Einschub Elementare Zahlentheorie

1) Definition: Eine Zahl $b \in \mathbb{Z}$ heißt teilbar durch $a \in \mathbb{Z}$ wenn es $c \in \mathbb{Z}$ gibt, sd. $a \cdot c = b$

Wir schreiben $a \mid b$ als „a teilt b"

2) Definition: Eine positive ganze Zahl, heißt prim, wenn sie nur durch 1 & durch sich selbst teilbar ist. 1 ist keine Primzahl.

3) Lemma von Euklid: $\overset{c \text{ prim, dann gilt}}{\vee} (c \mid a \cdot b) \rightarrow (c \mid a) \vee (c \mid b)$

4) Primfaktorzerlegung: jede positive ganze Zahl $a \neq 1$ kann eind. * als Produkt von Primfaktoren geschrieben werden.

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots$

* hier: bis auf Reihenfolge

5) Eine Zahl c heißt gemeinsamer Teiler von a und b, wenn gilt $c \mid a \wedge c \mid b$, a und b heißen teilerfremd, wenn der einzige gemeinsame Teiler die 1 ist. Zu zwei Zahlen a, b gibt es immer einen größten gemeinsamen Teiler.

6) Brüche können gekürzt werden und ein Bruch kann so dargestellt werden, dass Zähler und Nenner teilerfremd sind.

Ein Minimaler Körper $K = \{0, 1\}$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Die Konstruktion einer Erweiterung von $\mathbb{Q}$, in der $x^2 = 2$ lösbar ist

- Wir nennen die positive Lösung $\sqrt{2}$

Lemma 1.3.4 $\sqrt{2} \notin \mathbb{Q}$

Bew. Widerspruchsann.: $\sqrt{2} \in \mathbb{Q}$ und daher gibt es eine Darstellung $\sqrt{2} = \frac{p}{q}$ und p, q sind teilerfremd. Insbes. sind nicht beide durch 2 teilbar.

$\frac{p^2}{q^2} = 2 \Leftrightarrow \quad p^2 = 2q^2 \rightarrow 2 | p^2 \Rightarrow 2 | p \Rightarrow 2^2 | p^2$

$p^2 = 2^2 r^2$ mit $r = \frac{p}{2} \rightarrow 2^2 r^2 = 2q^2 \Rightarrow 2r^2 = q^2 \Rightarrow 2 | q$ ↯

Lemma 1.3.5: Für $a,b \in \mathbb{Q}$ gilt $a + b\sqrt{2} = 0 \Leftrightarrow a = 0 \wedge b = 0$

Bew.: „$\Leftarrow$" ist offensichtlich

„$\Rightarrow$" Widerspruchsann.: es gibt $a,b \in \mathbb{Q}$ mit $a \neq 0 \vee b \neq 0$ und $a + b\sqrt{2} = 0$

Zunächst gilt, wenn eine von beiden von 0 versch. ist, müssen es beide sein, da sonst entweder a oder $\sqrt{2}b$ stehenbleibt und nicht 0 wären. Wir können schreiben $\sqrt{2} = -ab^{-1} \rightarrow \sqrt{2}$ ist rational ↯

Wir definieren: $\mathbb{Q}(\sqrt{2}) = \{ a + \sqrt{2}b \in \mathbb{R} \mid a,b \in \mathbb{Q} \}$ „$\mathbb{Q}$ adjungiert $\sqrt{2}$".

Satz 1.3.6: $\mathbb{Q}(\sqrt{2})$ ist ein echter Teilkörper von $\mathbb{R}$, der $\mathbb{Q}$ als echten Teilkörper enthält. Er ist der kleinste Teilkörper von $\mathbb{R}$ der $\sqrt{2}$ enthält.

Bew.: 1) Zeige: $\mathbb{Q}(\sqrt{2})$ ist ein Körper bzgl. „+" & „·" aus $\mathbb{R}$

a) Für $a + \sqrt{2}b$ und $a' + \sqrt{2}b'$ liegen auch ihre Summe & Produkt in $\mathbb{Q}(\sqrt{2})$.

$(a + \sqrt{2}b) + (a' + \sqrt{2}b') = (a + a') + \sqrt{2}(b + b')$ ✓

$(a + \sqrt{2}b) \cdot (a' + \sqrt{2}b') = (aa' + 2bb') + \sqrt{2}(a'b + ab')$

b) Eindeutigkeit der „0" und von $(-a)$ sei „0" das Element mit $a = b = 0$. Dann ist die „0" in $\mathbb{R}$ und nach Lemma 1.3.5 ist dies die einzige „0" in $\mathbb{Q}(\sqrt{2})$. Zu $a + \sqrt{2}b$ ist $-a + \sqrt{2}(-b)$ das additiv Inverse.

c) Gruppeneigenschaften der Multiplikation $1 = 1 + \sqrt{2}\,0$ ist neutrales Element

Inverses: $a + \sqrt{2}b \neq 0 \quad (a + \sqrt{2}b)^{-1}$ in $\mathbb{R}$ ist $\frac{1}{a + \sqrt{2}b}$

$$\frac{1}{a+\sqrt{2}b} = \frac{a-\sqrt{2}b}{(a+\sqrt{2}b)(a-\sqrt{2}b)} = \frac{a-\sqrt{2}b}{a^2-2b^2} = \underbrace{\frac{a}{a^2-2b^2}}_{\in\mathbb{Q}} - \sqrt{2}\,\underbrace{\frac{b}{a^2-2b^2}}_{\in\mathbb{Q}} \in \mathbb{Q}(\sqrt{2})$$

Es bleibt zu zeigen: es gibt keinen kleineren Teilkörper von $\mathbb{R}$ mit $\sqrt{2}$

a) Jeder Teilkörper K von $\mathbb{R}$ enthält $\mathbb{Q}$, denn:

$1 \in K \Rightarrow 1+1 = 2 \in K \rightarrow n \cdot 1 \in K \ (\forall n \in \mathbb{Z}) \Rightarrow \mathbb{Z} \subset K$

$\mathbb{Z}$ ist additive Gruppe, aber $n^{-1} \notin \mathbb{Z}$ $n^{-1} \in K$

$m \cdot n^{-1} \in K$ für $m, n \in \mathbb{Z}$ $n \neq 0$

b) Sei nun $K \subset \mathbb{R}$ Teilkörper mit $\mathbb{Q} \subset K$ und $\sqrt{2} \in K$

Dann gilt $a + \sqrt{2}b \in K \ \forall a, b \in \mathbb{Q} \Rightarrow \mathbb{Q}(\sqrt{2}) \subset K$

und damit gibt es keinen echten Teilkörper von $\mathbb{Q}(\sqrt{2})$ der $\mathbb{Q}$ und $\sqrt{2}$ enthält

Alternativ können wir $\mathbb{Q}(\sqrt{2})$ über das kartesische Produkt definieren:

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q} \times \mathbb{Q}$ $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Q} \times \mathbb{Q}$

$\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} a+a' \\ b+b' \end{pmatrix}$

$\begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} aa' + 2bb' \\ a'b + b'a \end{pmatrix}$