Verzweigung und Trägheitsgrad

Seminar: Zahlentheorie, 10. Vortrag

Lara Eschenauer

21. Juni 2017

In diesem Vortrag wird die Dimension eines algebraischen Zahlenkörpers F mit den noch zu definierenden Verzweigungsindices und Trägheitsgraden gewisser Primideale des Rings der ganzalgebraischen Zahlen in F in Verbindung gesetzt.

Generalvoraussetzung. Sei F ein algebraischer Zahlenkörper von Dimension $|F : \mathbb{Q}| = n$, und sei $D \subseteq F$ der Ring der ganzalgebraischen Zahlen in F.

Vorüberlegungen: Sei $P \subseteq D$ ein Primideal.

- *Es existiert genau einen Primzahl $p \in Prim(\mathbb{Z})$ mit $p \in P$:* Der Schnitt $P \cap \mathbb{Z} \subseteq \mathbb{Z}$ ist nicht leer nach Lemma 2, ungleich $\mathbb{Z}$, da sonst $1 \in P$, also $P = D$, und abgeschlossen bezüglich der Addition.
  Ist $(a\mathbb{Z})(b\mathbb{Z}) \subseteq P \cap \mathbb{Z}$, so $(aD)(bD) \subseteq (P \cap \mathbb{Z})_D \subseteq P$, also $aD \subseteq P$ oder $bD \subseteq P$, also $a\mathbb{Z} = aD \cap \mathbb{Z} \subseteq P \cap \mathbb{Z}$ oder $b\mathbb{Z} = bD \cap \mathbb{Z} \subseteq P \cap \mathbb{Z}$.
  Damit ist $P \cap \mathbb{Z}$ ein Primideal von $\mathbb{Z}$; daher wird er von einer Primzahl $p \in \mathrm{Prim}(\mathbb{Z})$ erzeugt und enthält insbesondere keine weiteren Primzahlen.

- *Der Quotient D/pD besteht aus p^n Elementen:* Nach Proposition 12.2.2 existieren linear unabhängige $\omega_1, \dots \omega_n \in D$, sodass

  $$D = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n.$$

  Sei $S = \{\sum \gamma_i\omega_i \mid \gamma_i \in [0, p) \cap \mathbb{Z}\}$. Sei $\omega = \sum m_i\omega_i$, $m_i \in \mathbb{Z}$. Man findet $q_i, \gamma_i \in \mathbb{Z}$, $0 \leq \gamma_i < p$, sodass $m_i = q_ip + \gamma_i$, und es gilt

  $$\omega \equiv \sum \gamma_i\omega_i pD.$$

  Es ist $\sum \gamma_i\omega_i \in S$, also gibt es für jede Aq̈uivalenzklasse von D/pD mindestens einen Vertreter in S.
  Sei $\sum \gamma_i'\omega_i$ ein weiteres Element aus S mit $\sum \gamma_i\omega_i - \sum \gamma_i'\omega_i \equiv 0\ pD$, also $\sum(\gamma_i - \gamma_i')\omega_i \equiv 0\ pD$, also

  $$\sum(\gamma_i - \gamma_i')\omega_i = p\sum \delta_i\omega_i = \sum p\delta_i\omega_i$$

für gewisse $\delta_i \in \mathbb{Z}$. Es folgt aus der linearen Unabhängigkeit der ω_i, dass $\gamma_i - \gamma_i' = p\delta_i \in p\mathbb{Z}$. Wegen $0 \leq \gamma_i, \gamma_i' < p$ folgt $\gamma_i = \gamma_i'$.
Damit ist S ein Repräsentantensystem für D/pD, und es ergibt sich

$$|D/pD| = |S| = p^n.$$

- Anwendung des kanonischen Epimorphismus

$$\phi : D/pD \to D/P^j$$

für $1 \leq j \leq \mathrm{ord}_P(pD)$, gibt $|D/P^j| \cdot |\mathrm{Ker}(\phi)| = p^n$, also existiert ein $f \geq 1$ mit $|D/P^j| = p^f$.

Definition. Sei $P \subset D$ ein Primideal und sei $p \in P$ die Primzahl in P. Der Wert $\mathrm{ord}_P(pD) = \max\{t \geq 1 \mid pD \subseteq P^t\}$ heißt *Verzweigungsindex* von P.
Die Zahl $f \geq 1$ mit $|D/P| = p^f$ wird der *Trägheitsgradrad* von P gennant.

Es gibt eine bemerkenswerte Realation zwischen den Verzweigungsindices und Trägheitsgeraden gewisser Primideale von D und der Dimension $n = |F : \mathbb{Q}|$.

Theorem 3. *Sei $p \in \mathbb{P}$ und seien $P_1, \dots P_g$ die Primideale in D, die pD enthalten. Seien $e_i = ord_{P_i}(pD)$ die Verzweigungsindices und f_i die Trägheitsgrade der P_i. Dann ist*

$$\sum_{i=1}^{g} e_i f_i = n.$$

Wir verschieben den Beweis bis wir einen gewissen Hintergrund entwickelt haben.

Lemma. Sei R ein kommutativer Ring mit 1. Seien $A_1, \dots A_g \subseteq R$ Ideale, sodass $A_i + A_j = R$ für $i \neq j$. Dann ist

$$\bigcap_{i=1}^{g} A_i = \prod_{i=1}^{g} A_i.$$

Beweis. Der Beweis erfolgt per Induktion nach g. Für $g = 1$ ist die Aussage trivial.
Sei $g = 2$. „$\subseteq$“: Da $A_1 + A_2 = R$, findet man $a_1 \in A_1$, $a_2 \in A_2$, sodass

$a_1 + a_2 = 1$. Ist nun $a \in A_1 \cap A_2$, so gilt $a = aa_1 + aa_2 \in A_1A_2$. Es ergibt sich $A_1 \cap A_2 \subseteq A_1A_2$.
„$\supseteq$“: Trivial, denn für die Erzeuger a_1a_2, $a_i \in A_i$, ist offenbar $a_1a_2 \in A_1 \cap A_2$.
Sei nun $g > 2$, und die Aussage gelte für $g - 1$. Es ist

$$A_1 \cap A_2 \cap \cdots \cap A_g = A_1 \cap (A_2 \cap \cdots \cap A_g) \overset{IV}{=} A_1 \cap (A_2A_3 \dots A_g)$$

nach Induktionsvorraussetzung. Ist $A_1 + A_2A_3 \dots A_g = R$, so folgt das Gewünschte aus dem Fall $g = 2$. In der Tat ist

$$\begin{aligned} R &= (A_1 + A_2)(A_1 + A_3) \dots (A_1 + A_g) \\ &= A_1(\sum \dots) + A_2A_3 \dots A_g \subseteq A_1 + A_2A_3 \dots A_g \subseteq R. \end{aligned}$$

□

Beispiel. Seien $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$. Dann ist $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ nach Bezout, also $m\mathbb{Z} \cap n\mathbb{Z} = (m\mathbb{Z})(n\mathbb{Z})$.

Proposition 12.3.1. *Sei R ein kommutativer Ring mit 1 und seien $A_1, \dots, A_g \subseteq R$ Ideale, sodass $A_i + A_j = R$ für $i \neq j$. Sei $A = A_1A_2 \dots A_g$. Dann gilt*

$$R/A \cong R/A_1 \times R/A_2 \times \cdots \times R/A_g.$$

Beweis. Seien $\psi_i : R \to R/A_i$ die natürlichen Projektionen. Definiere

$$\psi : R \to R/A_1 \times R/A_2 \times \cdots \times R/A_g, x \mapsto (\psi_1(x), \dots, \psi_g(x)).$$

Dies ist offfensichtlich ein Homomorphismus. Aufgrund des ersten Isomorphiesatzes reicht es zu zeigen, dass ψ surjektiv ist und $\mathrm{Ker}(\psi) = A$.
Surjektiv: Es gilt nachzuweisen, dass für beliebige $x_1, \dots, x_g \in R$ ein $x \in R$ existiert, sodass $\psi_i(x) = x_i$, also $x \equiv x_i(A_i)$ für alle i.
Idee: Für alle i suche $u_i \in \bigcap_{j \neq i} A_j = \prod_{j \neq i} A_j$, sodass $u_i \equiv 1(A_i)$, das heißt sodass $v_i + u_i = 1$ für ein $v_i \in A_i$. Dann ist $x = x_1u_1 + \cdots + x_gu_g$ von der gesuchten Art.
Sei $i = 1$. Die Gleichung $v_1 + u_1 = 1$ ist äquivalent zu $A_1 + A_2A_3 \dots A_g = R$. Dies gilt wie im Lemma oben bereits gezeigt. Ähnlich argumentiert man für $i \neq 1$.
Kern: Offensichtlich ist $\mathrm{Ker}(\psi) = A_1 \cap A_2 \cap \cdots \cap A_g$. Das gewünschte folgt also aus vorigem Lemma. □

Diese Proposition nennt man den *Chinesischen Restsatz für Ringe*.

Beispiel: Chinesischer Restsatz für $\mathbb{Z}$. Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{e_i}$. Dan ist $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times p_r^{e_r}\mathbb{Z}$.

Zurück zu unserem kommutativen Ring D: Man möchte den Restsatz für den Beweis des Theorems nutzen. Es gilt also zu prüfen, ob Voraussetzungen der Proposition erfÏlt sind.
D ist ein kommutativer Ring mit 1; die $P_i^{e_i}$ sind Ideale von D, und erfüllen $pD = P_1^{e_1} \dots P_g^{e_g}$ nach Theorem 2. Folglich kann man den Chinesischen Restsatz für Ringe anwenden, falls $P_i^{e_i} + P_j^{e_j} = D$ für $i \neq j$.

Tatsächlich gilt die stärkere Aussage:

Lemma. Seien $P, Q \subset D$ zwei verschieden Primideale. Dann ist $P^a + Q^b = D$ für alle ganzen Zahlen $a, b \geq 1$.

Beweis. Per Induktion nach b: Sei $b = 1$. Zu zeigen: Für alle ganzen Zahlen $a \geq 1$ ist $P^a + Q = D$. Auch dies funktioniert per Induktion: Sei $a = 1$. Da $P, Q \subseteq D$ maximale Ideale sind, und $P \neq Q$, gilt $P + Q = D$. Sei nun $a > 1$ und die Behauptung gelte für $a - 1$. Es ist

$$\begin{aligned} P^a + Q &= P^a + PQ + Q \\ &= P(P^{a-1} + Q) + Q = P + Q = D. \end{aligned}$$

Damit ist der Induktionsanfang für die Induktion nach b gezeigt.
Sei nun $b > 1$ und für alle ganzen Zahlen $a \geq 1$ gilt $P^a + Q^{b-1} = D$. Dann ist

$$\begin{aligned} P^a + Q^b &= P^a + P^aQ + Q^b \\ &= P^a + (P^a + Q^{b-1})Q = P^a + Q = D \end{aligned}$$

für jede ganze Zahl $a \geq 1$. □

Zwischenbilanz: Es gilt $P_i^{e_i} + P_j^{e_j} = D$ für $i \neq j$ nach dem Lemma. Also ist Proposition 12.3.1 anwendbar und man erhält

$$D/pD \cong D/P_1^{e_1} \times D/P_2^{e_2} \times \cdots \times D/P_g^{e_g}.$$

Wie zu Anfang gezeigt gilt $|D/pD| = p^n$. Folglich

$$p^n = |D/pD| = |D/P_1^{e_1} \times D/P_2^{e_2} \times \cdots \times D/P_g^{e_g}| = \prod_{i=1}^{g} |D/P_i^{e_i}|.$$

Man erinnere sich, dass es sich bei den $|D/P_i^{e_i}|$ um p-Potenzen handelt. Da gerade $|D/P_i| = p^{f_i}$ ist, wäre es wünschenswert, wenn $|D/P_i^{e_i}| = |D/P_i|^{e_i}$.

In der Tat:

Proposition 12.3.2. *Sei $P \subseteq D$ ein Primideal, und sei $e \geq 1$. Dann ist*

$$|D/P^e| = |D/P|^e.$$

Beweis. Per Induktion nach $e \geq 1$: Die Aussage ist offenbar wahr, wenn $e = 1$. Ist $e > 1$, so ist $P^{e-1}/P^e \subseteq D/P^e$ eine Untergruppe und

$$(D/P^e)/(P^{e-1}/P^e) \cong D/P^{e-1}.$$

Lässt sich also zeigen, dass $|P^{e-1}/P^e| = p^f$, so folgt per Induktion nach $e \geq 1$, dass

$$|D/P^e| = |D/P^{e-1}| \cdot |P^{e-1}/P^e| = p^{(e-1)f} p^f = p^{ef}.$$

Anstelle von $|P^{e-1}/P^e| = p^f$ zeigen wir die stärkere Aussage

$$D/P \cong P^{e-1}/P^e,$$

indem wir einen surjektiven Homomorphismus $\alpha : D \to P^{e-1}/P^e$ erstellen.
Da $P^e \subsetneq P^{e-1}$, existiert ein $a \in P^{e-1} \setminus P^e$.
Behauptung: $(a) + P^e = P^{e-1}$: Da $P^e \subsetneq (a) + P^e$, existiert ein Ideal $Q \subseteq D$ mit

$$P^e = ((a) + P^e)Q$$

(vgl. Prop. 12.2.7). Unter Beachtung von Theorem 2 muss $(a) + P^e$ folglich eine Potenz von P sein, das heißt, es gibt ein $i \leq e - 1$ mit $(a) + P^e = P^i$; weil $(a) + P^e \subseteq P^{e-1}$, muss $i \geq e - 1$ gelten, also ist $(a) + P^e = P^{e-1}$.
Definiere

$$\alpha : D \to P^{e-1}/P^e, x \mapsto xa + P^e.$$

Dies ist ein surjektiver (Gruppen-) Homomorphismus (da $P^{e-1} = (a) + P^e$). Es gilt $x \in \mathrm{Ker}(\alpha)$ genau dann, wenn $xa \in P^e$, also genau dann, wenn $\mathrm{ord}_P(xa) \geq e$. Nun gilt nach Proposition 12.2.9(ii)

$$\mathrm{ord}_P(xa) = \mathrm{ord}_P((x)(a)) = \mathrm{ord}_P(x) + \mathrm{ord}_P(a).$$

Wegen $a \in P^{e-1} \setminus P^e$, also $(a) \subseteq P^{e-1}$ und $(a) \nsubseteq P^e$, ist $\mathrm{ord}_P(a) = e-1$, daher ist $x \in \mathrm{Ker}(\alpha)$ genau dann, wenn $\mathrm{ord}_P(x) \geq 1$, was äquivalent ist zu $x \in P$. Daher gilt nach dem ersten Isomorphiesatz für Gruppen $D/P \cong P^{e-1}/P^e$, und dies zeigt $|P^{e-1}/P^e| = p^f$. □

Wir können nun den Beweis von Theorem 3 abschließen: Nach Proposition 12.3.2 ist

$$p^n = \prod_{i=1}^{g} |D/P_i^{e_i}| = \prod_{i=1}^{g} p^{e_i f_i}.$$

Daraus folgt wie gewünscht $n = e_1 f_1 + e_2 f_2 + \cdots + e_g f_g$. □

Von nun an sei die Erweiterung $F/\mathbb{Q}$ galiossch; bei Vorliegen algebraischer Zahlenkörper, wie es hier der Fall ist, ist dies äquivalent dazu, dass alle Einbettungen von F in $\mathbb{C}$ bereits Automorphismen sind.
Die Galoisgruppe $G = Aut_{\mathbb{Q}}(F)$ besteht aus ebendiesen Automorphismen.

In diesem Fall lässt sich Theorem 3 noch verschärfen.:

Thorem 3′. *Sei $F/\mathbb{Q}$ eine Galois-Erweiterung. Sei $p \in \mathbb{Z}$, und seien $P_1, \dots P_g$ die Primideale in D, die pD enthalten. Seien $e_i = ord_{P_i}(pD)$ die Verzweigungsindices und f_i die Trägheitsgrade der P_i. Dann gelten*

$$e_1 = e_2 = \cdots = e_g \text{ und } f_1 = f_2 = \cdots = f_g.$$

Insbesondere ist $n = e_1 f_1 g$.

Auch für diesen Beweis braucht man noch etwas mehr Hintergrund.

Vorüberlegungen. Sei $A \subset D$ ein Ideal, $\sigma \in G$, und $\sigma A = \{\sigma(a) | a \in A\}$.

- *Es ist $\sigma A \subseteq D$:* Für $d \in D$ und $f \in \mathbb{Z}[X]$ normiert mit $f(d) = 0$ gilt $f(\sigma(d)) = \sigma(f(d)) = \sigma(0) = 0$, da $\sigma|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Also $\sigma(d) \in D$.
- *σA ist ein Ideal:* Es gilt $d\sigma(a) = \sigma(\sigma^{-1}(d)a) \in \sigma A$ für $d \in D$ und $a \in A$. Insbesondere ist $\sigma D = D$, weil $\sigma(1) = 1$.
- Es ist $D/\sigma A = \sigma D/\sigma A \cong D/A$ mittels $d + A \mapsto \sigma(d) + \sigma A$.
  Insbesondere folgt: Ist $P \subseteq D$ ein Primideal, so ist auch σP ein Primideal (wegen $P \subset D$ Primideal gdw. D/P Integritätsbereich).

Wie hilft uns das in der gegebenen Situation?

Proposition 12.3.3. *Sei $p \in \mathbb{P}$ eine Primzahl, und seien P_i und P_j zwei Primideale von D, die p enthalten. Dann existiert ein $\sigma \in G$, sodass $\sigma P_i = P_j$.*

Beweis. Angenommen, $P_j \notin \{\sigma P_i | \sigma \in G\}$. Da Primideale und maximale Ideale in D übereinstimmen sind jeweils $\sigma P_i + P_j = D$ und $\eta P_i + \sigma P_i = D$, für $\sigma, \eta \in G$, $\sigma P_i \neq \eta P_i$. Nach dem chinesischen Restsatz für Ringe (mit $A = P_j \cdot \prod_{\sigma P_i \in \{\sigma P_i | \sigma \in G\}} \sigma P_i$) existiert also ein $a \in P_j$ mit $a \equiv 1 (\sigma P_i)$ für alle $\sigma \in G$. Dann ist

$$N(a) = \prod_{\sigma \in G} \sigma(a) \in P_j \cap \mathbb{Z} = p\mathbb{Z}.$$

Insbesondere ist $N(a) \in P_i$, da $p\mathbb{Z} \subseteq pD \subseteq P_i$, also $\sigma(a) \in P_i$ für ein $\sigma \in G$, da P_i ein Primideal im kommutativen Ring D ist. Allerdings iist dann $a = \sigma^{-1}(\sigma(a)) \in \sigma^{-1} P_i$, obwohl $a \equiv 1 (\sigma^{-1} P_i)$ (Widerspruch!). □

Nun kann man das Theorem beweisen:

Beweis von Theorem 3′. Sei $i \in \{1, \ldots, g\}$. Nach obiger Proposition existiert ein $\sigma \in G$, sodass $\sigma P_1 = P_i$. Weil

$$D/P_1 \cong D/\sigma P_1 = D/P_i$$

also $p^{f_1} = |D/P_1| = |D/P_i| = p^{f_i}$ gilt, ist $f_1 = f_i$.
Weiter gilt

$$P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g} = pD = \sigma pD = \sigma(P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g}) = \sigma(P_1)^{e_1} \sigma(P_2)^{e_2} \ldots \sigma(P_g)^{e_g}.$$

Auf der linken Seite hat P_i den Exponenten e_i, auf der rechten Seite dagegen hat $P_i = \sigma P_1$ den Exponenten e_1. Aufgrund der eindeutigen Zerlegung von pD (Theorem 2), folgt $e_i = e_1$.
Damit sind $e_1 = e_2 = \cdots = e_g$ und $f_1 = f_2 = \cdots = f_g$. Da $\sum_{i=1}^{g} e_i f_i = n$ nach Theorem 3, gilt $e_1 f_1 g = n$. □

Literatur

Als Vorlage für diesen Vortrag diente Kapitel 12 §3 des Buchs:
K. Ireland, M. Rosen: A Classical Introduction to Modern Number Theory. second edition, Springer, New York, 1990.