EINFÜHRUNG IN DIE ZAHLENTHEORIE

(Oleg Bogopolski, SoSe 2020)

Vorwort

Dieses Skript besteht aus zwei Teilen, die entsprechend der analytischen und der algebraischen Zahlentheorie gewidmet sind. Im ersten Teil geben wir einen Beweis des Primzahlensatzes nach Erdős und Selberg:

Satz A. *Für jede positive reelle Zahl x sei $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich x sind. Dann gilt:*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Im zweiten Teil geben wir den Beweis zum großen Fermatschen Satz für die regulären Exponenten nach Kummer:

Satz B. *Für alle regulären Primzahlen $n \geqslant 3$ ist die Gleichung*

$$x^n + y^n = z^n$$

unlösbar in natürlichen Zahlen.

Der Appendix enthält zusätzliche Informationen, meistens ohne Beweise.

Dieses Skript entstand im Rahmen meiner Vorlesungen, die ich im Wintersemester 2012/13 und im Sommersemester 2020 an der Heinrich-Heine-Universität Düsseldorf gehalten habe. Der Kurs ist für Bachelor-und Masterstudierende geeignet, die bereits über Kenntnisse in Analysis I und Lineare Algebra I verfügen. Minimale Kenntnisse aus dem Standardkurs Algebra sind erwünscht, aber nicht notwendig, da die Hauptbegriffe (algebraische und separable Erweiterungen, etc.) auch in diesem Kurs eingeführt sind. Es ist geplant, etwa 80 Aufgaben mit vollen Lösungen dem Text anzufügen. Bitte fragen Sie mich zuerst, wenn Sie diesen Text verbreiten oder kopieren möchten.

Ich danke meiner Frau Marie-Theres Bochnig für die Korrektur des Textes bezüglich der deutschen Sprache.

Oleg Bogopolski

16.07.2020. Sprockhövel

Contents

Teil 1.

Einführung in die analytische Zahlentheorie

1. Der Ring von arithmetischen Funktionen

Sei $\mathbb{N} = \{1, 2, \dots\}$ die Menge von natürlichen Zahlen und sei $\mathbb{C}$ die Menge von komplexen Zahlen. Demnächst werden wir andere nützliche Objekte und Abbildungen zwischen diesen Objekten einführen.

Dabei werden wir Ringe, Gruppen, Homomorphismen und Isomorphismen benutzen (s. LA I). Zur Erinnerung: Für ein Ringhomomorphismus $f : A \to B$ ist Kern von f definiert durch

$$\ker(f) := \{x \in A \mid f(x) = 0\}.$$

1.1. Der Restklassenring $\mathbb{Z}_n$.

Definition 1.1. Für eine ganze Zahl z und eine natürliche Zahl n existieren ganze Zahlen q und r, so dass gilt:

$$z = qn + r, \;\; 0 \leqslant r < n.$$

Die Zahlen q und r sind eindeutig bestimmt.

Die Zahl r heißt *Rest* von m modulo n und wird mit $\mathrm{Rest}_n(z)$ bezeichnet. Ist $\mathrm{Rest}_n(z) = 0$, dann sagen wir, dass n ein *Teiler* von z ist und schreiben $n|z$. Der *größte gemeinsame Teiler* von n und z wird mit $\mathrm{ggT}(n, z)$ bezeichnet. Wir verabreden, dass $\mathrm{ggT}(0, n) = \mathrm{ggT}(n, 0) = n$ für jede natürliche Zahl n ist.

Des weiteren werden wir folgenden Satz benutzen.

Satz 1.2. (aus LA I) *Für je zwei natürliche Zahlen a und b existieren ganze Zahlen x und y mit*

$$ax + by = \mathrm{ggT}(a, b).$$

Aufgabe. Seien n, d zwei natürliche Zahlen mit $d|n$. Dann ist die folgende Abbildung ein Ringhomomorphismus:

$$\begin{aligned}\theta: \quad & \mathbb{Z}_n \to \mathbb{Z}_d, \\ & i \mapsto \mathrm{Rest}_d(i)\end{aligned}$$

Satz 1.3. *Seien n und m zwei teilerfremde natürliche Zahlen. Dann ist die Abbildung*

$$\begin{aligned}\theta: \quad & \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m, \\ & k \mapsto (\mathrm{Rest}_n(k), \mathrm{Rest}_m(k))\end{aligned}$$

ein Ringisomorphismus.

Beweis.

• θ ist ein Homomorphismus. Das folgt aus der obigen Aufgabe.

• θ ist injektiv. Um das zu zeigen, reicht es zu zeigen, dass $\ker(\theta) = \{0\}$ ist. Sei $k \in \ker(\theta)$. Dann gilt $\mathrm{Rest}_n(k) = \mathrm{Rest}_m(k) = 0$. Folglich ist k durch n und durch m teilbar. Da n und m teilerfremd sind, ist k durch nm teilbar. Dann ist $k = 0$ in $\mathbb{Z}_{nm}$.

• θ ist surjektiv. Das folgt aus dem Fakt, dass jede injektive Abbildung aus einer endlichen Menge in eine gleichmächtige Menge surjektiv ist. □

1.2. **Die Restklassengruppe $\mathbb{Z}_n^*$.**

Definition 1.4. Sei R ein kommutativer Ring mit einem Einselement e. Mit R^* bezeichnen wir die Menge aller invertierbaren Elemente aus R, also ist

$$R^* = \{b \in R \,|\, \exists a : ab = e\}.$$

Bemerkung 1.5. Bezüglich der Ringmultiplikation ist R^* eine kommutative Gruppe.

Beispiel. Für ein $n \in \mathbb{N}$ sei $\mathbb{Z}_n$ der Restklassenring modulo n.
Für $n = 8$ ist $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ und $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$. Die Multiplikationstabelle für die Gruppe $\mathbb{Z}_8^*$ ist

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Es ist wichtig zu verstehen, dass in dem Ring $\mathbb{Z}_1 = \{0\}$ das Element 0 gleichzeitig das Null- und - Einselement ist. Deswegen ist 0 in diesem Ring invertierbar und es gilt $\mathbb{Z}_1^* = \{0\}$.

Lemma 1.6. $\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n \mid \mathrm{ggT}(i,n) = 1\}$. (1.1)

Beweis. Für $n = 1$ stimmt diese Behauptung. Wir nehmen an, dass $n > 1$ ist.

• Zuerst beweisen wir, dass die linke Seite der Gleichung (1.1) in der rechten Seite enthalten ist.

Sei $a \in \mathbb{Z}_n^*$. Dann existiert ein $u \in \mathbb{Z}_n$ mit $au = 1$ in $\mathbb{Z}_n$. Also ist $au - 1$ durch n teilbar; folglich existiert ein $v \in \mathbb{Z}$ mit $au - 1 = nv$. Es gilt also

$$au + nv = 1.$$

Daraus folgt $\mathrm{ggT}(a,n) = 1$, also liegt a in der rechten Seite von (1.1).

• Nun sei a in der rechten Seite von (1.1), also gilt $\mathrm{ggT}(a,n) = 1$. Nach Satz 1.2 existieren ganze Zahlen x und y mit

$$ax + ny = 1.$$

Deswegen gilt $ax \equiv 1$ modulo n, also ist a invertierbar in $\mathbb{Z}_n$. □

Satz 1.7. *Seien n und m zwei teilerfremde natürliche Zahlen. Dann gilt*

$$\mathbb{Z}_{nm}^* \cong \mathbb{Z}_n^* \times \mathbb{Z}_m^*.$$

Etwas genauer: Die Abbildung

$$\begin{aligned} \theta' : \quad & \mathbb{Z}_{nm}^* \to \mathbb{Z}_n^* \times \mathbb{Z}_m^*, \\ & k \mapsto (\mathrm{Rest}_n(k), \mathrm{Rest}_m(k)) \end{aligned}$$

ein Gruppenisomorphismus.

Beweis. Aus dem Satz 1.3 wissen wir, dass die Ringe $\mathbb{Z}_{nm}$ und $\mathbb{Z}_n \times \mathbb{Z}_m$ isomorph sind. Deswegen sind ihre multiplikative Gruppen isomorph:

$$\begin{aligned} \mathbb{Z}_{nm}^* &\cong (\mathbb{Z}_n \times \mathbb{Z}_m)^* \\ &= \mathbb{Z}_n^* \times \mathbb{Z}_m^*. \end{aligned}$$

□

1.3. **Der Ring von arithmetischen Funktionen.** Eine *arithmetische Funktion* ist eine Funktion, deren Definitionsbereich $\mathbb{N}$ und Zielbereich $\mathbb{C}$ ist, also eine Funktion der Sorte $f : \mathbb{N} \to \mathbb{C}$. Die Menge aller arithmetischen Funktionen wird mit $\mathcal{AF}$ bezeichnet. Die Summe und das Produkt von zwei arithmetischen Funktionen ist ebenso eine arithmetische Funktion. Eine weitere Operation auf $\mathcal{AF}$ heißt *Faltung*:

Definition 1.8. Seien f und g zwei arithmetische Funktionen. Die *Faltung* von f und g ist eine neue arithmetische Funktion $f * g$, die durch die folgende Formel definiert ist:

$$(f * g)(n) = \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big) = \sum_{dd'=n} f(d) g(d').$$

Hier läuft die erste Summe über alle positiven Teiler d von n.

Wir definieren vier einfachste Funktionen von $\mathcal{AF}$, nämlich $\mathbf{0}$, $\mathbf{1}$, ρ und δ durch

$$\mathbf{0}(n) = 0 \text{ für alle } n \in \mathbb{N}$$

$$\mathbf{1}(n) = 1 \text{ für alle } n \in \mathbb{N}$$

$$\rho(n) = n \text{ für alle } n \in \mathbb{N}$$

$$\delta(n) = \begin{cases} 1, & \text{falls } n = 1, \\ 0, & \text{falls } n \neq 1. \end{cases}$$

Satz 1.9. *$(\mathcal{AF}, +, *)$ ist ein kommutativer Ring mit Nullelement $\mathbf{0}$ und Einselement δ. Insbesondere gelten die folgenden Gesetze für alle $f, g, h \in \mathcal{AF}$:*

$$f * g = g * f,$$

$$(f * g) * h = f * (g * h),$$

$$f * (g + h) = f * g + f * h.$$

Des weiteren definieren wir zwei wichtige Teilmengen des Ringes $\mathcal{AF}$; sie bilden Gruppen bezüglich $*$.

– Die Gruppe von invertierbaren arithmetischen Funktionen $\mathcal{IAF}$.

– Die Gruppe von multiplikativen arithmetischen Funktionen $\mathcal{MAF}$.

Definition 1.10. 1) Eine arithmetische Funktion f heißt *invertierbar* (bezüglich der Ringmultiplikation $*$), falls eine arithmetische Funktion g mit $f * g = \delta$ existiert. Die Menge aller invertierbaren arithmetischen Funktionen wird mit $\mathcal{IAF}$ bezeichnet (vgl. mit Definition 1.4).

2) Eine arithmetische Funktion f heißt *multiplikativ*, falls $f(nm) = f(n)f(m)$ für alle teilerfremden Zahlen $n, m \in \mathbb{N}$ gilt. Die Menge aller von $\mathbf{0}$ verschiedenen multiplikativen arithmetischen Funktionen wird mit $\mathcal{MAF}$ bezeichnet.

Satz 1.11. 1) *Eine arithmetische Funktion f ist invertierbar bezüglich $*$ genau dann, wenn $f(1) \neq 0$ ist. Also gilt*

$$\mathcal{IAF} = \{f \in \mathcal{AF} \mid f(1) \neq 0\}.$$

2) *Für jede multiplikative Funktion f gilt $f(1) = 1$.*

3) *Die Mengen $\mathcal{IAF}$ und $\mathcal{MAF}$ sind Gruppen bezüglich $*$. Die zweite Gruppe ist eine Untergruppe der ersten:*

$$\mathcal{MAF} \leqslant \mathcal{IAF}.$$

Beweis. 1) Nehmen wir an, dass f invertierbar bezüglich $*$ ist. Dann existiert eine arithmetische Funktion g mit $f * g = \delta$. Dann gilt $f(1)g(1) = (f * g)(1) = \delta(1) = 1$. Daraus folgt $f(1) \neq 0$.

Jetzt nehmen wir $f(1) \neq 0$ an und definieren eine arithmetische Funktion g induktiv:

$$g(n) = \begin{cases} \frac{1}{f(1)}, & \text{falls } n = 1, \\ -\frac{1}{f(1)} \sum\limits_{\substack{d|n \\ d\neq 1}} f(d)g(\frac{n}{d}), & \text{falls } n \neq 1. \end{cases}$$

Wir überprüfen $f * g = \delta$:

Für $n = 1$ gilt

$$(f * g)(1) = f(1)g(1) = \sum_{d_1 d_2 = 1} f(d_1)g(d_2) = f(1) \cdot \frac{1}{f(1)} = 1 = \delta(1).$$

Für $n > 1$ gilt

$$\begin{aligned} (f * g)(n) &= \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = f(1)g(n) + \sum_{\substack{d|n \\ d\neq 1}} f(d)g\Big(\frac{n}{d}\Big) \\ &= f(1) \cdot \Big(-\tfrac{1}{f(1)} \sum_{\substack{d|n \\ d\neq 1}} f(d)g(\tfrac{n}{d})\Big) + \sum_{\substack{d|n \\ d\neq 1}} f(d)g\Big(\frac{n}{d}\Big) = 0 = \delta(n). \end{aligned}$$

2) Nach Definition einer multiplikativen Funktion existiert ein $a \in \mathbb{N}$ mit $f(a) \neq 0$. Außerdem gilt $f(a) = f(1 \cdot a) = f(1)f(a)$. Daraus folgt $f(1) = 1$.

3) $\mathcal{IAF}$ ist eine Gruppe bezüglich $*$ (s. Bemerkung 1.5).
Jetzt überprüfen wir, dass $\mathcal{MAF}$ eine Gruppe bezüglich $*$ ist.

• Die Menge $\mathcal{MAF}$ ist abgeschlossen bezüglich $*$:
Seien f und h zwei multiplikative arithmetische Funktionen. Dann gilt für je

zwei teilerfremde Zahlen n, m:

$$\begin{aligned}(f*h)(nm) = &\sum_{d|nm} f(d)h(\tfrac{nm}{d})\\ &= \sum_{d_1|n,\ d_2|m} f(d_1d_2)h(\tfrac{nm}{d_1d_2})\\ &= \sum_{d_1|n,\ d_2|m} f(d_1)f(d_2)h(\tfrac{n}{d_1})h(\tfrac{m}{d_2})\\ &= \sum_{d_1|n} f(d_1)h(\tfrac{n}{d_1}) \cdot \sum_{d_2|n} f(d_2)h(\tfrac{n}{d_2}))\\ &= (f*h)(n)\cdot(f*h)(m).\end{aligned}$$

• Zu jedem $f \in \mathcal{MAF}$ existiert ein $g \in \mathcal{MAF}$ mit $f*g=\delta$:
Wir wissen schon, dass ein $g \in \mathcal{IAF}$ mit $f*g=\delta$ existiert. Es bleibt zu zeigen, dass $g(nm)=g(n)g(m)$ für alle teilerfremden Zahlen n, m gilt. Dabei verwenden wir die Induktion nach nm.

Aus $f(1)=1$ (s. Punkt 2)) und aus $f*g=\delta$ folgt $g(1)=1$. Somit gilt $g(nm)=g(n)g(m)$ für $n=m=1$.

Sei also $nm>1$. Nehmen wir an, dass wir die Multiplikativität von g für alle teilerfremden Zahlen n_1, m_1 mit $n_1m_1<nm$ bewiesen haben. Da $f*g=\delta$ ist, gilt

$$\sum_{d|k} f(d)g\Big(\frac{k}{d}\Big)=0$$

für alle $k>0$. Daraus und wegen $f(1)=1$ folgt

$$\begin{aligned}g(nm) &= -\sum_{\substack{d|nm\\ d\neq 1}} f(d)g(\tfrac{nm}{d})\\ &= -\sum_{\substack{d_1|n\ d_2|m\\ d_1d_2\neq 1}} f(d_1d_2)g(\tfrac{nm}{d_1d_2})\\ &= -\sum_{\substack{d_1|n\ d_2|m\\ d_1d_2\neq 1}} f(d_1)f(d_2)g(\tfrac{n}{d_1})g(\tfrac{m}{d_2})\\ &= -\Big(\sum_{d_1|n} f(d_1)g(\tfrac{n}{d_1})\cdot\sum_{d_2|m} f(d_2)g(\tfrac{m}{d_2})) - f(1)g(n)\cdot f(1)g(m)\Big)\\ &= -\Big(-f(1)g(n)\cdot f(1)g(m)\Big) = g(n)g(m).\end{aligned}$$

□

1.4. **Die Möbius-Funktion und die Euler-Funktion.**

Definition 1.12. Die Möbius-Funktion $\mu \in \mathcal{AF}$ ist definiert durch

$$\mu(n) = \begin{cases} 1, & \text{falls } n = 1, \\ (-1)^k, & \text{falls } n \text{ ein Produkt von } k \text{ verschiedenen Primzahlen ist,} \\ 0, & \text{falls } n \text{ durch Quadrat einer Primzahl teilbar ist.} \end{cases}$$

Wir haben

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

Satz 1.13. *Die Möbius-Funktion μ ist multiplikativ und für jedes $n \in \mathbb{N}$ gilt*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{falls } n = 1, \\ 0, & \text{falls } n \neq 1. \end{cases} \quad . \tag{1.2}$$

Die letzte Formel läßt sich kurz aufschreiben:

$$\mu * \mathbf{1} = \delta. \tag{1.2}'$$

Das heißt: μ ist das multiplikative Inverse zu $\mathbf{1}$ in dem Ring $(\mathcal{AF}, +, *)$.

Beweis. Die Multiplikativität von μ ist leicht zu überprüfen.

Wir beweisen die Formel (1.2). Diese Formel gilt für $n = 1$. Wir überprüfen sie für $n > 1$. Sei $n = p_1^{k_1} \dots p_\ell^{k_\ell}$ die Primzahlzerlegung von n. Dann hat jeder Teiler d von n die Form $d = p_1^{i_1} p_2^{i_2} \dots p_\ell^{i_\ell}$ mit $0 \leqslant i_s \leqslant k_s$ für $s = 1, \dots, \ell$. Wir haben $\mu(d) = \mu(p_1^{i_1})\mu(p_2^{i_2}) \dots \mu(p_\ell^{i_\ell})$. Dann gilt

$$\begin{aligned} \sum_{d|n} \mu(d) = \; & \Big(\mu(1) + \mu(p_1) + \dots + \mu(p_1^{k_1})\Big) \\ & \cdot \Big(\mu(1) + \mu(p_2) + \dots + \mu(p_2^{k_2})\Big) \\ & \vdots \\ & \cdot \Big(\mu(1) + \mu(p_\ell) + \dots + \mu(p_\ell^{k_\ell})\Big). \end{aligned}$$

Also gilt

$$\sum_{d|n} \mu(d) = \Big(1 + (-1)\Big) \cdot \Big(1 + (-1)\Big) \cdot \dots \cdot \Big(1 + (-1)\Big) = 0.$$

□

Satz 1.14. (Inversions-Formel von Möbius) *Für je zwei Funktionen $f, g \in \mathcal{AF}$ sind folgende Aussagen äquivalent:*

(1) *Für alle $n \in \mathbb{N}$ gilt*
$$g(n) = \sum_{d|n} f(d).$$

(2) *Für alle $n \in \mathbb{N}$ gilt*
$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, g(d).$$

Beweis. Die kurzen Schreibweisen von (1) und (2) sind $g = \mathbf{1} * f$ und $f = \mu * g$. Sie sind äquivalent, weil μ und $\mathbf{1}$ zueinander invers sind. □

Definition 1.15. Die Euler-Funktion $\varphi \in \mathcal{AF}$ ist definiert durch
$$\varphi(n) = |\mathbb{Z}_n^*|.$$
Also ist $\varphi(n)$ die Anzahl von Zahlen in der Folge $0, 1, 2, \ldots, n-1$, die teilerfremd zu n sind.

Wir haben

n	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4

Satz 1.16. *Es gelten folgende Aussagen:*

a) *Die Euler-Funktion φ ist multiplikativ.*

b) *Für jede Primzahl p und jede natürliche Zahl k gilt*
$$\varphi(p^k) = p^k - p^{k-1}.$$

c) *Ist $n \neq 1$ eine natürliche Zahl und $n = p_1^{k_1} \ldots p_\ell^{k_\ell}$ die Primzahlzerlegung von n, dann gilt*
$$\varphi(n) = \prod_{i=1}^{\ell} (p_i^{k_i} - p_i^{k_i-1}) = n \cdot \prod_{i=1}^{\ell} \Big(1 - \frac{1}{p_i}\Big).$$

d) *Für jedes $n \in \mathbb{N}$ gilt*
$$\sum_{d|n} \varphi(d) = n. \tag{1.3}$$

Diese Formel läßt sich kurz aufschreiben:
$$\varphi * \mathbf{1} = \rho.$$

Daraus folgt
$$\varphi = \rho * \mu.$$

Beweis. a) Seien n, m zwei teilerfremde Zahlen. Nach Satz 1.7 gilt $\mathbb{Z}_{nm}^* \cong \mathbb{Z}_n^* \times \mathbb{Z}_m^*$. Daraus folgt $\varphi(nm) = |\mathbb{Z}_{nm}^*| = |\mathbb{Z}_n^*| \cdot |\mathbb{Z}_m^*| = \varphi(n)\varphi(m)$.

b) Die Zahlen in $\{0, 1, \ldots, p^k - 1\}$, die *nicht* teilerfremd zu p^k sind, sind

$$0, p, 2p, \ldots, (p^{k-1} - 1)p.$$

Es gibt p^{k-1} solche Zahlen. Dann ist $\varphi(p^k) = p^k - p^{k-1}$.

c) Mit Hilfe von a) unf b) bekommen wir

$$\varphi(n) = \varphi(p_1^{k_1}) \ldots \varphi(p_\ell^{k_\ell}) = \prod_{i=1}^{\ell} (p_i^{k_i} - p_i^{k_i - 1}).$$

d) Diese Formel gilt für $n = 1$. Wir überprüfen sie für $n > 1$. Sei $n = p_1^{k_1} \ldots p_\ell^{k_\ell}$ die Primzahlzerlegung von n. Dann hat jeder Teiler d von n die Form $d = p_1^{i_1} p_2^{i_2} \ldots p_\ell^{i_\ell}$ mit $0 \leqslant i_s \leqslant k_s$ für $s = 1, \ldots, \ell$. Wir haben $\varphi(d) = \varphi(p_1^{i_1})\varphi(p_2^{i_2}) \ldots \varphi(p_\ell^{i_\ell})$. Dann gilt

$$\begin{aligned} \sum_{d|n} \varphi(d) = \; & \Big(\varphi(1) + \varphi(p_1) + \cdots + \varphi(p_1^{k_1})\Big) \\ & \cdot \Big(\varphi(1) + \varphi(p_2) + \cdots + \varphi(p_2^{k_2})\Big) \\ & \vdots \\ & \cdot \Big(\varphi(1) + \varphi(p_\ell) + \cdots + \varphi(p_\ell^{k_\ell})\Big). \end{aligned}$$

Also gilt

$$\begin{aligned} \sum_{d|n} \varphi(d) = \; & \Big(1 + (p_1 - 1) + \cdots + (p_1^{k_1} - p_1^{k_1 - 1})\Big) \\ & \cdot \Big(1 + (p_2 - 1) + \cdots + (p_2^{k_2} - p_2^{k_2 - 1})\Big) \\ & \vdots \\ & \cdot \Big(1 + (p_\ell - 1) + \cdots + (p_\ell^{k_\ell} - p_\ell^{k_\ell - 1})\Big), \end{aligned}$$

woraus folgt

$$\sum_{d|n} \varphi(d) = p_1^{k_1} p_2^{k_2} \ldots p_\ell^{k_\ell} = n.$$

□

2. Funktionen θ und ψ von Tschebyschew

Mit p oder p_i bezeichnen wir Primzahlen.

2.1. Die Funktion $\nu_p(n)$.

Definition 2.1. Sei n eine natürliche Zahl und sei p eine Primzahl. Wir definieren $\nu_p(n)$ als die maximale Zahl $k \in \mathbb{N} \cup \{0\}$, so dass p^k ein Teiler von n ist:

$$\nu_p(n) := \max\{k \in \mathbb{N} \cup \{0\} \mid p^k \text{ ist ein Teiler von } n\}.$$

Beispiel. $\nu_5(4) = 0$, $\nu_2(8) = 3$, $\nu_3(8) = 0$.

Es gilt

$$n = \prod_{p \leqslant n} p^{\nu_p(n)}.$$

Lemma 2.2. *Für jede Primzahl p und jede natürliche Zahl n gilt:*

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{i=1}^{[\ln n / \ln p]} \left[\frac{n}{p^i}\right]. \tag{2.0}$$

Hinweis.

1) Für jedes $i \in \mathbb{N}$ gibt es genau $[\frac{n}{p^i}]$ Zahlen in $\{1, 2, \ldots, n\}$, die durch p^i teilbar sind.
2) Ist p^i ein Teiler von n, dann gilt $p^i \leqslant n$. Daraus folgt $i \leqslant \frac{\ln x}{\ln p}$. Da i eine natürliche Zahl ist, gilt

$$i \leqslant \left[\frac{\ln x}{\ln p}\right].$$

□

2.2. Die Funktionen $\pi(x)$, $\theta(x)$, $\psi(x)$.

Definition 2.3. Die Funktion $\pi : \mathbb{R}_+ \to \mathbb{N}$ ist wie folgt definiert:

$$\pi(x) = \sum_{p \leqslant x} 1.$$

Also ist $\pi(x)$ die Anzahl von Primzahlen p, die kleiner oder n sind.

Am Ende des Kurses werden wir die folgende Formel beweisen:

$$\lim_{x \to \infty} \frac{\pi(x)}{(\frac{x}{\ln x})} = 1.$$

Definition 2.4. Die Tschebyschew-Funktionen $\theta : \mathbb{R}_+ \to \mathbb{R}$ und $\psi : \mathbb{R}_+ \to \mathbb{R}$ werden wie folgt definiert:

$$\begin{aligned} \theta(x) &= \sum_{p \leqslant x} \ln p = \ln \prod_{p \leqslant x} p, \\ \psi(x) &= \sum_{p^k \leqslant x} \ln p. \end{aligned}$$

Die letzte Summe läuft über alle Primzahlen p und alle natürlichen Zahlen k mit $p^k \leqslant x$. Jedes mal, wenn wir $p^k \leqslant x$ sehen, wird $\ln p$ addiert. Es ist klar, dass $k \leqslant \frac{\ln x}{\ln p}$ gilt. Da k eine natürlich Zahl ist, gilt

$$\psi(x) = \sum_{p^k \leqslant x} \ln p = \sum_{p \leqslant x} \Big[\frac{\ln x}{\ln p}\Big] \ln p. \tag{2.1}$$

Beispiel.

$$\begin{aligned} \theta(10) &= \ln 2 + \ln 3 + \ln 5 + \ln 7, \\ \psi(10) &= 3 \ln 2 + 2 \ln 3 + \ln 5 + \ln 7. \end{aligned}$$

Lemma 2.5. *Es gilt*

$$\theta(x) \leqslant \psi(x) \leqslant \pi(x) \ln x.$$

Beweis. Die erste Ungleichung ist klar. Die zweite folgt aus

$$\psi(x) \overset{(2.1)}{=} \sum_{p \leqslant x} \Big[\frac{\ln x}{\ln p}\Big] \ln p \leqslant \sum_{p \leqslant x} \ln x = \pi(x) \ln x.$$

□

Lemma 2.6. *Seien n, k natürliche Zahlen mit $1 \leqslant k \leqslant n$. Dann gilt*

$$\begin{aligned} \tbinom{n}{k-1} < \tbinom{n}{k} &\quad \text{genau dann wenn} \quad k < \tfrac{n+1}{2} \quad \text{ist,} \\ \tbinom{n}{k-1} > \tbinom{n}{k} &\quad \text{genau dann wenn} \quad k > \tfrac{n+1}{2} \quad \text{ist,} \\ \tbinom{n}{k-1} = \tbinom{n}{k} &\quad \text{genau dann wenn} \quad k = \tfrac{n+1}{2} \quad \text{ist} \end{aligned}$$

Hinweis. Wir betrachten den Wert

$$r(k) := \frac{\binom{n}{k}}{\binom{n}{k-1}} = \cdots = \frac{n-k+1}{k}.$$

Dann ist $r(k) < 1$ genau dann, wenn $k < \frac{n+1}{2}$ gilt.

□

Lemma 2.7. *Für alle $n \in \mathbb{N}$ gilt*

$$\frac{2^{2n}}{2n} \leqslant \binom{2n}{n} < 2^{2n}.$$

Beweis. Die zweite Ungleichung:

$$2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{n}{k} > \binom{2n}{n}.$$

Die zweite Ungleichung folgt aus

$$\begin{aligned} 2^{2n} &= \sum_{k=0}^{2n} \tbinom{n}{k} = 1 + \sum_{k=1}^{2n-1} \tbinom{n}{k} + 1 \\ &\leqslant 2 + (2n-1)\tbinom{2n}{n} \\ &\leqslant 2n\tbinom{2n}{n}. \end{aligned}$$

□

Satz 2.8. *Für jede $n \in \mathbb{N}$ gilt*

$$\prod_{p \leqslant n} p < 4^n. \tag{2.2}$$

Für jedes $x \in \mathbb{R}_+$ gilt

$$\theta(x) < x \ln 4. \tag{2.3}$$

Beweis. Sei $m \geqslant 1$. Wir bezeichnen

$$\begin{aligned} M &= \binom{2m+1}{m} = \binom{2m+1}{m+1} \\ &= \frac{(2m+1)2m(2m-1)\dots(m+2)}{m!}. \end{aligned}$$

Das ist eine ganze Zahl, da M ein Binoimialkoeffizient ist.
Es gilt

$$\begin{aligned} 2M &= \binom{2m+1}{m} + \binom{2m+1}{m+1} \\ &< \sum_{k=0}^{2m+1} \binom{2m+1}{k} \\ &= 2^{2m+1}, \end{aligned}$$

also gilt

$$M < 4^m.$$

Jede Primzahl p mit $m+2 \leqslant p \leqslant 2m+1$ ist ein Teiler des Produktes

$$(2m+1)2m(2m-1)\dots(m+2)$$

und ist kein Teiler von $m!$. Deswegen ist p ein Teiler von M. Dann ist

$$\prod_{m+2\leqslant p\leqslant 2m+1} p$$

ein Teiler von M. Daraus folgt

$$\prod_{m+2\leqslant p\leqslant 2m+1} p \leqslant M < 4^m. \tag{2.4}$$

Jetzt beweisen wir (2.2) per Induktion nach n. Diese Ungleichung gilt für $n = 1$ und $n = 2$. Sei $n \geqslant 3$. Nehmen wir an, dass (2.2) für alle natürlichen m mit $m < n$ gilt

Fall 1. Sei n gerade. Dann gilt

$$\prod_{p\leqslant n} p = \prod_{p\leqslant n-1} p < 4^{n-1} < 4^n.$$

Fall 2. Sei n ungerade. Dann ist $n = 2m+1$ für ein $m \in \mathbb{N}$ und es gilt (nach Induktion und mit Hilfe von (2.4)):

$$\prod_{p\leqslant n} p = \prod_{p\leqslant m+1} p \prod_{m+2\leqslant p\leqslant 2m+1} p < 4^{m+1}4^m = 4^{2m+1} = 4^n.$$

Die Ungleichung (2.3) folgt aus (2.2) (kleine Aufgabe). □

3. Theoreme von Tschebyschew

Satz 3.1. (Tschebyschew) *Es existieren positive Konstanten A und B mit*

$$Ax \leqslant \theta(x) \leqslant \psi(x) \leqslant \pi(x)\ln x \leqslant Bx. \tag{3.1}$$

für alle $x \geqslant 2$. Außerdem gilt

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x} = \liminf_{x\to\infty} \frac{\pi(x)}{x/\ln x} \geqslant \ln 2 \tag{3.2}$$

und

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x} = \limsup_{x\to\infty} \frac{\pi(x)}{x/\ln x} \leqslant \ln 4. \tag{3.3}$$

Beweis. Der Beweis besteht aus vier Teilen.

Teil 1. Wir zeigen folgenden Teil von (3.3):

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x} = \limsup_{x\to\infty} \frac{\pi(x)\ln x}{x}. \tag{3.3$'$}$$

Nach Lemma 2.5 gilt

$$\theta(x) \leqslant \psi(x) \leqslant \pi(x)\ln x.$$

Deswegen gilt

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} \leqslant \limsup_{x\to\infty} \frac{\psi(x)}{x} \leqslant \limsup_{x\to\infty} \frac{\pi(x)\ln x}{x}.$$

Um die Gleichungen (3.3$'$) zu beweisen, reicht es, folgenden zu beweisen:

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} \geqslant \limsup_{x\to\infty} \frac{\pi(x)\ln x}{x}. \tag{3.3$''$}$$

Das werden wir jetzt tun. Sei $0 < \delta < 1$ beliebig. Dann gilt

$$\begin{aligned}
\theta(x) &\geqslant \sum_{x^{1-\delta}<p\leqslant x} \ln p \\
&\geqslant \sum_{x^{1-\delta}<p\leqslant x} (1-\delta)\ln x \\
&= (1-\delta)(\pi(x) - \pi(x^{1-\delta}))\ln x \\
&\geqslant (1-\delta)(\pi(x) - x^{1-\delta})\ln x.
\end{aligned}$$

Daraus folgt

$$\frac{\theta(x)}{x} \geqslant (1-\delta)\Big(\frac{\pi(x)\ln x}{x} - \frac{\ln x}{x^\delta}\Big).$$

Aus Ana I wissen wir

$$\lim_{x\to\infty} \frac{\ln x}{x^\delta} = 0.$$

Deswegen gilt

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} \geqslant (1-\delta) \limsup_{x\to\infty} \frac{\pi(x)\ln x}{x}.$$

Da diese Ungleichung für alle $0 < \delta < 1$ gilt, impliziert sie (3.3″).

Teil 2. Um (3.3) komplett zu beweisen, reicht es (wegen Teil 1), folgendes zu zeigen:

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} \leqslant \ln 4.$$

Das folgt aber aus $\theta(x) < x \ln 4$, siehe Satz 2.8.

Teil 3. Es gilt

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x} = \liminf_{x\to\infty} \frac{\pi(x)\ln x}{x}.$$

Den Beweis dafür bekommen wir aus Teil 1, wenn wir dort überall $\limsup\limits_{x\to\infty}$ durch $\liminf\limits_{x\to\infty}$ ersetzen.

Teil 4. Um (3.2) komplett zu beweisen, reicht es (wegen Teil 3), folgendes zu zeigen:

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geqslant \ln 2.$$

Sei $n \in \mathbb{N}$. Wir bezeichnen $N = \binom{2n}{n}$. Es gilt

$$N = \binom{2n}{n} = \frac{(2n)(2n-1)\dots(n+1)}{n!} = \frac{(2n)!}{(n!)^2} = \prod_{p\leqslant 2n} p^{\nu_p((2n)!)-2\nu_p(n!)}. \quad (3.4)$$

Mit Hilfe von Lemma 2.2 erhalten wir

$$\begin{aligned}\nu_p((2n)!) - 2\nu_p(n!) &= \Big(\Big[\tfrac{2n}{p}\Big] + \Big[\tfrac{2n}{p^2}\Big] + \dots\Big) - 2\Big(\Big[\tfrac{n}{p}\Big] + \Big[\tfrac{n}{p^2}\Big] + \dots\Big) \\ &= \Big(\Big[\tfrac{2n}{p}\Big] - 2\Big[\tfrac{n}{p}\Big]\Big) + \Big(\Big[\tfrac{2n}{p^2}\Big] - 2\Big[\tfrac{n}{p^2}\Big]\Big) + \dots.\end{aligned}$$

Merken wir an: $[2t] - 2[t] \in \{0, 1\}$ für jedes $t \in \mathbb{R}_+$. Dann gilt

$$0 \leqslant \nu_p((2n)!) - 2\nu_p(n!) \leqslant \Big[\frac{\ln\, 2n}{\ln p}\Big].$$

Daraus und aus (3.4) folgt

$$N \leqslant \prod_{p \leqslant 2n} p^{\left[\frac{\ln\, 2n}{\ln p}\right]}. \tag{3.5}$$

Nach Lemma 2.7 gilt

$$\frac{2^{2n}}{2n} \leqslant N. \tag{3.6}$$

Aus (3.5) und (3.6) folgt

$$\frac{2^{2n}}{2n} \leqslant \prod_{p \leqslant 2n} p^{\left[\frac{\ln\, 2n}{\ln p}\right]}.$$

Durch die Logarithmierung erhalten wir

$$2n \ln 2 - \ln 2n \leqslant \sum_{p \leqslant 2n} \Big[\frac{\ln\, 2n}{\ln p}\Big] \ln p \overset{(2.1)}{=} \psi(2n).$$

Sei $x \geqslant 2$. Sei n eine natürliche Zahl mit

$$2n \leqslant x < 2n + 2.$$

Dann haben wir

$$\begin{aligned}\psi(x) &\geqslant \psi(2n) \geqslant 2n \ln 2 - \ln 2n \\ &> (x - 2) \ln 2 - \ln x = x \ln 2 - \ln x - 2 \ln 2.\end{aligned}$$

Daraus folgt

$$\liminf_{x \to \infty} \frac{\psi(x)}{x} \geqslant \ln 2.$$

Somit ist (3.6) bewiesen.

Die Behauptung (3.5) folgt aus (3.6), (3.7) und aus Lemma 2.5. □

4. Mangoldt-Funktion und Theoreme von Mertens

Lemma 4.1. *Sei f eine arithmetische Funktion und sei $g : [2, \infty] \to \mathbb{R}$ eine Funktion mit stetiger Ableitung. Für jedes $y \in [2, \infty)$ definieren wir*

$$\mathcal{F}(y) = \sum_{2 \leqslant n \leqslant y} f(n).$$

Dann gilt für jedes $x \geqslant 2$:

$$\sum_{2 \leqslant n \leqslant x} f(n)g(n) = \mathcal{F}(x)g(x) - \int_2^x \mathcal{F}(t)g'(t)\,\mathrm{dt}. \tag{4.1}$$

Hinweis. Für jedes $m \in \mathbb{N}$, $m \geqslant 2$, und jedes $t \in \mathbb{R}$ mit $m \leqslant t < m+1$ gilt $\mathcal{F}(t) = \mathcal{F}(m)$. Dann gilt

$$\int_m^{m+1} \mathcal{F}(t)g'(t)\,\mathrm{dt} = \mathcal{F}(m)\int_m^{m+1} g'(t)\,\mathrm{dt} = \mathcal{F}(m)(g(m+1) - g(m)).$$

□

Folgerung 4.2. *Für jedes reeelles $x \geqslant 2$ gilt*

$$\sum_{n \leqslant x} \ln n = x \ln x - x + O(\ln x). \tag{4.2}$$

Definition 4.3. Wir definieren arithmetische Funktionen ℓ und Λ durch

$$\ell(n) = \begin{cases} \ln p, & \text{falls } n = p \in \mathrm{Prim}, \\ 0, & \text{sonst} \end{cases}$$

$$\Lambda(n) = \begin{cases} \ln p, & \text{falls } n = p^k \text{ für einige } p \in \mathrm{Prim} \text{ und } k \in \mathbb{N}, \\ 0, & \text{sonst} \end{cases}$$

Die Funktion Λ heißt *Mangoldt-Funktion.*

Bemerkung. Es gilt:

$$\sum_{n \leqslant x} \Lambda(n) = \sum_{p^k \leqslant x} \ln p = \psi(x). \tag{4.3}$$

$$\sum_{d \mid n} \Lambda(d) = \ln n. \tag{4.4}$$

Satz 4.4. *Für $x \geqslant 2$ gilt*

$$\sum_{m\leqslant x}\psi\Big(\frac{x}{m}\Big) = \sum_{d\leqslant x}\Lambda(d)\Big[\frac{x}{d}\Big] = x\ln x - x + O(\ln x). \tag{4.5}$$

Beweis.

$$\begin{aligned}\sum_{m\leqslant x}\psi\big(\tfrac{x}{m}\big) &\overset{(4.3)}{=} \sum_{m\leqslant x}\sum_{d\leqslant\frac{x}{m}}\Lambda(d) \;= \sum_{dm\leqslant x}\Lambda(d) = \sum_{d\leqslant x}\Lambda(d)\big[\tfrac{x}{d}\big]\\ &= \sum_{n\leqslant x}\sum_{d|n}\Lambda(d)\\ &\overset{(4.4)}{=} \sum_{n\leqslant x}\ln n \overset{(4.2)}{=} x\ln x - x + O(\ln x).\end{aligned}$$

□

Satz 4.5. (Erster Satz von Mertens). *Für $x \geqslant 2$ gelten*

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n} = \ln x + O(1) \tag{4.6}$$

und

$$\sum_{p\leqslant x}\frac{\ln p}{p} = \ln x + O(1). \tag{4.7}$$

Beweis. Nach Tschebyschew-Satz 4.1 gilt $\psi(x) = O(x)$. Wir haben

$$\begin{aligned}x\ln x - x + O(\ln x) &\overset{(4.5)}{=} \sum_{d\leqslant x}\Lambda(d)\Big[\frac{x}{d}\Big]\\ &= \sum_{d\leqslant x}\Lambda(d)\Big(\frac{x}{d} - \Big\{\frac{x}{d}\Big\}\Big)\\ &= x\sum_{d\leqslant x}\frac{\Lambda(d)}{d} - \sum_{d\leqslant x}\Lambda(d)\Big\{\frac{x}{d}\Big\}\\ &\overset{(4.3)}{=} x\sum_{d\leqslant x}\frac{\Lambda(d)}{d} + O(\psi(x))\\ &\overset{(3.1)}{=} x\sum_{d\leqslant x}\frac{\Lambda(d)}{d} + O(x).\end{aligned}$$

Wir dividieren diese Gleichung durch x und erhalten die Formel (4.6). Die Formel (4.7) folgt aus (4.6) und

$$\begin{aligned}\sum_{n\leqslant x}\frac{\Lambda(n)}{n}-\sum_{p\leqslant x}\frac{\ln p}{p} &= \sum_{\substack{p^k\leqslant x\\ k\geqslant 2}}\frac{\ln p}{p^k}\\ &\leqslant \sum_{p\leqslant x}\ln p\sum_{k=2}^{\infty}\frac{1}{p^k}\\ &\leqslant \sum_{p\leqslant x}\frac{\ln p}{p(p-1)}\\ &\leqslant \sum_{m=2}^{\infty}\frac{\ln m}{m(m-1)}\\ &= O(1).\end{aligned}$$

Satz 4.6. (Zweiter Satz von Mertens) *Es existiert eine Konstante C, so dass*

$$\sum_{p\leqslant x}\frac{1}{p}=\ln\ln x+C+O\Big(\frac{1}{\ln x}\Big) \tag{4.8}$$

für jedes $x\geqslant 2$ gilt.

Beweis. Wir haben

$$\sum_{p\leqslant x}\frac{1}{p}=\sum_{p\leqslant x}\frac{\ln p}{p}\frac{1}{\ln p}=\sum_{2\leqslant n\leqslant x}f(n)g(n),$$

wobei

$$f(n)=\begin{cases}\dfrac{\ln p}{p}, & \text{falls } n=p\in\text{Prim},\\ 0, & \text{sonst}\end{cases}$$

und

$$g(t)=\frac{1}{\ln t}\quad \text{für } t>1$$

ist.

Wir setzen

$$\mathcal{F}(t)=\sum_{2\leqslant n\leqslant t}f(n)=\sum_{p\leqslant t}\frac{\ln p}{p}.$$

Nach Satz 4.5 haben wir

$$\mathcal{F}(t) = \ln t + r(t) \quad \text{mit } r(t) = O(1).$$

Aus $r(t) = O(1)$ und

$$\int \frac{1}{t(\ln t)^2}\,\mathrm{dt} = -\frac{1}{\ln t}$$

folgt

$$\int_2^\infty \frac{r(t)}{t(\ln t)^2}\,\mathrm{dt} = O\Big(\frac{1}{\ln 2}\Big) \quad \text{und} \quad \int_x^\infty \frac{r(t)}{t(\ln t)^2}\,\mathrm{dt} = O\Big(\frac{1}{\ln x}\Big). \tag{4.9}$$

Schließlich haben wir

$$\begin{aligned}
\sum_{p\leqslant x}\frac{1}{p} &= \sum_{2\leqslant n\leqslant x} f(n)g(n) \\
&\overset{(4.1)}{=} \mathcal{F}(x)g(x) - \int_2^x \mathcal{F}(t)g'(t)\,\mathrm{dt} \\
&= \frac{\ln x + r(x)}{\ln x} + \int_2^x \frac{\ln t + r(t)}{t(\ln t)^2}\,\mathrm{dt} \\
&= 1 + O\Big(\frac{1}{\ln x}\Big) + \int_2^x \frac{1}{t\ln t}\,\mathrm{dt} + \int_2^x \frac{r(t)}{t(\ln t)^2}\,\mathrm{dt} \\
&= 1 + O\Big(\frac{1}{\ln x}\Big) + \Big(\ln\ln x - \ln\ln 2\Big) + \Big(\int_2^\infty \frac{r(t)}{t(\ln t)^2}\,\mathrm{dt} - \int_x^\infty \frac{r(t)}{t(\ln t)^2}\,\mathrm{dt}\Big) \\
&= 1 + O\Big(\frac{1}{\ln x}\Big) + \Big(\ln\ln x - \ln\ln 2\Big) + \int_2^\infty \frac{r(t)}{t(\ln t)^2}\,\mathrm{dt} + O\Big(\frac{1}{\ln x}\Big) \\
&\overset{(4.9)}{=} \ln\ln x + C + O\Big(\frac{1}{\ln x}\Big)
\end{aligned}$$

mit

$$C = 1 - \ln\ln 2 + \int_2^\infty \frac{r(t)}{t(\ln t)^2}\,\mathrm{dt}.$$

Das letzte Integral konvergiert absolut wegen $r(t) = O(1)$ und

$$\int_2^\infty \frac{1}{t(\ln t)^2}\,\mathrm{dt} = \frac{1}{\ln 2}.$$

□

5. Einige nützliche Summen

5.1. Euler-Konstante.

Lemma 5.1. *Es existiert eine Konstante $\gamma > 0$ (sie heißt* Euler-Konstante*) und eine Funktion $r : [1, \infty) \to \mathbb{R}$, so dass für jedes reelle $x \geqslant 1$ gilt:*

$$\sum_{n \leqslant x} \frac{1}{n} = \ln x + \gamma + r(x) \quad \text{und} \quad |r(x)| < \frac{1}{x}. \tag{5.1}$$

Beweis. Wir werden eine Variante von Lemma 4.1 mit Funktionen $f(n) = 1$, $g(t) = \frac{1}{t}$ und $\mathcal{F}(t) = \sum_{n \leqslant t} f(n) = [t]$ anwenden:

$$\begin{aligned}
\sum_{n \leqslant x} \frac{1}{n} &= \sum_{n \leqslant x} f(n)g(n) \\
&= \mathcal{F}(x)g(x) - \int_1^x \mathcal{F}(t)g'(t)\mathrm{dt} \\
&= \frac{[x]}{x} + \int_1^x \frac{[t]}{t^2}\mathrm{dt} \\
&= \frac{x - \{x\}}{x} + \int_1^x \frac{t - \{t\}}{t^2}\mathrm{dt} \\
&= 1 - \frac{\{x\}}{x} + \int_1^x \frac{1}{t}\mathrm{dt} - \int_1^x \frac{\{t\}}{t^2}\mathrm{dt} \\
&= 1 - \frac{\{x\}}{x} + \ln x - \int_1^x \frac{\{t\}}{t^2}\mathrm{dt} \\
&= \ln x + \underbrace{\Big(1 - \int_1^\infty \frac{\{t\}}{t^2}\mathrm{dt}\Big)}_{\gamma} + \underbrace{\Big(\int_x^\infty \frac{\{t\}}{t^2}\mathrm{dt} - \frac{\{x\}}{x}\Big)}_{r(x)}
\end{aligned}$$

Dann folgt Lemma 5.1 aus den Einschätzungen:

$$0 < \int_1^\infty \frac{\{t\}}{t^2}\mathrm{dt} < \int_1^\infty \frac{1}{t^2}\mathrm{dt} = 1$$

und

$$0 < \int_x^\infty \frac{\{t\}}{t^2}\mathrm{dt} < \int_x^\infty \frac{1}{t^2}\mathrm{dt} = \frac{1}{x}.$$

□

Folgerung 5.2. *Für jedes reelle $x \geqslant 1$ gilt*

$$\ln x = \sum_{n \leqslant x} \frac{1}{n} - \gamma + O\Big(\frac{1}{x}\Big) \tag{5.2}$$

5.2. **Verschiedene Summen von Logarithmen.** Bequemlichkeitshalber wiederholen wir eine Folgerung aus Vorlesung 4.

Folgerung 4.2. Für jedes reelle $x \geqslant 2$ gilt

$$\sum_{n \leqslant x} \ln n = x \ln x - x + O(\ln x). \tag{4.2}$$

Lemma 5.3. *Für jedes reelle $x \geqslant 2$ gilt*

$$\sum_{n \leqslant x} \ln^2 n = x \ln^2 x - 2x \ln x + 2x + O\Big(\ln^2 x\Big). \tag{5.3}$$

Hinweis. Setze $f(1) = 1$, $g(t) = \ln^2 t$, $\mathcal{F}(t) = \sum\limits_{n \leqslant t} f(t) = [t]$. Danach läuft der Beweis analog zum Beweis von Lemma 5.1. □

Lemma 5.4. *Für jedes reelle $x \geqslant 2$ gilt*

$$\sum_{n \leqslant x} \ln^2\Big(\frac{x}{n}\Big) = 2x + O\Big(\ln^2 x\Big). \tag{5.4}$$

Beweis.

$$\begin{aligned}
\sum_{n \leqslant x} \ln^2\Big(\frac{x}{n}\Big) &= \sum_{n \leqslant x} \big(\ln x - \ln n\big)^2 \\
&= \sum_{n \leqslant x} \big(\ln^2 x - 2 \ln x \ln n + \ln^2 n\big) \\
&= [x] \ln^2 x - 2 \ln x \sum_{n \leqslant x} \ln n + \sum_{n \leqslant x} \ln^2 n \\
&\underset{(5.3)}{\overset{(4.2)}{=}} [x] \ln^2 x - 2 \ln x \, \big(x \ln x - x + O(\ln x)\big) + \big(x \ln^2 x - 2x \ln x + 2x + O(\ln^2 x)\big) \\
&= 2x + O\big(\ln^2 x\big).
\end{aligned}$$

□

5.3. **Harmonische Summe mit Möbius-Koeffizienten.**

Satz 5.5.

$$\sum_{n\leqslant x}\frac{\mu(n)}{n}=O(1). \tag{5.5}$$

Beweis. Einerseits gilt

$$\sum_{dm\leqslant x}\mu(d)=\sum_{n\leqslant x}\sum_{d|n}\mu(d)\overset{(1.2)}{=}1. \tag{5.6}$$

Andererseits gilt

$$\begin{aligned}\sum_{dm\leqslant x}\mu(d) &= \sum_{d\leqslant x}\mu(d)\left[\frac{x}{d}\right]\\ &= \sum_{d\leqslant x}\mu(d)\Big(\frac{x}{d}-\Big\{\frac{x}{d}\Big\}\Big)\\ &= x\sum_{d\leqslant x}\frac{\mu(d)}{d}-\sum_{d\leqslant x}\mu(d)\Big\{\frac{x}{d}\Big\}\\ &\overset{\circledast}{=} x\sum_{d\leqslant x}\frac{\mu(d)}{d}+O(x),\end{aligned} \tag{5.7}$$

$\circledast$ Die letzte Gleichung gilt wegen $|\mu(d)|\leqslant 1$ und $0\leqslant\left\{\frac{x}{d}\right\}<1$ und wegen

$$\sum_{d\leqslant x}1=O(x).$$

Dann folgt aus (5.6) und (5.7):

$$1=x\sum_{d\leqslant x}\frac{\mu(d)}{d}+O(x),$$

worauf (5.5) folgt. □

Unser Ziel ist, folgende Formel zu beweisen:

$$\lim_{x\to\infty}\frac{\pi(x)}{\left(\frac{x}{\ln x}\right)}=1.$$

Dafür brauchen wir einige Verallgemeinerungen der Mangoldt-Funktion.

5.4. **Mangoldt-Funktionen der r-ten Ordnung.** In Definition 4.3 wurde eine wichtige arithmetische Funktion – die Mangoldt-Funktion – wie folgt definiert.

$$\Lambda(n) = \begin{cases} \ln p, & \text{falls } n = p^k \text{ für einige } p \in \text{Prim und } k \in \mathbb{N}, \\ 0, & \text{sonst} \end{cases}$$

Wir definieren noch eine arithmetische Funktion:

$$L(n) = \ln n.$$

Nach Aufgabe 2 des Blatts 2 gilt

$$\mathbf{1} * \Lambda = L \tag{5.8}$$

und

$$\Lambda = \mu * L. \tag{5.9}$$

Definition 5.6. Für $r \in \mathbb{N} \cup \{0\}$ definieren wir die r-te Mangoldt-Funktion durch

$$\Lambda_r = \mu * L^r, \tag{5.10}$$

wobei $L^r(n) = \ln^r(n)$ ist. Insbesondere gilt $\Lambda_0 = \mu * \mathbf{1} = \delta$ und $\Lambda_1 = \Lambda$.

Satz 5.7. *Für alle $n \in \mathbb{N}$ gilt*

$$\Lambda_2 = \Lambda \cdot L + \Lambda * \Lambda. \tag{5.11}$$

Beweis. Nach Aufgabe 3 des Blatts 1 ist die punktweise Multiplikation mit L eine Ableitung auf dem Ring $(\mathcal{AF}, +, *)$. Das bedeutet, dass die folgenden Formeln für alle $f, g \in \mathcal{AF}$ erfüllt sind:

$$\begin{aligned} L \cdot (f + g) &= L \cdot f + L \cdot g, \\ L \cdot (f * g) &= f * (L \cdot g) + (L \cdot f) * g \end{aligned} \tag{5.12}$$

Daraus folgt

$$L^2 = L \cdot L \overset{(5.8)}{=} L \cdot (\mathbf{1} * \Lambda) \overset{(5.12)}{=} \mathbf{1} * (L \cdot \Lambda) + (L \cdot \mathbf{1}) * \Lambda = \mathbf{1} * (\Lambda \cdot L) + L * \Lambda.$$

Deswegen gilt

$$\begin{aligned} \Lambda_2 = \mu * L^2 &= \mu * \mathbf{1} * (\Lambda \cdot L) + \mu * L * \Lambda \\ &\overset{(1.2)'}{=} \delta * (\Lambda \cdot L) + \mu * L * \Lambda. \\ &\overset{(5.9)}{=} \Lambda \cdot L + \Lambda * \Lambda. \end{aligned}$$

□

6. Selberg-Formeln

Aus der Gleichung (5.11) folgt, dass für jedes reelle $x \geqslant 1$ gilt

$$\sum_{n\leqslant x} \Lambda_2(n) = \sum_{n\leqslant x} \Lambda(n)\ln n + \sum_{n\leqslant x} \Lambda * \Lambda(n). \tag{6.1}$$

Wir werden jede der drei Summen abschätzen (folgende drei Lemmata) und schließlich Satz 7.3 (Selberg-Formeln) beweisen.

Lemma 6.1. *Für jedes reelle $x \geqslant 2$ gilt*

$$\sum_{n\leqslant x} \Lambda(n)\ln n = \sum_{p\leqslant x} \ln^2 p + O(x). \tag{6.2}$$

Beweis. Es gilt

$$\begin{aligned}\sum_{n\leqslant x} \Lambda(n)\ln n = \sum_{p^k\leqslant x} \ln p\,\ln p^k &= \sum_{p^k\leqslant x} k\ln^2 p \\ &= \sum_{p\leqslant x} \ln^2 p + \sum_{\substack{p^k\leqslant x\\ k\geqslant 2}} k\ln^2 p. \\ &\overset{\circledast}{=} \sum_{p\leqslant x} \ln^2 p + O(x).\end{aligned}$$

Erklärung zu $\circledast$: Wenn $p^k \leqslant x$ und $k \geqslant 2$ ist, dann ist $p \leqslant \sqrt{x}$. Deswegen gilt

$$\begin{aligned}\sum_{\substack{p^k\leqslant x\\ k\geqslant 2}} k\ln^2 p &= \sum_{p\leqslant\sqrt{x}} \sum_{2\leqslant k\leqslant[\frac{\ln x}{\ln p}]} k\ln^2 p \\ &= \sum_{p\leqslant\sqrt{x}} \ln^2 p \sum_{2\leqslant k\leqslant[\frac{\ln x}{\ln p}]} k \\ &\leqslant \sum_{p\leqslant\sqrt{x}} \ln^2 p \left(\frac{\ln x}{\ln p}\right)^2 \\ &\leqslant \sqrt{x}\ln^2 x \\ &= O(x).\end{aligned}$$

□

Lemma 6.2. *Für jedes reelle $x \geqslant 2$ gilt*

$$\sum_{n\leqslant x} \Lambda * \Lambda(n) = \sum_{pq\leqslant x} \ln p \ln q + O(x). \tag{6.3}$$

Beweis.

$$\begin{aligned}
\sum_{n\leqslant x} \Lambda * \Lambda(n) &= \sum_{n\leqslant x} \sum_{n=uv} \Lambda(u)\Lambda(v) \\
&= \sum_{uv\leqslant x} \Lambda(u)\Lambda(v) \\
&= \sum_{p^k q^\ell \leqslant x} \ln p \ln q \\
&= \sum_{pq\leqslant x} \ln p \ln q + \sum_{\substack{p^k q^\ell \leqslant x \\ k\geqslant 2}} \ln p \ln q + \sum_{\substack{p^k q^\ell \leqslant x \\ \ell\geqslant 2}} \ln p \ln q \\
&= \sum_{pq\leqslant x} \ln p \ln q + 2 \sum_{\substack{p^k q^\ell \leqslant x \\ k\geqslant 2}} \ln p \ln q.
\end{aligned}$$

Es bleibt nur den zweiten Summand einzuschätzen.

$$\begin{aligned}
\sum_{\substack{p^k q^\ell \leqslant x \\ k\geqslant 2}} \ln p \ln q &= \sum_{\substack{p^k \leqslant x \\ k\geqslant 2}} \sum_{q^\ell \leqslant x/p^k} \ln p \ln q \\
&= \sum_{\substack{p^k \leqslant x \\ k\geqslant 2}} \ln p \ \ \psi\Big(\frac{x}{p^k}\Big) \\
&\overset{(3.1)}{=} \sum_{\substack{p^k \leqslant x \\ k\geqslant 2}} \ln p \ \ O\Big(\frac{x}{p^k}\Big) = x \ O\Big(\sum_{\substack{p^k \leqslant x \\ k\geqslant 2}} \frac{\ln p}{p^k}\Big) = x \ O\Big(\sum_{p\leqslant x} \ln p \ \ \sum_{k=2}^{\infty} \frac{1}{p^k}\Big) \\
&= x \ O\Big(\sum_{p\leqslant x} \frac{\ln p}{p(p-1)}\Big) \\
&= xO(1).
\end{aligned}$$

□

Bemerkung. Mit Hilfe des Tschebyschew Satzes 3.1 haben wir

$$\sum_{n\leqslant x}\Lambda(n)=\sum_{p^k\leqslant x}\ln p=\psi(x)\overset{(3.1)}{=}O(x). \tag{6.4}$$

Lemma 6.3. *Für alle reelle $x\geqslant 1$ gilt*

$$\sum_{n\leqslant x}\Lambda_2(n)=2x\ln x+O(x). \tag{6.5}$$

Beweis. Wir haben

$$\begin{aligned}
\sum_{n\leqslant x}\Lambda_2(n) &= \sum_{n\leqslant x}\mu*L^2(n)\\
&= \sum_{n\leqslant x}\sum_{dk=n}\mu(d)\ln^2 k\\
&= \sum_{d\leqslant x}\sum_{k\leqslant\frac{x}{d}}\mu(d)\ln^2 k\\
&= \sum_{d\leqslant x}\mu(d)\sum_{k\leqslant\frac{x}{d}}\ln^2 k\\
&\overset{(5.3)}{=} \sum_{d\leqslant x}\mu(d)\Big(\frac{x}{d}\ln^2\frac{x}{d}-\frac{2x}{d}\ln\frac{x}{d}+\frac{2x}{d}+O\Big(\ln^2\frac{x}{d}\Big)\Big)\\
&= x\sum_{d\leqslant x}\frac{\mu(d)}{d}\Big(\ln\frac{x}{d}\Big)\Big(\ln\frac{x}{d}-2\Big)+2x\sum_{d\leqslant x}\frac{\mu(d)}{d}+O\Big(\sum_{d\leqslant x}\ln^2\frac{x}{d}\Big) \qquad (\text{weil } |\mu(d)|\leqslant 1)\\
&\underset{(5.4)}{\overset{(5.5)}{=}} x\sum_{d\leqslant x}\frac{\mu(d)}{d}\Big(\ln\frac{x}{d}\Big)\Big(\ln\frac{x}{d}-2\Big)+2xO(1)+O(2x+\ln^2 x)\\
&\overset{(4.2)}{=} x\sum_{d\leqslant x}\frac{\mu(d)}{d}\Big(\ln\frac{x}{d}\Big)\Big(\sum_{m\leqslant\frac{x}{d}}\frac{1}{m}-\gamma-2+O\Big(\frac{d}{x}\Big)\Big)+O(x)\\
&= x\sum_{d\leqslant x}\frac{\mu(d)}{d}\Big(\ln\frac{x}{d}\Big)\sum_{m\leqslant\frac{x}{d}}\frac{1}{m}-(\gamma+2+O(1))x\sum_{d\leqslant x}\frac{\mu(d)}{d}\ln\frac{x}{d}+O(x)\\
&= x\sum_{dm\leqslant x}\frac{\mu(d)}{dm}\Big(\ln\frac{x}{d}\Big)-(O(1))x\sum_{d\leqslant x}\frac{\mu(d)}{d}\ln\frac{x}{d}+O(x)\\
&\overset{\circledast}{=} \Big(2x\ln x+O(x)\Big)+\Big(O(1)xO(1)\Big)+O(x)\\
&= 2x\ln x+O(x).
\end{aligned}$$

Erklärung zu $\circledast$:

$$\begin{aligned}
\sum_{dm\leqslant x}\frac{\mu(d)}{dm}\ln\frac{x}{d} &= \sum_{n\leqslant x}\sum_{d\mid n}\frac{\mu(d)}{n}(\ln x-\ln d)\\
&= \ln x\sum_{n\leqslant x}\frac{1}{n}\sum_{d\mid n}\mu(d)-\sum_{n\leqslant x}\frac{1}{n}\sum_{d\mid n}\mu(d)\ln d\\
&\overset{(1.2)}{=} \ln x-\sum_{n\leqslant x}\frac{1}{n}\sum_{d\mid n}\mu(d)\Big(\ln n-\ln\frac{n}{d}\Big)\\
&= \ln x-\sum_{n\leqslant x}\frac{\ln n}{n}\sum_{d\mid n}\mu(d)+\sum_{n\leqslant x}\frac{1}{n}\sum_{d\mid n}\mu(d)\ln\frac{n}{d}\\
&\underset{(5.9)}{\overset{(1.2)}{=}} \ln x-0+\sum_{n\leqslant x}\frac{\Lambda(n)}{n}\\
&\overset{(4.6)}{=} 2\ln x+O(1).
\end{aligned}$$

Erklärung zu $\Cap$:

$$\begin{aligned}
\sum_{d\leqslant x}\frac{\mu(d)}{d}\ln\frac{x}{d} &\overset{(5.2)}{=} \sum_{d\leqslant x}\frac{\mu(d)}{d}\Big(\sum_{m\leqslant\frac{x}{d}}\frac{1}{m}-\gamma+O\Big(\frac{d}{x}\Big)\Big)\\
&= \sum_{dm\leqslant x}\frac{\mu(d)}{dm}-\gamma\sum_{d\leqslant x}\frac{\mu(d)}{d}+O(1)\\
&\overset{(5.5)}{=} \sum_{dm\leqslant x}\frac{\mu(d)}{dm}-\gamma O(1)+O(1)\\
&= \sum_{n\leqslant x}\frac{1}{n}\sum_{d\mid n}\mu(d)+O(1)\\
&\overset{(1.2)}{=} O(1).
\end{aligned}$$

□

Satz 6.4. (Selberg-Formeln) *Für alle reelle $x \geqslant 1$ gelten*

$$\sum_{p \leqslant x} \ln^2 p + \sum_{pq \leqslant x} \ln p \ln q = 2x \ln x + O(x). \tag{6.6}$$

$$\theta(x) \ln x + \sum_{p \leqslant x} \ln p \cdot \theta\Big(\frac{x}{p}\Big) = 2x \ln x + O(x). \tag{6.7}$$

(Hier sind p und q Primzahlen.)

Beweis. Die Formel (6.6) folgt aus (6.1) und drei vorherigen Lemmata. Wir beweisen (6.7). Dafür benutzen wir die arithmetische Funktion

$$\ell(n) = \begin{cases} \ln p, & \text{falls } n = p \in \text{Prim}, \\ 0, & \text{sonst} \end{cases}$$

und die Formel

$$\theta(n) = \sum_{n \leqslant x} \ell(n).$$

Es gilt

$$\begin{aligned} \sum_{p \leqslant x} \ln^2 p &= \sum_{n \leqslant x} \ell(n) \ln n \\ &\overset{(4.1)}{=} \theta(x) \ln x - \int_1^x \frac{\theta(t)}{t} \,\mathrm{dt} \qquad (6.8) \\ &\overset{(3.1)}{=} \theta(x) \ln x + O(x). \end{aligned}$$

Außerdem gilt

$$\sum_{pq \leqslant x} \ln p \ln q = \sum_{p \leqslant x} \ln p \sum_{q \leqslant \frac{x}{p}} \ln q = \sum_{p \leqslant x} \ln p \cdot \theta\Big(\frac{x}{p}\Big) \tag{6.9}$$

Wir substituieren (6.8) und (6.9) in (6.6) und erhalten (6.7). □

7. Noch zwei Selberg-Formeln

Zuerst beweisen wir zwei technische Lemmata.

Lemma 7.1. *Für jedes $k \in \mathbb{N}$ gilt*

$$\int_2^x \frac{\mathrm{d}t}{\ln^k t} = O\Big(\frac{x}{\ln^k x}\Big). \tag{7.1}$$

Beweis.

$$\begin{aligned}
\int_2^x \frac{\mathrm{d}t}{\ln^k t} &= \int_2^{\sqrt{x}} \frac{\mathrm{d}t}{\ln^k t} + \int_{\sqrt{x}}^x \frac{\mathrm{d}t}{\ln^k t} \\
&\leqslant \int_2^{\sqrt{x}} \frac{\mathrm{d}t}{\ln^k 2} + \int_{\sqrt{x}}^x \frac{\mathrm{d}t}{\ln^k \sqrt{x}} \\
&= (\sqrt{x}-2)\frac{1}{\ln 2} + (x-\sqrt{x})\frac{1}{\ln^k \sqrt{x}} \\
&= (\sqrt{x}-2)\frac{1}{\ln 2} + (x-\sqrt{x})\frac{2^k}{\ln^k x} \\
&\leqslant \frac{\sqrt{x}}{\ln 2} + \frac{2^k x}{\ln^k x} = O\Big(\frac{x}{\ln^k t}\Big).
\end{aligned}$$

□

Lemma 7.2. *Für $x \geqslant 3$ gilt*

$$\sum_{p \leqslant x} \frac{\ln p}{p\Big(1 + \ln \frac{x}{p}\Big)} = O(\ln\ln x). \tag{7.2}$$

Beweis. Zuerst beweisen wir, dass eine Konstante $C > 0$ existiert, so dass für jedes $x \geqslant 3$ und jedes $j \in \mathbb{N}$ gilt:

$$\sum_{\frac{x}{e^j} < p \leqslant \frac{x}{e^{j-1}}} \frac{\ln p}{p} < C.$$

Für $\frac{x}{e^j} \leqslant 2$ ist $\frac{x}{e^{j-1}} \leqslant 2e$, somit ist die linke Seite nicht größer als $\frac{\ln 2}{2} + \frac{\ln 3}{3} + \frac{\ln 5}{5}$. Für $\frac{x}{e^j} \geqslant 2$ folgt die Aussage aus dem Mertens-Satz 4.5:

$$\sum_{\frac{x}{e^j}<p\leqslant\frac{x}{e^{j-1}}}\frac{\ln p}{p}=\Big(\ln\frac{x}{e^{j-1}}+O(1)\Big)-\Big(\ln\frac{x}{e^j}+O(1)\Big)=O(1).$$

Merken wir an: Aus $p\leqslant\frac{x}{e^{j-1}}$ folgt $j\leqslant 1+\ln\frac{x}{p}$. Deswegen gilt

$$\sum_{\frac{x}{e^j}<p\leqslant\frac{x}{e^{j-1}}}\frac{\ln p}{p\Big(1+\ln\frac{x}{p}\Big)}\leqslant\sum_{\frac{x}{e^j}<p\leqslant\frac{x}{e^{j-1}}}\frac{\ln p}{pj}=\frac{1}{j}O(1)=O\Big(\frac{1}{j}\Big).$$

Daraus folgt

$$\sum_{p\leqslant x}\frac{\ln p}{p\Big(1+\ln\frac{x}{p}\Big)}=\sum_{j=1}^{[\ln x]+1}\sum_{\frac{x}{e^j}<p\leqslant\frac{x}{e^{j-1}}}\frac{\ln p}{p\Big(1+\ln\frac{x}{p}\Big)}=\sum_{j=1}^{[\ln x]+1}O\Big(\frac{1}{j}\Big)\overset{(5.1)}{=}O(\ln\ln x).$$

□

Satz 7.3. (weitere Selberg-Formeln) *Für alle reelle $x\geqslant 1$ gilt*

$$\sum_{p\leqslant x}\ln p+\sum_{pq\leqslant x}\frac{\ln p\ln q}{\ln pq}=2x+O\Big(\frac{x}{1+\ln x}\Big).\tag{7.3}$$

Für alle reelle $x\geqslant 3$ gilt

$$\theta(x)\ln x=\sum_{pq\leqslant x}\frac{\ln p\ln q}{\ln pq}\,\theta\Big(\frac{x}{pq}\Big)+O\Big(x\ln\ln x\Big).\tag{7.4}$$

(Hier sind p und q Primzahlen.)

Beweis. Zuerst beweisen wir (7.3). Für $1<x<e$ gilt diese Formel. Deswegen setzen wir $x\geqslant e$ voraus. Sei

$$\ell(n)=\begin{cases}\ln p, & \text{falls } n=p\in\mathrm{Prim},\\ 0, & \text{sonst.}\end{cases}$$

Wir haben

$$\sum_{n\leqslant x}(\ell*\ell)(n)=\sum_{n\leqslant x}\sum_{d_1d_2=n}\ell(d_1)\ell(d_2)=\sum_{d_1d_2\leqslant x}\ell(d_1)\ell(d_2)=\sum_{pq\leqslant x}\ln p\ln q.\tag{7.5}$$

Nun betrachten wir die arithmetische Funktion

$$f(n) = \ell(n)\ln n + (\ell * \ell)(n)$$

und die assozierte Funktion

$$\mathcal{F}(x) = \sum_{n\leqslant x} f(n).$$

Wir haben

$$\begin{aligned}
\mathcal{F}(x) &= \sum_{n\leqslant x} f(n) \\
&= \sum_{n\leqslant x} \ell(n)\ln n + (\ell * \ell)(n) \\
&\overset{(7.5)}{=} \sum_{p\leqslant x} \ln^2 p + \sum_{pq\leqslant x} \ln p \ln q \\
&\overset{(6.6)}{=} 2x\ln x + O(x).
\end{aligned} \tag{7.6}$$

Jetzt werden wir die linke Seite von (7.3) mit Hilfe der Formel (4.1) umformen:

$$\begin{aligned}
\sum_{p\leqslant x} \ln p + \sum_{pq\leqslant x} \frac{\ln p \ln q}{\ln pq} &= \sum_{2\leqslant n\leqslant x} \frac{\ell(n)\ln n + (\ell * \ell)(n)}{\ln n} \\
&= \sum_{2\leqslant n\leqslant x} f(n)g(n) \qquad\qquad (\text{mit } \ g(x) = \frac{1}{\ln x}) \\
&\overset{(4.1)}{=} \mathcal{F}(x)g(x) - \int_2^x \mathcal{F}(t)\, g'(t)\,\mathrm{dt} \\
&\overset{(7.6)}{=} \frac{2x\ln x + O(x)}{\ln x} - \int_2^x \frac{2t\ln t + O(t)}{t\ln^2 t}\,\mathrm{dt} \\
&= 2x + O\Big(\frac{x}{\ln x}\Big) \\
&\overset{\circledast}{=} 2x + O\Big(\frac{x}{1+\ln x}\Big).
\end{aligned} \tag{7.3}'$$

Erklärung zu $\circledast$: Für $x \geqslant e$ gilt

$$\frac{x}{\ln x} \leqslant \frac{2x}{1+\ln x}.$$

Jetzt beweisen wir (7.4). Zuerst wird (7.3) mit anderen Variablen umgeschrieben:

$$\sum_{q\leqslant \frac{x}{p}} \ln q + \sum_{qr\leqslant \frac{x}{p}} \frac{\ln q \ln r}{\ln qr} = 2\frac{x}{p} + O\Big(\frac{x}{p(1+\ln \frac{x}{p})}\Big). \tag{7.3$'$}$$

Dann gilt

$$\begin{aligned}
\sum_{pq\leqslant x} \ln p \ln q \;&= \sum_{p\leqslant x} \ln p \sum_{q\leqslant \frac{x}{p}} \ln q \\
&\overset{(7.3)'}{=} \sum_{p\leqslant x} \ln p \Big(-\sum_{qr\leqslant \frac{x}{p}} \frac{\ln q \ln r}{\ln qr} + \frac{2x}{p} + O\Big(\frac{x}{p(1+\ln \frac{x}{p})}\Big)\Big) \\
&= -\sum_{pqr\leqslant x} \frac{\ln p \ln q \ln r}{\ln qr} + 2x \sum_{p\leqslant x} \frac{\ln p}{p} + O\Big(x \sum_{p\leqslant x} \frac{\ln p}{p(1+\ln \frac{x}{p})}\Big)\Big) \\
&\underset{(7.2)}{\overset{(4.7)}{=}} -\sum_{pqr\leqslant x} \frac{\ln p \ln q \ln r}{\ln qr} + 2x\Big(\ln x + O(1)\Big) + O\Big(x \ln\ln x\Big) \\
&= -\sum_{qr\leqslant x} \frac{\ln q \ln r}{\ln qr} \sum_{p\leqslant \frac{x}{qr}} \ln p + 2x \ln x + O\Big(x \ln\ln x\Big) \\
&= -\sum_{qr\leqslant x} \frac{\ln q \ln r}{\ln qr}\, \theta\Big(\frac{x}{qr}\Big) + 2x \ln x + O\Big(x \ln\ln x\Big).
\end{aligned} \tag{7.7}$$

Bequemlichkeitshalber reproduzieren wir hier die erste Selberg Formel aus Vorlesung 6:

$$\sum_{p\leqslant x} \ln^2 p = -\sum_{pq\leqslant x} \ln p \ln q + 2x \ln x + O(x). \tag{6.6}$$

Aus (7.7) und (6.6) folgt

$$\sum_{p\leqslant x} \ln^2 p = \sum_{qr\leqslant x} \frac{\ln q \ln r}{\ln qr}\, \theta\Big(\frac{x}{qr}\Big) + O\Big(x \ln\ln x\Big). \tag{7.8}$$

Wir haben noch

$$\sum_{p\leqslant x} \ln^2 p \overset{(6.9)}{=} \theta(x) \ln x + O(x). \tag{7.9}$$

Aus (7.8) und (7.9) folgt (7.4). □

8. Eine Ungleichung für $R(x) = \theta(x) - x$

Unser Ziel ist, die folgende Formel zu beweisen:

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1. \tag{8.1}$$

Wir bezeichnen

$$R(x) = \theta(x) - x.$$

Dann ist (8.1) zu $R(x) = o(x)$ äquivalent. Diese Abschätzung wird aus der Ungleichung (8.6) abgeleitet.

Für den Beweis dieser Ungleichung benötigen wir vier Lemmata. Das erste Lemma ist eine Variante des schon bekannten Lemmas 4.1.

Lemma 8.1. *Seien f und g zwei arithmetische Funktionen. Für jedes $y \in [1, \infty)$ definieren wir*

$$\mathcal{F}(y) = \sum_{n\leqslant y} f(n).$$

Dann gilt für jedes $x \geqslant 1$:

$$\sum_{n\leqslant x} f(n)g(n) = \sum_{n\leqslant x-1} \mathcal{F}(n)\big(g(n) - g(n+1)\big) + \mathcal{F}(x)g([x]). \tag{8.2}$$

Lemma 8.2. *Es gilt*

$$a_k b_{k+1} + \sum_{1\leqslant n\leqslant k} a_n(b_n - b_{n+1}) = a_1 b_1 + \sum_{2\leqslant n\leqslant k} (a_n - a_{n-1})b_n. \tag{8.3}$$

Lemma 8.3. (s. Aufgabe 2 des Übungsblatts 4) *Für $x > e$ gilt*

$$\sum_{n\leqslant x} \frac{1}{n(1+\ln n)} = O(\ln\ln x). \tag{8.4}$$

Lemma 8.4. (s. Aufgabe 3 des Übungsblatts 4) *Für $x > e$ gilt*

$$\sum_{pq\leqslant x} \frac{\ln p \ln q}{pq \ln pq} = \ln x + O(\ln\ln x). \tag{8.5}$$

Satz 8.5. *Für $x > 1$ gilt*

$$|R(x)| \leqslant \frac{1}{\ln x} \sum_{n \leqslant x} \left| R\Big(\frac{x}{n}\Big) \right| + o(x). \tag{8.6}$$

Beweis. In der Selberg-Formel (6.7) ersetzen wir $\theta(x)$ durch $R(x) + x$:

$$\begin{aligned} 2x \ln x + O(x) &\overset{(6.7)}{=} \theta(x) \ln x + \sum_{p \leqslant x} \ln p \cdot \theta\Big(\frac{x}{p}\Big) \\ &= (R(x) + x) \ln x + \sum_{p \leqslant x} \ln p \cdot \Big(R\Big(\frac{x}{p}\Big) + \frac{x}{p} \Big) \\ &= R(x) \ln x + x \ln x + \sum_{p \leqslant x} \ln p \cdot R\Big(\frac{x}{p}\Big) + x \sum_{p \leqslant x} \frac{\ln p}{p} \\ &\overset{(4.7)}{=} R(x) \ln x + \sum_{p \leqslant x} \ln p \cdot R\Big(\frac{x}{p}\Big) + 2x \ln x + O(x). \end{aligned}$$

Daraus folgt

$$R(x) \ln x = -\sum_{p \leqslant x} R\Big(\frac{x}{p}\Big) \ln p + O(x). \tag{8.7}$$

Jetzt ersetzen wir in der Selberg-Formel (7.4) die Funktion $\theta(x)$ durch $R(x)+x$:

$$\begin{aligned} (R(x) + x) \ln x &= \sum_{pq \leqslant x} \frac{\ln p \ln q}{\ln pq} \Big(R\Big(\frac{x}{pq}\Big) + \frac{x}{pq} \Big) + O\Big(x \ln \ln x\Big) \\ &= \sum_{pq \leqslant x} \frac{\ln p \ln q}{\ln pq} R\Big(\frac{x}{pq}\Big) + x \sum_{pq \leqslant x} \frac{\ln p \ln q}{pq \ln pq} + O\Big(x \ln \ln x\Big) \\ &\overset{(8.5)}{=} \sum_{pq \leqslant x} \frac{\ln p \ln q}{\ln pq} R\Big(\frac{x}{pq}\Big) + x \ln x + O\Big(x \ln \ln x\Big) \end{aligned}$$

Daraus folgt

$$R(x) \ln x = \sum_{pq \leqslant x} \frac{\ln p \ln q}{\ln pq} R\Big(\frac{x}{pq}\Big) + O(x \ln \ln x). \tag{8.8}$$

Jetzt addieren wir (8.7) und (8.8) und benutzen die Dreiecksungleichung:

$$
\begin{aligned}
2|R(x)|\ln x &\leqslant \sum_{p\leqslant x} \ln p \,\Big|R\Big(\frac{x}{p}\Big)\Big| + \sum_{pq\leqslant x} \frac{\ln p \ln q}{\ln pq}\,\Big|R\Big(\frac{x}{pq}\Big)\Big| + O(x\ln\ln x)\\
&= \sum_{n\leqslant x} \ell(n)\,\Big|R\Big(\frac{x}{n}\Big)\Big| + \sum_{n\leqslant x} \frac{\ell * \ell(n)}{\ln n}\,\Big|R\Big(\frac{x}{n}\Big)\Big| + O(x\ln\ln x)\\
&= \sum_{n\leqslant x} \Big(\ell(n) + \frac{\ell * \ell(n)}{\ln n}\Big)\,\Big|R\Big(\frac{x}{n}\Big)\Big| + O(x\ln\ln x).
\end{aligned}
\tag{8.9}
$$

Die letzte Summe werden wir mit Hilfe des Lemmas 8.1 abschätzen. Seien

$$
f(n) = \ell(n) + \frac{\ell * \ell(n)}{\ln n} \quad \text{und} \quad g(n) = \Big|R\Big(\frac{x}{n}\Big)\Big|.
$$

Dann gilt

$$
\mathcal{F}(x) = \sum_{n\leqslant x} f(n) = \sum_{n\leqslant x} \Big(\ell(n) + \frac{\ell * \ell(n)}{\ln n}\Big) \overset{(7.3)'}{\underset{(7.3)}{=}} 2x + O\Big(\frac{x}{1+\ln x}\Big)
$$

Wir haben

$$
\begin{aligned}
&\sum_{n\leqslant x} \Big(\ell(n) + \frac{\ell * \ell(n)}{\ln n}\Big)\,\Big|R\Big(\frac{x}{n}\Big)\Big|\\
&= \sum_{n\leqslant x} f(n)g(n)\\
&\overset{(8.2)}{=} \sum_{n\leqslant x-1} \mathcal{F}(n)\big(g(n) - g(n+1)\big) + \mathcal{F}(x)g([x])\\
&= \sum_{n\leqslant x-1} \Big(2n + O\Big(\frac{n}{1+\ln n}\Big)\Big)\,\Big(\Big|R\Big(\frac{x}{n}\Big)\Big| - \Big|R\Big(\frac{x}{n+1}\Big)\Big|\Big)\\
&\qquad\qquad + \Big(2x + O\Big(\frac{x}{1+\ln x}\Big)\Big)\,\Big|R\Big(\frac{x}{[x]}\Big)\Big|.
\end{aligned}
\tag{8.9$'$}
$$

Des Weiteren werden wir einige Terme in dem letzten Ausdruck abschätzen.

Abschätzung 1.

$$\begin{aligned}\Big|R\Big(\frac{x}{n}\Big)\Big| - \Big|R\Big(\frac{x}{n+1}\Big)\Big| &= \Big|\theta\Big(\frac{x}{n}\Big) - \frac{x}{n}\Big)\Big| - \Big|\theta\Big(\frac{x}{n+1} - \frac{x}{n+1}\Big)\Big| \\ &\leqslant \Big|\theta\Big(\frac{x}{n}\Big) - \theta\Big(\frac{x}{n+1}\Big) - \Big(\frac{x}{n} - \frac{x}{n+1}\Big)\Big| \\ &\leqslant \Big|\theta\Big(\frac{x}{n}\Big) - \theta\Big(\frac{x}{n+1}\Big)\Big| + \Big|\frac{x}{n} - \frac{x}{n+1}\Big| \\ &< \theta\Big(\frac{x}{n}\Big) - \theta\Big(\frac{x}{n+1}\Big) + \frac{x}{n^2}.\end{aligned}$$

Abschätzung 2.

$$\begin{aligned}&\sum_{n\leqslant x-1}\Big(\frac{n}{1+\ln n}\Big)\Big(\Big|R\Big(\frac{x}{n}\Big)\Big| - \Big|R\Big(\frac{x}{n+1}\Big)\Big|\Big) \\ &\leqslant \sum_{n\leqslant x-1}\Big(\frac{n}{1+\ln n}\Big)\Big(\theta\Big(\frac{x}{n}\Big) - \theta\Big(\frac{x}{n+1}\Big) + \frac{x}{n^2}\Big) \\ &= \sum_{n\leqslant x-1}\Big(\frac{n}{1+\ln n}\Big)\Big(\theta\Big(\frac{x}{n}\Big) - \theta\Big(\frac{x}{n+1}\Big)\Big) + \sum_{n\leqslant x-1}\frac{x}{n(1+\ln n)} \\ &\overset{(8.4)}{=} \sum_{n\leqslant x-1}\Big(\frac{n}{1+\ln n}\Big)\Big(\theta\Big(\frac{x}{n}\Big) - \theta\Big(\frac{x}{n+1}\Big)\Big) + O(x\ln\ln x) \\ &\overset{(8.3)}{=} \theta(x) + \sum_{2\leqslant n\leqslant x-1}\Big(\frac{n}{1+\ln n} - \frac{n-1}{1+\ln(n-1)}\Big)\theta\Big(\frac{x}{n}\Big) + O(x\ln\ln x) \\ &\leqslant \theta(x) + \sum_{2\leqslant n\leqslant x-1}\Big(\frac{1}{1+\ln n}\Big)\theta\Big(\frac{x}{n}\Big) + O(x\ln\ln x) \\ &= \sum_{1\leqslant n\leqslant x-1}\Big(\frac{1}{1+\ln n}\Big)\theta\Big(\frac{x}{n}\Big) + O(x\ln\ln x) \\ &\overset{(3.1)}{=} O\Big(x\sum_{1\leqslant n\leqslant x-1}\Big(\frac{1}{n(1+\ln n)}\Big)\Big) + O(x\ln\ln x) \\ &\overset{(8.4)}{=} O(x\ln\ln x).\end{aligned}$$

Abschätzung 3.

$$\sum_{n\leqslant x-1} n\left(\left|R\Big(\frac{x}{n}\Big)\right| - \left|R\Big(\frac{x}{n+1}\Big)\right|\right)$$

$$= \sum_{n\leqslant x} \left|R\Big(\frac{x}{n}\Big)\right| - [x]\left|R\Big(\frac{x}{[x]}\Big)\right|$$

$$= \sum_{n\leqslant x} \left|R\Big(\frac{x}{n}\Big)\right| + O(x)\,O(1).$$

Abschätzung 4.

$$\Big(2x + O\Big(\frac{x}{1+\ln x}\Big)\Big)\left|R\Big(\frac{x}{[x]}\Big)\right| = O(x)O(1) = O(x).$$

Letzter Schritt. Wir substituieren die Abschätzungen 2-4 in (8.9)′ und erhalten

$$\sum_{n\leqslant x}\Big(\ell(n) + \frac{\ell * \ell(n)}{\ln n}\Big)\left|R\Big(\frac{x}{n}\Big)\right| = \sum_{n\leqslant x}\left|R\Big(\frac{x}{n}\Big)\right| + O(x\ln\ln x).$$

Nun substituieren wir diesen Ausdruck in (8.9) und dividieren die linke und die rechte Seite der Ungleichung durch $\ln x$. Dann erhalten wir (8.6). □

9. Eine schwache Form der Gleichung $R(x) = o(x)$

Unser Endziel ist, folgendes zu zeigen:

$$\lim_{x\to\infty} \frac{R(x)}{x} = 0. \tag{9.1}$$

In diesem Abschnitt werden wir etwas schwächere Aussage – Satz 9.6 – beweisen. Eine ganz schwache (aber nicht offensichtliche) Aussage klingt so:

Für jedes $\delta > 0$ existieren unendlich viele n mit $\frac{|R(n)|}{n} < \delta$.

In Vorlesung 10 werden wir Satz 9.6 und die Ungleichung (8.5) benutzen, um (9.1) zu beweisen.

Lemma 9.1. (Aufgabe 1 des Übungsblatts 5) *Für $x > 1$ gilt*

$$\sum_{k\leqslant n\leqslant x} \frac{1}{n^2} = \frac{1}{k} - \frac{1}{x} + O\Big(\frac{1}{k^2}\Big). \tag{9.2}$$

Lemma 9.2. *Für $x > 1$ gilt*

$$\sum_{n\leqslant x} \frac{\theta(n)}{n^2} = \ln x + O(1). \tag{9.3}$$

Beweis. Zuerst schränken wir eine Summe nach oben ein:

$$\sum_{k\leqslant x} \frac{\ell(k)}{k^2} < \sum_{k=1}^{\infty} \frac{\ell(k)}{k^2} < \sum_{k=1}^{\infty} \frac{\ln k}{k^2} := C < \infty. \tag{9.4}$$

Wir haben

$$\begin{aligned}
\sum_{n\leqslant x} \frac{\theta(n)}{n^2} = \sum_{n\leqslant x}\sum_{k\leqslant n} \frac{\ell(k)}{n^2} \quad &= \sum_{k\leqslant x} \Big(\ell(k) \sum_{k\leqslant n\leqslant x} \frac{1}{n^2}\Big) \\
&\overset{(9.2)}{=} \sum_{k\leqslant x} \ell(k)\Big(\frac{1}{k} - \frac{1}{x} + O\Big(\frac{1}{k^2}\Big)\Big) \\
&= \sum_{k\leqslant x} \frac{\ell(k)}{k} - \frac{\theta(x)}{x} + O\Big(\sum_{k\leqslant x} \frac{\ell(k)}{k^2}\Big)\Big) \\
&\underset{(9.4)}{\overset{(3.1)}{=}} \sum_{p\leqslant x} \frac{\ln(p)}{p} + O(1) + O(C) \\
&\overset{(4.7)}{=} \ln x + O(1). \qquad \square
\end{aligned}$$

Folgerung 9.3. *Es existiert eine Konstante $c \geqslant 1$, so dass für jedes $x > 1$ gilt:*

$$\Big|\sum_{n\leqslant x} \frac{R(n)}{n^2}\Big| < c. \tag{9.5}$$

Beweis. Wir haben

$$\sum_{n\leqslant x} \frac{R(n)}{n^2} = \sum_{n\leqslant x} \frac{\theta(n)-n}{n^2} \underset{(5.1)}{\overset{(9.3)}{=}} (\ln x + O(1)) - (\ln x + O(1)) = O(1).$$

□

Lemma 9.4. *Es existiert eine Konstante $A > 0$, so dass für $1 < u \leqslant t$ gilt*

$$|R(t) - R(u)| \leqslant (t-u) + \frac{At}{1+\ln t}. \tag{9.6}$$

Beweis. Sei $1 < u \leqslant t$. Wir haben

$$R(t) - R(u) = (\theta(t) - t) - (\theta(u) - u) = -(t-u) + \sum_{u<p\leqslant t} \ln p. \tag{9.7}$$

Jetzt werden wir die letzte Summe mit Hilfe der Selberg-Formel (7.3) abschätzen. Bequemlichkeitshalber reproduzieren wir sie hier:

$$\sum_{p\leqslant x} \ln p + \sum_{pq\leqslant x} \frac{\ln p \ln q}{\ln pq} = 2x + O\Big(\frac{x}{1+\ln x}\Big). \tag{7.3}$$

Mit Hilfe dieser Formel erhalten wir

$$\begin{aligned} 0 \leqslant \sum_{u<p\leqslant t} \ln p &\leqslant \sum_{u<p\leqslant t} \ln p + \sum_{u<pq\leqslant t} \frac{\ln p \ln q}{\ln pq} \\ &= 2(t-u) + O\Big(\frac{t}{1+\ln t}\Big) + O\Big(\frac{u}{1+\ln u}\Big) \\ &= 2(t-u) + O\Big(\frac{t}{1+\ln t}\Big), \end{aligned} \tag{9.8}$$

weil die Funktion $\dfrac{t}{1+\ln t}$ monoton wachsend auf $[1,\infty)$ ist. Aus (9.7) und (9.8) folgt

$$-(t-u) \leqslant R(t) - R(u) \leqslant (t-u) + O\Big(\frac{t}{1+\ln t}\Big).$$

Daraus folgt (9.6). □

Satz 9.5. *Sei $c \geqslant 1$ die Konstante aus der Folgerung 9.3 und sei $0 < \delta < 1$. Dann existiert eine reelle Zahl $x_1(\delta) > 1$, so dass für alle $x \geqslant x_1(\delta)$ das Intervall $(x, e^{4c/\delta}x]$ eine natürlichen Zahl n enthält, für die gilt:*

$$\Big|\frac{R(n)}{n}\Big| < \delta. \tag{9.9}$$

Beweis. Sei $x_1(\delta) > 1$ eine Zahl, so dass für alle $x \geqslant x_1(\delta)$ gilt

$$\frac{\ln x}{x} < \delta. \tag{9.10}$$

Sei $x \geqslant x_1(\delta) > 1$ beliebig; insbesondere gilt (9.10). Sei $\rho := e^{4c/\delta}$.

Fall 1. Nehmen wir an:
Für alle $n \in (x, \rho x]$ gilt $R(n) \geqslant 0$ oder für alle $n \in (x, \rho x]$ gilt $R(n) \leqslant 0$.
Sei

$$m^* = \min\Big\{\frac{|R(n)|}{n} : n \in (x, \rho x]\Big\}.$$

Dann gilt

$$\begin{aligned} 2c \overset{(9.5)}{>} \sum_{x<n\leqslant \rho x} \frac{|R(n)|}{n}\cdot\frac{1}{n} \;&\geqslant\; m^* \sum_{x<n\leqslant\rho x}\frac{1}{n} \\ &\overset{(5.1)}{>}\; m^*\Big(\Big(\ln\rho x+\gamma-\frac{1}{\rho x}\Big)-\Big(\ln x+\gamma+\frac{1}{x}\Big)\Big) \\ &> m^*\Big(\ln\rho-\frac{2}{x}\Big) >\; m^*\Big(\frac{4c}{\delta}-2\Big). \end{aligned}$$

Daraus und aus $c \geqslant 1$ und $0 < \delta < 1$ folgt

$$0 \leqslant m^* < \delta.$$

Nach Definition von m^* existiert ein $n \in (x, \rho x]$ mit $\dfrac{|R(n)|}{n} = m^* < \delta$.

Fall 2. Nehmen wir an:
Es existieren ganze Zahlen $n-1$ und n in dem Intervall $(x, \rho x]$, so dass gilt:

$$R(n-1)R(n) \leqslant 0. \tag{9.11}$$

Wir haben $n - 1 > x > 1$, deswegen gilt $n \geqslant 3$. Außerdem gilt

$$\begin{aligned} R(n) - R(n-1) \;&= \theta(n) - \theta(n-1) - 1 \\ &= \begin{cases} \ln n - 1 > 0, & \text{falls } n \in \text{Prim}, \\ -1, & \text{sonst.} \end{cases} \end{aligned}$$

Dann ist

$$|R(n) - R(n-1)| < \ln n. \tag{9.12}$$

Aus (9.11) und (9.12) folgt

$$|R(n)| < \ln n.$$

Deswegen gilt

$$\frac{|R(n)|}{n} < \frac{\ln n}{n} \overset{(9.10)}{<} \delta.$$

□

Satz 9.6. *Sei $c \geqslant 1$ die Konstante aus der Folgerung 9.3 und sei $0 < \delta < 1$. Dann existiert eine Zahl $x_2(\delta) > 1$, so dass für alle $x \geqslant x_2(\delta)$ das Intervall $(x, e^{4c/\delta}x]$ ein Teilintervall $(y, e^{\delta/2}y]$ enthält, so dass*

$$\Big|\frac{R(t)}{t}\Big| < 6\delta \tag{9.13}$$

für jedes $t \in (y, e^{\delta/2}y]$ gilt.

Beweis. Wir setzen

$$x_2(\delta) = \max\{e^{A/\delta}, x_1(\delta)\}, \tag{9.14}$$

wobei $A > 0$ die Konstante aus Lemma 9.4 und $x_1(\delta) > 1$ eine Zahl aus Satz 9.5 sind. Sei $x > x_2(\delta)$. Nach Satz 9.5 existiert eine natürliche Zahl $n \in (x, e^{4c/\delta}x]$, für die gilt:

$$\Big|\frac{R(n)}{n}\Big| < \delta. \tag{9.15}$$

Fall 1. Sei $e^{\delta/2}n \leqslant e^{4c/\delta}x$.

Wir beweisen, dass $(n, e^{\delta/2}n]$ das gewünschte Teilintervall ist. Offensichtlich gilt $(n, e^{\delta/2}n] \subseteq (x, e^{4c/\delta}x]$. Es bleibt zu beweisen, dass (9.13) für alle $t \in (n, e^{\delta/2}n]$ gilt. Für eine solche t gilt

$$\begin{aligned} |R(t)| &\overset{(9.6)}{\leqslant} |R(n)| + (t-n) + \frac{At}{\ln t} \overset{\substack{(9.15)\\(9.14)}}{\leqslant} \delta n + (t-n) + \frac{At}{A/\delta} \\ &= t\Big(\delta\frac{n}{t} + \Big(1 - \frac{n}{t}\Big) + \delta\Big) \leqslant t\Big(\delta + \Big(1 - e^{-\delta/2}\Big) + \delta\Big) \leqslant 3\delta t. \end{aligned}$$

Somit ist (9.13) erfüllt.

Fall 2. Sei $e^{\delta/2}n > e^{4c/\delta}x$.

Wir beweisen, dass $(e^{-\delta/2}n, n]$ das gewünschte Teilintervall ist. Es gilt $(e^{-\delta/2}n, n] \subseteq (x, e^{4c/\delta}x]$, weil $e^{-\delta/2}n > e^{-\delta}e^{4c/\delta}x > x$ gilt. Es bleibt zu beweisen, dass (9.13) für alle $t \in (e^{-\delta/2}n, n]$ gilt. Für eine solche t gilt

$$\begin{aligned} |R(t)| &\overset{(9.6)}{\leqslant} |R(n)| + (n-t) + \frac{An}{\ln n} \overset{(9.15)}{\underset{(9.14)}{\leqslant}} \delta n + (n-t) + \frac{Ae^{\delta/2}t}{A/\delta} \\ &= t\Big(\delta\frac{n}{t} + \Big(\frac{n}{t} - 1\Big) + \delta e^{\delta/2}\Big) \leqslant t\Big(\delta e^{\delta/2} + \Big(e^{\delta/2} - 1\Big) + \delta e^{\delta/2}\Big) \\ &\leqslant 3\delta e^{\delta/2}t \leqslant 6\delta t. \end{aligned}$$

□

10. Beweis zu $R(x) = o(x)$. Beweis von Prime Number Theorem (PNT)

Satz 10.1. (PNT) *Es gilt*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1. \tag{10.1}$$

Ursprünglich haben diesen Satz Hadamard und Valle-Pussen mit Hilfe von zeta-Funktion und Funktionentheorie bewiesen. Den "elementaren" Beweis (also ohne komplexen Zahlen und Sätze der Funktionentheorie), haben Selberg und Erdős mit Hilfe von Selberg-Formeln entdeckt. Wir werden eine Variante dieses Beweises präsentieren. Hauptsächlich basiert dieser Beweis auf Satz 8.5: Für $x > 1$ gilt:

$$|R(x)| \leqslant \frac{1}{\ln x} \sum_{n\leqslant x} \left| R\Big(\frac{x}{n}\Big) \right| + o(x). \tag{8.6}$$

Für einen "glatten" Verlauf des Beweises von PNT brauchen wir eine glatte (integrale) Variante dieser Ungleichung, s. (10.2).

Satz 10.2. *Es gilt*

$$|R(x)| \leqslant \frac{1}{\ln x} \int_1^x \left| R\Big(\frac{x}{t}\Big) \right| \mathrm{dt} + o(x). \tag{10.2}$$

Im Beweis des Satzes 10.2 werden wir das folgende elementare Lemma benutzen.

Lemma 10.3. *Sei $f : [1, \infty] \to \mathbb{R}$ eine positive monoton fallende Funktion. Dann gilt für jedes $x \geqslant 1$:*

$$\sum_{k=1}^{[x]} f(k) \leqslant f(1) + \int_1^{[x]} f(t)\,\mathrm{dt}. \tag{10.3}$$

Beweis.

$$\sum_{k=2}^{[x]} f(k) = \sum_{k=2}^{[x]} \int_{k-1}^{k} f(k)\,\mathrm{dt} \leqslant \sum_{k=2}^{[x]} \int_{k-1}^{k} f(t)\,\mathrm{dt} = \int_1^{[x]} f(t)\,\mathrm{dt}.$$

□

Beweis des Satzes 10.2. Wir werden den Unterschied zwischen der Summe in (8.6) und dem Integral in (10.2) abschätzen:

$$
\begin{aligned}
& \Big| \int_1^x \big|R\Big(\frac{x}{t}\Big)\big| \,\mathrm{dt} - \sum_{n\leqslant x} \big|R\Big(\frac{x}{n}\Big)\big| \Big| \\
= \quad & \Big| \sum_{n=1}^{[x]-1} \int_n^{n+1} \big|R\Big(\frac{x}{t}\Big)\big| \,\mathrm{dt} + \int_{[x]}^{x} \big|R\Big(\frac{x}{t}\Big)\big| \,\mathrm{dt} - \sum_{n=1}^{[x]-1} \big|R\Big(\frac{x}{n}\Big)\big| - \big|R\Big(\frac{x}{[x]}\Big)\big| \Big| \\
\leqslant \quad & \Big| \sum_{n=1}^{[x]-1} \int_n^{n+1} \Big(\big|R\Big(\frac{x}{t}\Big)\big| - \big|R\Big(\frac{x}{n}\Big)\big| \Big) \,\mathrm{dt} \Big| + O(1) \\
\leqslant \quad & \sum_{n=1}^{[x]-1} \int_n^{n+1} \Big| \big|R\Big(\frac{x}{t}\Big)\big| - \big|R\Big(\frac{x}{n}\Big)\big| \Big| \,\mathrm{dt} + O(1) \\
\leqslant \quad & \sum_{n=1}^{[x]-1} \int_n^{n+1} \Big| R\Big(\frac{x}{n}\Big) - R\Big(\frac{x}{t}\Big) \Big| \,\mathrm{dt} + O(1) \\
\overset{(9.6)}{\leqslant} \quad & \sum_{n=1}^{[x]-1} \int_n^{n+1} \Big(\Big(\frac{x}{n} - \frac{x}{t}\Big) + \frac{A\cdot x/n}{1+\ln(x/n)} \Big) \,\mathrm{dt} + O(1) \\
\leqslant \quad & \sum_{n=1}^{[x]-1} \int_n^{n+1} \Big(\Big(\frac{x}{n} - \frac{x}{n+1}\Big) + \frac{A\cdot x/n}{1+\ln(x/n)} \Big) \,\mathrm{dt} + O(1) \\
\leqslant \quad & \sum_{n=1}^{[x]-1} \Big(\frac{x}{n} - \frac{x}{n+1}\Big) + \sum_{n=1}^{[x]-1} \frac{A\cdot x/n}{1+\ln(x/n)} + O(1) \\
\overset{(10.3)}{\leqslant} \quad & x - \frac{x}{[x]} + \frac{Ax}{1+\ln x} + \int_1^{[x]-1} \frac{A\cdot x/t}{1+\ln(x/t)} \,\mathrm{dt} + O(1) \\
\leqslant \quad & x + 0 + o(x) - \frac{Ax}{\ln(1+\ln(x/t))} \Big|_1^{[x]-1} \\
\leqslant \quad & x + o(x) - \frac{Ax}{\ln(1+\ln(x/([x]-1)))} + \frac{Ax}{\ln(1+\ln x)} \\
\leqslant \quad & x + o(x) + 0 + o(x) = x + o(x).
\end{aligned}
$$

Daraus und aus (8.6) folgt (10.2). □

Beweis des Satzes 10.1. Wir bezeichnen

$$U(x) := \frac{|R(x)|}{x}.$$

Nach Theorem 3.1 von Tschebyschev ist $\lim\limits_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$ zu $\lim\limits_{x\to\infty} \frac{\theta(x)}{x} = 1$ äquivalent. Da $R(x) = \theta(x) - x$ ist, ist das Letzte zu folgendem äquivalent:

$$\lim_{x\to\infty} U(x) = 0. \tag{10.4}$$

Wir beweisen also (10.4).

Bemerkung. Nach Tschebyschev-Satz 3.1 gilt

$$\limsup_{x\to\infty} \frac{R(x)}{x} = \limsup_{x\to\infty} \frac{\theta(x)}{x} - 1 \leqslant \ln 4 - 1 < 1 \tag{10.5}$$

und

$$\liminf_{x\to\infty} \frac{R(x)}{x} = \liminf_{x\to\infty} \frac{\theta(x)}{x} - 1 \geqslant \ln 2 - 1 > -1. \tag{10.6}$$

Die Funktion $U(x)$ erfüllt folgende drei Bedingungen:

(1) (folgt aus (10.5) und (10.6))
Es existiert eine Zahl $A_0 > 0$, so dass für alle $x \geqslant A_0$ gilt:

$$0 \leqslant U(x) < 1.$$

(2) (abgeleitet aus Satz 10.2)

$$U(x) \leqslant \frac{1}{\ln x} \int_1^x U\Big(\frac{x}{t}\Big) \cdot \frac{1}{t}\,\mathrm{dt} + o(1).$$

(3) (abgeleitet aus Satz 9.6)
Für jedes $0 < \delta < 1$ existiert $x_2(\delta) > 1$, so dass für alle $x \geqslant x_2(\delta)$ das Intervall $(x, e^{4c/\delta}x]$ ein Teilintervall $(y, e^{\delta/2}y]$ enthält, so dass

$$U(t) < 6\delta$$

für jedes $t \in (y, e^{\delta/2}y]$ gilt.

Nun übergehen wir zu den "exponentiellen" Variablen. Dafür bezeichnen wir

$$u(x) = U(e^x).$$

Dann können die Bedingungen (1)-(3) wie folgt umgeschrieben werden:

(a) Es existiert eine Zahl $A_0 > 0$, so dass für alle $x \geqslant A_0$ gilt:

$$0 \leqslant u(x) < 1.$$

(b) (in (2) setze e^x statt x und substituiere $t = e^s$)

$$u(x) \leqslant \frac{1}{x}\int_0^x u(x-s)\,\mathrm{d}s + o(1) = \frac{1}{x}\int_0^x u(s)\,\mathrm{d}s + o(1).$$

(c) (in (3) setze e^x statt x, e^y statt y und e^t statt t)
Für jedes $0 < \delta < 1$ existiert $x_3(\delta) > 0$, so dass für alle $x \geqslant x_3(\delta)$ das Intervall $(x, x + 4c/\delta]$ ein Teilintervall der Länge $\delta/2$ enthält, so dass

$$u(t) < 6\delta$$

für jedes t aus diesem Teilintervall gilt.

Sei $0 < \varepsilon \leqslant 1$ beliebig. Nehmen wir an, dass eine Zahl $A > 0$ existiert, so dass für alle $x \geqslant A$ gilt:

$$u(x) \leqslant \varepsilon. \tag{10.7}$$

O.B.d.A. können wir voraussetzen, dass gilt:

$$A > \frac{52c}{\varepsilon}. \tag{10.8}$$

Wir werden zeigen, dass eine Zahl $A' > 0$ existiert, so dass für alle $x \geqslant A'$ gilt:

$$u(x) \leqslant \varepsilon\Big(1 - \frac{\varepsilon^2}{1354c}\Big).$$

Wir setzen

$$\delta = \varepsilon/13. \tag{10.9}$$

Sei $x > A$ beliebig. Wir bedecken das Intervall $[A, x]$ mit Intervallen der Länge $4c/\delta$:

$$\Big[A, A + \frac{4c}{\delta}\Big],\ \Big[A + \frac{4c}{\delta}, A + \frac{8c}{\delta}\Big],\ \ldots,\ \Big[A + \frac{4c(N-1)}{\delta}, A + \frac{4cN}{\delta}\Big],$$

wobei $N \in \mathbb{N}$ folgende Ungleichung erfüllt:

$$A + \frac{4c(N-1)}{\delta} \leqslant x < A + \frac{4cN}{\delta}. \tag{10.10}$$

Auf jeden dieser Intervalle gilt $u \leqslant \varepsilon$, siehe Annahme (10.7), und jeder dieser Intervalle ein Teilintervall der Länge $\delta/2$ enthällt auf dem $u < 6\delta$ gilt, siehe Bedingung (c). Deswegen gilt für jedes $j = 1, \ldots, N$:

$$\int\limits_{A+\frac{4c(j-1)}{\delta}}^{A+\frac{4cj}{\delta}} u(s)\,\mathrm{ds} \leqslant \Big(\frac{4c}{\delta} - \frac{\delta}{2}\Big)\cdot\varepsilon + \delta\cdot 6\delta \overset{(10.9)}{=} \frac{4c}{\delta}\cdot\varepsilon\Big(1 - \frac{\varepsilon^2}{1352c}\Big).$$

Daraus folgt

$$\begin{aligned}\int_A^x u(s)\,\mathrm{ds} \leqslant \sum_{j=1}^{N} \int\limits_{A+\frac{4c(j-1)}{\delta}}^{A+\frac{4cj}{\delta}} u(s)\,\mathrm{ds} \quad &\leqslant \frac{4cN}{\delta}\cdot\varepsilon\Big(1 - \frac{\varepsilon^2}{1352c}\Big)\\ &\overset{(10.10)}{\leqslant} \Big(x - A + \frac{4c}{\delta}\Big)\cdot\varepsilon\Big(1 - \frac{\varepsilon^2}{1352c}\Big)\\ &\underset{(10.9)}{\overset{(10.8)}{<}} x\varepsilon\Big(1 - \frac{\varepsilon^2}{1352c}\Big).\end{aligned}$$

Dann gilt

$$\begin{aligned}\int_0^x u(s)\,\mathrm{ds} = \underbrace{\int_0^A u(s)\,\mathrm{ds}}_{M} + \int_A^x u(s)\,\mathrm{ds} \quad &\leqslant M + x\varepsilon\Big(1 - \frac{\varepsilon^2}{1352c}\Big)\\ &< x\varepsilon\Big(1 - \frac{\varepsilon^2}{1353c}\Big)\end{aligned}$$

für alle groß genug x. Daraus folgt

$$u(x) \overset{\mathbf{(b)}}{\leqslant} \frac{1}{x}\int_0^x u(s)\,\mathrm{ds} + o(1) < \varepsilon\Big(1 - \frac{\varepsilon^2}{1354c}\Big)$$

für alle groß genug x. Somit haben wir bewiesen, dass eine Zahl $A' > 0$ existiert, so dass für alle $x \geqslant A'$ gilt:

$$u(x) \leqslant \varepsilon\Big(1 - \frac{\varepsilon^2}{1354c}\Big).$$

Nun definieren wir die Folge $(\varepsilon_i)_{i\in\mathbb{N}}$ durch $\varepsilon_1 = 1$ und $\varepsilon_{i+1} = \varepsilon_i\Big(1 - \frac{\varepsilon_i^2}{1354c}\Big)$. Diese Folge ist positiv und monoton fallend. Deswegen hat diese Folge ein Limes, sagen wir $\epsilon_0 = \lim\limits_{i\to\infty}\varepsilon_i$. Es gilt $0 \leqslant \epsilon_0 < 1$ und $\epsilon_0 = \epsilon_0\Big(1 - \frac{\epsilon_0^2}{1354c}\Big)$. Deswegen gilt $\epsilon_0 = 0$. Das bedeutet, dass $\lim\limits_{x\to\infty} u(x) = 0$ gilt. Folglich gilt (10.4). Der Satz 10.1 ist bewiesen. □

Teil 2.
Einführung in die algebraische Zahlentheorie

11. Endliche und algebraische Erweiterungen

Definition 11.1. Seien K, E zwei Körper.

1) Der Körper E heißt *Erweiterung* des Körpers K, falls $K \subseteq E$ ist. In dem Fall kann man E als Vektorraum über K betrachten. Die Dimension dieses Vektorraums wird mit $[E : K]$ bezeichnet.
2) Die Erweiterung E heißt *endlich* über K, falls $[E : K]$ endlich ist.
3) Ein Element $\alpha \in E$ heißt *algebraisch* über K, falls ein nichtnullsches Polynom $p(x) \in K[x]$ existiert, so dass $p(\alpha) = 0$ ist. Beispiel dazu: $\alpha = 5\sqrt{2} + \sqrt{3} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$.
4) Die Erweiterung E heißt *algebraisch* über K, falls jedes Element von E algebraisch über K ist.

Definition 11.2. Sei R ein kommutativer Ring. Ein Polynom $f(x) \in R[x]$ heißt *reduzibel* über R, falls zwei Polynome $f_1(x), f_2(x) \in R[x]$ existieren, so dass $f(x) = f_1(x)f_2(x)$ und $1 \leqslant \mathrm{Grad}\,(f_i(x)) < \mathrm{Grad}(f(x))$ für $i = 1, 2$ gilt. Ein Polynom $f(x) \in R[x]$ heißt *irreduzibel* über R, falls es nicht reduzibel ist.

Satz 11.3. Sei $\alpha \in E$ algebraisch über K. Wir betrachten die Menge von Polynomen über K, die α annulieren:

$$\mathrm{Ann}_K(\alpha) = \{f(x) \in K[x] \mid f(\alpha) = 0\}.$$

Es gelten:

1) Die Menge $\mathrm{Ann}_K(\alpha) \setminus \{0\}$ enthält genau ein Polynom $p(x)$ des minimalen Grades und mit dem Hauptkoeffizient gleich 1.
(Dieses Polynom heißt *minimales Polynom* für α über K und wird mit $m_\alpha(x)$ bezeichnet.)
2) $p(x)$ ist ein Teiler jedes Polynoms $f(x)$ aus $\mathrm{Ann}_K(\alpha)$.
3) $p(x)$ ist irreduzibel über K.

Satz 11.4. Sei E eine Erweiterung von K und sei $\alpha \in E$. Ein Polynom $f(x) \in K[x]$ ist das minimale Polynom für α genau dann, wenn folgende drei Eigenschaften erfüllt sind:

1) $q(\alpha) = 0$,
2) Der Hauptkoeffizient von $q(x)$ ist gleich 1,
3) $q(x)$ ist irreduzibel über K.

Beispiel. Das Polynom $x^4 - 10x^2 + 1$ ist das minimale Polynom für $\alpha = \sqrt{2} + \sqrt{3}$ über $\mathbb{Q}$.

Satz 11.5. Jede endliche Erweiterung E über K ist algebraisch über K.

Wir werden sehen, dass algebraische Erweiterungen E über K existieren, die unendlich über K sind.

Satz 11.6. Seien $k \subseteq K \subseteq E$ endliche Erweiterungen. Dann gilt $[E : k] = [E : K][K : k]$. Ist $\{u_i\}_{i\in I}$ eine Basis von K über k und ist $\{v_j\}_{j\in J}$ eine Basis von E über K, dann ist $\{u_i v_j\}_{(i,j)\in I\times J}$ eine Basis von E über k.

Definition 11.7. Sei $K \subseteq E$ eine Erweiterung. Für $\alpha \in E$ bezeichnen wir mit $K(\alpha)$ den kleinsten Körper in E, der K und α enthält. Es ist leicht zu sehen:

$$K(\alpha) = \Big\{ \frac{f(\alpha)}{g(\alpha)} \,|\, f(x), g(x) \in K[x] \text{ und } g(\alpha) \neq 0 \Big\}.$$

Wir bezeichnen

$$K[\alpha] = \{f(\alpha) \,|\, f(x) \in K[x]\}.$$

Analog definiert man $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ und $K[\alpha_1, \alpha_2, \ldots, \alpha_n]$.

Satz 11.8. Sei α algebraisch über K. Dann ist $K(\alpha) = K[\alpha]$. Außerdem gilt:

$$[K(\alpha) : K] = \mathrm{Grad}(m_\alpha(x)).$$

Eine Basis von $K(\alpha)$ über K ist $1, \alpha, \ldots, \alpha^{n-1}$, wobei $n = \mathrm{Grad}(m_\alpha(x))$ ist.

Beispiel. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$ ist eine algebraische Erweiterung von $\mathbb{Q}$, die unendlich über $\mathbb{Q}$ ist.

Satz 11.9. (Eisenstein-Kriterium.) Sei $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$ und sei p eine Primzahl. Nehmen wir an, dass folgendes gilt:

1) $p \nmid a_n$,
2) $p \mid a_i$ für $0 \leqslant i \leqslant n-1$,
3) $p^2 \nmid a_0$.

Dann ist $p(x)$ irreduzibel über $\mathbb{Z}$ und über $\mathbb{Q}$.

Satz 11.10. Sei $E = K(\alpha_1, \ldots, \alpha_n)$ und alle α_i algebraisch über K. Dann ist E endlich über K und folglich algebraisch über K.

Lemma 11.11. (Gauss) Ein Polynom $f(x) \in \mathbb{Z}[x]$ ist irreduzibel über $\mathbb{Z}$ genau dann, wenn es irreduziebel über $\mathbb{Q}$ ist.

12. Norm, Spur und Diskriminante

Definition 12.1. Sei E eine endliche Erweiterung von K. Sei $\alpha \in E$. Wir betrachten die Abblidung

$$\begin{aligned} \varphi_\alpha : \quad & E \to E, \\ & x \mapsto \alpha x. \end{aligned}$$

Diese Abbildung ist K-linear. Sei $\omega = \{\omega_1, \ldots, \omega_n\}$ eine Basis von E über K. Wir multiplizieren die Elemente von ω mit α und schreiben diese Produkte als lineare Kombinationen der Basiselemente mit Koeffizienten aus K:

$$\begin{aligned} \alpha\omega_1 &= a_{11}\omega_1 + \cdots + a_{1n}\omega_n \\ &\vdots \\ \alpha\omega_n &= a_{n1}\omega_1 + \cdots + a_{nn}\omega_n \end{aligned}$$

Daraus entsteht die Darstellungsmatrix der linearen Abbildung φ_α in der Basis ω :

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}.$$

Das Polynom $\chi_\alpha(x) = \det(xE_n - A)$ heißt *charakteristisches Polynom von α.* Die Zahl $\det(A)$ heißt *Norm von α* und wird mit $N_{E/K}(\alpha)$ bezeichnet. Die Zahl $\mathrm{Spur}(A) = a_{11} + \cdots + a_{nn}$ heißt *Spur von α* und wird mit $\mathrm{Sp}_{E/K}(\alpha)$ bezeichnet. Wenn die Körper K und E fixiert sind, werden wir einfach $N(\alpha)$ und $\mathrm{Sp}(\alpha)$ schreiben.

Bemerkung.

1) Das Polynom $\chi_\alpha(x)$ und die Zahlen $N_{E/K}(\alpha)$, $\mathrm{Sp}_{E/K}(\alpha)$ hängen nicht von der Wahl der Basis ω ab.
2) $\chi_\alpha(x) = x^n - \mathrm{Sp}_{E/K}(\alpha)x^{n-1} + \cdots + (-1)^n N_{E/K}(\alpha)$.

Beispiel. Sei $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Dann ist $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ eine Basis von E über $\mathbb{Q}$. Es gelten:

1) $N_{E/\mathbb{Q}}(\sqrt{6}) = 36$,
2) $\mathrm{Sp}_{E/\mathbb{Q}}(\sqrt{6}) = 0$,
3) $\chi_{\sqrt{6}}(x) = (x^2 - 6)^2$,
4) $m_{\sqrt{6}}(x) = x^2 - 6$.

Satz 12.2. Seien E^* und K^* die multiplikativen Gruppen der Körper E und K entsprechend und sei $n = [E : K]$ endlich. Dann gilt:

(1) $N_{E/K} : E^* \to K^*$ ist ein Homomorphismus.

(2) $\mathrm{Sp}_{E/K} : E \to K$ ist eine K-lineare Abbildung.

(3) $N_{E/K}(k\alpha) = k^n \cdot N_{E/K}(\alpha)$ für alle $k \in K$.

(4) $\mathrm{Sp}_{E/K}(k\alpha) = k \cdot \mathrm{Sp}_{E/K}(\alpha)$ für alle $k \in K$.

Satz 12.3. Seien $L \subseteq K \subseteq E$ endliche Körpererweiterungen. Dann gelten:

$$N_{E/L} = N_{K/L} \circ N_{E/K},$$
$$\mathrm{Sp}_{E/L} = \mathrm{Sp}_{K/L} \circ \mathrm{Sp}_{E/K}.$$

Satz 12.4. Sei $K \subseteq E$ eine endliche Körpererweiterung und sei $\alpha \in E$. Dann ist das charakteristische Polynom von α eine Potenz des minimalen Polynoms von α:

$$\chi_\alpha(x) = (m_\alpha(x))^k.$$

Definition 12.5. Sei $K \subseteq E$ eine Körpererweiterung mit $[E : K] = n < \infty$. Sei $(\alpha_1, \ldots, \alpha_n)$ ein Tupel von Elementen von E. Die folgende Zahl aus K heißt *Diskriminante* dieses Tupels:

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} \mathrm{Sp}(\alpha_1\alpha_1) & \ldots & \mathrm{Sp}(\alpha_1\alpha_n) \\ \vdots & & \vdots \\ \mathrm{Sp}(\alpha_n\alpha_1) & \ldots & \mathrm{Sp}(\alpha_n\alpha_n) \end{pmatrix}.$$

Satz 12.6. Sei $K \subseteq E$ eine Körpererweiterung mit $[E : K] = n < \infty$. Sei $(\alpha_1, \ldots, \alpha_n)$ ein Tupel von Elementen von E. Dann gelten:

(1) Wenn $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$ ist, dann ist $(\alpha_1, \ldots, \alpha_n)$ eine Basis von E über K.

(2) Wenn $\mathrm{char}(L) = 0$ ist und $(\alpha_1, \ldots, \alpha_n)$ eine Basis von E über K, dann ist $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

Satz 12.7. Seien $(\alpha_1, \ldots, \alpha_n)$ und $(\beta_1, \ldots, \beta_n)$ zwei Basen von E über K. Sei $\alpha_i = \sum_{j=1}^n c_{ij}\beta_j$, wobei $c_{ij} \in K$ ist. Dann gilt

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(c_{ij}))^2 \Delta(\beta_1, \ldots, \beta_n).$$

13. Weitere wichtige Definitionen und Sätze über Körpererweiterungen

Weiter sind einige wichtige Definitionen und Sätze gegeben, die wir wegen Zeitmangels nicht ausführlich besprechen (beweisen) können. Den Stoff kann man in dem Buch von S. Lang "Algebra" (Kapitel: "Algebraic extensions") finden.

13.1. **Algebraischer Abschluss.**

Definition 13.1. Ein Körper L heißt *algebraisch abgeschlossen*, falls jedes Polynom in $L[X]$ des Grades $\geqslant 1$ eine Nullstelle in L hat.

Definition 13.2. Sei $k \subseteq L$ eine Körpererweiterung. Der Körper L heißt *algebraischer Abschluss* von k, falls das Folgende gilt:
1) L ist algebraisch abgeschlossen,
2) L ist algebraisch über k.

Satz 13.3. Für jeden Körper k existiert ein algebraischer Abschluss von k. Seien L_1, L_2 zwei algebraische Abschlüsse von k, dann existiert ein Isomorphismus $\varphi : L_1 \to L_2$ mit $\varphi_{|k} = id$.

Einen algebraischen Abschluss von k bezeichnen wir mit k^{a}.

Bemerkung. Es gibt algebraisch abgeschlossene, aber nicht algebraische Erweiterungen von k. Ein Beispiel dazu: $k(t)^{\mathrm{a}}$, wobei $k(t)$ der Körper aller rationalen Funktionen von t über k ist:

$$k(t) := \left\{ \frac{f(t)}{g(t)} \mid f(t), g(t) \in k[t], g(t) \neq 0 \right\}.$$

Ein anderes Beispiel: $\mathbb{C}$ ist eine algebraisch abgeschlossene, aber nicht algebraische Erweiterung von $\mathbb{Q}$.

13.2. **Erweiterungen von Einbettungen.**

Definition 13.4. Sei $k \subseteq K$ eine Körpererweiterung und sei L ein Körper. Seien $\sigma : k \to L$ und $\tau : K \to L$ zwei Einbettungen (d.h. injektive Homomorphismen). Man sagt, dass τ eine *Erweiterung* von σ ist, falls $\tau_{|k} = \sigma$ ist.

Satz 13.5. Sei $K = k(\alpha)$, wobei α algebraisch über k ist. Jede Einbettung $\sigma : k \to L$ von k in einen algebraisch abgeschlossenen Körper L hat genau n Erweiterungen $\tau : K \to L$, wobei n die Anzahl der verschiedenen Nullstellen von $m_\alpha(x)$ in k^{a} ist.

13.3. **Separable Erweiterungen.** Der folgende Satz ist eine Verallgemeinerung des Satzes 13.5.

Satz 13.6. Sei $k \subseteq K$ eine algebraische Erweiterung von k. Jede Einbettung $\sigma : k \to L$ von k in einen algebraisch abgeschlossenen Körper L kann bis zu einer Einbettung $\tau : K \to L$ erweitert werden.

Die Kardinalität der Menge der Erweiterungen hängt nur von k und K ab (also nicht von L und σ). Diese Kardinalität heißt *Separabilitätsgrad* von K über k und wird als $[K : k]_s$ bezeichnet. Es gilt $[K : k]_s \leqslant [K : k]$.

Definition 13.7.

1) Eine endliche Erweiterung $k \subseteq K$ heißt *separabel*, falls $[K : k]_s = [K : k]$ gilt.

2) Ein algebraisches Element α über k heißt *separabel*, falls $m_\alpha(x)$ keine vielfachen Nullstellen hat.

Satz 13.8.

1) Eine endliche Erweiterung $k \subseteq k(\alpha)$ ist separabel genau dann, wenn α separabel ist.

2) Seien $k \subseteq k_1 \subseteq K$ endliche Erweiterungen. Dann gilt: Die Erweiterung $k \subseteq K$ ist separabel genau dann, wenn beide Erweiterungen $k \subseteq k_1$ und $k_1 \subseteq K$ separabel sind.

3) Seien $k \subseteq k_1 \subseteq K$ endliche Erweiterungen. Dann gilt:

$$[K : k]_s = [K : k_1]_s [k_1 : k]_s.$$

Satz 13.9. Eine endliche Erweiterung $k \subseteq K$ ist separabel genau dann, wenn jedes $\alpha \in K$ separabel über k ist.

Satz 13.10. Sei $k \subseteq K$ eine separable Erweiterung mit endlichem Grad $[K : k] = n$ und seien $\tau_1, \tau_2, \ldots, \tau_n$ alle Einbettungen von K in k^{a} (über k). Dann gilt für jedes $\alpha \in K$:

$$\chi_\alpha(x) = (x - \tau_1(\alpha))(x - \tau_2(\alpha)) \ldots (x - \tau_n(\alpha)).$$

Folgerung 13.11. Sei $k \subseteq K$ eine separable Erweiterung mit endlichem Grad $[K : k] = n$ und seien $\tau_1, \tau_2, \ldots, \tau_n$ alle Einbettungen von K in k^{a} (über k). Dann gilt für jedes $\alpha \in K$:

$$\mathrm{Sp}_{K/k}(\alpha) = \tau_1(\alpha) + \tau_2(\alpha) + \ldots + \tau_n(\alpha),$$
$$N_{K/k}(\alpha) = \tau_1(\alpha) \cdot \tau_2(\alpha) \cdot \ldots \cdot \tau_n(\alpha).$$

Satz 13.12. Sei $k \subseteq K$ eine separable Erweiterung mit $[K : k] = n < \infty$ und seien $\tau_1, \ldots, \tau_n$ alle Einbettungen von K in k^{a} über k. Seien $\alpha_1, \ldots, \alpha_n \in K$. Dann gilt:

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(\tau_j(\alpha_i)))^2 = \begin{vmatrix} \tau_1(\alpha_1) & \ldots & \tau_n(\alpha_1) \\ \vdots & & \vdots \\ \tau_1(\alpha_n) & \ldots & \tau_n(\alpha_n) \end{vmatrix}^2 .$$

14. Zahlkörper und Ganzheitssringe

Definition 14.1. Ein Körper K heißt *Zahlkörper*, falls $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ ist und $[K : \mathbb{Q}]$ endlich ist.

Definition 14.2. Ein $\alpha \in \mathbb{C}$ heißt *ganze algebraische Zahl*, falls eine der drei äquivalenten Bedingungen erfüllt ist:

(a) Es existiert ein Polynom $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ mit Koeffizienten aus $\mathbb{Z}$ und dem Hauptkoeffizient 1, so dass $f(\alpha) = 0$ gilt.

(b) Die Koeffizienten des minimalen Polynoms $m_\alpha(x, \mathbb{Q})$ liegen in $\mathbb{Z}$.

(c) Die Koeffizienten des charakteristischen Polynoms $\chi_\alpha(x, \mathbb{Q})$ liegen in $\mathbb{Z}$.

Bemerkung. Aus (c) folgt: Die Spuren und die Normen von ganzen algebraischen Zahlen liegen in $\mathbb{Z}$.

Bezeichnung. Des Weiteren sei $\mathcal{O}_\mathbb{C}$ die Menge aller ganzen algebraischen Zahlen in $\mathbb{C}$.

Satz 14.3. Die Menge $\mathcal{O}_\mathbb{C}$ bildet einen Ring.

Definition 14.4. Sei K ein Zahlkörper. Der Ring $\mathcal{O}_K = \mathcal{O}_\mathbb{C} \cap K$ heißt *Ring der ganzen algebraischen Zahlen in K* oder *Ganzheitsring von K*.

Lemma 14.5. *Es gilt* $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.

Satz 14.6. Sei $m \in \mathbb{Z} \setminus \{0, 1\}$ quadratfrei (d.h. es existiert keine Primzahl p mit $p^2|m$) und sei $K = \mathbb{Q}(\sqrt{m})$. Dann gilt:

(a) Die Zahl $\alpha = a + b\sqrt{m} \in K$ mit $a, b \in \mathbb{Q}$ liegt in $\mathcal{O}_K$ genau dann, wenn die folgenden Zahlen in $\mathbb{Z}$ liegen:

$$\begin{aligned} \mathrm{Sp}(\alpha) &= 2a, \\ N(\alpha) &= a^2 - b^2 m. \end{aligned} \tag{14.1}$$

(b) Es gilt

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}\,] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{m}, & \text{falls } m \equiv 2 \text{ oder } 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{m}}{2}] = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{m}}{2}, & \text{falls } m \equiv 1 \pmod 4. \end{cases} \tag{14.2}$$

Bemerkung. Es gilt

$$\left(\mathbb{Z} \oplus \mathbb{Z}\sqrt{m}\right) \subseteq \left(\mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{m}}{2}\right). \tag{14.3}$$

Tatsächlich, es gilt $\sqrt{m} = -1 + 2\frac{1+\sqrt{m}}{2}$.

Beweis des Satzes. Die Formeln $\mathrm{Sp}(\alpha) = 2a$ und $N(\alpha) = a^2 - b^2 m$ sind leicht zu überprüfen.

Zu (a): Wir haben $\chi_\alpha(x) = x^2 - \mathrm{Sp}(\alpha)x + N(\alpha)$. Dann folgt (a) aus Definitzion 14.2.

Zu (b):
$\supseteq$: Im Fall $m \equiv 2$ oder $3 \pmod 4$ müssen wir zeigen, dass 1 und $\sqrt{m}$ in $\mathcal{O}_K$ liegen. Das folgt aus dem Fakt, dass die Minimalpolynome $x - 1$ und $x^2 - m$ dieser Zahlen in $\mathbb{Z}[x]$ liegen.

Im Fall $m \equiv 1 \mod 4$ müssen wir noch zeigen, dass $\frac{1+\sqrt{m}}{2}$ in $\mathcal{O}_K$ liegt. Das folgt direkt aus (a):

$$\mathrm{Sp}\Big(\frac{1+\sqrt{m}}{2}\Big) = 2{\cdot}\frac{1}{2} = 1 \in \mathbb{Z}, \quad N\Big(\frac{1+\sqrt{m}}{2}\Big) = \Big(\frac{1}{2}\Big)^2 - \Big(\frac{1}{2}\Big)^2 m = \frac{1-m}{4} \in \mathbb{Z}.$$

$\subseteq$: Sei $\alpha = a + b\sqrt{m} \in \mathcal{O}_K$ mit $a, b \in \mathbb{Q}$. Wir zeigen, dass α in der rechten Seite der Formel (14.2) liegt.

Ist $b = 0$, dann gilt $\alpha = a \in \mathcal{O}_K \cap \mathbb{Q} \overset{\text{Lem } 14.5}{=} \mathbb{Z}$, und wir sind fertig.

Sei $b \neq 0$. Wir schreiben $b = \frac{p}{q}$ mit $p, q \in \mathbb{Z}$, $q > 0$ und $\mathrm{ggT}(p, q) = 1$. Da $\alpha \in \mathcal{O}_K$ ist, gilt nach (a):

$$\underbrace{2a}_{X}, \ \underbrace{a^2 - b^2 m}_{Y} \in \mathbb{Z}. \tag{14.4}$$

Wir haben

$$X^2 - 4Y = 4b^2 m = 4\Big(\frac{p}{q}\Big)m.$$

Daraus folgt

$$q^2\Big(X^2 - 4Y\Big) = 4p^2 m. \tag{14.5}$$

Da p und q teilerfremd sind, gilt $q^2 | 4m$. Da m quadratfrei ist, gilt $q^2 | 4$, also ist $q = 1$ oder $q = 2$. □

Fall 1. Sei $q = 1$.
Da $b = \frac{p}{q}$ ist, ist $b \in \mathbb{Z}$. Dann folgt aus (14.4): $2a, a^2 \in \mathbb{Z}$. Daraus folgt $a \in \mathbb{Z}$. Deswegen gilt

$$\alpha = a + b\sqrt{m} \ \in \ \mathbb{Z} \oplus \mathbb{Z}\sqrt{m} \ \overset{(14.3)}{\subseteq} \ \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{m}}{2}.$$

Fall 2. Sei $q = 2$.
Dann ist p ungerade wegen $\mathrm{ggT}(p, q) = 1$. Außerdem folgt aus (14.5):

$$X^2 - 4Y = p^2 m. \tag{14.6}$$

Wäre X gerade, dann hätten wir $4|p^2 m$ und folglich $4|m$, was unmöglich ist, da m quadratfrei ist. Also ist X ungerade. Deswegen gilt $X^2 \equiv 1 (\mathrm{mod}\ 4)$ und $p^2 \equiv 1 (\mathrm{mod}\ 4)$. Dann folgt aus (14.6):

$$m \equiv 1 \ (\mathrm{mod}\ 4).$$

Die folgende Zeile zeigt, dass $\mathcal{O}_K$ in der rechten Seite von (14.2) liegt:

$$\alpha = a + b\sqrt{m} \overset{(14.4)}{=} \frac{X}{2} + \frac{p}{2}\sqrt{m} = \frac{X-p}{2} + p\Big(\frac{1+\sqrt{m}}{2}\Big) \in \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{m}}{2}.$$

□

15. Einheiten, Primelemente und irreduzible Elemente

Definition 15.1. Sei R ein kommutativer Ring mit 1.

1) Seien $x, y \in R$. Man sagt, dass y ein *Teiler* von x ist, falls ein $z \in R$ mit $x = yz$ existiert. In dem Fall schreibt man $y|x$.
2) Ein Element $x \in R$ heißt *Einheit* in R, falls ein $y \in R$ mit $xy = 1$ existiert.
   Die Menge der Einheiten in R ist eine multiplikative Gruppe. Diese Gruppe heißt *Einheitsgruppe* von R und wird mit R^* bezeichnet.
3) Zwei Elemente $\alpha, \beta \in R$ heißen assoziiert, wenn eine Einheit $\varepsilon \in (\mathcal{O}_K)^*$ mit $\alpha = \varepsilon\beta$ existiert. In diesem Fall schreiben wir $\alpha \sim \beta$.
4) Ein Element $0 \neq x \in R$ heißt *Primelement* in R, falls das Folgende gilt:
   (a) x ist keine Einheit;
   (b) für alle $a, b \in R$ gilt:
   Ist x ein Teiler von ab, dann ist x ein Teiler von a oder b.
5) Ein Element $0 \neq x \in R$ heißt *irreduzibel* in R, falls das Folgende gilt:
   (a) x ist keine Einheit;
   (b) aus $x = yz$ mit $y, z \in R$ folgt, dass y oder z eine Einheit in R ist.

Satz 15.2. Für jeden Zahlkörper K gilt

$$(\mathcal{O}_K)^* = \{\alpha \in \mathcal{O}_K \mid N(\alpha) = \pm 1\}.$$

Beweis.
$\subseteq$: Sei $\alpha \in (\mathcal{O}_K)^*$. Dann existiert $\beta \in (\mathcal{O}_K)^*$ mit $\alpha\beta = 1$. Daraus folgt $N(\alpha)N(\beta) = N(1) = 1$. Da die Normen von ganzen algebraischen Zahlen in $\mathbb{Z}$ liegen, folgt $N(\alpha) = \pm 1$.
$\supseteq$: Nehmen wir an, dass $\alpha \in \mathcal{O}_K$ und $N(\alpha) = \pm 1$ gilt. Nach Definition 14.2 liegen die Koeffizienten des charakteristischen Polynoms

$$\chi_\alpha(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0.$$

in $\mathbb{Z}$ und es gilt $c_0 = N(\alpha)$, also gilt $c_0 = \pm 1$. Dann gilt

$$0 = \chi_\alpha(\alpha) = \alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0.$$

Wir teilen diese Gleichung durch α^n:

$$0 = 1 + c_{n-1}\alpha^{-1} + \cdots + c_1(\alpha^{-1})^{n-1} + c_0\alpha^{-n}.$$

Dann ist α^{-1} eine Nullstelle des Polynoms

$$f(x) = 1 + c_{n-1}x + \cdots + c_1 x^{n-1} + c_0 x^n.$$

Da $c_0 = \pm 1$ ist, ist α^{-1} eine ganze algebraische Zahl nach Definition 14.2. $\square$

Beispiel. Für $K = \mathbb{Q}(\sqrt{-5})$ gilt $(\mathcal{O}_K)^* = \{-1, 1\}$.

15.1. Existenz und Eindeutigkeit einer Zerlegung in Primelemente und in irreduzible Elemente in Ganzheitsringen $\mathcal{O}_K$.

Bemerkung 15.3. Offensichtlich ist $\mathbb{Z}^* = \{\pm 1\}$ und es gilt $\mathrm{Prim}(\mathbb{Z}) = \mathrm{Irred}(\mathbb{Z})$. Für alle kommutativen Ringe R mit 1 gilt

$$\mathrm{Prim}(R) \subseteq \mathrm{Irred}(R).$$

Diese Inklusion kann aber strikt sein. Als Beispiel betrachten wir den Ganzheitsring $\mathcal{O}_K$ mit $K = \mathbb{Q}(\sqrt{-5})$. Dann ist 2 irreduzibel in $\mathcal{O}_K$, aber nicht prim:

a) 2 ist irreduzibel in $\mathcal{O}_K$, sonst hätten wir $2 = a_1 a_2$ für einige $a_1, a_2 \in \mathcal{O}_K \setminus (\mathcal{O}_K)^*$. Das impliziert

$$4 = N(2) = N(a_1)N(a_2)$$

mit $N(a_1), N(a_2) \neq \pm 1$. Da die Normen in $\mathbb{Z}$ liegen, gilt

$$N(a_1) = N(a_2) = 2.$$

Als ein Element von $\mathcal{O}_K$ kann a_1 in der Form $a_1 = n + m\sqrt{-5}$ mit $n, m \in \mathbb{Z}$ geschrieben werden. Dann gilt $2 = N(a_1) = n^2 + 5m^2$, ein Widerspruch.

b) 2 ist nicht prim in $\mathcal{O}_K$, weil 2 ein Teiler von

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \tag{15.1}$$

aber kein Teiler von $(1 + \sqrt{-5})$ oder $(1 - \sqrt{-5})$ ist.

Bemerkung 15.4. 1) Es gibt Ganzheitsringe $\mathcal{O}_K$, in denen nicht jedes Element $\alpha \in \mathcal{O}_K \setminus (\mathcal{O}_K)^*$ in Primelemente zerlegt werden kann (s. Beispiel 15.5). Wenn aber eine solche Zerlegung $\alpha = a_1 a_2 \dots a_n$ existiert, dann ist sie eindeutig im folgenden Sinne:

Sei $\alpha = b_1 b_2 \dots b_m$ eine andere Zerlegung von α in Primelemente. Dann gilt $n = m$ und es existiert eine Permutation $\sigma \in S_n$, so dass a_i mit $b_{\sigma(i)}$ für alle i assoziiert ist.

2) In jedem Ganzheitsring $\mathcal{O}_K$ kann jedes Element $\alpha \in \mathcal{O}_K \setminus (\mathcal{O}_K)^*$ in irreduzible Elemente zerlegt werden.

In der Tat, wenn α selbst nicht irreduzibel ist, dann ist $\alpha = a_1 a_2$ für einige $a_1, a_2 \in \mathcal{O}_K \setminus (\mathcal{O}_K)^*$. Dann gilt $N(\alpha) = N(a_1)N(a_2)$ mit $N(a_i) \neq \pm 1$ für $i = 1, 2$. Nach Induktion per $|N(\alpha)|$ können a_1, a_2, und somit α, in irreduzible Elemente zerlegt werden.

Es gibt Beispiele von Ganzheitsringen, in denen die Eindeutigkeit der Zerlegung in irreduzible Elemente verloren geht (s. die Gleichung (15.1), in der alle Elemente irreduzibel in $\mathcal{O}_K$ sind).

Diese Bemerkung kann kurz in folgender Tabelle gefasst werden:

	in Primelemente	in irreduzible Elemente
Existiert eine Zerlegung	nicht immer	immer
Eindeutigkeit der Zerlegungen	immer	nicht immer

Beispiel 15.5. Sei $K = \mathbb{Q}(\sqrt{-5})$. Beweisen Sie, dass die Zahl 141 nicht in Primzahlen in $\mathcal{O}_K$ zerlegt werden kann.

Beweis. Nehmen wir an, dass

$$141 = \prod_{i=1}^{n} p_i$$

ist, wobei $p_i \in \mathrm{Prim}(\mathcal{O}_K)$ ist. Nach der obigen Bemerkung ist $n \geqslant 2$. Aus $141 = 3 \cdot 47$ folgt $p_i | 3$ oder $p_i | 47$ in $\mathcal{O}_K$.

Fall 1. Nehmen wir an, dass $p_i | 3$ in $\mathcal{O}_K$ für ein i ist.
Sei $3 = p_i q_i$ für ein $q_i \in \mathcal{O}_K$. Dann gilt $N(p_i)N(q_i) = N(3) = 9$. Da p_i keine Einheit ist, ist $N(p_i) \neq 1$. Auch ist $N(p_i) \neq 3$ (s. Satz 14.6). Dann ist $N(p_i) = 9$ und $N(q_i) = 1$, also ist $q_i = \pm 1$ und $p_i = \pm 3$. Dann gilt $3 \in \mathrm{Prim}(\mathcal{O}_K)$. Aus

$$3 \cdot 2 = 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

folgt, dass 3 eine der Zahlen $(1 + \sqrt{-5}), (1 - \sqrt{-5})$ in $\mathcal{O}_K$ teilt, was unmöglich ist.

Fall 2. Nehmen wir an, dass $p_i | 47$ in $\mathcal{O}_K$ für alle i ist.
Dann ist $47 = p_i q_i$ für einige $q_i \in \mathcal{O}_K$. Dann gilt:

$$\prod_{i=1}^{n} q_i = \prod_{i=1}^{n} (p_i q_i) / \prod_{i=1}^{n} p_i = 47^n / 141 = 47^{n-1} / 3.$$

Diese Zahl liegt aber nicht in $\mathcal{O}_K$, ein Widerspruch. □

Des Weiteren benötigen wir das Legendre-Symbol $\left(\frac{a}{p}\right)$. Seine Definition und Eigenschaften sind im Appendix A zu finden. Es wird also empfohlen, Appendix A zu lesen.

15.2. **Primelemente in $\mathcal{O}_K$, wobei $K = \mathbb{Q}(\sqrt{-5})$ ist.**

Lemma 15.6. Sei K ein Zahlkörper und sei n eine zusammengesetzte Zahl in $\mathbb{Z}$. Dann liegt n nicht in $\mathrm{Prim}(\mathcal{O}_K)$.

Beweis. Da $n \in \mathbb{Z}$ zusammengesetzt ist, ist $n = k\ell$ für einige $k, \ell \in \mathbb{Z}$ mit $|k|, |\ell| \geqslant 2$. Es ist klar, dass $k, \ell \notin (\mathcal{O}_K)^*$ ist. Wäre n eine Primzahl in $\mathcal{O}_K$, dann hätten wir $n|k$ oder $n|\ell$ in $\mathcal{O}_K$. O.B.d.A. ist $n|k$, also ist $k = n\alpha$ für ein $\alpha \in \mathcal{O}_K$. Aber $\alpha = \frac{k}{n}$ liegt nicht in $\mathcal{O}_K$, weil $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ ist. □

Satz 15.7. Sei $K = \mathbb{Q}(\sqrt{-5})$ und sei p eine Primzahl in $\mathbb{Z}$. Dann gilt

$$p \in \mathrm{Prim}(\mathcal{O}_K) \Leftrightarrow \left(\frac{-5}{p}\right) = -1.$$

Beweis. Nach Satz 14.6 (b) gilt:

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}.$$

Der Fall $p = 5$ ist trivial: $5 \notin \mathrm{Prim}(\mathcal{O}_K)$, weil $5|\sqrt{-5} \cdot \sqrt{-5}$, aber $\frac{\sqrt{-5}}{5} \notin \mathcal{O}_K$ ist. Nun betrachten wir den Fall $p \neq 5$.

1) Sei $\left(\frac{-5}{p}\right) = 1$. Dann existiert $a \in \mathbb{Z}$ mit $a^2 \equiv -5 \,(\mathrm{mod}\ p)$. Dann gilt

$$p|(a^2 + 5) = (a + \sqrt{-5})(a - \sqrt{-5}).$$

Es ist klar, dass $(a \pm \sqrt{-5}) \in \mathcal{O}_K$, aber $p \nmid (a \pm \sqrt{-5})$ ist. Daraus folgt $p \notin \mathrm{Prim}(\mathcal{O}_K)$.

2) Sei $\left(\frac{-5}{p}\right) = -1$. Wir zeigen, dass $p \in \mathrm{Prim}(\mathcal{O}_K)$ gilt. Dafür müssen wir zeigen: Wenn

$$p|(a + b\sqrt{-5})(a_1 + b_1\sqrt{-5}) \tag{15.2}$$

in $\mathcal{O}_K$ gilt, dann teilt p einen dieser Faktoren in $\mathcal{O}_K$. Nehmen wir also (15.2) an. Dann folgt

$$N(p)|\ N(a + b\sqrt{-5}) \cdot N(a_1 + b_1\sqrt{-5}),$$

$$p^2|(a^2 + 5b^2)(a_1^2 + 5b_1^2).$$

O.B.d.A. gilt

$$p|(a^2 + 5b^2). \tag{15.3}$$

Wenn $p|b$ ist, dann ist $p|a$ und $p|(a + b\sqrt{-5})$ in $\mathcal{O}_K$.

Wenn $p \nmid b$ ist, dann ist b in $\mathbb{Z}_p$ invertierbar. Wir schreiben (15.3) in der Form

$$a^2 \equiv -5b^2 \,(\ \mathrm{mod}\ p).$$

Daraus folgt die Kongruenz

$$(a/b)^2 \equiv -5(\bmod p),$$

wobei wir a durch b in $\mathbb{Z}_p$ teilen. Dann haben wir $\left(\frac{-5}{p}\right) = 1$; ein Widerspruch. □

Satz 15.8. Sei $K = \mathbb{Q}(\sqrt{-5})$ und sei $\alpha = a + b\sqrt{-5} \in \mathcal{O}_K$ mit $a, b \in \mathbb{Z}$, $b \neq 0$. Dann gilt

$$\alpha \in \mathrm{Prim}(\mathcal{O}_K) \Leftrightarrow N(\alpha) = a^2 + 5b^2 \in \mathrm{Prim}(\mathbb{Z}).$$

Der direkte (also ohne weitere Kenntnisse) Beweis dieses Satzes besitzt 3 Seiten. Der kluge Beweis eines allgemeinen Satzes ist im Appendix B enthalten, s. Folgerung 26.7. Ihn kann man nach Vorlesung 17 + Satz 18.3 lesen.

16. Faktorringe, maximale Ideale und Primideale

Wichtige Beobachtung. Sei $K = \mathbb{Q}(\sqrt{-5})$.

1) Es ist leicht zu sehen, dass 2 und 3 keine Primzahlen in $\mathcal{O}_K$ sind: Betrachte

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

2) Die Zahlen 2, 3, 6 können nicht in Primzahlen in dem Ring $\mathcal{O}_K$ zerlegt werden.

Unser großes Ziel ist zu zeigen, dass jedes Ideal in $\mathcal{O}_K$ eindeutig in das Produkt von Primidealen zerlegt werden kann. Dafür benötigen wir einige Definitionen:

- Primideal
- Integritätsbereich
- Noetherscher Ring
- Ganzabgeschlossener Ring
- Dedekindscher Ring.

16.1. **Grundlegende Definitionen.** Sei R ein kommutativer Ring mit 1.

- Eine nichtleere Teilmenge $A \subseteq R$ heißt *Ideal* in R, falls:
  1) aus $x, y \in A$ folgt $x - y \in A$,
  2) aus $x \in A$ und $r \in R$ folgt $xr \in A$.

Es ist klar, dass ein Ideal in R ein Unterring von R ist. Nicht jeder Unterring von R ist ein Ideal in R: Sei $R = \mathbb{Z}[x]$ und sei $A := \mathbb{Z}[x^2]$. Dann ist A ein Unterring in R, aber kein Ideal.

- Seien $a_1, \ldots, a_k$ Elemente von R. Das *von $a_1, \ldots, a_k$ erzeugte Ideal* ist:

$$(a_1, \ldots, a_k) := a_1R + \cdots + a_kR := \{a_1r_1 + \cdots + a_kr_k \,|\, r_1, \ldots, r_k \in R\}.$$

Ein Ideal A in R heißt *endlich erzeugt*, falls in A endlich viel Elemente $a_1, \ldots, a_k$ existieren, so dass $A = (a_1, \ldots, a_k)$ gilt.

- Ein Ideal A in R heißt *Hauptideal*, falls A von einem Element erzeugt ist.

- Die Summe und das Produkt von zwei Idealen A und B von R wird so definiert:

$$A + B : = \{a + b \,|\, a \in A,\, b \in B\},$$
$$AB : = \{a_1b_1 + \cdots + a_kb_k \,|\, k \in \mathbb{N},\, a_i \in A,\, b_i \in B,\, i = 1, \ldots, k\}$$

Es ist klar, dass $A + B$ und AB wieder Ideale in R sind. Außerdem gilt

$$AB \subseteq A \cap B.$$

- Sei A ein Ideal in R. Für ein Element $x \in R$ heißt die Menge

$$[x] := x + A := \{x + a \,|\, a \in A\}$$

Nebenklasse von A in R mit dem Repräsentant x. Die Menge aller Nebenklassen von A in R

$$\{[x] \,|\, x \in R\}$$

mit der Addition $[x] + [y] := [x + y]$ und $[x] \cdot [y] := [xy]$ ist ein Ring. Der Ring heißt *Faktorring* von R modulo A und wird mit R/A bezeichnet.

Das folgende Beispiel zeigt, wie wichtig die Faktorringe sind.

Beispiel:

1) Für $n \in \mathbb{N}$ gilt $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ (der Restklassenring modulo n).
2) Es gilt $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ (der Körper von komplexen Zahlen).
3) Sei p eine Primzahl und sei $f(x)$ ein irreduzibles Polynom in $\mathbb{Z}_p[x]$ des Grades k. Dann ist $\mathbb{Z}_p[x]/(f(x))$ ein Körper der Ordnung p^k.

16.2. **Maximale Ideale und Primideale.**

Definition 16.1. Sei R ein kommutativer Ring mit 1.

1) Ein Ideal A in R heißt *echt*, falls $A \neq R$ ist.
2) Ein Ideal A in R heißt *maximal*, falls A ein echtes Ideal ist und kein Ideal B in R mit $A \subsetneqq B \subsetneqq R$ existiert.

Satz 16.2. Sei R ein kommutativer Ring mit 1. Dann liegt jedes echte Ideal von R in einem maximalen Ideal.

Hinweis. Der Beweis erfolgt mit Hilfe des Zornschen Lemmas aus Logik.

Satz 16.3. Sei R ein kommutativer Ring mit 1 und sei A ein echtes Ideal in R. Der Faktorring R/A ist genau dann ein Körper, wenn A maximal ist.

Beweis. 1) Sei A ein maximales Ideal in R. Wir beweisen, dass für jedes nichtnullsche Element in R/A ein Inverses existiert. Sei also $x + A \neq 0 + A$ ein Element von R/A. Dann ist $x \notin A$. Wir betrachten das Ideal $xR + A$ in R. Da $1 \in R$ ist, ist $x \in xR + A$. Dann ist das Ideal $xR + A$ größer als A. Dann ist $xR + A = R$ und somit existieren ein $r \in R$ und ein $a \in A$ mit $xr + a = 1$. Daraus folgt $(x + A)(r + A) = (1 + A)$.

2) Sei A kein maximales Ideal in R. Dann existiert ein Ideal B in R mit $A \subsetneqq B \subsetneqq R$. Wir nehmen $b \in B \setminus A$ und zeigen, dass kein Inverses zu $b + A$ in R/A existiert. Wenn ein solches Inverses $(c + A)$ existiert, dann gilt $(b+A)(c+A) = (1+A)$. Dann ist $bc = 1+a$. Dann ist $1 = bc-a \in BR+A \subseteq BR + B = B$. Daraus folgt $R = B$. Ein Widerspruch. □

Definition 16.4. Sei R ein kommutativer Ring. Ein Ideal A in R heißt *prim*, falls A echt ist und für je zwei Ideale B und C in R gilt:

$$\text{aus } BC \subseteq A \text{ folgt } B \subseteq A \text{ oder } C \subseteq A.$$

Behauptung 16.5. Sei R ein kommutativer Ring mit 1. Ein $x \in R \setminus \{0\}$ ist genau dann prim, wenn das von x erzeugte Hauptideal $(x) := xR$ prim ist.

Satz 16.6. Sei R ein kommutativer Ring mit 1. Ein Ideal A in R ist prim genau dann, wenn $A \neq R$ und R/A nullteilerfrei ist.

Beweis. 1) Sei R/A nicht nullteilerfrei. Dann existieren $x + A \neq 0 + A$ und $y + A \neq 0 + A$ mit $(x + A)(y + A) = 0 + A$. Daraus folgt $x \notin A$, $y \notin A$ und $xy \in A$. Wir betrachten die Ideale $B := xR + A$ und $C := yR + A$. Dann ist $B \subsetneqq A$, $C \subsetneqq A$ und $BC \subseteq A$. Deswegen ist A nicht prim.

2) Sei A nicht prim. Dann existieren Ideale B und C in R mit $B \subsetneqq A$, $C \subsetneqq A$ und $BC \subseteq A$. Wir wählen $x \in B \setminus A$, $y \in C \setminus A$. Dann ist $x \notin A$, $y \notin A$ und $xy \in A$. Daraus folgt $x + A \neq 0 + A$, $y + A \neq 0 + A$ und $(x + A)(y + A) = 0 + A$. Also ist R/A nicht nullteilerfrei. □

Satz 16.7. Sei R ein kommutativer Ring mit 1. Dann gilt:
1) Jedes maximale Ideal in R ist prim.
2) Wenn A prim ist und R/A endlich ist, dann ist A maximal.

Beweis. 1) Sei A ein maximales Ideal in R. Dann ist R/A ein Körper, insbesondere ist R/A nullteilerfrei. Nach Satz 16.6 ist A prim.

2) R/A ist ein endlicher kommutativer nullteilerfreier Ring mit 1. Man kann leicht zeigen, dass R/A ein Körper ist. Dann ist A maximal nach Satz 16.3. □

17. Diskriminante. Noethersche Ringe

In diesem Abschnitt definieren wir noethersche Ringe und beweisen, dass der Ring $\mathcal{O}_K$ noethersch ist. Auch wird die Diskriminante des Zahlkörpers K definiert. Wir erinnern uns, dass ein Zahlkörper eine endliche Erweiterung von $\mathbb{Q}$ in $\mathbb{C}$ ist.

Definition 17.1. Sei R ein nullteilerfreier kommutativer Ring mit 1. Für je zwei Elemente $a, b \in R$ mit $b \neq 0$ betrachten wir einen formalen Ausdruck $\frac{a}{b}$. Auf der Menge aller solcher Ausdrucke definieren wir eine Relation $\sim$ durch

$$\frac{a}{b} \sim \frac{x}{y} \Leftrightarrow ay = bx.$$

Diese Relation ist eine Äquivalenzrelation. Die Äquivalenzklasse von $\frac{a}{b}$ wird mit $[\frac{a}{b}]$ bezeichnet. Wir haben also

$$\left[\frac{a}{b}\right] := \left\{\frac{x}{y} \mid \frac{a}{b} \sim \frac{x}{y}\right\}.$$

Der *Quotientenkörper* von R ist die Menge aller solcher Klassen

$$\left\{\left[\frac{a}{b}\right] \mid a, b \in R, b \neq 0\right\}$$

zusammen mit zwei Verknüpfungen $+$ und $\cdot$, die folgendermaßen definiert sind:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right], \qquad \left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

Der Quotientenkörper von R wird mit $\mathrm{Quot}(R)$ bezeichnet.

Bemerkung. $\mathbb{Q} = \mathrm{Quot}(Z)$

Satz 17.2. Sei K ein Zahlkörper. Für jedes $\alpha \in K$ existiert ein $m \in \mathbb{N}$ mit $\alpha m \in \mathcal{O}_K$.

Beweis. Da α algebraisch über $\mathbb{Q}$ ist, ist α eine Nullstelle eines Polynoms

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

mit $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. Sei $m \in \mathbb{N}$ eine Zahl, so dass $ma_i \in \mathbb{Z}$ für alle i ist. Wir multiplizieren die Gleichung $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ mit m^n:

$$(\alpha m)^n + a_{n-1}m(\alpha m)^{n-1} + \cdots + a_0 m^n = 0.$$

Daraus folgt: αm ist eine Nullstelle des Polynoms

$$x^n + a_{n-1}mx^{n-1} + \cdots + a_0 m^n$$

mit ganzen Koeffizienten. Also ist $\alpha m \in \mathcal{O}_K$. □

Folgerung 17.3. Sei K ein Zahlkörper. Dann ist $\mathrm{Quot}(\mathcal{O}_K) \cong K$.

Beweis. Die Abbildung

$$\begin{aligned}\varphi: \ \mathrm{Quot}(\mathcal{O}_K) &\to K,\\ \left[\frac{\beta}{\gamma}\right] &\mapsto \frac{\beta}{\gamma}\end{aligned}$$

ist ein wohldefinierter injektiver Homomorphismus. Wir beweisen, dass φ surjektiv ist. Sei $\alpha \in K$. Nach Satz 17.2 existiert ein $m \in \mathbb{N}$, so dass die Zahl $\beta := \alpha m$ in $\mathcal{O}_K$ liegt. Dann ist $\alpha = \frac{\beta}{m}$. Daraus folgt $\varphi(\left[\frac{\beta}{m}\right]) = \alpha$. □

Satz 17.4. Sei K ein Zahlkörper. Jedes nichtnullsche Ideal A in $\mathcal{O}_K$ enthält eine Basis $\alpha_1, \ldots, \alpha_n$ von K über $\mathbb{Q}$.

Beweis. Sei $\omega_1, \ldots, \omega_n$ eine Basis von K über $\mathbb{Q}$. Nach Satz 17.2 existiert ein $m \in \mathbb{N}$, so dass $m\omega_1, \ldots, m\omega_n$ in $\mathcal{O}_K$ liegen. Wählen wir ein beliebiges $a \in A \setminus \{0\}$. Dann liegen die Elemente $am\omega_1, \ldots, am\omega_n$ in A. Diese Elemente sind linear unabhängig über $\mathbb{Q}$. Da $\dim_{\mathbb{Q}} K = n$ ist, bilden diese Elemente eine Basis von K über $\mathbb{Q}$. □

Satz 17.5. Sei K ein Zahlkörper und sei A ein nichtnullsches Ideal in $\mathcal{O}_K$. Dann gilt:

1) Das Ideal A enthält Zahlen $\alpha_1, \ldots, \alpha_n$, für die das Folgende gilt:
   a) $\alpha_1, \ldots, \alpha_n$ ist eine Basis von K über $\mathbb{Q}$;
   b) $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.
2) Die Zahl $\Delta(\alpha_1, \ldots, \alpha_n)$ liegt in $\mathbb{Z} \setminus \{0\}$ und hängt nicht von der Wahl der Zahlen in 1) ab.

Beweis. 1) Seien $\alpha_1, \ldots, \alpha_n$ Zahlen aus A die eine Basis von K über $\mathbb{Q}$ bilden. Da diese Zahlen in $\mathcal{O}_K$ liegen, liegen die Zahlen $\mathrm{Sp}(\alpha_i\alpha_j)$ in $\mathbb{Z}$. Somit liegt die Diskriminante $\Delta(\alpha_1, \ldots, \alpha_n)$ in $\mathbb{Z}$.

Deswegen existieren die Zahlen $\alpha_1, \ldots, \alpha_n$ in A, die eine Basis von K über $\mathbb{Q}$ bilden und der Absolutbetrag $|\Delta(\alpha_1, \ldots, \alpha_n)|$ minimal ist. Wir beweisen, dass $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$ gilt.

Sei $\alpha \in A$ beliebig. Dann ist $\alpha = \gamma_1\alpha_1 + \cdots + \gamma_n\alpha_n$ für einige $\gamma_1, \ldots, \gamma_n \in \mathbb{Q}$. Nehmen wir an, dass irgendein γ_i nicht in $\mathbb{Z}$ liegt. O.B.d.A. ist $\gamma_1 \notin \mathbb{Z}$. Wir schreiben $\gamma_1 = m + \theta$ mit $m \in \mathbb{Z}$ und $0 < \theta < 1$. Wir betrachten die Elemente

$$\begin{aligned}\beta_1 &:= \alpha - m\alpha_1 \ = \theta\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n,\\ \beta_2 &:= \alpha_2,\\ &\vdots\\ \beta_n &:= \alpha_n.\end{aligned}$$

Diese Elemente liegen in A und bilden eine andere Basis von K über $\mathbb{Q}$. Die Übergangsmatrix von $\alpha_1, \ldots, \alpha_n$ zu $\beta_1, \ldots, \beta_n$ ist

$$C = \begin{pmatrix} \theta & \gamma_2 & \gamma_3 & \ldots & \gamma_n \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Nach Satz 12.7 gilt

$$\Delta(\beta_1, \ldots, \beta_n) = (\det(C))^2 \cdot \Delta(\alpha_1, \ldots, \alpha_n). \tag{17.1}$$

Da $(\det(C))^2 = \theta^2 < 1$ ist, erhalten wir einen Widerspruch mit der Minimalität von $|\Delta(\alpha_1, \ldots, \alpha_n)|$.

2) Sei $\alpha_1, \ldots, \alpha_n$ eine Basis von K über $\mathbb{Q}$ mit $A = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. Am Anfang des Beweises haben wir bemerkt, dass $\Delta(\alpha_1, \ldots, \alpha_n)$ in $\mathbb{Z}$ liegt. Nach Satz 12.6 ist diese Zahl ungleich 0.

Sei $\beta_1, \ldots, \beta_n$ eine Basis von K über $\mathbb{Q}$ mit $A = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n$. Sei C die Übergangsmatrix von der α-Basis zur β-Basis und D die Übergangsmatrix von der β-Basis zur α-Basis. Dann sind die Einträge von C und D aus $\mathbb{Z}$ und es gilt $CD = E$. Daraus folgt $\det(C) = \pm 1$. Aus (17.1) folgt

$$\Delta(\beta_1, \ldots, \beta_n) = \Delta(\alpha_1, \ldots, \alpha_n).$$

□

Definition 17.6. Sei K ein Zahlkörper und sei A ein nichtnullsches Ideal in $\mathcal{O}_K$.

i) Die Zahlen $\alpha_1, \ldots, \alpha_n$ in A aus Satz 17.5.1) heißt *Ganzheitsbasis von A*.

ii) Die Zahl $\Delta(\alpha_1, \ldots, \alpha_n)$ im Satz 17.5.2) heißt *Diskriminante von A* und wird mit $\delta(A)$ bezeichnet.

iii) Die Diskriminante von $\mathcal{O}_K$ ist besonders wichtig und heißt *Diskriminante des Körpers K über $\mathbb{Q}$* und wird mit $\delta(K)$ bezeichnet.

Satz 17.7. Sei $K = \mathbb{Q}(\sqrt{m})$, wobei $m \in \mathbb{Z} \setminus \{0\}$ quadratfrei ist. Dann gilt

$$\delta(K) = \begin{cases} 4m & \text{falls } m \equiv 2, 3 \pmod 4, \\ m & \text{falls } m \equiv 1 \pmod 4. \end{cases}$$

Beweis. Im Satz 14.6 ist eine ganzzahlige Basis von $\mathcal{O}_K$ gegeben. Die Diskriminante $\delta(\mathcal{O}_K)$ wird dann nach Definition berechnet. □

Definition 17.8. Sei R ein kommutativer Ring mit 1. Der Ring heißt *noethersch*, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:

1) jede unendliche aufsteigende Kette $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ von Idealen in R stabilisiert sich, d.h. es existiert ein $n \in \mathbb{N}$ mit $A_n = A_{n+1} = \dots$.

2) jedes Ideal A in R ist endlich erzeugt, d.h. es existieren endlich viel $a_1, \dots, a_k \in A$ mit $A = a_1R + a_2R + \dots + a_kR$.

Beispiel.
a) Der Ring $\mathbb{Z}$ und jeder Körper K sind noethersch.
b) Der Ring $\mathbb{Q}[X_1, X_2, \dots]$ in unendlich vielen Unbestimmten ist nicht noethersch, da das Ideal, das von allen Unbestimmten erzeugt wird, nicht endlich erzeugt ist.

Satz 17.9. (Hilbertscher Basissatz) Sei R ein kommutativer Ring mit 1. Ist R noethersch, so ist auch der Polynomring $R[x]$ noethersch. Insbesondere sind die Ringe $\mathbb{Z}[X_1, \dots, X_n]$ und $K[X_1, \dots, X_n]$ noethersch, wobei K ein Körper ist.

Satz 17.10. Sei K ein Zahlkörper. Dann ist der Ganzheitsring $\mathcal{O}_K$ noethersch.

Beweis. Sei A ein nichtnullsches Ideal in $\mathcal{O}_K$. Nach Satz 17.5 existieren $\alpha_1, \dots, \alpha_n \in A$ mit $A = \alpha_1\mathbb{Z} + \dots + \alpha_n\mathbb{Z}$, wobei $n = [K : \mathbb{Q}]$ ist. Dann gilt $A = A\mathcal{O}_K = \alpha_1\mathcal{O}_K + \dots + \alpha_n\mathcal{O}_K$. Also ist A endlich erzeugt. □

18. Der Ganzheitsring $\mathcal{O}_K$ ist dedekindsch

Lemma 18.1. Sei K ein Zahlkörper. Jedes nichtnullsche Ideal A des Ganzheitsringes $\mathcal{O}_K$ enthält eine nichtnullsche Zahl aus $\mathbb{Z}$.

Beweis. Sei $0 \neq \alpha \in A$ beliebig. Da $\alpha \in \mathcal{O}_K$ ist, liegen die Koeffizienten des Minimalpolynoms $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ in $\mathbb{Z}$. Wegen der Irreduzibilität von $m_\alpha(x)$ gilt $a_0 \neq 0$. Dann folgt die Behauptung aus

$$a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) \in A.$$

□

Lemma 18.2. Sei K ein Zahlkörper. Sei A ein nichtnullsches Ideal in $\mathcal{O}_K$. Dann ist der Faktorring $\mathcal{O}_K/A$ endlich.

Beweis. Nach Lemma 18.1 besitzt A eine nichtnullsche Zahl $m \in \mathbb{Z}$. Dann gilt

$$(m) \subseteq A \subseteq \mathcal{O}_K.$$

Es genügt zu zeigen, dass der Faktorring $\mathcal{O}_K/(m)$ endlich ist. Wir haben

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n,$$

wobei $\omega_1, \ldots, \omega_n$ eine passende Basis von K über Q ist. Dann gilt

$$(m) = m\mathcal{O}_K = m\mathbb{Z}\omega_1 + \cdots + m\mathbb{Z}\omega_n.$$

Sei $\omega \in \mathcal{O}_K$ beliebig. Dann existieren $z_1, \ldots, z_n \in \mathbb{Z}$ mit

$$\omega = z_1\omega_1 + \cdots + z_n\omega_n.$$

Sei $\overline{z_i} \in \{0, 1, \ldots, m-1\}$ der minimale nichtnegative Rest von z_i modulo m. Es gilt

$$z_i \equiv \overline{z_i} \ (\mathrm{mod}\ m).$$

Wir definieren

$$\overline{\omega} = \overline{z_1}\omega_1 + \cdots + \overline{z_n}\omega_n.$$

Dann gilt

$$\omega \equiv \overline{\omega} \ (\mathrm{mod}\ (m)).$$

Die Anzahl von möglichen $\overline{\omega}$ ist m^n. Deswegen gilt

$$|\mathcal{O}_K/(m)| = m^n.$$

und

$$|\mathcal{O}_K/A| \Big| m^n.$$

□

Bemerkung. Ein anderer Beweis des Satzes 18.2 kann aus Satz 26.3 abgeleitet werden.

Satz 18.3. Sei K ein Zahlkörper. Jedes nichtnullsche Primideal in $\mathcal{O}_K$ ist maximal.

Beweis. Nach Lemma 18.2 ist $\mathcal{O}_K/A$ endlich. Dann folgt die Aussage aus Satz 16.7. □

Definition 18.4. Ein *Integritätsbereich* ist ein nichtnullscher Ring R mit folgenden Eigenschaften:

1) R ist kommutativ und mit 1.
2) R ist nullteilerfrei (d.h. aus $ab = 0$ folgt $a = 0$ oder $b = 0$).

Definition 18.5. Ein Integritätsbereich R heißt *ganzabgeschlossen*, falls gilt: Ist $\alpha \in \mathrm{Quot}(R)$ eine Nullstelle eines monischen Polynoms $f(x) \in R[x]$, so ist $\alpha \in R$.

Satz 18.6. Sei K ein Zahlkörper. Dann ist $\mathcal{O}_K$ ganzabgeschlossen.

Beweis. Nach Folgerung 17.3 ist $K = \mathrm{Quot}(\mathcal{O}_K)$. So müssen wir das Folgende beweisen:
Sei $\alpha \in K$ eine Nullstelle eines Polynoms $x^n + a_{n-1}x^{n-1} + \cdots + a_0$
mit Koeffizienten $a_i \in \mathcal{O}_K$. Dann ist $\alpha \in \mathcal{O}_K$.

Da $a_i \in \mathcal{O}_K$ ist, ist a_i ist eine Nullstelle eines Polynoms

$$x^{n_i} + b_{i,n_i-1}x^{n_i-1} + \cdots + b_{i,0}$$

mit Koeffizienten $b_{i,j} \in \mathbb{Z}$. Sei M ein von

$$\{\alpha^k a_0^{k_0} \dots a_{n-1}^{k_{n-1}} \mid 0 \leqslant k \leqslant n-1,\ 0 \leqslant k_i \leqslant n_i - 1\}$$

erzeugtes $\mathbb{Z}$-Modul. Dann ist $\alpha M \subseteq M$. Wie im Beweis des Satzes 14.3 folgt daraus, dass $\alpha \in \mathcal{O}_K$ ist.

Definition 18.7. Ein Ring R heißt *dedekindscher* Ring falls das Folgende gilt:

1) R ist ein Integritätsbereich;
2) R ist noethersch;
3) R ist ganzabgeschlossen;
4) jedes nichtnullsche Primideal in R ist maximal.

Folgerung 18.8. Für jeden Zahlkörper K ist der Ring $\mathcal{O}_K$ dedekindsch.

Beweis. Der Beweis folgt aus den Sätzen 17.10, 18.3 und 18.6. □

Definition 18.9. Sei R ein Integritätsbereich. Zwei nichtnullsche Ideale A, B in R heißen *äquivalent*, falls zwei nichtnullsche Elemente α, β in R mit

$$(\alpha)A = (\beta)B$$

existieren. In dem Fall schreibt man $A \sim B$. (Man kann nachprüfen, dass $\sim$ eine Äquivalenzrelation auf der Menge aller nichtnullschen Ideale von R ist.) Sei $[A]$ die Äquivalenzklasse, die das Ideal A enthält:

$$[A] := \{B \mid B \sim A\}.$$

Die Anzahl von Äquivalenzklassen aller nichtnullschen Ideale von R heißt *Idealklassenzahl* und wird mit h_R bezeichnet.

Aufgabe 18.10. Sei R ein Integritätsbereich.

1) Sei A ein nichtnullsches Ideal in R. Dann gilt $[A] = [R]$ genau dann, wenn A ein Hauptideal ist.
2) Es gilt $h_R = 1$ genau dann, wenn jedes Ideal in R ein Hauptideal ist.

Lemma 18.10. Sei K ein Zahlkörper. Dann existiert ein $M \in \mathbb{N}$ mit der folgenden Eigenschaft:

Für jedes $\gamma \in K$ existieren eine natürliche Zahl $1 \leqslant k \leqslant M$ und ein Element $\omega \in \mathcal{O}_K$, so dass gilt:

$$|N(k\gamma - \omega)| < 1.$$

Beweis. Nach Satz 17.2 existiert eine Basis $\alpha_1, \ldots, \alpha_n$ von K über $\mathbb{Q}$, so dass

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$$

gilt. Es gilt auch

$$K = \mathbb{Q}\alpha_1 + \cdots + \mathbb{Q}\alpha_n.$$

Dann kann jedes $\gamma \in K$ in der Form

$$\gamma = q_1\alpha_1 + \cdots + q_n\alpha_n$$

geschrieben werden, wobei $q_1, \ldots, q_n \in \mathbb{Q}$ ist. Mit Bezeichnungen

$$\begin{aligned} [\gamma] &:= \quad [q_1]\alpha_1 + \cdots + [q_n]\alpha_n, \\ \{\gamma\} &:= \quad \{q_1\}\alpha_1 + \cdots + \{q_n\}\alpha_n. \end{aligned}$$

haben wir $\gamma = [\gamma] + \{\gamma\}$ und $[\gamma] \in \mathcal{O}_K$. Wir bezeichnen $\{\gamma\}_i := \{q_i\}$. Dann gilt

$$\{\gamma\} = \sum_{i=1}^{n} \{\gamma\}_i \alpha_i, \quad 0 \leqslant \{\gamma\}_i < 1, \;\; i = 1, \ldots, n.$$

Sei $m \in \mathbb{N}$ beliebig. Wir betrachten die Zahlen

$$\gamma, 2\gamma, \ldots, (m^n+1)\gamma.$$

Dann existieren natürliche Zahlen $1 \leqslant s < t \leqslant m^n$, so dass für $i = 1, \ldots, n$ gilt:

$$\Big|\{t\gamma\}_i - \{s\gamma\}_i\Big| \leqslant \frac{1}{m}. \tag{18.1}$$

Wir setzen $n := t - s$ und $\omega := [t\gamma] - [s\gamma]$. Dann ist $1 \leqslant n < M$, $\omega \in \mathcal{O}_K$, und es gilt

$$n\gamma - \omega = t\gamma - s\gamma - ([t\gamma] - [s\gamma]) = \{t\gamma\} - \{s\gamma\} = \sum_{i=1}^{n} (\underbrace{\{t\gamma\}_i - \{s\gamma\}_i}_{:=p_i})\alpha_i.$$

Seien $\sigma_1, \ldots, \sigma_n$ alle Einbettungen von K über $\mathbb{Q}$. Dann gilt

$$N(n\gamma - \omega) = N\Big(\sum_{i=1}^{n} p_i\alpha_i\Big) = \prod_{j=1}^{n} \sigma_j\Big(\sum_{i=1}^{n} p_i\alpha_i\Big) = \prod_{j=1}^{n} \Big(\sum_{i=1}^{n} p_i\sigma_j(\alpha_i)\Big).$$

Daraus folgt

$$|N(n\gamma - \omega)| \overset{(18.1)}{\leqslant} \frac{1}{m^n} \cdot \prod_{j=1}^{n} \Big(\sum_{i=1}^{n} |\sigma_j(\alpha_i)|\Big).$$

Das letzte Produkt ist eine Konstante, die hängt nicht von $\gamma \in K$ ab. Deswegen kann m so gewählt werden, dass $|N(n\gamma - \omega)| < 1$ gelten wird. □

Satz 18.11. Sei K ein Zahlkörper. Dann ist die Idealklassenzahl von $\mathcal{O}_K$ endlich.

Beweis. Sei $0 \neq \beta \in A$ eine Zahl mit minimaler Norm. Nach Lemma 18.10 existiert $M \in \mathbb{N}$, so dass folgendes gilt:

Für jedes $\alpha \in A$ existieren eine natürliche Zahl $1 \leqslant n_\alpha \leqslant M$ und ein Element $\omega_\alpha \in \mathcal{O}_K$ mit

$$\Big|N\big(n_\alpha \frac{\alpha}{\beta} - \omega_\alpha\big)\Big| < 1.$$

Daraus folgt

$$\big|N\big(\underbrace{n_\alpha\alpha - \omega_\alpha\beta}_{\in A}\big)\big| < \big|N(\beta)\big|.$$

Wegen der Minimalität von $|N(\beta)|$ haben wir $n_\alpha\alpha - \omega_\alpha\beta = 0$. Daraus folgt $n_\alpha\alpha \in (\beta)$ und schließlich

$$M!A \subseteq (\beta).$$

Deswegen haben wir die Inklusion

$$B := \frac{1}{\beta} M! A \subseteq \mathcal{O}_K.$$

Außerdem ist B ein Ideal in $\mathcal{O}_K$, es gilt $M! \in B$ (wegen $\beta \in A$) und es gilt

$$(M!)A = (\beta)B.$$

Also ist $A \sim B$. Es bleibt zu bemerken, dass es nur endlich viele Ideale B in $\mathcal{O}_K$ mit $(M!) \subseteq B$ gibt. Das folgt aus dem Fakt, dass der Faktorring $\mathcal{O}_K/(M!)$ endlich ist (s. Lemma 18.2). □

19. Idealklassengruppe von K. Zerlegung von Idealen in $\mathcal{O}_K$ in Primideale

Ziel dieser Volesung ist, folgende Behauptungen über Ideale in $\mathcal{O}_K$ zu beweisen:

1) Für jedes nichtnullsche Ideal A in $\mathcal{O}_K$ existiert ein $k \in \mathbb{N}$, so dass A^k ein Hauptideal ist.

2) Sind A, B, C drei nichtnullsche Ideale in $\mathcal{O}_K$ mit $AB = AC$, dann gilt $B = C$.

3) Sind A, B zwei nichtnullsche Ideale in $\mathcal{O}_K$ mit $A \subseteq B$, dann existiert ein Ideal C in $\mathcal{O}_K$ mit $A = BC$.

4) Jedes nichtnullsche und echte Ideal A in $\mathcal{O}_K$ kann in Primideale zerlegt werden.

Außerdem wird die Idealklassengruppe definiert. Es wird festgestellt, dass sie endlich und kommutativ ist.

Lemma 19.1. Sei $A \neq \{0\}$ ein Ideal in $\mathcal{O}_K$ und sei $\beta \in K$, so dass $\beta A \subseteq A$ ist. Dann ist $\beta \in \mathcal{O}_K$.

Beweis. Der Beweis folgt aus dem Fakt, dass A ein $\mathbb{Z}$-Modul ist. □

Lemma 19.2. Seien $A, B \neq \{0\}$ Ideale in $\mathcal{O}_K$, so dass $A = AB$ ist. Dann ist $B = \mathcal{O}_K$.

Beweis. Nach Satz 17.5 existieren $\alpha_1, \ldots, \alpha_n \in A$, so dass $A = (\alpha_1, \ldots, \alpha_n)$ ist. Wegen $A = AB$ existieren $b_{i,j} \in B$, so dass gilt:

$$\begin{aligned} \alpha_1 &= b_{11}\alpha_1 + \cdots + b_{1n}\alpha_n, \\ &\vdots \\ \alpha_n &= b_{n1}\alpha_1 + \cdots + b_{nn}\alpha_n. \end{aligned}$$

Dann ist 1 ein Eigenwert der Koeffizientenmatrix $\mathcal{B} = (b_{ij})$. Somit ist 1 eine Nullstelle des charakteristischen Polynoms $\chi_{\mathcal{B}}(x) = x^n + \beta_{n-1}x^{n-1} + \cdots + \beta_0$ mit Koeffizienten aus dem Ideal B. Deswegen gilt $1 = -(\beta_{n-1} + \cdots + \beta_0) \in B$ und folglich ist $B = \mathcal{O}_K$. □

Satz 19.3. Sei K ein Zahlkörper. Für jedes Ideal $A \neq \{0\}$ in $\mathcal{O}_K$ existiert ein $k \in \mathbb{N}$ mit $1 \leqslant k \leqslant h_K$, so dass A^k ein Hauptideal ist. Hier ist h_K die Idealklassenzahl von K.

Beweis. Nach dem Schubladenprinzip existieren $1 \leqslant i < j \leqslant h_K + 1$ mit $A^i \sim A^j$. Deswegen gilt $(\alpha)A^i = (\beta)A^j$ für einige $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$. Dann gilt

$$A^i = \frac{\beta}{\alpha} A^{j-i} \cdot A^i. \tag{19.1}$$

Nach Lemma 19.1 liegt jedes Element von $\frac{\beta}{\alpha}A^{j-i}$ in $\mathcal{O}_K$. Außerdem ist $\frac{\beta}{\alpha}A^{j-i}$ ein Ideal in $\mathcal{O}_K$. Dann folgt aus (19.1) und Lemma 19.2 die Gleichung

$$\frac{\beta}{\alpha} A^{j-i} = \mathcal{O}_K.$$

Also ist $\frac{\alpha}{\beta}\mathcal{O}_K = A^{j-i} \subseteq \mathcal{O}_K$. Nach Lemma 19.1 gilt $\frac{\alpha}{\beta} \in \mathcal{O}_K$. Deswegen ist

$$A^{j-i} = \frac{\alpha}{\beta}\,\mathcal{O}_K$$

ein Hauptideal in $\mathcal{O}_K$. □

Satz 19.4. Sei K ein Zahlkörper. Die Menge

$$\{[A] \,|\, A \text{ ist ein nichtnullsches Ideal in } \mathcal{O}_K\}$$

mit der Multiplikation $[A]\cdot[B] := [AB]$ bildet eine Gruppe. Sie ist kommutativ und endlich. Das Einselement dieser Gruppe ist $[\mathcal{O}_K]$.

Beweis. Wir überprüfen, dass jedes Element $[A]$ der oberen Menge ein Inverses hat. Nach Satz 19.3 existiert $k \in \mathbb{N}$, so dass A^k einem Hauptideal äquivalent ist. Jedes Hauptideal in $\mathcal{O}_K$ ist aber dem Ideal $\mathcal{O}_K$ äquivalent. Also gilt $[A^k] = [\mathcal{O}_K]$. Deswegen ist $[A]^{k-1}$ das Inverse zu $[A]$. □

Definition 19.5. Die Gruppe aus dem Satz 19.4 heißt *Idealklassengruppe* von K und wird mit $Cl(K)$ bezeichnet.

Satz 19.6. Seien $A, B \neq \{0\}$ Ideale in $\mathcal{O}_K$, so dass $A \subseteq B$ gilt. Dann existiert ein Ideal C in $\mathcal{O}_K$ mit $A = BC$.

Beweis. Nach Satz 19.3 existiert ein $k \in \mathbb{N}$, so dass $B^k = (\beta)$ ein Hauptideal ist. Wir setzen $C = \frac{1}{\beta}B^{k-1}A$. Dann ist

$$C \subseteq \frac{1}{\beta}B^{k-1}B = \frac{1}{\beta}(\beta) = \mathcal{O}_K$$

Zudem ist C ist ein Ideal in $\mathcal{O}_K$, und es gilt

$$BC = \frac{1}{\beta}B^kA = \frac{1}{\beta}(\beta)A = A.$$

□

Bezeichnung. Sei R ein kommutativer Ring mit 1. Für zwei Ideale A, B in R schreiben wir $B|A$, falls $A \subseteq B$ gilt.

Bemerkung. Diese Bezeichnung ist sinnvoll wegen der folgenden schönen Umformulierungen:

1) Umformulierung des Satzes 19.6: Seien $A, B \neq \{0\}$ Ideale in $\mathcal{O}_K$. Ist $B|A$, dann ist $A = BC$ für ein Ideal C in $\mathcal{O}_K$.
2) Umformulierung der Definition 16.4: Sei R ein kommutativer Ring. Ein Ideal A in R heißt *prim*, falls A echt ist und für je zwei Ideale B und C in R gilt: aus $A|(BC)$ folgt $A|B$ oder $A|C$.

Satz 19.7. Seien $A, B, C \neq \{0\}$ Ideale in $\mathcal{O}_K$, so dass $AB = AC$ gilt. Dann gilt $B = C$.

Beweis. Nach Satz 19.3 existiert ein $k \in \mathbb{N}$, so dass $A^k = (\alpha)$ ein Hauptideal ist. Aus $AB = AC$ folgt $A^kB = A^kC$. Deswegen gilt $(\alpha)B = (\alpha)C$ und somit $B = C$. □

Lemma 19.8. Sei B ein Ideal in $\mathcal{O}_K$ mit $\{0\} \neq B \neq \mathcal{O}_K$ ist. Dann existieren ein Primideal P und ein Ideal B_1 in $\mathcal{O}_K$ mit $B = PB_1$. Außerdem gilt $B \subsetneq B_1$.

Beweis. Es existiert ein Maximalideal P in $\mathcal{O}_K$ mit $B \subseteq P$. Nach Satz 16.7 ist P prim. Nach Satz 19.6 existiert ein Ideal B_1 in $\mathcal{O}_K$, für das gilt:

$$B = PB_1.$$

Offensichtlich ist $B \subseteq B_1$. Zudem gilt $B \neq B_1$, sonst hätten wir

$$\mathcal{O}_KB = B = PB_1 = PB$$

und somit $\mathcal{O}_K = P$ (s. Satz 19.7), ein Widerspruch. □

Satz 19.9. Sei A ein Ideal in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$. Dann ist

$$A = P_1 P_2 \dots P_k$$

für einige (nicht unbedingt verschiedene) Primideale $P_1, P_2, \dots, P_k$ in $\mathcal{O}_K$.

Beweis. Wir setzen $A_0 = A$. Da $A_0 \neq \mathcal{O}_K$ ist, ist $A_0 = P_1 A_1$ für ein Primideal P_1 und ein Ideal A_1 mit $A_0 \subsetneqq A_1$ (s. Lemma 19.8). Nun definieren induktiv einige Ideale in $\mathcal{O}_K$: Nehmen wir an, dass wir für ein $k \in \mathbb{N}$ und alle $i = 1, \dots, k$ ein Primideal P_i und ein Ideal A_i mit

$$A_{i-1} = P_i A_i \text{ und } A_{i-1} \subsetneqq A_i$$

definiert haben. Ist $A_k = \mathcal{O}_K$, dann beenden wir den Prozess. In dem Fall gilt

$$A_0 = P_1 A_1 = P_1 P_2 A_2 = \dots = P_1 P_2 \dots P_k A_k = P_1 P_2 \dots P_k,$$

und wir haben die gewünschte Zerlegung. Ist $A_k \neq \mathcal{O}_K$, dann können wir diesen Prozess fortsetzen: Nach Lemma 19.8 existiert ein Primideal P_{k+1} und ein Ideal A_{k+1} mit

$$A_k = P_{k+1} A_{k+1} \text{ und } A_k \subsetneqq A_{k+1}.$$

Der Prozess kann aber nicht unendlich sein, sonst hätten wir eine unendliche aufsteigende Kette von Idealen

$$A_0 \subsetneqq A_1 \subsetneqq A_2 \subsetneqq \dots$$

in $\mathcal{O}_K$, was dem Satz 17.10 widerspricht. □

Aufgabe 19.10. Sei $K = \mathbb{Q}(\sqrt[3]{5})$. Folgendes ist bekannt:

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt[3]{5} + \mathbb{Z}(\sqrt[3]{5})^2. \tag{19.2}$$

Zerlegen Sie das Hauptideal (3) in $\mathcal{O}_K$ in Primideale.

Lösung. Sei $\alpha = \sqrt[3]{5}$. Wir prüfen nach, dass das Folgende gilt:
1) $(3) = (3, 1+\alpha)^3$;
2) $(3, 1+\alpha)$ ist ein Primideal in $\mathcal{O}_K$.

Zu 1): Es gilt $(3, 1+\alpha)^2 = (9,\ 3+3\alpha,\ 1+2\alpha+\alpha^2)$. Daraus folgt

$$\begin{aligned}
(3, 1+\alpha)^3 &= (27,\ 9+9\alpha,\ 3+6\alpha+3\alpha^2,\ 1+3\alpha+3\alpha^2+\alpha^3)\\
&= (27,\ 9+9\alpha,\ 3+6\alpha+3\alpha^2,\ 6+3\alpha+3\alpha^2)\\
&= (27,\ 9+9\alpha,\ 3+6\alpha+3\alpha^2,\ 3-3\alpha)\\
&= (27,\ 9+9\alpha+3[3-3\alpha],\ 3+6\alpha+3\alpha^2,\ 3-3\alpha)\\
&= (27,\ 18,\ 3+6\alpha+3\alpha^2,\ 3-3\alpha)\\
&= (9,\ 3+6\alpha+3\alpha^2,\ 3-3\alpha)\\
&= (9,\ 3+6\alpha+3\alpha^2+[\alpha+3][3-3\alpha],\ 3-3\alpha)\\
&= (9,\ 12,\ 3-3\alpha)\\
&= (3,\ 3-3\alpha)\\
&= (3).
\end{aligned}$$

Zu 2): Wir zeigen, dass der Faktorring $\mathcal{O}_K/(3, 1+\alpha)$ genau 3 Elemente enthält. Dann wird das Ideal $(3, 1+\alpha)$ maximal und somit prim in $\mathcal{O}_K$.

Bezeichnung. Sei I ein Ideal in $\mathcal{O}_K$. Für zwei Elemente $\omega_1, \omega_2 \in \mathcal{O}_K$ schreiben wir

$$\omega_1 \equiv \omega_2 \ (\mathrm{mod}\ I),$$

falls $\omega_1 - \omega_2 \in I$ gilt. In diesem Fall gilt $\omega_1 + I = \omega_2 + I$, also sind die zwei Nebenklassen gleich.

Wir setzen $I = (3, 1+\alpha)$ und zeigen, dass für ein beliebiges Element $\omega \in \mathcal{O}_K$ ein $\omega_1 \in \{0, 1, 2\}$ mit $\omega \equiv \omega_1 \ (\mathrm{mod}\ I)$ existiert.

Nach (19.2) kann ω in der Form $\omega = a\alpha^2 + b\alpha + c$ geschrieben werden, wobei $a, b, c \in \mathbb{Z}$ gilt. Als Vorbereitung teilen wir das Polynom $ax^2 + bx + c$ durch $x + 1$ mit einem Rest:

$$ax^2 + bx + c = (x+1)(ax + (b-a)) + (a - b + c).$$

Da I die Zahl $\alpha + 1$ enthält, haben wir

$$\omega = \alpha^2 + b\alpha + c = \underbrace{(\alpha + 1)(a\alpha + (b - a))}_{\in I} + (a - b + c) \equiv a - b + c \pmod{I}.$$

Da I auch die Zahl 3 enthält, haben wir

$$\omega \equiv a - b + c \equiv r \pmod{I}$$

für ein $r \in \{0, 1, 2\}$.

Damit haben wir gezeigt, dass der Faktorring $\mathcal{O}_K/I$ höchstens 3 Nebenkassen

$$0 + I,\ 1 + I, 2 + I$$

enthält. Nun zeigen wir, dass diese Nebenklassen verschieden sind. Im Hinblick auf einen Widerspruch nehmen wir an:

$$1 + I = 2 + I.$$

Dann gilt $1 \in I$. Daraus folgt $1 = 1^3 \in I^3 \overset{1)}{=} (3) = 3\mathcal{O}_K$. Ein Widerspruch. Andere Varianten führen auch zu einem Widerspruch.

20. Die Eindeutigkeit der Zerlegung von Idealen in $\mathcal{O}_K$ in Primideale

Satz 20.1. Sei $\{0\} \neq A \neq \mathcal{O}_K$ ein Ideal in $\mathcal{O}_K$. Dann gilt

$$\mathcal{O}_K \supsetneq A \supsetneq A^2 \supsetneq A^3 \supsetneq \dots \text{ und } \bigcap_{i=1}^{\infty} A^i = \{0\}.$$

Beweis. Wäre $A^i = A^{i+1}$ für ein i, dann hätten wir

$$A^i \mathcal{O}_K = A^i = A^{i+1} = A^i A$$

und folglich $\mathcal{O}_K = A$ (s. Satz 19.7), ein Widerspruch.

Wir setzen $B := \bigcap_{i=1}^{\infty} A^i$. Wäre $B \neq \{0\}$, dann würde der Faktorring $\mathcal{O}_K/B$ endlich nach Lemma 18.2. Andererseits besitzt der Faktorring $\mathcal{O}_K/B$ eine unendliche absteigende Kette von Idealen

$$\mathcal{O}_K/B \supsetneq A/B \supsetneq A^2/B \supsetneq A^3/B \supsetneq \dots$$

Ein Widerspruch. □

Definition 20.2. Sei P ein Primideal und sei A ein Ideal in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$. Wir setzen $P^0 := \mathcal{O}_K$ und definieren die *Ordnung* von A bezüglich P durch

$$\operatorname{ord}_P(A) := \max\{k \geqslant 0 \mid A \subseteq P^k\}.$$

Bemerkung. Dieses Maximum existiert nach Satz 20.1. Man kann die Definition folgendermaßen umformulieren:

$$\operatorname{ord}_P(A) = k \iff A \subseteq P^k \text{ und } A \not\subseteq P^{k+1}.$$

Mit Hilfe der Bezeichnung aus Vorlesung 19 können wir diese noch einmal umformulieren:

$$\operatorname{ord}_P(A) = k \iff P^k | A \text{ und } P^{k+1} \nmid A.$$

Satz 20.3. Sei P ein Primideal und seien A, B Ideale in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$ und $\{0\} \neq B \neq \mathcal{O}_K$. Dann gilt:

1) $\operatorname{ord}_P(P) = 1$;
2) $\operatorname{ord}_P(P') = 0$ falls $P' \neq P$ ein Primideal ist;
3) $\operatorname{ord}_P(AB) = \operatorname{ord}_P(A) + \operatorname{ord}_P(B)$.

Beweis. 1) Die Einbettung $P \subseteq P$ ist trivial und die "nicht-Einbettung" $P \nsubseteq P^2$ folgt aus Satz 20.1.

2) Wäre $\mathrm{ord}_P(P') \geqslant 1$, dann hätten wir $P' \subseteq P$. Da Primideale in $\mathcal{O}_K$ gleichzeitig Maximalideale sind, erhalten wir einen Widerspruch.

3) Wir bezeichnen $s = \mathrm{ord}_P(A)$ und $t = \mathrm{ord}_P(B)$. Dann gilt $A \subseteq P^s$, $A \nsubseteq P^{s+1}$ und $B \subseteq P^t$, $B \nsubseteq P^{t+1}$. Daraus folgt $AB \subseteq P^{s+t}$. Es bleibt zu zeigen, dass $AB \nsubseteq P^{s+t+1}$ gilt.

Nehmen wir $AB \subseteq P^{s+t+1}$ an. Nach Satz 19.6 existieren Ideale C, A_1, und B_1, so dass $AB = P^{s+t+1}C$, $A = P^sA_1$ und $B = P^tB_1$ gilt. Daraus folgt

$$P^{s+t+1}C = P^{s+t}A_1B_1.$$

Das impliziert $PC = A_1B_1$ (s. Satz 19.7). Da P prim ist, ist $P|A_1$ oder $P|B_1$. O.B.d.A. ist $P|A_1$, also gilt $A_1 \subseteq P$. Dann gilt $A = P^sA_1 \subseteq P^{s+1}$. Ein Widerspruch. □

Satz 20.4. Sei A ein Ideal in $\mathcal{O}_K$ mit $\{0\} \neq A \neq \mathcal{O}_K$. Dann kann A in der Form

$$A = P_1^{n_1}P_2^{n_2}\dots P_k^{n_k}$$

geschrieben werden, wobei $P_1, \dots, P_k$ verschiedene Primideale in $\mathcal{O}_K$ sind und $n_1, \dots, n_k \in \mathbb{N}$ ist. Diese Zerlegung ist eindeutig bis auf einer Permutation von $P_1, \dots, P_k$. Außerdem gilt $n_i = \mathrm{ord}_{P_i}(A)$ für alle i.

Beweis. Die Existenz der Zerlegung wurde im Satz 19.9 formuliert. Nun zeigen wir die Eindeutigkeit. Zuerst beweisen wir die Eindeutigkeit der Primideale $P_1, \dots, P_k$. Nehmen wir an, dass es eine Zerlegung

$$A = P' \cdot \dots$$

mit einem Primideal $P' \notin \{P_1, \dots, P_k\}$ gibt. Dann gilt $A \subseteq P'$, woraus (mit Hilfe des Satzes 20.3) folgt

$$1 \leqslant \mathrm{ord}_{P'}(A) = \mathrm{ord}_{P'}(P_1^{n_1}P_2^{n_2}\dots P_k^{n_k}) = \sum_{j=1}^{k}\big(n_j \cdot \mathrm{ord}_{P'}(P_j)\big) = 0.$$

Ein Widerspruch. Die Eindeutigkeit von Exponenten n_i folgt aus der Formel

$$\mathrm{ord}_{P_i}(A) = \sum_{j=1}^{k}\big(n_j \cdot \mathrm{ord}_{P_i}(P_j)\big) = n_i.$$

□

21. Erste Anwendung: Die Gleichung $y^2 = x^3 - 5$

Lemma 21.1. Für $K = \mathbb{Q}(\sqrt{-5})$ gilt $h_K = 2$.

Beweis. Des Weiteren werden wir die Definition 26.1 der Norm eines Ideals in $\mathcal{O}_K$ und den Satz von Minkowski 27.2 benutzen.

Nach Satz 27.2 ist jedes nichtnullsche Ideal in $\mathcal{O}_K$ einem der Ideale $\mathfrak{A}$ mit $N(\mathfrak{A}) \leqslant 2$ äquivalent. Ist $N(\mathfrak{A}) = 1$, dann ist $\mathfrak{A} = \mathcal{O}_K$. Sei $N(\mathfrak{A}) = 2$. Dann besteht der Faktorring $\mathcal{O}_K/\mathfrak{A}$ aus zwei Nebenklassen $0 + \mathfrak{A}$ und $1 + \mathfrak{A}$. Deswegen ist $2(1 + \mathfrak{A}) = 0 + \mathfrak{A}$, also gilt $2 \in \mathfrak{A}$ und somit $2\mathcal{O}_K \subset \mathfrak{A} \subset \mathcal{O}_K$. Der Faktorring $\mathcal{O}_K/2\mathcal{O}_K$ besteht aus 4 Nebenklassen

$$2\mathcal{O}_K + 0,\ 2\mathcal{O}_K + 1,\ 2\mathcal{O}_K + \alpha,\ 2\mathcal{O}_K + (1 + \alpha).$$

und hat nur ein Ideal der Ordnung 2 – das besteht aus der ersten und vierten Nebenklasse. Dann ist $\mathfrak{A} = (2, 1 + \alpha)$. Dann besteht die Idealklassengruppe $Cl(K)$ aus zwei Elementen: $[\mathcal{O}_K]$ und $[(2, 1 + \alpha)]$. □

Lemma 21.2. Sei $K = \mathbb{Q}(\sqrt{-5})$. Die Hauptideale

$$A = (2, 1 + \sqrt{-5})_{\mathcal{O}_K}, \quad B = (\sqrt{-5})_{\mathcal{O}_K}$$

in $\mathcal{O}_K$ sind prim, und es gilt

$$(2)_{\mathcal{O}_K} = A^2. \tag{21.1}$$

Beweis. Wir bezeichnen $\alpha = \sqrt{-5}$. Nach Satz 14.6 gilt $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha$.

Wir zeigen Formel (21.1):

$$\begin{aligned} A^2 &= (2, 1 + \alpha)_{\mathcal{O}_K}(2, 1 + \alpha)_{\mathcal{O}_K} = (4, 2(1 + \alpha), (1 + \alpha)^2)_{\mathcal{O}_K} \\ &= (4, 2 + 2\alpha, -4 + 2\alpha)_{\mathcal{O}_K} = (4, 2 + 2\alpha,\ 6)_{\mathcal{O}_K} = (2, 2 + 2\alpha)_{\mathcal{O}_K} = (2)_{\mathcal{O}_K}. \end{aligned}$$

Wir zeigen, dass das Ideal A prim ist. Dafür werden wir zeigen, dass der Faktorring $\mathcal{O}_K/A$ genau 2 Nebenklassen enthält. Dann wird A maximal und somit prim.

Zuerst zeigen wir, dass jedes $\omega \in \mathcal{O}_K$ zu 0 oder 1 modulo A äquivalent ist. Wir schreiben ω in der Form $\omega = a\alpha + b$ mit $a, b \in \mathbb{Z}$. Da $1 + \alpha \in A$ ist, gilt

$$\omega \equiv \omega - a(1 + \alpha) \ (\mathrm{mod}\ A) = b - a \ (\mathrm{mod}\ A).$$

Da $2 \in A$ ist, ist $b - a$ zu 0 oder 1 modulo A äquivalent. Also enthällt $\mathcal{O}_K$ höchstens zwei Nebenklassen $0 + A$ und $1 + A$. Wären diese Nebenklassen gleich, dann hätten wir $1 \in A$ und somit $1 \in A^2 = 2\mathcal{O}_K$, was unmöglich ist.

Analog kann gezeigt werden, dass B prim ist. □

Satz 21.3. Die Gleichung $y^2 = x^3 - 5$ hat keine Lösung über $\mathbb{Z}$.

Beweis. Nehmen wir an, dass diese Gleichung eine Lösung $(x, y) \in \mathbb{Z}^2$ hat. Um das zu widerlegen, werden wir mit dem Ganzheitsring $\mathcal{O}_K$ arbeiten, wobei $K = \mathbb{Q}(\sqrt{-5})$ ist. In $\mathcal{O}_K$ haben wir die Gleichung

$$(y + \sqrt{-5}) \cdot (y - \sqrt{-5}) = x^3.$$

Schreiben wir diese in der Form einer "Idealen-Gleichung":

$$(y + \sqrt{-5})_{\mathcal{O}_K} \cdot (y - \sqrt{-5})_{\mathcal{O}_K} = (x^3)_{\mathcal{O}_K}. \tag{21.2}$$

Behauptung. Es gibt kein Primideal P in $\mathcal{O}_K$, das die beiden Ideale $(y + \sqrt{-5})_{\mathcal{O}_K}$ und $(y - \sqrt{-5})_{\mathcal{O}_K}$ teilt.

Beweis. Sei $P \subseteq \mathcal{O}_K$ ein solches Primideal. Dann gilt

$$P|(2\sqrt{-5})_{\mathcal{O}_K} \text{ und } P|(x^3)_{\mathcal{O}_K}. \tag{21.3}$$

Nach Lemma 21.2 hat das Ideal $(2\sqrt{-5})_{\mathcal{O}_K}$ folgende Zerlegung in Primideale:

$$(2\sqrt{-5})_{\mathcal{O}_K} = A^2 B.$$

Dann ist $P = A$ oder $P = B$.

Fall 1. $P = A$.

Nach Lemma 21.2 ist $P^2 = (2)_{\mathcal{O}_K}$ und nach Formel (21.3) gilt $P^2|(x^3)_{\mathcal{O}_K}$.

Deswegen gilt $(2)_{\mathcal{O}_K}|(x^3)_{\mathcal{O}_K}$ und somit $(x^3)_{\mathcal{O}_K} \subseteq (2)_{\mathcal{O}_K}$. Dann kann x^3 in der Form

$$x^3 = 2(a + b\sqrt{-5})$$

mit $a, b \in \mathbb{Z}$ geschrieben werden. Dann gilt $x^3 = 2a$, $b = 0$. Insbesondere ist $2|x$ in $\mathbb{Z}$. Daraus folgt

$$y^2 = x^3 - 5 \equiv -5 \pmod 8.$$

Deswegen ist y ungerade, also kann in der Form $2n+1$ mit $n \in \mathbb{Z}$ geschrieben werden. Wir haben

$$y^2 = (2n + 1)^2 = 4n(n + 1) + 1 \equiv 1 \pmod 8.$$

Ein Widerspruch.

Fall 2. $P = B$.

Dann ist $P^2 = (5)_{\mathcal{O}_K}$. Analog zu Fall 1 erhalten wir $5|x$ in $\mathbb{Z}$. Aus $y^2 = x^3 - 5$ folgt auch $5|y$. Dann ist $25|y^2$, aber $25 \nmid x^3 - 5$. Ein Widerspruch.

Die Behauptung ist bewiesen. □

Nun betrachten wir Zerlegungen von Idealen $(y+\sqrt{-5})_{\mathcal{O}_K}$, $(y-\sqrt{-5})_{\mathcal{O}_K}$ und $(x)_{\mathcal{O}_K}$ in Primidealen:

$$(y+\sqrt{-5})_{\mathcal{O}_K} = \prod_{i=1}^{s} P_i^{e_i}, \qquad (y-\sqrt{-5})_{\mathcal{O}_K} = \prod_{j=1}^{t} Q_j^{f_j}, \qquad (x)_{\mathcal{O}_K} = \prod_{i=1}^{\ell} R_k^{g_k}$$

Aus (21.2) folgt

$$\prod_{i=1}^{s} P_i^{e_i} \prod_{j=1}^{t} Q_j^{f_j} = \prod_{k=1}^{\ell} R_k^{3g_k}.$$

Da alle P_i und Q_j verschieden sind und die Zerlegung in Primideale eindeutig ist, gilt $3|e_i$ und $3|f_j$ für alle i, j. Dann ist

$$(y+\sqrt{-5})_{\mathcal{O}_K} = I^3 \tag{21.4}$$

für ein Ideal I in $\mathcal{O}_K$. In der Idealklasengruppe $Cl(K)$gilt

$$[\mathcal{O}_K] = [(y+\sqrt{-5})_{\mathcal{O}_K}] = [I]^3.$$

Nach Lemma 21.1 ist $|Cl(K)| = 2$. Das impliziert $[\mathcal{O}_K] = [I]$. Deswegen ist I ein Hauptideal und es kann in der Form

$$I = (a+b\sqrt{-5})\mathcal{O}_K \tag{21.5}$$

mit $a, b \in \mathbb{Z}$ geschrieben werden. Aus (21.4) und (21.5) erhalten wir

$$(y+\sqrt{-5})\mathcal{O}_K = (a+b\sqrt{-5})^3\mathcal{O}_K.$$

Dann gilt

$$y+\sqrt{-5} = u \cdot (a+b\sqrt{-5})^3$$

für ein $u \in \mathcal{O}_K^*$. Es ist leicht zu berechnen, dass $\mathcal{O}_K^* = \{-1, 1\}$ ist. O.B.d.A. ist $u = 1$. Wir haben

$$y+\sqrt{-5} = (a+b\sqrt{-5})^3 = a^3 - 15ab^2 + (3a^2 - 5b)b\sqrt{-5}.$$

Dann gilt $(3a^2 - 5b)b = 1$. Diese führt zu einem Widersprich. □

22. Fermatscher Satz: Vorbereitung

Folgender Satz wurde vermutet von Fermat im Jahr etwa 1640 und bewiesen von Wiles im Jahr 1994.

Satz 22.1. (Wiles) Für $n \geqslant 3$ ist die Gleichung $x^n + y^n = z^n$ unlösbar in $\mathbb{N}$.

Offensichtlich reicht es, diesen Satz für $n = 4$ und alle Primzahlen $n \geqslant 3$ zu beweisen. Kummer hat diesen Satz für die sogenannten regulären Primzahlen bewiesen (s. seine Arbeiten der Jahre 1847 und 1850). Für $n \leqslant 100$ gibt es nur drei Primzahlen, die nicht regulär sind: $37, 59, 67$. Wir werden den Beweis von Kummer zu einem großen Teil geben.

Allgemeine Vorbereitung. Sei $l \geqslant 3$ eine Primzahl. Wir betrachten die Zahlkörper $K = \mathbb{Q}(\zeta)$, wobei

$$\zeta = e^{2\pi i/\ell} = \cos(2\pi/\ell) + i\sin(2\pi/\ell)$$

ist. Es ist klar, dass $\zeta^\ell = 1$ ist.

• Die Zahlen $1, \zeta, \ldots, \zeta^{\ell-1}$ sind alle Nullstellen des Polynoms $x^\ell - 1$. Das Polynom

$$\frac{x^\ell - 1}{x - 1} = x^{\ell-1} + x^{\ell-2} + \cdots + 1 = \prod_{i=1}^{\ell-1} (x - \zeta^i) \tag{22.1}$$

ist irreduzibel über $\mathbb{Q}$ (s. Übungsblatt 6). Deswegen ist

$$m_\zeta(x) = x^{\ell-1} + x^{\ell-2} + \cdots + 1.$$

Insbesondere gilt $[K : \mathbb{Q}] = \ell - 1$. Daraus folgt, dass

$$1, \zeta, \ldots, \zeta^{\ell-2}$$

eine Basis von K über $\mathbb{Q}$ ist.

• Folgende Zahl spielt eine wichtige Rolle im weiteren Beweis:

$$\lambda = 1 - \zeta.$$

Es kann bewiesen werden, dass

$$1, \lambda, \ldots, \lambda^{\ell-2}.$$

auch eine Basis von K über $\mathbb{Q}$ ist.

• Da $[K : \mathbb{Q}] = \ell - 1$ ist, existieren genau $\ell - 1$ Einbettungen von K in $\mathbb{C}$:

$$\begin{aligned} \tau_i : \quad & K \hookrightarrow \mathbb{C}, \\ & \zeta \mapsto \zeta^i, \end{aligned} \tag{22.2}$$

$i = 1, \ldots, \ell - 1$. Diese Einbettungen sind Automorphismen des Körpers K. Es gilt also

$$\mathrm{Aut}_{\mathbb{Q}}(K) = \{\tau_1, \ldots, \tau_{\ell-1}\}.$$

Den folgenden Gruppenisomorphismus werden wir aber nicht benutzen:

$$\mathrm{Aut}_{\mathbb{Q}}(K) \cong (\mathbb{Z}_\ell)^* \cong \mathbb{Z}_{\ell-1}.$$

Definition 22.2. Zwei Zahlen $\alpha, \beta \in \mathcal{O}_K$ heißen *assoziiert*, falls eine Einheit $\varepsilon \in \mathcal{O}_K^*$ existiert, so dass $\alpha = \beta\varepsilon$ gilt. In dem Fall schreiben wir $\alpha \sim \beta$.

Bemerkung. Zwei Hauptideale $(\alpha)_{\mathcal{O}_K}$ und $(\beta)_{\mathcal{O}_K}$ sind gleich genau dann, wenn die Zahlen α und β äquivalent sind:

$$(\alpha)_{\mathcal{O}_K} = (\beta)_{\mathcal{O}_K} \;\Leftrightarrow\; \alpha \sim \beta.$$

Lemma 22.3. Sei $\lambda = 1 - \zeta$. Dann gilt:

1) $N(\lambda) = \ell$,
2) $(1 - \zeta^i) \sim \lambda$ für alle $i = 1, \ldots, \ell - 1$.
3) $\ell \sim \lambda^{\ell-1}$,

Beweis.
Zu 1): Wir haben

$$N(\lambda) = \prod_{j=1}^{\ell-1} \tau_j(\lambda) \overset{(22.2)}{=} (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{\ell-2}) \overset{(22.1)}{=} \ell.$$

Etwas allgemeiner gilt

$$N(1-\zeta^i) = N(\tau_i(\lambda)) = \prod_{j=1}^{\ell-1} \tau_j(\tau_i(\lambda)) = \prod_{i=1}^{\ell-1} \tau_i(\lambda) = N(\lambda) = \ell.$$

für $i = 1, \ldots, \ell - 1$.

Zu 2): Wir haben

$$1 - \zeta^i = (1-\zeta)\epsilon_i$$

mit $\epsilon_i = 1 + \zeta + \cdots + \zeta^{i-1} \in \mathcal{O}_K$. Daraus folgt

$$\underbrace{N(1-\zeta^i)}_{\ell} = \underbrace{N(1-\zeta)}_{\ell} N(\epsilon_i).$$

Deswegen gilt $N(\epsilon_i) = 1$, also ist $\epsilon_i \in \mathcal{O}_K^*$.

Zu 3): Wir haben

$$\ell = \prod_{i=1}^{\ell-1}(1-\zeta^i) = \prod_{i=1}^{\ell-1}(1-\zeta)\epsilon_i = (1-\zeta)^{\ell-1}\varepsilon$$

mit $\varepsilon = \prod_{i=1}^{\ell-1} \epsilon_i \in \mathcal{O}_K^*$. □

Lemma 22.4. Es gilt $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{\ell-2}$.

Beweis. Wir bezeichnen

$$A = \mathbb{Z} + \mathbb{Z}\zeta + \cdots + \mathbb{Z}\zeta^{\ell-2}.$$

Die Inklusion $A \subseteq \mathcal{O}_K$ ist klar. Wir beweisen $\mathcal{O}_K \subseteq A$. Sei also $\alpha \in \mathcal{O}_K$. Zuerst schreiben wir α als eine Linearkombination von $1, \zeta, \ldots, \zeta^{\ell-2}$ mit Koeffizienten a_i aus $\mathbb{Q}$:

$$\alpha = a_0 + a_1\zeta + \cdots + a_{\ell-2}\zeta^{\ell-2}.$$

Wir werden zeigen, dass alle a_i in $\mathbb{Z}$ liegen. Da $\mathrm{Sp}(1) = [K : \mathbb{Q}] = \ell - 1$ und $\mathrm{Sp}(\zeta^i) = -1$ für $i = 1, \ldots, \ell - 1$ ist, gilt

$$\mathrm{Sp}(\alpha) = \ell a_0 - \sum_{i=0}^{\ell-2} a_i.$$

Man kann berechnen

$$\mathrm{Sp}(\zeta\alpha) = -\sum_{i=0}^{\ell-2} a_i, \quad \mathrm{Sp}(\zeta^k\alpha) = -\ell a_{\ell-k} - \sum_{i=0}^{\ell-2} a_i, \quad k = 2, \ldots, \ell - 2.$$

Da die Spuren von ganzen algebraischen Zahlen in $\mathbb{Z}$ liegen, gilt $\ell a_k \in \mathbb{Z}$ für $k = 0, \ldots, \ell - 2$. Deswegen gilt $\ell\alpha \in A$. Das $\mathbb{Z}$-Modul A kann auch in der Form

$$A = \mathbb{Z} + \mathbb{Z}\lambda + \cdots + \mathbb{Z}\lambda^{\ell-2}.$$

geschrieben werden. Deswegen können wir $\ell\alpha$ als eine Linearkombination von $1, \lambda, \ldots, \lambda^{\ell-2}$ mit Koeffizienten b_i aus $\mathbb{Z}$ aufschreiben:

$$\ell\alpha = b_0 + b_1\lambda + \cdots + b_{\ell-2}\lambda^{\ell-2}. \tag{22.3}$$

Es bleibt zu zeigen, dass alle b_i durch ℓ teilbar sind. Nehmen wir an, dass für ein $0 \leqslant s < \ell - 2$ schon bewiesen ist, dass alle Koeffizienten b_i mit $i < s$ durch ℓ teilbar sind. Wir splitten die rechte Seite von (22.3) in drei Summanden:

$$\ell\alpha = \sum_{i<s} b_i\lambda^i + b_s\lambda^s + \sum_{j>s} b_j\lambda^j \tag{22.4}$$

Da $\lambda^{\ell-1} | \ell$ in $\mathcal{O}_K$ ist, gilt $\lambda^{s+1} | b_i$ in $\mathcal{O}_K$ für alle $i < s$. Somit sind die linke Seite und die zwei Summen in der rechten Seite von (22.4) durch λ^{s+1} in $\mathcal{O}_K$ teilbar.

Deswegen ist auch $b_s\lambda^s$ durch λ^{s+1} teilbar. Daraus folgt $\lambda | b_s$ in $\mathcal{O}_K$ und somit $N(\lambda) | N(b_s)$ in $\mathbb{Z}$. Also erhalten wir $\ell | b_s^\ell$ in $\mathbb{Z}$ und somit $\ell | b_s$. □

Lemma 22.5. Für jede Einheit $\varepsilon \in \mathcal{O}_K^*$ existieren eine Zahl $a \in \mathbb{N}$ und eine reelle Einheit $\varepsilon_0 \in \mathcal{O}_K^*$ mit $\varepsilon = \zeta^a\varepsilon_0$.

23. Erster Fall des Fermatschen Satzes für reguläre Primzahlen

Definition 23.1. Eine Primzahl $\ell > 2$ heißt *regulär*, wenn die Idealklassengruppe von $\mathbb{Q}(\zeta)$, wobei $\zeta = e^{2\pi i/\ell}$ ist, keine Elemente der Ordnung ℓ enthält.

Lemma 23.2. Sei ℓ eine Primzahl. Seien x, y zwei teilerfremde ganze Zahlen mit $\ell \nmid (x+y)$. Dann sind die Hauptideale

$$(x+y)\mathcal{O}_K, (x+\zeta y)\mathcal{O}_K, \ldots, (x+\zeta^{\ell-1}y)\mathcal{O}_K$$

paarweise teilerfremd in $\mathcal{O}_K$, wobei $K = \mathbb{Q}(\zeta)$ mit $\zeta = e^{2\pi i/\ell}$ ist.

Beweis. Nehmen wir an, dass ein Primideal $P \subseteq \mathcal{O}_K$ und einige Zahlen $i \neq j \pmod{\ell}$ existieren, so dass gilt:

$$P|(x+\zeta^i y)_{\mathcal{O}_K} \text{ und } P|(x+\zeta^j y)_{\mathcal{O}_K}. \tag{23.1}$$

Mit Hilfe des Lemmas 22.3 erhalten wir

$$(x+\zeta^j y) - (x+\zeta^i y) = (\zeta^j - \zeta^i)y \sim (1-\zeta)y.$$

Daraus folgt

$$((1-\zeta)y)_{\mathcal{O}_K} \subseteq (x+\zeta^j y)_{\mathcal{O}_K} + (x+\zeta^i y)_{\mathcal{O}_K}.$$

Da P ein Teiler von jedem dieser Summanden ist, ist P ein Teiler von $((1-\zeta)y)_{\mathcal{O}_K}$. Da P ein Primideal ist, gilt

$$P|(1-\zeta)_{O_K} \text{ oder } P|(y)_{O_K}.$$

Analog gilt

$$P|(1-\zeta)_{O_K} \text{ oder } P|(x)_{O_K}.$$

Insbesondere gilt

$$(1-\zeta) \in P \text{ oder } x, y \in P.$$

Da $\mathrm{ggT}(x,y) = 1$ ist, existieren $x, y \in \mathbb{Z}$ mit $xu + yv = 1$. Gelte $x, y \in P$, dann hätten wir $1 \in P$, ein Widerspruch. Also gilt

$$(1-\zeta) \in P.$$

Mit Hilfe das Lemmas 22.3 leiten wir daraus ab:

$$\ell \in P \text{ und } (1-\zeta^j) \in P. \tag{23.2}$$

Außerdem gilt $(x+y) \in P$ wegen

$$(x+y) = (x+\zeta^j y) + (1-\zeta^j)y \underset{(23.2)}{\overset{(23.1)}{\in}} P + P$$

Da $\mathrm{ggT}(\ell, (x+y)) = 1$ ist, gilt $1 \in P$ wie oben. Ein Widerspruch. □

Lemma 23.3. Sei $n \in \mathbb{Z}$. Ist $3 \nmid n$, dann hat n^3 den Rest 1 oder -1 modulo 9.

Satz 23.4. (Erster Fall des Fermatschen Satzes für reguläre Primzahlen) Sei $\ell \geqslant 3$ eine reguläre Primzahl. Dann existieren keine ganze Zahlen x, y, z, die jeweils teilerfremd zu ℓ sind und $x^\ell + y^\ell = z^\ell$ erfüllen.

Beweis. Für $\ell = 3$ folgt die Aussage aus Lemma 23.3. Nun betrachten wir den Fall $\ell \geqslant 5$. Nehmen wir an, dass solche Zahlen x, y, z existieren. O.B.d.A. können wir annehmen, dass sie paarweise teilerfremd sind. Nach dem kleinen Fermatschen Satz (s. Appendix A) gilt

$$x^\ell \equiv x \ (\mathrm{mod}\ \ell), \quad y^\ell \equiv y \ (\mathrm{mod}\ \ell), \quad z^\ell \equiv z \ (\mathrm{mod}\ \ell).$$

Daraus folgt

$$x + y \equiv z \ (\mathrm{mod}\ \ell).$$

Nach Voraussetzung gilt $\ell \nmid z$, somit gilt

$$\ell \nmid (x + y).$$

Sei $\zeta = e^{2\pi i/\ell}$. Dann gilt

$$(x + y)(x + \zeta y) \dots (x + \zeta^{\ell-1} y) = z^\ell.$$

Schreiben wir diese in der Form einer "Idealen-Gleichung":

$$(x + y)_{\mathcal{O}_K} (x + \zeta y)_{\mathcal{O}_K} \dots (x + \zeta^{\ell-1} y)_{\mathcal{O}_K} = (z)^\ell_{\mathcal{O}_K}.$$

Nach Lemma 23.2 sind die Ideale auf der linken Seite paarweise teilerfremd. Dann sind sie ℓ-te Potenzen einiger Ideale in $\mathcal{O}_K$. Insbesondere ist

$$(x + \zeta y)_{\mathcal{O}_K} = A^\ell$$

für ein Ideal A in $\mathcal{O}_K$. Daraus folgt $[A]^\ell = [\mathcal{O}_K]$. Da ℓ regulär ist, gilt $[A] = [\mathcal{O}_K]$, also ist $A = (\alpha)_{\mathcal{O}_K}$ für ein $\alpha \in \mathcal{O}_K$. Wir haben also

$$(x + \zeta y)_{\mathcal{O}_K} = (\alpha^\ell)_{\mathcal{O}_K}.$$

Deswegen existiert $\varepsilon \in \mathcal{O}_K^*$ mit

$$x + \zeta y = \varepsilon \alpha^\ell. \tag{23.3}$$

Wir schreiben α als eine Linearkombination von $1, \lambda, \dots, \lambda^{\ell-2}$ mit Koeffizienten b_i aus $\mathbb{Z}$:

$$\alpha = b_0 + b_1 \lambda + \dots + b_{\ell-2} \lambda^{\ell-2}.$$

Dann ist

$$\alpha^\ell \equiv b_0^\ell + b_1^\ell \lambda^\ell + \dots + b_{\ell-2}^\ell \lambda^{\ell(\ell-2)} \ (\mathrm{mod}\ \ell).$$

Aus Lemma 22.3 3) folgt $\ell \mid \lambda^\ell$ in $\mathcal{O}_K$. Deswegen gilt

$$\alpha^\ell \equiv b_0^\ell \ (\mathrm{mod}\ \ell).$$

Daraus und aus dem kleinen Fermatschen Satz folgt

$$\alpha^\ell \equiv b_0 \ (\mathrm{mod}\ \ell). \tag{23.4}$$

Nach Lemma 22.5 existiert $a \in \mathbb{N}$ und eine reelle Einheit $\varepsilon_0 \in \mathcal{O}_K^*$ mit

$$\varepsilon = \zeta^a \varepsilon_0. \tag{23.5}$$

Aus (23.3)-(23.5) folgt

$$x + \zeta y \equiv \zeta^a \varepsilon_0 b_0 \ (\mathrm{mod}\ \ell),$$

also

$$\zeta^{-a} x + \zeta^{1-a} y \equiv \varepsilon_0 b_0 \ (\mathrm{mod}\ \ell).$$

Mit Hilfe der komplexen Konjugation erhalten wir

$$\zeta^a x + \zeta^{a-1} y \equiv \varepsilon_0 b_0 \ (\mathrm{mod}\ \ell).$$

Daraus folgt

$$x\zeta^a + y\zeta^{a-1} - x\zeta^{-a} - y\zeta^{1-a} \equiv 0 \ (\mathrm{mod}\ \ell). \tag{23.6}$$

Bemerkung. Ist $a_0 + a_1\zeta + \cdots + a_{\ell-2}\zeta^{\ell-2} \equiv 0 \ (\mathrm{mod}\ \ell)$ mit $a_0, \ldots, a_{\ell-2} \in \mathbb{Z}$, dann gilt $\ell | a_i$ für alle i.

Mit Hilfe dieser Bemerkung folgt aus (23.6), dass $\ell | x$ oder $\ell | y$ oder $\ell | (x - y)$ gilt. Die ersten zwei Fälle sind unmöglich nach der Voiraussetzung. Also gilt

$$x \equiv y \ (\mathrm{mod}\ \ell). \tag{23.7}$$

Die Gleichung $x^\ell + y^\ell = z^\ell$ kann noch in der Form $x^\ell + (-z)^\ell = (-y)^\ell$ geschrieben werden. Dann folgt analog

$$x \equiv -z \ (\mathrm{mod}\ \ell). \tag{23.8}$$

Am Anfang des Beweises haben wir gezeigt:

$$x + y \equiv z \ (\mathrm{mod}\ \ell). \tag{23.9}$$

Aus (23.7)-(23.9) folgt

$$3x \equiv 0 \ (\mathrm{mod}\ \ell).$$

Da $\ell \geqslant 5$ ist, gilt $\ell | x$. Ein Widerspruch. □

24. Zweiter Fall des Fermatschen Satzes für reguläre Primzahlen(wird geschrieben)

Satz 24.1. (Zweiter Fall des Fermatschen Satzes für reguläre Primzahlen) Sei ℓ eine reguläre Primzahl. Dann existieren keine ganzen Zahlen x, y, z, so dass sie paarweise teilerfremd sind, ℓ ein Teiler einer dieser Zahlen ist und $x^\ell + y^\ell = z^\ell$ gilt.

Appendix

25. Appendix A

25.1. Satz von Euler und Kleiner Fermatschen Satz.

Satz 25.1. (Satz von Euler) Seien n, a zwei teilerfremde Zahlen aus $\mathbb{N}$. Dann gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

wobei φ die Eulersche Funktion ist.

Folgerung 25.2. (Kleiner Fermatschen Satz) Sei ℓ eine Primzahl. Für jede ganze Zahl a gilt

$$a^{\ell} \equiv a \pmod{\ell}.$$

25.2. Legendre-Symbol.

Definition 25.3. Sei p eine Primzahl und sei $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$. Das Legendre-Symbol $\left(\frac{a}{p}\right)$ ist durch die folgende Formel definiert:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } \exists\, x \in \mathbb{Z}: \quad x^2 \equiv a \mod p, \\ -1 & \text{falls } \nexists\, x \in \mathbb{Z}: \quad x^2 \equiv a \mod p. \end{cases}$$

Eine Zahl $a \in \mathbb{Z}$ heißt quadratischer Rest modulo p, falls $\left(\frac{a}{p}\right) = 1$ ist.

Lemma 25.4. Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$ und $\mathrm{ggT}(b,p) = 1$. Dann gilt:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

Insbesondere gilt

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

Außerdem gilt für jedes $n \in \mathbb{Z}$:

$$\left(\frac{a - pn}{p}\right) = \left(\frac{a}{p}\right).$$

Satz 25.5. (Gauß, Euler) Sei p eine ungerade Primzahl. Dann gelten:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{falls } p \equiv \pm 1 \mod 8, \\ -1 & \text{falls } p \equiv \pm 3 \mod 8. \end{cases}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 4, \\ -1 & \text{falls } p \equiv 3 \mod 4. \end{cases}$$

Daraus folgt

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 8, \\ 1 & \text{falls } p \equiv 3 \mod 8, \\ -1 & \text{falls } p \equiv 5 \mod 8, \\ -1 & \text{falls } p \equiv 7 \mod 8. \end{cases}$$

Satz 25.6. (Reziprozitätssatz von Gauß) Seien p, q zwei verschiedene Primzahlen, $p, q \geqslant 3$. Dann gilt

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

Satz 25.7. Das Polynom $x^4 + 1$ ist irreduzibel über $\mathbb{Z}$, aber es ist reduzibel über $\mathbb{Z}_p$ für jede Primzahl p.

Beweis. Das Polynom $f(x) = x^4 + 1$ ist irreduzibel über $\mathbb{Z}$, da das Polynom $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ irreduzibel über $\mathbb{Z}$ nach dem Eisenstein-Kriterium ist. Jetzt beweisen wir, dass $f(x)$ reduzibel über $\mathbb{Z}_p$ für jede Primzahl p ist.

Wir haben $x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1) = x^4 + (2 - a^2)x^2 + 1$, falls $a^2 \equiv 2 \mod p$ ist. Eine solche a existiert für $p \equiv \pm 1 \mod 8$.

Wir haben $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1) = x^4 + (-2 - a^2)x^2 + 1$, falls $a^2 \equiv -2 \mod p$ ist. Eine solche a existiert für $p \equiv 3 \mod 8$.

Wir haben $x^4 + 1 = (x^2 + a)(x^2 - a) = x^4 - a^2$, falls $a^2 \equiv -1 \mod p$ ist. Eine solche a existiert für $p \equiv 1 \mod 4$, insbesondere für $p \equiv 5 \mod 8$. $\square$

26. Appendix B

26.1. Normen von Idealen in Ganzheitsringen.

Definition 26.1. Sei K ein Zahlkörper und sei A ein Ideal in $\mathcal{O}_K$. Die *Norm* von A ist die Zahl

$$N(A) := |\mathcal{O}_K : A|.$$

Folgenden Satz werden wir nicht beweisen.

Satz 26.2. (Multiplikativität von Normen) Sei K ein Zahlkörper. Für je zwei Ideale A, B in $\mathcal{O}_K$ gilt

$$N(AB) = N(A)N(B).$$

Satz 26.3. Sei K ein Zahlkörper und sei $0 \neq \alpha \in \mathcal{O}_K$ eine Zahl. Wir bezeichnen $A = (\alpha)$. Dann gilt

$$N(A) = |N(\alpha)|.$$

Beweis. Nach Satz 17.5 enthält der Ganzheitsring $\mathcal{O}_K$ die Zahlen $\alpha_1, \ldots, \alpha_n$, für die das Folgende gilt:

a) $\alpha_1, \ldots, \alpha_n$ ist eine Basis von K über $\mathbb{Q}$;
b) $\mathcal{O}_K = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

Wir bezeichnen $\beta_i = \alpha\alpha_i$. Dann ist $\beta_1, \ldots, \beta_n$ ebenfalls eine Basis von K über $\mathbb{Q}$, und es gilt

$$(\alpha) = \alpha\mathcal{O}_K = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_n.$$

Wir haben also ein freies $\mathbb{Z}$-Modul $\mathcal{O}_K$ mit der $\mathbb{Z}$-Basis $\alpha_1, \ldots, \alpha_n$ und sein freies $\mathbb{Z}$-Untermodul $(\alpha\mathcal{O}_K)$ mit der $\mathbb{Z}$-Basis $\beta_1, \ldots, \beta_n$. Es existieren $c_{i,j} \in \mathbb{Z}$, so dass folgendes gilt:

$$\begin{aligned} \beta_1 &= \alpha\alpha_1 = c_{11}\alpha_1 + \cdots + c_{1n}\alpha_n, \\ &\ldots \\ \beta_n &= \alpha\alpha_n = c_{n1}\alpha_1 + \cdots + c_{nn}\alpha_n. \end{aligned}$$

Mit Hilfe von $\mathbb{Z}$-Elementartransformationen kann die Matrix $C = (c_{ij})$ zur Diagonalform D gebracht werden. Mit anderen Worten besitzen die $\mathbb{Z}$-Module $\mathcal{O}_K$ und $(\alpha)\mathcal{O}_K$ andere $\mathbb{Z}$-Basen $\alpha'_1, \ldots, \alpha'_n$ und $\beta'_1, \ldots, \beta'_n$, so dass $\beta'_i = d_i\alpha'_i$ für einige $d_1, \ldots, d_n \in \mathbb{Z}$ gilt:

$$\begin{aligned} \beta'_1 &= d_1\alpha'_1 \\ \beta'_2 &= \quad d_2\alpha'_2 \\ &\vdots \\ \beta'_n &= \quad\quad d_n\alpha'_n. \end{aligned}$$

Es gilt $\mathcal{O}_K = \mathbb{Z}\alpha'_1 + \cdots + \mathbb{Z}\alpha'_n$ und $(\alpha\mathcal{O}_K) = \mathbb{Z}d_1\alpha'_1 + \cdots + \mathbb{Z}d_n\alpha'_n$. Als Repräsentanten von Nebenklassen von $(\alpha\mathcal{O}_K)$ in $\mathcal{O}_K$ können die Elemente $k_1\alpha'_1 + \cdots + k_n\alpha'_n$ mit $0 \leqslant k_i \leqslant |d_i| - 1$ gewählt werden. Die Anzahl dieser Repräsentanten ist

$$|\mathcal{O}_K : (\alpha)| = |d_1 d_2 \dots d_n| = |\det(D)| = |\det(C)| = |N(\alpha)|.$$

□

Folgerung 26.4. Sei K ein Zahlkörper und sei $A = (\alpha_1, \dots, \alpha_s)$ ein Ideal in $\mathcal{O}_K$ mit $\alpha_i \neq 0$ für alle i. Dann gilt

$$N(A) \,\Big|\, \mathrm{ggT}\{N(\alpha_1), \dots, N(\alpha_s)\}.$$

Beweis. Wegen $(\alpha_i) \subseteq A \subseteq \mathcal{O}_K$ und wegen der Multiplikativität von Indizes gilt $\underbrace{|\mathcal{O}_K : (\alpha_i)|}_{N(\alpha_i)} = \underbrace{|\mathcal{O}_K : A|}_{N(A)} \cdot |A : (\alpha_i)|$. □

Beispiel. Sei $K = \mathbb{Q}(\sqrt{-5})$. Wir beweisen, dass das Ideal $A = (3, 1 + \sqrt{-5})$ in $\mathcal{O}_K$ die Norm 3 hat. Zuerst berechnen wir die Normen der Erzeuger von A: $N(3) = 9$, $N(1 + \sqrt{-5}) = 6$. Dann ist $N(A)$ ein Teiler von $\mathrm{ggT}(9, 6) = 3$, also ist $N(A)$ gleich 1 oder 3.

Nehmen wir an, dass $N(A) = 1$ gilt. Dann gilt $A = \mathcal{O}_K$. Insbesondere kann 1 als eine lineare Kombination von 3 und $1 + \sqrt{-5}$ mit Koeffizienten aus $\mathcal{O}_K$ ausgedruckt werden:

$$1 = 3\underbrace{(a + b\sqrt{-5})}_{\in\mathcal{O}_K} + (1 + \sqrt{-5})\underbrace{(c + d\sqrt{-5})}_{\in\mathcal{O}_K}, \qquad (a, b, c, d \in \mathbb{Z}).$$

Daraus folgt

$$\begin{cases} 1 = & 3a + c - 5d, \\ 0 = & 3b + c + d. \end{cases}$$

Durch Substraktion erhalten wir $1 = 3(a - b - 2d)$, ein Widerspruch. Also gilt $N(A) = 3$. □

Bemerkung. Sei K ein Zahlkörper. Für jedes nichtnullsche Ideal A in $\mathcal{O}_K$ gilt

$$N(A) = \mathrm{ggT}\{N(a) \,:\, a \in A\}.$$

26.2. **Primelemente in Ganzheitsringen.** Folgendes einfache Lemma wird oft gebraucht.

Lemma 26.5. Sei K ein Zahlkörper und sei $\alpha \in \mathcal{O}_K$. Dann gilt $\alpha | N(\alpha)$ in $\mathcal{O}_K$.

Beweis. Seien $\mathrm{id} = \tau_1, \ldots, \tau_n$ alle Einbettungen von K in $\mathbb{C}$ über $\mathbb{Q}$. Da $\alpha \in \mathcal{O}_K$ ist, ist auch $\tau_i(\alpha) \in \mathcal{O}_K$ für alle i. Nach Folgerung 13.11 gilt $N(\alpha) = \tau_1(\alpha) \cdot \ldots \cdot \tau_n(\alpha)$. Daraus folgt $\alpha | N(\alpha)$ in $\mathcal{O}_K$. □

In den Beweisen der Folgerungen benutzen wir Behauptung 16.5 und Satz 16.7.

Folgerung 26.6. Sei K ein Zahlkörper vom Grad $n = [K : \mathbb{Q}]$. Sei $\alpha \in \mathcal{O}_K$. Dann gilt:

1) Ist $\alpha \in \mathrm{Prim}(\mathcal{O}_K)$, dann ist $|N(\alpha)| = p^\ell$ für einige $p \in \mathrm{Prim}(\mathbb{N})$ und $1 \leqslant \ell \leqslant n$.
2) Ist $|N(\alpha)| \in \mathrm{Prim}(\mathbb{N})$, dann ist $\alpha \in \mathrm{Prim}(\mathcal{O}_K)$.

Beweis. 1) Sei $\alpha \in \mathrm{Prim}(\mathcal{O}_K)$. Dann ist (α) ein Primideal in $\mathcal{O}_K$. Dann ist (α) ein Maximalideal in $\mathcal{O}_K$. Dann ist $O_K/(\alpha)$ ein Körper. Nach Satz 26.3 hat der Körper die Ordnung $|N(\alpha)|$. Die Ordnung jedes endlichen Körpers ist aber eine Potenz einer Primzahl. Deswegen ist $|N(\alpha)| = p^\ell$ für ein $p \in \mathrm{Prim}(\mathbb{N})$ und ein $\ell \in \mathbb{N}$. Nach Lemma 26.5 gilt $\alpha | N(\alpha)$ in $\mathcal{O}_K$. Deswegen gilt $\alpha | p$ in $\mathcal{O}_K$. Daraus folgt $N(\alpha) | N(p)$ in $\mathbb{Z}$. Dann folgt die Behauptung aus $N(p) = p^n$.

2) Sei $|N(\alpha)| = p \in \mathrm{Prim}(\mathbb{N})$. Dann ist $|\mathcal{O}_K : (\alpha)| = p$ nach Satz 26.3. Deswegen ist das Ideal (α) maximal in $\mathcal{O}_K$ und folglich prim. □

Folgerung 26.7. Sei $[K : \mathbb{Q}] = 2$ und sei $\alpha \in \mathcal{O}_K \setminus \Big(\mathrm{Prim}(\mathbb{Z}) \cdot (\mathcal{O}_K)^*\Big)$. Dann gilt:

$$\alpha \in \mathrm{Prim}(\mathcal{O}_K) \iff N(\alpha) \in \mathrm{Prim}(\mathbb{Z}).$$

Beweis. Sei $\alpha \in \mathrm{Prim}(\mathcal{O}_K)$. Nach Folgerung 26.6 ist $|N(\alpha)| = p^\ell$ für einige $p \in \mathrm{Prim}(\mathbb{N})$ und $\ell \in \{1, 2\}$. Wir müssen zeigen, dass $\ell = 1$ gilt.

Nehmen wir $\ell = 2$ an. Aus Lemma 26.5 folgt $\alpha | p^\ell$ und somit $\alpha | p$ in $\mathcal{O}_K$. Es gilt also $p = \alpha\beta$ für ein $\beta \in \mathcal{O}_K$. Dann ist

$$p^2 = N(p) = N(\alpha)N(\beta) = \pm p^2 N(\beta).$$

Daraus folgt $N(\beta) = 1$ und $\beta \in (\mathcal{O}_K)^*$. Dann ist

$$\alpha = p\beta^{-1} \in \Big(\mathrm{Prim}(\mathbb{Z}) \cdot (\mathcal{O}_K)^*\Big).$$

Ein Widerspruch. Also gilt $\ell = 1$.

Die andere Richtung ist in Folgerung 26.6 enthalten. □

27. Appendix C

Definition 27.1. Wir definieren $\theta : \mathbb{C} \to \mathbb{C}$ durch $\theta(a+bi) = a - bi$, wobei $a, b \in \mathbb{R}$ ist.

Sei K ein Zahlkörper. Eine Einbettung $\sigma : K \hookrightarrow \mathbb{C}$ heißt *komplexe Einbettung*, falls $\sigma(K)$ nicht komplett in $\mathbb{R}$ liegt. Zu jeder komplexen Einbettung σ gibt es eine konjugierte Einbettung $\overline{\sigma} = \theta \circ \sigma$.

Satz 27.2. (Satz von Minkowski) Sei K ein Zahlkörper mit dem Grad $[K : \mathbb{Q}] = n$, der Diskriminante $\Delta(K)$ und der Anzahl s von Paaren zueinander konjugierter komplexer Einbettungen von K in $\mathbb{C}$.

Jedes nichtnullsche Ideal I in $\mathcal{O}_K$ ist einem Ideal A in $\mathcal{O}_K$ mit

$$N(A) \leqslant \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\delta(K)|}.$$

äquivalent.

Satz 27.3. Sei K ein Zahlkörper. In $\mathcal{O}_K$ gibt es nur endlich viele Ideale A mit einer gegebenen Norm.

Beweis. Wir fixieren ein $m \in \mathbb{N}$ und betrachten ein Ideal A in $\mathcal{O}_K$ mit $|\mathcal{O}_K/A| = m$. Nach Lagrange-Satz gilt $m(1+A) = 0+A$. Daraus folgt $m \in A$ und somit $m\mathcal{O}_K \subseteq A$. Die Faktorgruppe $\mathcal{O}_K/m\mathcal{O}_K$ ist endlich und hat die Ordnung $m^{[K:\mathbb{Q}]}$. Deswegen gibt es nur endlich viele Möglichkeiten für A. □

Folgerung 27.4. Es existiert eine obere Schranke für die Idealklassentahl h_K, die nur vom Grad $[K : \mathbb{Q}]$ und die Diskriminante $\Delta(K)$ abhängt.

Satz 27.5. Sei $K = \mathbb{Q}(\theta)$ ein Zahlkörper vom Grad $n = [K : \mathbb{Q}]$, wobei θ eine ganze algebraische Zahl ist. Sei $m = |\Delta(K)|$. Dann ist

$$\mathcal{O}_K = \mathbb{Z}[\theta] + M,$$

wobei M die folgende endliche Menge ist:

$$M := \left\{ \frac{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}}{m} \,|\, 0 \leqslant a_i < m,\ 0 \leqslant i < n \right\} \cap \mathcal{O}_K.$$

Satz 27.6. (Verzweigungssatz) wird geschrieben