linearen Unabhängigkeit der ω_i, dass $\gamma_i - \gamma_i'$ durch a teilbar ist. Da $0 \leq \gamma_i, \gamma_i' < a$ folgt $\gamma_i = \gamma_i'$. Daher ist S ein Repräsentantensystem von Nebenklassen und $D/(a)$ hat a^n Elemente. □

Korollar 1
D ist ein noetherscher Ring. d.h. für eine Folge von Idealen $A_1 \subseteq A_2 \subseteq \ldots$ existiert ein $N \in \mathbb{N}$, so dass $A_m = A_N$ für alle $m \geq N$.

Beweis.
Weil D/A_1 endlich ist, gibt es nur endlich viele Ideale die A_1 enthalten. □

Korollar 2
Jedes Primideal von D ist maximal.

Beweis.
Wenn $P \trianglelefteq D$ ein Primideal ist, dann ist D/P ein endlicher Integritätsring. Ein solcher Ring ist ein Körper. Da D/P ein Körper ist, ist P maximal. □

Der Ring D ist auch ganz abgeschlossen. Das heißt, wenn $\alpha \in F$ Nullstelle eines Polynoms aus $D[x]$ mit Leitkoeffizientem gleich 1, dann folgt sofort $\alpha \in D$. Dies zeigt man mit Prop. 6.1.4. In standard Algebra-Texten wird außerdem gezeigt, dass wenn ein Integritätsring noethersch ist, dann ist jedes Ideal Produkt von Primidealen auf eindeutige Weise. Ein solcher Ring ist also ein Dedekindring. Hier werden wir diese Tatsache allerdings auf eine andere Weise beweisen, indem wir ausnutzen, dass die sog. Klassenzahl von D endlich ist. Aber zunächst zeigen wir:

(i) Wenn A,B und C Ideale sind, und $AB = AC$ so folgt $B = C$.

(ii) Wenn A und B Ideale sind, und $A \subseteq B$, dann existiert ein Ideal C mit $A = BC$.

Lemma 3
Sei $A \trianglelefteq D$ ein Ideal. Ist $\beta \in F$ mit $\beta A \subseteq A$, dann $\beta \in D$.

Beweis.
Nach Prop. 12.2.2 ist A ein endlich erzeugtes $\mathbb{Z}$-Modul, also folgt die Behauptung mit Prop. 6.1.4. □

Lemma 4
Seien $A, B \trianglelefteq D$ Ideale mit $A = AB$, dann $B = D$.

Beweis.

Sei $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Ganzheitsbasis für A. Weil $A = AB$ gibt es $b_{ij} \in B$ mit $\alpha_i = \sum_j b_{ij}\alpha_j$. Es folgt das die Determinante der Matrix $(b_{ij} - \delta_{ij})_{ij}$ gleich 0 ist. Daraus folgt: $1 \in B \Rightarrow B = D$. □

Prop. 12.2.4
Seien $A, B \trianglelefteq D$ Ideale und $\omega \in D$ mit $(\omega)A = BA$. Dann $(\omega) = B$

Beweis.

Wenn $\beta \in B$ gilt $\beta\omega^{-1}A \subseteq A$ nach Voraussetzung, also nach Lemma 3: $\beta\omega^{-1} \in D$. Somit folgt $B \subseteq (\omega)$ und so ist $\omega^{-1}B \subseteq D$ ein Ideal. Weil $A = \omega^{-1}BA$ gilt nach Lemma 4: $\omega^{-1}B = D$ und so $(\omega) = B$. □

Quellen

Als Vorlage für diesen Vortrag diente Kapitel 12 §1, 2 des Buchs:

K. Ireland, M. Rosen "**A Classical Introduction to Modern Number Theory**", second edition, Springer, 1990.