Seminarvortrag zum Thema

Kreisteilungskörper, Teil 2

von Florian Dittrich

Vorgetragen am 12.07.2017 bei Herrn Bogopolski

Diese Seminararbeit und der zugehörige Vortrag behandeln Kapitel 13, §2 ab Satz 13.2.3 aus dem Buch *A Classical Introduction to Modern Number Theory* [1]. Es wird dabei auf Themen aus vorherigen Vorträgen zurückgegriffen, die jeweils in Form einer Erinnerung wiederholt werden.

Erinnerung (an den Vortrag 11 vom 05.07.)

Für $n \in \mathbb{N}$ ist $\zeta_n := e^{2\pi i/n}$ eine n-te *Einheitswurzel* und es gilt $\zeta_n^n = (e^{2\pi i/n})^n = e^{2\pi i} = 1$.
$\mathbb{Q}(\zeta_n)$ ist der *Kreisteilungskörper* der n-ten Einheitswurzel.

Zum Wiedereinstieg in das Thema wird das folgende Lemma betrachtet, das in [1] als Lemma 3 zu Satz 13.2.9 vorkommt und erst für spätere Sätze wieder gebraucht wird.

1. Lemma: Für $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m,n) = 1$ gilt $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$.

Beweis: Nach obiger Definition gilt $\zeta_{mn}^m = (\zeta_{mn})^m = (e^{2\pi i/mn})^m = e^{2\pi i/n} = \zeta_n$ und $\zeta_{mn}^n = \zeta_m$ analog. Daher sind $\zeta_m, \zeta_n \in \mathbb{Q}(\zeta_{mn})$ und es folgt $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$. Nach dem Lemma von Bèzout existieren nun $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(m,n) = 1 = am + bn$. Mit dieser Darstellung folgt $\zeta_{mn} = \zeta_{mn}^{am+bn} = \zeta_{mn}^{am}\,\zeta_{mn}^{bn} = (\zeta_{mn}^m)^a\,(\zeta_{mn}^n)^b = \zeta_n^a\,\zeta_m^b \in \mathbb{Q}(\zeta_m, \zeta_n)$ mit obigen Umformungen und damit $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m, \zeta_n)$. □

Erinnerung (an den Vortrag 8 vom 07.06.)

Sei L/K eine algebraische Körpererweiterung und $\alpha \in L$. Seien $\sigma_1, \ldots, \sigma_n$ die Einbettungen von L in einen algebraischen Abschluss von K, die fixieren. Dann sind $\alpha^{(j)} = \sigma_j(\alpha)$ die konjugierten zu α und es gilt speziell $\alpha^{(1)} = \alpha$. Damit ist $\mathrm{Spur}(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)}$ die *Spur* von α und für $\alpha_1, \ldots, \alpha_n$ ist $\Delta(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Spur}(\alpha_i\alpha_j))$ mit $i, j \in \{1, \ldots, n\}$ die *Diskriminante*. Die Spur ist mit $\mathrm{Spur}(\alpha + \beta) = \mathrm{Spur}(\alpha) + \mathrm{Spur}(\beta)$ und $\mathrm{Spur}(c\beta) = c\,\mathrm{Spur}(\beta)$ für $\alpha, \beta \in L/K$ und $c \in K$ linear. Weiter ist die *Norm* von α durch $N(\alpha) = \alpha^{(1)} \ldots \alpha^{(n)}$ definiert.

Hier ist zu beachten, dass $\mathrm{Spur}(\alpha_i\alpha_j)$ eine Matrix ist und streng genommen als

$$\mathrm{Spur}(\alpha_i\alpha_j) \mathrel{\hat{=}} \Big(\mathrm{Spur}(\alpha_i\alpha_j)\Big)_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}} = \begin{pmatrix} \mathrm{Spur}(\alpha_1\,\alpha_1) & \ldots & \mathrm{Spur}(\alpha_1\,\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Spur}(\alpha_n\,\alpha_1) & \ldots & \mathrm{Spur}(\alpha_n\,\alpha_n) \end{pmatrix}$$

geschrieben werden müsste. Zur besseren Übersichtlichkeit wird darauf aber verzichtet.

2. Lemma: Sei $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ ein algebraischer Zahlenkörper vom Grad n und $D \subseteq \mathbb{Q}(\zeta_m)$ der Ring der ganzalgebraischen Zahlen. Sei $\alpha_1, \ldots, \alpha_n \in D$ eine Basis von $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ und $\Delta = \Delta(\alpha_1, \ldots, \alpha_n)$ die Diskriminante dieser Basis, dann gilt $\Delta D \subseteq \mathbb{Z}\,\alpha_1 + \ldots \mathbb{Z}\,\alpha_n$.

BEWEIS: Sei $w \in D$ beliebig, dann ist es als $w = \sum_{i=1}^{n} r_i\,\alpha_i$ mit $r_i \in \mathbb{Q}$ darstellbar.
Es folgt $w\alpha_j = \sum_{i=1}^{n} r_i\,\alpha_i\alpha_j$ durch Multiplikation mit α_j und weiter

$$\mathrm{Spur}(w\alpha_j) = \mathrm{Spur}\left(\sum_{i=1}^{n} r_i\,\alpha_i\,\alpha_j\right) = \sum_{i=1}^{n} \mathrm{Spur}(r_i\,\alpha_i\,\alpha_j) = \sum_{i=1}^{n} r_i\ \mathrm{Spur}(\alpha_i\,\alpha_j)$$

durch Anwendung der Spur auf die Gleichung. Dieses lineare Gleichungssystem

$$\begin{pmatrix} \mathrm{Spur}(w\alpha_1) \\ \vdots \\ \mathrm{Spur}(w\alpha_n) \end{pmatrix} = \begin{pmatrix} \mathrm{Spur}(\alpha_1\,\alpha_1) & \dots & \mathrm{Spur}(\alpha_1\,\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Spur}(\alpha_n\,\alpha_1) & \dots & \mathrm{Spur}(\alpha_n\,\alpha_n) \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$$

lässt sich mit der Cramerschen Regel auflösen nach

$$r_i = \frac{\det(A_i)}{\det(A)} = \frac{\det(A_i)}{\Delta} \text{ mit } A = \mathrm{Spur}(\alpha_i\,\alpha_j) \text{ für } i,j \in \{1,\dots,n\}.$$

Dabei gilt $\Delta \neq 0$, weil $\alpha_1,\dots,\alpha_n$ eine Basis ist. Da α_i, α_j und w ganzalgebraische Zahlen sind, gilt nun $\mathrm{Spur}(w\alpha_j), \mathrm{Spur}(\alpha_i\,\alpha_j) \in \mathbb{Z}$ und es folgt schließlich

$$w = \sum_{i=1}^{n} r_i\,\alpha_i = \sum_{i=1}^{n} \frac{\det(A_i)}{\Delta} \implies \Delta w = \sum_{i=1}^{n} \det(A_i)\,\alpha_i \implies \Delta D = \sum_{i=1}^{n} \mathbb{Z}\,\alpha_i.$$

□

Damit lässt sich nun der Ausdruck Δw für jede ganzalgebraische Zahl w als Linearkombination mit Faktoren aus $\mathbb{Z}$ darstellen, während w allgemein bisher nur mit Faktoren aus $\mathbb{Q}$ darstellbar ist. Diese Erkentnis wird in Satz 7 verwendet, um zu zeigen, das noch weitere Elemente Faktoren aus $\mathbb{Z}$ haben.

Erinnerung (an den Vortrag 11 vom 05.07.)

Seien ζ_n die n-ten primitiven Einheitswurzeln und $n \in \mathbb{N}$, dann wird das Polynom

$$\Phi_n(x) = \prod_{\mathrm{ggT}(a,n)=1} (x - \zeta_n^a) \text{ mit } a \in \{1,\dots,n-1\}$$

als *n-tes Kreisteilungspolynom* bezeichnet. Die Nullstellen von $\Phi_n(x)$ sind genau die primitiven n-ten Einheitswurzeln. Der Grad von $\Phi_n(x)$ ist $\phi(n)$, die Anzahl der zu n teilerfremden Zahlen.

3. Satz: Sei $m \in \mathbb{N}$, p prim mit $p \nmid m$ und P ein Primideal in D, dass p enthält,
dann sind die Äquivalenzklassen von $1, \zeta_m, \dots, \zeta_m^{m-1}$ in D/P alle disjunkt.
Des weiteren ist f der Grad von P, falls $p^f \equiv 1 \mod m$ gilt.

BEWEIS: Für $w \in D$ sei $\overline{w}$ die zugehörige Äquivalenzklasse in D/P. Aus $x^m - 1 = \prod_{i=0}^{m-1}(x - \zeta_m^i)$ folgt $1 + x + \dots + x^{m-1} = \prod_{i=1}^{m-1}(x - \zeta_m^i)$ mit Polynomdivision durch $x - 1$.
Setze nun $x = 1$, dann sind $1 + \dots + 1 = m = \prod_{i=1}^{m-1}(1 - \zeta_m^i)$ und damit $\overline{m} = \prod_{i=1}^{m-1} \overline{(1 - \zeta_m^i)}$.
Nun wir per Widerspruch gezeigt, dass $\overline{m} \neq \overline{0}$ ist. Nehme dazu $\overline{m} = \overline{0}$ an, dann
wäre $m \in P$ und mit $p \in P$ würde wegen $p \nmid m$ auch $\overline{1} \in P$ folgen, ein Widerspruch.
Damit ist nun $\overline{m} = \prod_{i=1}^{m-1} \overline{(1 - \zeta_m^i)} \neq \overline{0}$ und es folgt $1 - \overline{\zeta_m^i} \neq 0 \Rightarrow \overline{\zeta_m^i} \neq \overline{1}$ für alle
$i \in \{1,\dots,m\}$, da das Produkt keine Nullstelle haben darf. Damit folgt nun auch $\overline{\zeta_m^i} \neq \overline{\zeta_m^j}$

für $i, j \in \{1, \ldots, m\}$ mit $i \neq j$ und mit $\zeta_m^i \neq \zeta_m^j$ die Behauptung.

Für die Nebenbehauptung betrachte die Elemente in $\{\zeta_m^i \mid i \in \{1, \ldots, m-1\}\}$, die eine zyklische Untergruppe der Ordnung m in der multiplikativen Gruppe von D/P bilden. Diese hat die Ordnung $p^f - 1$ und damit ist $p^f \equiv 1 \mod m$ nach dem Satz von Lagrange. □

Anmerkung: Das Lemma von Gauß liefert folgendes Korollar:
Sei $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = (a_n x^n + \cdots + a_0)(c_l x^l + \cdots + c_0)/d$ mit $\mathrm{ggT}(a_0, \ldots, a_k) = 1$ und $a_i, b_i, c_i, d \in \mathbb{Z}$, dann sind $a_k = 1$, $c_l = d$ und $d \mid c_{l-1}, \ldots, d \mid c_0$.

Erinnerung: Im folgenden wird oft auf den kleinen fermatschen Satz zurückgegriffen, nach dem $a^p \equiv a \mod p$ für $a \in \mathbb{Z}$ und p prim gilt.

4. Theorem Das m-te Kreisteilungspolynom $\Phi_m(x)$ ist irreduzibel in $\mathbb{Z}[x]$.

Beweis: Sei $f(x)$ das Minimalpolynom von ζ_m, dann ist es nach Definition irreduzibel und es gilt $f(x) \mid (x^m - 1)$ in $\mathbb{Q}[x]$, also $x^m - 1 = f(x)\, g(x)$. Nun ist $f(x)$ nach dem Lemma von Gauß normiert und es gilt $f(x) \in \mathbb{Z}[x]$, da ζ_m eine algebraische Zahl ist. Nach Definition wird ζ_m vom Minimalpolynom $f(x)$ mit $f(\zeta_m) = 0$ annuliert und es gilt offensichtlich $\Phi_m(\zeta_m^a) = 0$ für $a \in \{1, \ldots, m\}$. Nun soll gezeigt werden, dass $f(x)$ die gleichen Nullstellen wie $\Phi_m(x)$ hat.

Aus $\Phi_m(x) = \prod_{a=1, \mathrm{ggT}(a,m)=1}^{m-1}(x - \zeta_m^a)$ folgt grad $\Phi_m(x) = \phi(m)$ und nach Satz 3 sind alle Nullstellen von $\Phi_m(x)$ verschieden. Es gilt $f(\zeta_m^p) = 0$ für p prim mit $p \nmid m$ und damit auch $f(\zeta_m^a) = 0$ durch die Primfaktorzerlegung $a = p_1 \ldots p_l$.
Daher annuliert $f(x)$ alle Nullstellen von $\Phi_m(x)$ und es ist grad $f(x) \geq$ grad $\Phi_m(x)$.
Da $f(x)$ das Minimalpolynom ist, muss aber grad $f(x) \leq \mathrm{grad}\Phi_m(x) = \phi(m)$ gelten.
Daraus folgt grad $f(x) = \phi(m)$ und weiter $f(x) = \Phi_m(x)$, da beide die gleichen Nullstellen haben und normiert sind.

Nun bleibt noch zu zeigen, dass in der Darstellung $x^m - 1 = f(x)g(x) = \Phi_m(x)g(x)$ keine Nullstellen in $g(x)$ liegen. Nehme dazu an, es gäbe mit $g(\zeta_m^p) = 0$ eine solche Nullstelle, dann folgt $\overline{g}(\overline{\zeta_m^p}) = \overline{0}$ für Äquivalenzklassen modulo p und damit auch

$$\overline{g}(\overline{\zeta_m}^p) = (\overline{b}(\overline{\zeta}^p)^l + \cdots + \overline{b_0}) = \overline{b}^p\overline{\zeta}^{pl} + \cdots + \overline{b_0}^p = \overline{g}(\overline{\zeta_m})^p = \overline{0}.$$

Mit Fermat folgt $g(\zeta_m)^p \equiv g(\zeta) \equiv 0 \mod p$. Damit wäre nun aber $\overline{f}(\overline{\zeta_m}) \neq 0$, was $f(\zeta_m)$ implizieren würde. Ein Widerspruch zur Definition des Minimalpolynoms. Demnach kann keine Nullstelle in $g(x)$ liegen und die Behauptung ist gezeigt. □

5. Korollar: Der Index $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ teilt $\phi(m)$.

Beweis: Dies folgt direkt aus $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \dim \mathbb{Q}(\zeta_m)/\mathbb{Q} = \mathrm{grad}\ f(x) = \mathrm{grad}\ \Phi_m(x) = \phi(m)$, wobei $f(x)$ wie im Beweis von Theorem 4 das Minimalpolynom von ϕ_m ist. □

Erinnerung (an den Vortrag 8 vom 07.06.)
Es wurde bereits an die *Norm* $N(\alpha) = \alpha^{(1)} \ldots \alpha^{(n)}$ von α erinnert. Für diese gilt $N(\alpha\beta) = N(\alpha)N(\beta)$ mit $\alpha, \beta \in L/K$.

Erinnerung (an Satz 12.1.4)

Seien $1, \beta, \ldots, \beta^{n-1} \in L$ linear unabhängig über K und $f(x) \in K[x]$ das Minimalpolynom von β über K. Falls L/K seperabel ist, gilt $\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{n(n-1)/2} N(f'(\beta))$, wobei $f'(x)$ die Ableitung von $f(x)$ ist.

6. Lemma: Die Diskriminante $\Delta = \Delta(1, \zeta, \ldots, \zeta_m^{\phi(m)-1})$ teilt $m^{\phi(m)}$.

BEWEIS: Differenziere $x^m - 1 = \Phi_m(x)g(x)$ aus Theorem 4 mit der Produktregel zu $mx^{m-1} = \Phi'_m(x)g(x) + \Phi_m(x)g'(x)$. Setze $x = \zeta_m$, dann ist $m\zeta_m^{m-1} = \Phi'_m(\zeta_m)g(\zeta_m)$, da der andere Term wegen $\Phi_m(\zeta_m) = 0$ wegfällt. Nach dem erinnerten Satz gilt nun $\pm N(\Phi'_m(\zeta_m)) = \Delta(1, \zeta, \ldots, \zeta_m^{m-1})$. Mit $N(\zeta_m^{m-1}) = N(\zeta_m) \ldots N(\zeta_m) = 1$ liefert eine Anwendung der Norm auf obigen Ausdruck

$$N(m\zeta_m^{m-1}) = N(m)N(\zeta_m^{m_1} = m^{\phi(m)} = N(\Phi'_m(\zeta_m)g(\zeta_m)) = \Delta N(g(\zeta_m)).$$

Dabei gilt $\Delta(1, \zeta_m, \ldots, \zeta_m^{m-1}) \neq 0$, da $1, \zeta_m, \ldots, \zeta_m^{m-1}$ nach Theorem 4 eine Basis von $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ ist und $N(m) = m \ldots m = \phi(m)$. □

7. Satz: Sei $m \in \mathbb{N}$, p prim mit $p \nmid m$ und $w \in D$, dann gibt es ein Element $d := \sum_{i=1}^{m-1} \alpha_i \zeta_m^i \in \mathbb{Z}[\zeta_m]$ mit $w \equiv d \mod p$.

BEWEIS: Setze $\Delta = \Delta(1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1})$, dann gilt $\Delta \mid m^{\phi(m)}$ nach Lemma 6 und mit $p \nmid m$ folgt $p \nmid \Delta$. Daher gibt es ein $\Delta' \in \mathbb{Z}$ mit $\delta'\Delta \equiv 1 \mod p$ und $\Delta'\Delta w \equiv w \mod p$ nach Multiplikation mit w. Mit Lemma 2 folgt $\Delta w \in \mathbb{Z}[\zeta_m]$ und damit ist $d = \Delta'\Delta w \in \mathbb{Z}[\zeta_m]$. □

Dieser Satz ermöglicht es nun, mit w als Linearkombination mit Faktoren aus $\mathbb{Z}$ zu arbeiten, solange nur Kongruenz gefordert ist. Die Darstellung $w \equiv \Delta'\Delta w \mod p$ wird dagegen nicht weiter verwendet.

8. Korollar: Sei $m \in \mathbb{N}$, p prim mit $p \nmid m$ und $p^n \equiv 1 \mod m$ mit $n \in \mathbb{N}$, dann gilt $w^{p^n} \equiv w \mod p$.

BEWEIS: Nach Satz 7 lässt sich w darstellen als Kongruenz $w \equiv \sum_{i=1}^{m-1} \alpha_i \zeta_m^i \mod p$ mit $\alpha_i \in \mathbb{Z}$ und nach Fermat mit $\alpha_i^p \equiv \alpha_i \mod p$ ist nun $w^p \equiv \sum_{i=1}^{m-1} \alpha_i \zeta_m^{pi} \mod p$. Wiederholtes Anwenden liefert schließlich $w^{p^n} \equiv \sum_{i=1}^{m-1} \alpha_i \zeta_m^{p^n i} \equiv \sum_{i=1}^{m-1} \alpha_i \zeta_m^i \equiv w \mod p$ mit $\zeta_m^{p^n} = \zeta_m$ aus der Voraussetzung $p^n \equiv 1 \mod m$. □

Erinnerung (an den Vortrag 10 vom 28.06.)

Für ein Primideal P gilt genau eine der folgenden Aussagen:

- Es gilt $(p) = p_1 p_2$, dann sagt man, p zerfällt
- Es gilt $(p) = p$, dann sagt man, p bleibt prim
- Es gilt $(p) = p^2$, dann wird p als verzweigt bezeichnet.

9. Satz: Sei $m \in \mathbb{N}$ und p prim mit $p \nmid m$, dann ist jedes Primideal P in D, dass p enthält, unverzweigt.

BEWEIS durch Widerspruch: Angenommen, p wäre verzweigt, dann wäre $(p) \subseteq p^2$. Wähle nun ein $w \in P$ mit $w \notin P^2$. Es gibt solche w, da $P^2 \subset P$ eine echte Teilmenge ist. Wegen $p^n \geq 2$ ist nun aber w in $w^{p^n} = w^p \cdot w^{p^n - 1} \equiv w \mod p$ aufteilbar und aus $w^p, w^{p^n-1} \in P$ folgt $w \in P^2$, ein Widerspruch zur Wahl von w. □

Erinnerung: Der Automorphismus σ_p schickt ζ_m auf ζ_m^p für $p \nmid m$.

10. Satz: Für alle $w \in D$ gilt $\sigma_p w \equiv w^p \mod p$.

BEWEIS: Nach Satz 7 ist wieder $w \equiv \sum_{i=1}^{m-1} \alpha_i \zeta_m^i \mod p$. Die Anwendung von σ_p liefert $\sigma_p w \equiv \sum_{i=1}^{m-1} \alpha_i \zeta_m^{pi} \equiv \sum_{i=1}^{m-1} \alpha_i^p \zeta^{pi} \equiv (\sum_{i=1}^{m-1} \alpha_i \zeta_m^i)^p \equiv w^p \mod p$ mit Fermat, da $a_i \in \mathbb{Z}$. □

11. Korollar: Sei P ein Primideal in D, das p enthält, dann gilt $\sigma_p P = P$.

BEWEIS: Für beliebiges $w \in P$ folgt $\sigma_p w \equiv w^p \equiv 0 \mod P$ nach obigem Satz und damit $\sigma_p P \subseteq P$, sonst wäre $P \subseteq \sigma_p^{-1} P$. Da $\sigma_p P$ aber schon maximal ist, folgt die Behauptung. □

Bisher wurden nur einige kleine Sätze und Lemmata bewiesen, die auch den kompletten Vortrag gefüllt haben. Diese werden aber benötigt, um die folgenden, weiterführenden Sätze zu beweisen. Ziel ist es dabei, Aussagen über die Verzweigung von (p) zu machen. Da die meisten dieser Sätze einen längeren Beweis erfordern, wird darauf an dieser Stelle verzichtet und nur ein Ausblick gegeben, entsprechende Beweisskizzen sind in [1] zu finden. Die Sätze entsprechen dabei den Nummern 13.2.7 bis 13.2.10.

12. Theorem: Sei p prim mit $p \nmid m$ und f die kleinste positive ganzalgebraische Zahl, für die $p^f \equiv \mod m$ ist, dann gilt $(p) = P_1 P_2 \dots P_g$ in $D \subseteq \mathbb{Q}(\zeta_m)$, wobei jedes P_i den Grad f hat und $g = \phi(m)/f$.

13. Satz: Sei p prim in $\mathbb{Z}$, dann ist l in $\mathbb{Q}(\zeta_l)$ vollständig verzweigt. Dabei ist $L = (1 - \zeta_l)$ ein Primideal vom Grad 1 und $(l) = L^{l-1}$.

14. Satz: Sei P ein Primideal in $\mathbb{Q}(\zeta_m)$ mit $P \cap \mathbb{Z} = p\mathbb{Z}$ und p gerade, dann ist P genau dann verzweigt, wenn $p \mid m$. Im Fall $p = 2$ ist P genau dann verzweigt, wenn $4 \mid m$.

15. Satz: Sei p prim mit $p \nmid m$ und D der Ring der ganzalgebraischen Zahlen in $\mathbb{Q}(\zeta_p, \zeta_m)$, dann gilt $pD = (P_1 P_2 \dots P_g)^{p-1}$, wobei die P_i alle disjunkte Primideale vom Grad f sind und $g = \phi(m)/f$ ist. f ist dabei die kleinste natürliche Zahl, für die $p^f \equiv 1 \mod m$ gilt.

16. Satz: Mit l prim gilt $D = \mathbb{Z}[\zeta_l]$.

Literatur und Quellen

[1] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory.* 2. Auflage, Springer 1990, ISBN 978-1-4419-3094-1

[2] M. Aigner: *Zahlentheorie.* 1. Auflage, Vieweg+Teubner 2012, ISBN 978-3-8348-1805-8