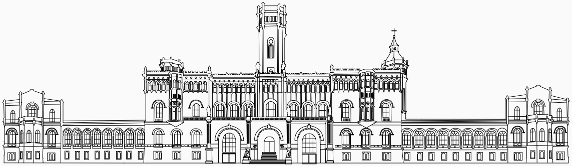
Leibniz Universität Hannover

Der Čebotarevsche Dichtigkeitssatz

Seminar Zahlentheorie

Leo Kayser

23. Juli 2020



Inhalt

Die Formulierung des Dichtigkeitssatzes

Zweierlei Maß auf der Menge der Primideale

Sei K ein Zahlkörper, wir notieren $\mathcal{P}_K := \{\, \mathfrak{p} \subset \mathcal{O}_K \mid \mathfrak{p} \text{ prim} \,\}$.

Definition 1: (Natürliche Dichtigkeit, Dirichletsche Dichtigkeit)

Sei $\mathcal{S} \subseteq \mathcal{P}_K$. Im Falle der Existenz des Grenzwertes

$$d(\mathcal{S}) = \lim_{x \to \infty} \frac{\#\{\, \mathfrak{p} \in \mathcal{S} \mid N(\mathfrak{p}) \leq x \,\}}{\#\{\, \mathfrak{p} \in \mathcal{P}_K \mid N(\mathfrak{p}) \leq x \,\}}$$

heißt $d(\mathcal{S})$ die natürliche Dichtigkeit von $\mathcal{S}$. Ebenso sei im Falle der Existenz

$$\delta(\mathcal{S}) = \lim_{s \searrow 1} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s}}$$

$\delta(\mathcal{S})$ die dirichletsche Dichtigkeit (oder einfach nur Dichtigkeit) von $\mathcal{S}$.

Ist dieser Bruch überhaupt definiert?

Definition 2: (Dedekindsche Zetafunktion)

Die für jedes $\delta > 0$ auf $\mathrm{Re}(s) > 1 + \delta$ absolut gleichmäßig konvergente Reihe

$$\zeta_K(s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} N(\mathfrak{a})^{-s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad a_n = \#\{\, \mathfrak{a} \subseteq \mathcal{O}_K \mid N(\mathfrak{a}) = n \,\}$$

definiert eine auf $\mathrm{Re}(s) > 1$ holomorphe Funktion, die Dedekindsche Zetafunktion.

$\Longrightarrow$ Für $s > 1$ ist

$$\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s} \leq \sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s} \leq \zeta_K(s) < \infty.$$

Eigenschaften der dirichletschen Dichtigkeit

Lemma 3: Eigenschaften von δ

Seien $\mathcal{S}, \mathcal{T} \subseteq \mathcal{P}_K$ Teilmengen, die eine Dichtigkeit besitzen. Dann ist

(i) $\delta(\mathcal{S}) \in [0,1]$, $\delta(\mathcal{P}_K) = 1$.

(ii) Falls $\mathcal{S} \subseteq \mathcal{T}$, so ist $\delta(\mathcal{S}) \leq \delta(\mathcal{T})$, und $\mathcal{T} \setminus \mathcal{S}$ hat Dichtigkeit $\delta(\mathcal{T}) - \delta(\mathcal{S})$.

(iii) Sind $\mathcal{S}$ und $\mathcal{T}$ disjunkt, so besitzt $\mathcal{S} \,\dot\cup\, \mathcal{T}$ Dichtigkeit $\delta(\mathcal{S}) + \delta(\mathcal{T})$.

(iv) Mengen $\mathcal{E}$ mit $\sum_{\mathfrak{p} \in \mathcal{E}} N(\mathfrak{p})^{-1} < \infty$ (etwa wenn $\#\mathcal{E} < \infty$) haben Dichtigkeit 0.

(v) Sind $\mathcal{S} \setminus \mathcal{T}$ und $\mathcal{T} \setminus \mathcal{S}$ endlich, so ist $\delta(\mathcal{S}) = \delta(\mathcal{T})$.

Beweis.

(i) Für $s > 1$ ist $0 \leq \sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s} \leq \sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s}$, also liegt der Bruch stets in $[0,1]$.

Beweis von Lemma 3

(ii) Falls $\mathcal{S} \subseteq \mathcal{T}$, so ist $\delta(\mathcal{S}) \leq \delta(\mathcal{T})$, und $\mathcal{T} \setminus \mathcal{S}$ hat Dichtigkeit $\delta(\mathcal{T}) - \delta(\mathcal{S})$.

Die Reihe über $\mathfrak{p} \in \mathcal{T}$ beinhaltet die Summanden der Reihe über $\mathfrak{p} \in \mathcal{S}$.
Die zweite Aussage ist Linearität des Grenzwerts.

(iii) Sind $\mathcal{S}$ und $\mathcal{T}$ disjunkt, so besitzt $\mathcal{S} \,\dot{\cup}\, \mathcal{T}$ Dichtigkeit $\delta(\mathcal{S}) + \delta(\mathcal{T})$.

Folgt ebenfalls aus der Linearität des Grenzwerts.

(iv) Mengen $\mathcal{E}$ mit $\sum_{\mathfrak{p} \in \mathcal{E}} N(\mathfrak{p})^{-1} < \infty$ haben Dichtigkeit 0.

Würde sofort folgt, wenn $\sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-1} = \infty$; dies werden wir später sehen.

(v) Sind $\mathcal{S} \setminus \mathcal{T}$ und $\mathcal{T} \setminus \mathcal{S}$ endlich, so ist $\delta(\mathcal{S}) = \delta(\mathcal{T})$.

Da $\mathcal{S} \,\dot{\cup}\, (\mathcal{T} \setminus \mathcal{S}) = \mathcal{S} \cup \mathcal{T} = \mathcal{T} \,\dot{\cup}\, (\mathcal{S} \setminus \mathcal{T})$, ist

$$\delta(\mathcal{S}) \overset{\text{(iv)}}{=} \delta(\mathcal{S}) + \delta(\mathcal{T} \setminus \mathcal{S}) \overset{\text{(iii)}}{=} \delta(\mathcal{T}) + \delta(\mathcal{S} \setminus \mathcal{T}) \overset{\text{(iv)}}{=} \delta(\mathcal{T}). \qquad \square$$

Nur über $\mathbb{Q}$ „fleißige“ Primideale zählen

Beispiel 4: (Primideale mit Primzahlnorm)

Sei $\mathcal{P}_{K,1} := \{\, \mathfrak{p} \in \mathcal{P}_K \mid N(\mathfrak{p}) \text{ ist prim} \,\}$ und $\mathcal{P}_{K,\geq 2} := \mathcal{P}_K \setminus \mathcal{P}_{K,1}$. Dann ist

$$\delta(\mathcal{P}_{K,1}) = 1, \qquad \delta(\mathcal{P}_{K,\geq 2}) = 0.$$

In der Tat, zu gegebener Primzahl $p \in \mathcal{P}_{\mathbb{Q}}$ gibt es höchstens $[K : \mathbb{Q}]$ verschiedene Primideale mit Absolutnorm p^f $(f \geq 1)$, je nach Zerlegung. Daher ist

$$\sum_{\mathfrak{p} \in \mathcal{P}_{K,\geq 2}} N(\mathfrak{p})^{-1} \leq \sum_{p \in \mathcal{P}_{\mathbb{Q}}} \frac{[K : \mathbb{Q}]}{p^2} \leq [K : \mathbb{Q}] \cdot \zeta_{\mathbb{Q}}(2) < \infty.$$

Mit Lemma 3(iv) schließen wir $\delta(\mathcal{P}_{K,\geq 2}) = 0$, aus 3(ii) folgt $\delta(\mathcal{P}_{K,1}) = 1$.

Das Artinsymbol in nicht-abelschen Erweiterungen

- Sei L/K eine galoissche Erweiterung von Zahlkörpern; $\mathfrak{p} \in \mathcal{P}_K$ unverzweigt in L.
  $\rightsquigarrow$ Verschiedene Primideale $\mathfrak{P}/\mathfrak{p}$ liefern ggf. unterschiedliche $\left(\frac{L/K}{\mathfrak{P}}\right) \in G = \mathrm{Gal}(L/K)$.
- Sind allerdings $\mathfrak{P}, \mathfrak{P}' \in \mathcal{P}_L$, so ist ([Neu92, Satz I.9.1], [Cox14, Corollary 5.21])

$$\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P}' \cap \mathcal{O}_K \quad \Longleftrightarrow \quad \mathfrak{P}' = \sigma(\mathfrak{P}),\ \sigma \in G \quad \Longrightarrow \quad \left(\frac{L/K}{\mathfrak{P}'}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}.$$

- Dies zeigt, dass die Menge

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \left\{ \left(\frac{L/K}{\mathfrak{P}}\right) \,\middle|\, \mathfrak{P}/\mathfrak{p} \right\} \subseteq G$$

eine Konjugationsklasse $C_G(\tau)$ in Galoisgruppe bildet.

Satz 5: (Čebotarevscher Dichtigkeitssatz)

Sei $\mathcal{C} = C_G(\tau)$ eine Konjugationsklasse in G. Dann besitzt die Menge

$$\mathcal{S} = \left\{ \mathfrak{p} \in \mathcal{P}_K \;\middle|\; \mathfrak{p} \text{ ist unverzweigt in } L \text{ und } \left(\tfrac{L/K}{\mathfrak{p}}\right) = \mathcal{C} \right\}$$

die Dirichletsche Dichtigkeit, und sogar die natürliche Dichtigkeit

$$\delta(\mathcal{S}) = \frac{|\mathcal{C}|}{|G|} = \frac{|\mathcal{C}|}{[L:K]}.$$

Insbesondere enthält $\mathcal{S}$ stets unendlich viele Primideale.

Beweis. [Jan96, Chapter V, Theorem 10.4], den abelschen Fall beweisen wir später! ($\square$)

Ein numerisches Beispiel

Beispiel 6: (Der Zerfällungskörper von $x^3 - 2$) Sei $K = \mathbb{Q}$, L der Zerfällungskörper von $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ und $G = \mathrm{Gal}(L/K) \cong S_3$.

Die Konjugationsklassen dieser Gruppe sind

(1) die Identität $\{\mathrm{id}\}$,
(2) die drei Transpositionen $\{(12), (23), (13)\}$ und
(3) die zwei 3-Zykel $\{(123), (132)\}$.

Betrachte die ersten Primzahlen bis N und zähle, wie oft welche Klasse als $\left(\frac{L/K}{(p)}\right)$ auftritt, so erwarten wir annähernd

Klasse	$C_G(\mathrm{id})$	$C_G((12))$	$C_G((123))$
Anteil	$\frac{1}{6} = 0,1\overline{6}$	$\frac{1}{2} = 0.5$	$\frac{1}{3} = 0.\overline{3}$

Der Magma-Code

Beispiel Folgender Magma-Code berechnet den tatsächlichen Anteil für uns:

```
_<x> := PolynomialRing(Rationals());
L := SplittingField(x^3-2);
G := GaloisGroup(L);
dL := Discriminant(Integers(L));
N := 1000000;
count := {**}; // Multimenge, zählt Auftreten der Repräsentanten.
for p in PrimesUpTo(N) do
   if not IsZero(dL mod p) then // Verzweigung abfangen.
      Include(~count,ClassRepresentative(G,FrobeniusElement(L,p)));
   end if;
end for;
print [RealField() | c/#count : c in Multiplicities(count)];
```

Unmittelbare Anwendungen

Es gibt unendlich viele voll zerlegte Primideale

Korollar 7: (Dichtigkeitssatz für abelsche Erweiterungen)

Sei L/K eine Erweiterung von Zahlkörpern, N die normale Hülle von L über K.

(i) $\mathfrak{p} \in \mathcal{P}_K$ ist genau dann in L voll zerlegt, wenn $\mathfrak{p}$ in N voll zerlegt ist.

(ii) Die Menge der voll zerlegten Primideale von K in L besitzt Dichtigkeit $\frac{1}{[N:K]}$.

Beweis. (i) Ist aus Zahlentheorie I bekannt, siehe etwa [Neu92, Kapitel I.9 Aufgabe 4].

(ii) Wegen (i) können wir L durch N ersetzen.

$$\mathfrak{p} \text{ voll zerlegt} \iff \mathfrak{p} \text{ unverzweigt und } f_{\mathfrak{P}/\mathfrak{p}} = 1 \iff \left(\frac{N/K}{\mathfrak{p}}\right) = \mathrm{id}_N$$

Die voll zerlegten Primideale entsprechen also der einelementigen Konjugationsklasse $\mathcal{C} = \{\mathrm{id}_N\} \subset G$. Damit folgt die Aussage aus dem Dichtigkeitssatz 5. □

Die Artinabbildung ist *sehr* surjektiv

Korollar 8: (Dichtigkeitssatz für abelsche Erweiterungen)

Sei L/K eine abelsche Erweiterung und $\mathfrak{m}$ ein Modulus, den alle in L verzweigten Primideale teilen. Sei ein Element $\sigma \in G$ gegeben, dann hat die Menge

$$\mathcal{S} = \left\{ \mathfrak{p} \nmid \mathfrak{m} \;\middle|\; \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma \right\}$$

die Dichtigkeit $\delta(\mathcal{S}) = \frac{1}{[L:K]}$, und ist unendlich.

Beweis. Da $\mathcal{S}$ bis auf endlich viele Teiler von $\mathfrak{m}$ mit der Menge

$$\left\{ \mathfrak{p} \in \mathcal{P}_K \;\middle|\; \mathfrak{p} \text{ ist unverzweigt in } L \text{ und } \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma \right\}$$

übereinstimmt, besitzt $\mathcal{S}$ nach Satz 5 Dichtigkeit $\delta(\mathcal{S}) = \frac{1}{[L:K]}$. □

Satz 9: (Dirichletscher Primzahlsatz)

Sind a, n teilerfremde natürliche Zahlen. Dann ist

$$\delta(\{\, p \text{ **Primzahl** } \mid p \equiv a \bmod n \,\}) = \frac{1}{\varphi(n)}.$$

Beweis. Sei $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta_n)$ für eine feste primitive n-te Einheitswurzel, $\mathfrak{m} = (n) \subseteq \mathbb{Z}$. Dann ist nach dem letzten Vortrag für $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ und $p \nmid n$

$$p \equiv a \bmod n \quad \Longleftrightarrow \quad \left(\frac{L/K}{p}\right) = (\zeta_n \mapsto \zeta_n^a) \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Die Aussage nun aus dem Dichtigkeitssatz 8 für die abelsche Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ vom Grad $\varphi(n)$.

Zerlegte Primideale bestimmen die Erweiterung

Voll zerlegte Primideale

Definition 10: $(\mathrm{Spl}_{L/K}, \widetilde{\mathrm{Spl}}_{L/K})$

Sei L/K eine Erweiterung von Zahlkörpern. Wir notieren

$$\mathrm{Spl}_{L/K} := \{\, \mathfrak{p} \in \mathcal{P}_K \mid \mathfrak{p} \text{ ist voll zerlegt in } L \,\}\,.$$

für die Menge der in L voll zerlegten Primideale aus K. Sei weiterhin

$$\widetilde{\mathrm{Spl}}_{L/K} := \left\{\, \mathfrak{p} \in \mathcal{P}_K \;\middle|\; \mathfrak{p} \text{ unverzweigt in } L \text{ und } f_{\mathfrak{P}/\mathfrak{p}} = 1 \text{ für ein } \mathfrak{P} \in \mathcal{P}_L \,\right\}.$$

- $\mathrm{Spl}_{L/K} \subseteq \widetilde{\mathrm{Spl}}_{L/K}$
- L/K galois $\implies \mathrm{Spl}_{L/K} = \widetilde{\mathrm{Spl}}_{L/K}$, da $f_{\mathfrak{P}/\mathfrak{p}}$, $e_{\mathfrak{P}/\mathfrak{p}}$ unabhängig von $\mathfrak{P}$ über $\mathfrak{p}$. (♣)

Fast gleiche Mengen

Seien $\mathcal{S}, \mathcal{T}$ Mengen. Wir schreiben

- $\mathcal{S} \mathrel{\dot\subseteq} \mathcal{T}$, falls $\mathcal{S} \subseteq \mathcal{T} \cup \Sigma$ für eine endliche Menge $\Sigma \subseteq \mathcal{P}_K$;
- $\mathcal{S} \doteq \mathcal{T}$, falls $\mathcal{S} \mathrel{\dot\subseteq} \mathcal{T}$ und $\mathcal{T} \mathrel{\dot\subseteq} \mathcal{S}$.

Satz 11

Seien L und M endliche Erweiterungen von K.

(i) Ist L/K galoissch, so gilt $L \subseteq M \iff \widetilde{\mathrm{Spl}}_{M/K} \mathrel{\dot\subseteq} \mathrm{Spl}_{L/K}$.

(ii) Ist M/K galoissch, so gilt $L \subseteq M \iff \mathrm{Spl}_{M/K} \mathrel{\dot\subseteq} \mathrm{Spl}_{L/K}$.

Beweis von Satz 11 (i): L/K galois $\rightsquigarrow$ $L \subseteq M \iff \widetilde{\mathrm{Spl}}_{M/K} \dot{\subseteq} \mathrm{Spl}_{L/K}$

Beweis. (i) „$\Rightarrow$“: Sei $\mathfrak{p} \in \widetilde{\mathrm{Spl}}_{M/K}$.

- $e_{(-)/\mathfrak{p}}$, $f_{(-)/\mathfrak{p}}$ sind multiplikativ im Turm $M/L/K \implies \mathfrak{p} \in \widetilde{\mathrm{Spl}}_{L/K}$
- L/K galoissch $\overset{(\clubsuit)}{\implies} \mathfrak{p} \in \mathrm{Spl}_{L/K}$

„$\Leftarrow$“: Sei N eine Galoiserweiterung von K, welche L und M enthält.

$$\begin{tikzcd}[column sep=small] & N \arrow[dl, dash] \arrow[dr, dash] & \\ L \arrow[rr, dashed, dash, "?"] & & M \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \qquad \overset{\text{HS}}{\leftrightsquigarrow} \qquad \begin{tikzcd}[column sep=small] & 1 \arrow[dl, dash] \arrow[dr, dash] & \\ \mathrm{Gal}(N/L) \arrow[rr, dashed, dash, "?"] & & \mathrm{Gal}(N/M) \\ & \mathrm{Gal}(N/K) \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$$\rightsquigarrow \quad L \subseteq M \iff \mathrm{Gal}(N/M) \subseteq \mathrm{Gal}(N/L) \iff \sigma_{|L} = \mathrm{id}_L \ \forall \sigma \in \mathrm{Gal}(N/M).$$

Beweis von Satz 11 (i): Eine Zwischenbehauptung

Sei also $\sigma \in G := \mathrm{Gal}(N/M)$. Nach dem Dichtigkeitssatz 5 gibt es ein in N unverzweigtes $\mathfrak{p} \in \mathcal{P}_K$ mit $\left(\frac{N/K}{\mathfrak{p}}\right) = C_G(\sigma)$, also ein $\mathfrak{P} \in \mathcal{P}_N$ mit $\left(\frac{N/K}{\mathfrak{P}}\right) = \sigma$.

Behauptung: $\mathfrak{p} \in \widetilde{\mathrm{Spl}}_{M/K}$ Z.z. ist $f(\mathfrak{P}'/\mathfrak{p}) = 1$ für ein $\mathfrak{P}'/\mathfrak{p}$.

Sei $\mathfrak{P}' := \mathfrak{P} \cap \mathcal{O}_M$. Dann gilt für $\alpha \in \mathcal{O}_M$

$$\alpha \overset{\sigma \in G}{=} \sigma(\alpha) = \left(\frac{N/M}{\mathfrak{P}}\right)(\alpha) \overset{\mathrm{Def}}{\equiv} \alpha^{N\mathfrak{p}} \bmod \mathfrak{P}'.$$

In diesem endlichen Körper ist nun $\mathrm{Fix}\left(\mathcal{O}_M/\mathfrak{P}', (-)^{N\mathfrak{p}}\right) = \mathcal{O}_K/\mathfrak{p}$, daher folgt

$$\mathcal{O}_M/\mathfrak{P}' = \mathcal{O}_K/\mathfrak{p} \quad \Longrightarrow \quad f(\mathfrak{P}'/\mathfrak{p}) = 1.$$

Beweis von Satz 11(i): Der Dichtigkeitssatz kommt ins Spiel

Nach dem Dichtigkeitssatz gibt es unendlich viele solcher $\mathfrak{p}$.

Nach Annahme ist $\widetilde{\mathrm{Spl}}_{M/K} \dot{\subseteq} \mathrm{Spl}_{L/K} \implies$ es gibt ein $\mathfrak{p} \in \mathcal{P}_K$ mit

- $\mathfrak{p}$ ist unverzweigt und $\left(\frac{N/K}{\mathfrak{p}}\right) = C_G(\sigma)$; sei $\mathfrak{P}/\mathfrak{p}$ prim mit $\sigma = \left(\frac{N/K}{\mathfrak{P}}\right)$.
- $\mathfrak{p} \in \mathrm{Spl}_{L/K}$, d.h. $\mathfrak{p}$ ist in L voll zerlegt, d.h. $\left(\frac{L/K}{\mathfrak{p}}\right) = \{\mathrm{id}_L\}$

Da das Artinsymbol mit Zwischenkörpern verträglich ist (r = Restriktion), folgt

$$\sigma_{|L} = r \circ \left(\frac{N/K}{\mathfrak{P}}\right) = \left(\frac{L/K}{\mathfrak{P} \cap L}\right) = \left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{id}_L.$$

Beweis von Satz 11 (ii): M/K galois $\rightsquigarrow L \subseteq M \iff \mathrm{Spl}_{M/K} \dot{\subseteq} \mathrm{Spl}_{L/K}$

(ii) „$\Rightarrow$“: Genauso wie bei (i).

„$\Leftarrow$“: Sei L' die normale Hülle von L über K; nach Satz 7(i) ist $\mathrm{Spl}_{L/K} = \mathrm{Spl}_{L'/L}$.

$$\rightsquigarrow \quad \widetilde{\mathrm{Spl}}_{M/K} \overset{(\clubsuit)}{=} \mathrm{Spl}_{M/K} \dot{\subseteq} \mathrm{Spl}_{L/K} = \mathrm{Spl}_{L'/K} .$$

Mit der Aussage aus (i) folgern wir $L \subseteq L' \overset{\text{(i)}}{\subseteq} M$. $\square$

Galoiserweiterungen sind bestimmt durch $\operatorname{Spl}_{L/K}$

Korollar 12

Seien L und M Galoiserweiterungen von K. Dann ist

(i) $L \subseteq M \iff \operatorname{Spl}_{M/K} \subseteq \operatorname{Spl}_{L/K} \iff \operatorname{Spl}_{M/K} \dot{\subseteq} \operatorname{Spl}_{L/K}$.

(ii) $L = M \iff \operatorname{Spl}_{M/K} = \operatorname{Spl}_{L/K} \iff \operatorname{Spl}_{M/K} \doteq \operatorname{Spl}_{L/K}$.

Beweis. (i) ist ein Spezialfall von Satz 11; (ii) folgt sofort aus (i). □

Verfeinerung eines Satzes von gestern

Korollar 13: (Eine Verschärfung von [Cox14, Corollary 8.7])

Sei L/K abelsch. Wir haben folgende Äquivalenz

$$L \subseteq M \quad \Longleftrightarrow \quad \exists \mathfrak{m} : \ \ker(\Phi_{L/M,\mathfrak{m}}) \cap \mathcal{P}_K \mathrel{\dot{\subseteq}} \ker(\Phi_{L/K,\mathfrak{m}}) \cap \mathcal{P}_K ,$$

wobei $\mathfrak{m}$ von allen in L oder M verzweigenden Primidealen aus $\mathcal{P}_K$ geteilt wird.

Beweis. Die Menge ist fast $\mathrm{Spl}_{L/K}$ (bzw. $\mathrm{Spl}_{M/K}$):

$$\ker(\Phi_{L/K,\mathfrak{m}}) \cap \mathcal{P}_K \doteq \left\{ \mathfrak{p} \in \mathcal{P}_K \;\middle|\; \mathfrak{p} \text{ unverzweigt und } \left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{id}_L \right\} = \mathrm{Spl}_{L/K},$$

daher folgt die Aussage aus vorigem Satz. $\square$

Zusammenhang mit unserer Leitfrage

Sei $n \in \mathbb{N}$ quadratfrei, $n \not\equiv 3 \bmod 4$ und $K = \mathbb{Q}(\sqrt{-n})$.

Satz 14: (Charakterisierung des Hilbertschen Klassenkörpers)

Ist $M/\mathbb{Q}$ eine Galoiserweiterung, so sind äquivalent:

(a) $\mathrm{Spl}_{M/\mathbb{Q}} \doteq \mathcal{L} = \{\, p \text{ prim} \mid p = x^2 + ny^2 \,\}$;

(b) M ist der Hilbertsche Klassenkörper L von K.

Beweis. Für eine Primzahl $p \nmid 2n$ sind nach [Cox14, Theorem 5.26]

$$p = x^2 + ny^2 \iff p \text{ ist voll zerlegt in } L.$$

$\mathcal{L}$ stimmt also bis auf die $p \mid 2n$ mit der Menge $\mathrm{Spl}_{L/\mathbb{Q}}$ überein.

Nach Korollar 12 ist $L = M$ genau dann wenn $\mathrm{Spl}_{M/\mathbb{Q}} \doteq \mathrm{Spl}_{L/\mathbb{Q}}$. $\square$

Eine Beweisskizze des Dichtigkeitssatzes

Abelsche Charaktere

Sei G eine endliche abelsche Gruppe. Die Charaktergruppe von G ist

$$\widehat{G} := \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}^\times) = \{\, \chi\colon G \to \mathbb{C}^\times \text{ Gruppenhom.} \,\}\,.$$

Lemma 15 Seien $\chi_1, \chi_2 \in \widehat{G}$, $\sigma, \tau \in G$.

(a) $|\widehat{G}| = |G|$.

(b) $\sum_{\sigma \in G} \chi_1(\sigma^{-1})\chi_2(\sigma) = |G|$ falls $\chi_1 = \chi_2$, 0 sonst.

(c) $\sum_{\chi \in \widehat{G}} \chi(\sigma^{-1})\chi(\tau) = |G|$ falls $\sigma = \tau$, 0 sonst. (Die Orthogonalitätsrelationen)

(d) $\prod_{\chi \in \widehat{G}} (1 - \chi(\sigma)) = (1 - X^f)^{|G|/f}$, wobei $f = \mathrm{ord}_G(\sigma)$.

Dirichletsche L-Reihen

Sei K ein Zahlkörper, $\mathfrak{m} = \mathfrak{c}\mathfrak{m}_\infty$ ein Modulus für K, $\mathrm{Cl}(\mathfrak{m}) := I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$.

Definition 16: (Dirichletsche L-Reihe)

Sei χ ein Charakter von $\mathrm{Cl}(\mathfrak{m})$. Die Dirichletsche L-Reihe ist

$$L_{\mathfrak{c}}(s,\chi) := \sum_{(\mathfrak{a},\mathfrak{c})=1} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}\nmid\mathfrak{c}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} \qquad \mathrm{Re}(s) > 1.$$

Spezialfall $\chi = 1$ (konstant): Dedekindsche Zetafunktion

$$\zeta_{K,\mathfrak{c}}(s) = L_{\mathfrak{c}}(s,1) = \sum_{(\mathfrak{a},\mathfrak{c})=1} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}\nmid\mathfrak{c}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}.$$

Analytische Fortsetzbarkeit

Satz 17: (Existenz der analytischen Fortsetzung über 1 hinweg)

$L_{\mathfrak{c}}(s, \chi)$ besitzt eine analytische Fortsetzung auf die Halbebene $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$.

- Ist $\chi = 1$, so hat $L_{\mathfrak{c}}(s, 1) = \zeta_{K,\mathfrak{c}}(s)$ einen einfachen Pol bei $s = 1$.
- Anderenfalls ist $L_{\mathfrak{c}}(s, \chi)$ holomorph auf der gesamten Halbebene.

Sei nun L/K abelsch und $\mathfrak{m}$ so gewählt (Artin-Reziprozität), dass $\ker(\Phi_{\mathfrak{m}})$ eine Kongruenzuntergruppe ist.

Wir haben einen surjektiven Gruppenhomomorphismus $\overline{\Phi}_{\mathfrak{m}} \colon \mathrm{Cl}(\mathfrak{m}) \to G := \mathrm{Gal}(L/K)$.

$$\rightsquigarrow \qquad \widehat{G} \ni (\chi \colon G \to \mathbb{C}^\times) \quad \xmapsto{\circ \overline{\Phi}_{\mathfrak{m}}} \quad (\chi \circ \overline{\Phi}_{\mathfrak{m}} \colon \mathrm{Cl}(\mathfrak{m}) \to \mathbb{C}^\times) \in \widehat{\mathrm{Cl}(\mathfrak{m})}$$

Darstellung der Zetafunktion

Satz 18

Sei $\mathfrak{C} = \mathfrak{c}\mathcal{O}_L$, dann ist

$$\zeta_{L,\mathfrak{C}}(s) = \prod_{\chi \in \widehat{G}} L_{\mathfrak{c}}(s, \chi \circ \overline{\Phi}_{\mathfrak{m}}).$$

Beweis. Sei zunächst $\mathfrak{p} \nmid \mathfrak{m}$ prim fest. Die Primideale $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ haben alle Trägheitsgrad $f = f_{\mathfrak{P}_i/\mathfrak{p}}$, die Ordnung von $\Phi_{\mathfrak{m}}(\mathfrak{p}) = \left(\frac{L/K}{\mathfrak{p}}\right)$ ist f.

$$\prod_{\mathfrak{P}/\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right) \overset{N(\mathfrak{P})=N(\mathfrak{p})^f}{=} \left(1 - \frac{1}{N(\mathfrak{p})^{sf}}\right)^{|G|/f} \overset{\text{Lem. 15}}{=} \prod_{\chi \in \widehat{G}} \left(1 - \frac{\chi(\overline{\Phi}_{\mathfrak{m}}(\mathfrak{p}))}{N(\mathfrak{p})^s}\right).$$

Produkt über alle $\mathfrak{p} \nmid \mathfrak{m}$ von beiden Seiten $\rightsquigarrow$ Eulerprodukte^{-1} der obigen Funktionen. $\square$

$L_{\mathfrak{c}}(1, \chi_1) \neq 0$

Korollar 19

(i) Ist $\chi_1 \in \widehat{G}$ nichttrivial, so ist $L_{\mathfrak{c}}(1, \chi_1) \neq 0$.

(ii) $\zeta_{K,\mathfrak{c}}(s)$ hat Wachstumsverhalten $\log \zeta_{K,\mathfrak{c}}(s) = -\log(s-1) + O(1), \quad s \to 1^+$.

Beweis. (i) Da $\overline{\Phi}_{\mathfrak{m}} : \operatorname{Cl}(\mathfrak{m}) \to G$ surjektiv ist, ist $\chi \circ \overline{\Phi}_{\mathfrak{m}}$ nichttrivial für $\chi \neq 1$, insbesondere ist $L_{\mathfrak{c}}(s, \chi \circ \overline{\Phi}_{\mathfrak{m}})$ holomorph um 1.

$$\underbrace{\zeta_{L,\mathfrak{C}}(s)}_{\text{Pol von Ord. 1}} = \underbrace{\zeta_{K,\mathfrak{c}}(s)}_{\text{Pol von Ord. 1}} \cdot \prod_{\substack{\chi \in \widehat{G} \\ \chi \neq 1}} \underbrace{L_{\mathfrak{c}}(s, \chi \circ \overline{\Phi}_{\mathfrak{m}})}_{\text{regulär in 1}}$$

Wäre ein $L_{\mathfrak{c}}(1, \chi) = 0$, so würde sich der Pol wegkürzen. $\lightning$

(ii) ist eine Umformulierung der Aussage, dass $\zeta_{K,\mathfrak{c}}(s)$ einen einfachen Pol bei 1 hat. $\square$

Nur Primideale zählen

Lemma 20 Sei χ ein Charakter von $\mathrm{Cl}(\mathfrak{m})$, dann ist

$$\log L_{\mathfrak{c}}(s,\chi) = \sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} + O(1), \quad s \to 1^+.$$

Insbesondere ist $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s} = -\log(s-1) + O(1)$ (was Lemma 3(iv) beweist).

„Beweis“. Setzen wir für die $L_{\mathfrak{c}}(s,\chi)$ das Eulerprodukt ein, erhalten wir

$$\log \prod_{\mathfrak{p}\nmid\mathfrak{c}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{\mathfrak{p}\nmid\mathfrak{c}} -\log\left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right) \overset{\text{log-Reihe}}{=} \sum_{\mathfrak{p}\nmid\mathfrak{c}} \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^k$$

Man *kann zeigen*, dass $\sum_{\mathfrak{p}\nmid\mathfrak{c}} \sum_{k=2}^{\infty} \frac{\chi(\mathfrak{p})^k}{k \cdot N(\mathfrak{p})^{ks}}$ für $s \to 1^+$ beschränkt bleibt. „$\square$“

Der Beweis des Dichtigkeitssatzes für abelsche Erweiterungen

Sei $\sigma \in \mathrm{Gal}(L/K)$ und $\mathcal{S} = \left\{ \mathfrak{p} \in \mathcal{P}_K \;\middle|\; \mathfrak{p} \nmid \mathfrak{c}, \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma \right\}$. Wir wollen also zeigen, dass

$$\delta(\mathcal{S}) = \lim_{s \searrow 1} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s}} = \frac{1}{|G|}.$$

Wir wenden das Dirichletsche Charakterargument an: Wir werten

$$f(s) := \sum_{\chi \in \widehat{G}} \chi(\sigma^{-1}) \log L_{\mathfrak{c}}(s, \chi \circ \overline{\Phi}_{\mathfrak{m}}).$$

auf zwei verschiedene Weisen aus.

Einerseits ist nach Korollar 19 und Lemma 20

$$f(s) = \log \zeta_{K,\mathfrak{c}}(s) + O(1) = \sum_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-s} + O(1).$$

Der Orthogonalitätstrick

Andererseits ist nach vorangegangenem Lemma 20

$$\begin{aligned}
\sum_{\chi\in\widehat{G}} \chi(\sigma^{-1}) \log L_{\mathfrak{c}}(s, \chi\circ\overline{\Phi}_{\mathfrak{m}}) &= \sum_{\chi\in\widehat{G}} \chi(\sigma^{-1}) \sum_{\mathfrak{p}\nmid\mathfrak{c}} \frac{\chi(\overline{\Phi}_{\mathfrak{m}}(\mathfrak{p}))}{N(\mathfrak{p})^s} + O(1) \\
&= \sum_{\mathfrak{p}\nmid\mathfrak{c}} \left(\sum_{\chi\in\widehat{G}} \chi(\sigma^{-1})\chi(\overline{\Phi}_{\mathfrak{m}}(\mathfrak{p})) \right) \frac{1}{N(\mathfrak{p})^s} + O(1) \\
&\overset{\text{Ortho.}}{=} \sum_{\substack{\mathfrak{p}\nmid\mathfrak{c} \\ \Phi_{\mathfrak{m}}(\mathfrak{p})=\sigma}} |G| \frac{1}{N(\mathfrak{p})^s} + O(1) \\
&= |G| \sum_{\mathfrak{p}\in\mathcal{S}} N(\mathfrak{p})^{-s} + O(1).
\end{aligned}$$

Zusammensetzen bringt $\sum_{\mathfrak{p}\in\mathcal{P}_K} N(\mathfrak{p})^{-s} = |G| \sum_{\mathfrak{p}\in\mathcal{S}} N(\mathfrak{p})^{-s} + O(1).$ $\square$

Quellenverweise

[Cox14] David A. Cox. Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2014. ISBN: 9781118400746.

[FJ08] Michael D. Fried und Moshe Jarden. Field Arithmetic. Springer Berlin Heidelberg, 2008. DOI: 10.1007/978-3-540-77270-5.

[Jan96] Gerald. J. Janusz. Algebraic Number Fields. Advances in the Mathematical Sciences. American Mathematical Society, 1996. ISBN: 9780821804292.

[Neu92] Jürgen Neukirch. Algebraische Zahlentheorie. Springer Berlin Heidelberg, 1992. DOI: 10.1007/978-3-540-37663-7.