Def. 4 Eine Menge $\mathbb{K}$ mit zwei Abbildungen $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (heißen Addition und Multiplikation; wir werden $a \cdot b$ bzw. $a + b$ statt $\cdot(a, b)$, $+(a, b)$ schreiben) ist ein kommutativer Ring, falls:

(R1) $(\mathbb{K}, +)$ ist eine abel'sche Gruppe, deren neutrales Element werden wir mit 0 bezeichen;

(R2) die Multiplikation „$\cdot$" ist assoziativ und kommutativ.

(R3) es gilt das Distributivgesetz, d. h. für alle $a, b, c \in \mathbb{K}$ ist $a \cdot (b + c) = a \cdot b + a \cdot c$.

Bsp. $(\mathbb{R}, \cdot, +)$ und $(\mathbb{C}, \cdot, +)$ sind kommutative Ringe.

Lemma 4 $(\mathbb{K}, \cdot, +)$ sei ein kommutativer Ring. Dann ist $k \cdot 0 = 0$ (für alle $k \in \mathbb{K}$)

Beweis. $k \cdot 0 = k \cdot (0 + 0) \overset{\text{Distributivgesetz}}{=} k \cdot 0 + k \cdot 0 \qquad (*)$.

Wir addieren $-(0 \cdot k)$ zu den Seiten der Gleichung $(*)$: $0 = k \cdot 0$. $\square$

Kommutativer Ring $(\mathbb{Z}_q, +, \cdot)$

Wir werden auf $\mathbb{Z}_q$ die Struktur eines kommutativen Rings definieren. $(\mathbb{Z}, \overset{\mathrm{mod}\ q}{+})$ ist schon eine abel'sche Gruppe, wir müssen „$\cdot$“ definieren. Setze $[a] \overset{\mathrm{mod}\ q}{\cdot} [b] := [a \cdot b]$.

Bsp. $[1] \overset{\mathrm{mod}\ 5}{\cdot} [2] = [2]$, $[2] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [6] = [1]$, $[4] \overset{\mathrm{mod}\ 5}{\cdot} [3] = [12] = [2]$.

Bemerkung Die Multiplikation $\overset{\mathrm{mod}\ q}{\cdot}$ ist wohldefiniert:falls wir statt a und b die anderen Repräsentanten der Äquivalenzklassen $[a]$ und $[b]$ nehmen, wird das Ergebnis nicht geändert. Tatsächlich,

$$[a + k_1 \cdot q] \overset{\mathrm{mod}\ q}{\cdot} [b + k_2 \cdot q] = [(a + k_1 \cdot q) \cdot (b + k_2 \cdot q)] =$$
$$[a \cdot b + \underbrace{(k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot q)}_{\in \mathbb{Z}} \cdot q] = [a \cdot b].$$

Beweis von (R2) und (R3)

ist wie in Lemma 3

(R3) $[a] \overset{\text{mod } q}{\cdot} ([b] \overset{\text{mod } q}{+} [c]) = [a \cdot (b + c)] = [a \cdot b + a \cdot c] = [a] \overset{\text{mod } q}{\cdot} [b] \overset{\text{mod } q}{+} [a] \overset{\text{mod } q}{\cdot} [c]$.

Rechnen Sie selbst in $\mathbb{Z}_5$

$$[2] \cdot [5] + [6] \cdot [3] + [7] \cdot [4] =$$

$$= [2] \cdot [0] + [1] \cdot [3] + [2] \cdot [-1] = [0] + [3] - [2] = [1].$$

Rechnen Sie bitte noch einmal in $\mathbb{Z}_5$

$$[153] \cdot [1723] + ([1600] \cdot [371] - [3]) \cdot [6] =$$

$$[3] \cdot [3] + ([0] - [3]) \cdot [1] = [9 - 3] = [6] = [1]$$

Anwendung: Teilbarkeitsregeln im Dezimalsystem

Seien $\alpha_n, \alpha_{n-1}, ..., \alpha_0 \in \{0, ..., 9\}$.
$\alpha_n\alpha_{n-1}...\alpha_0$ sei die Zahl $\alpha_n \cdot 10^n + ... + \alpha_0$.
(Bsp. $237 = 2 \cdot 100 + 3 \cdot 10 + 7$).
Frage: $2 \mid \alpha_n\alpha_{n-1}...\alpha_0$*?* (In Worten: teilt 2 die Zahl $\alpha_n\alpha_{n-1}...\alpha_0$)?
Die Antwort wissen Sie seit der Schule (die Zahl ist gerade g.d.w. die letze Ziffer 0,2,4,6, oder 8 ist); jetzt werden wir diese Antwort beweisen; die Methode erlaubt es uns, Teilbarkeitsregeln für beliebige Zahl selber zu konstruieren.
Frage umformulieren: *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_2$*?*
Weil $[a] = [0]$ (in $\mathbb{Z}_2$) g.d.w. $2 \mid a - 0$.
Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_2$*?*
Ausrechnen:

$$[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [\alpha_n \cdot 10^n] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_0 \cdot 1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [10^n] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [10] \overset{\text{mod } 2}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 2}{+} ... \overset{\text{mod } 2}{+} [\alpha_1] \overset{\text{mod } 2}{\cdot} [0] \overset{\text{mod } 2}{+} [\alpha_0] \overset{\text{mod } 2}{\cdot} [1]$$
$$= [\alpha_n \cdot 0 + ... + \alpha_1 \cdot 0 + \alpha_0 \cdot 1] = [\alpha_0].$$

Antwort: $[\alpha_n\alpha_{n-1}...\alpha_0] = [0] \iff [\alpha_0] = [0]$ in $\mathbb{Z}_2$
Antwort umformulieren: $\alpha_n\alpha_{n-1}...\alpha_0$ ist g.d. durch 2 teilbar, wenn α_0 durch 2 teilbar ist.

Frage: $3 \mid \alpha_n\alpha_{n-1}...\alpha_0$*?*

Frage umformulieren: *Ist* $[\alpha_n \cdot 10^n + ... + \alpha_0 \cdot 1] = [0]$ *in* $\mathbb{Z}_3$*?*

Wir rechnen $[10^k] = \underbrace{[10] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{\cdot} ... \overset{\text{mod } 3}{\cdot} [10]}_{k \text{ mal}}$ in $\mathbb{Z}_3$ aus:

k	$[10^k]$ in $\mathbb{Z}_3$
0	$[1]$
1	$[10] = [3 \cdot 3 + 1] = [1]$
2	$[10^2] = [10] \cdot [10] = [1] \cdot [1] = [1]$
3	$[10^3] = [10^2 \cdot 10] = [1] \cdot [1] = [1]$
$\vdots$	$\vdots$

Deswegen:

$$
\begin{aligned}
&[\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 + \alpha_0 \cdot 1] \\
&= [\alpha_n] \overset{\text{mod } 3}{\cdot} [10^n] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [10] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
&= [\alpha_n] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} ... \overset{\text{mod } 3}{+} [\alpha_1] \overset{\text{mod } 3}{\cdot} [1] \overset{\text{mod } 3}{+} [\alpha_0] \overset{\text{mod } 3}{\cdot} [1] \\
&= [\alpha_n + ... + \alpha_1 + \alpha_0].
\end{aligned}
$$

Antwort: $\alpha_n\alpha_{n-1}...\alpha_0$ *ist g.d. durch 3 teilbar, wenn* $\alpha_n + \alpha_{n-1} + ... + \alpha_0$ *durch 3 teilbar ist.*

Frage: $4 \mid \alpha_n\alpha_{n-1}...\alpha_0$? *Ist* $[\alpha_n\alpha_{n-1}...\alpha_0] = [0]$ *in* $\mathbb{Z}_4$?

Ausrechnen 10^k in $\mathbb{Z}_4$:

k	$[10^k]$ in $\mathbb{Z}_4$
0	$[1]$
1	$[2]$
2	$[2] \overset{\text{mod } 4}{\cdot} [2] = [0]$
3	$[2] \overset{\text{mod } 4}{\cdot} [0] = [0]$
$\vdots$	$\vdots$
$n \geq 3$	$[2] \overset{\text{mod } 4}{\cdot} [0] = 0$

Antwort: $\alpha_n\alpha_{n-1}...\alpha_0$ *ist g.d. durch 4 teilbar, wenn* $2 \cdot \alpha_1 + \alpha_0$ *durch 4 teilbar ist.*

Bsp. 16 *ist durch 4 teilbar, da* $2 \cdot 1 + 1 \cdot 6 = 8$ *durch 4 teilbar ist.*

$$
\begin{aligned}
&[\alpha_n \cdot 10^n + ... + \alpha_1 \cdot 10 \cdot \alpha_0 \cdot 1] \\
&= [\alpha_n] \overset{\text{mod } 4}{\cdot} [10^n] \overset{\text{mod } 4}{+} ... \overset{\text{mod } 4}{+} [\alpha_1] \overset{\text{mod } 4}{\cdot} [10] \overset{\text{mod } 4}{+} [\alpha_0] \overset{\text{mod } 4}{\cdot} [1] \\
&= [\alpha_n] \overset{\text{mod } 4}{\cdot} [0] \overset{\text{mod } 4}{+} ... \overset{\text{mod } 4}{+} [\alpha_1] \overset{\text{mod } 4}{\cdot} [2] \overset{\text{mod } 4}{+} \alpha_0 \overset{\text{mod } 4}{\cdot} [1] \\
&= [2 \cdot \alpha_1 + \alpha_0].
\end{aligned}
$$

Frage: $7 \mid \alpha_n\alpha_{n-1}...\alpha_0$?

Ausrechnen 10^k in $\mathbb{Z}_7$:

k	$[10^k]$ in $\mathbb{Z}_7$
0	$[1]$
1	$[3]$
2	$[3] \overset{\text{mod } 7}{\cdot} [3] = [9] = [2]$
3	$[3] \overset{\text{mod } 7}{\cdot} [2] = [6] = [-1]$
4	$[3] \overset{\text{mod } 7}{\cdot} [-1] = [-3]$
5	$[3] \overset{\text{mod } 7}{\cdot} [-3] = [-9] = [-2]$
6	$[3] \overset{\text{mod } 7}{\cdot} [-2] = [-6] = [1]$
$\vdots$	$\vdots$
$6k$	$[1]$
$6k+1$	$[3]$
$6k+2$	$[2]$
$6k+3$	$[-1]$
$6k+4$	$[-3]$
$6k+5$	$[-2]$
$\vdots$	$\vdots$

Bsp. 9387480337647754305649 ist durch 7 teilbar, weil

$$1\cdot 9+3\cdot 4+2\cdot 6-1\cdot 5-3\cdot 0-2\cdot 3$$
$$+1\cdot 4+3\cdot 5+2\cdot 7-1\cdot 7-3\cdot 4-2\cdot 6$$
$$+1\cdot 7+3\cdot 3+2\cdot 3-1\cdot 0-3\cdot 8-2\cdot 4$$
$$+1\cdot 7+3\cdot 8+2\cdot 3-1\cdot 9-3\cdot 0-2\cdot 0$$
$$= 42 \text{ durch 7 teilbar ist.}$$

Antwort: $\alpha_n...\alpha_0$ *ist g.d. durch 7 teilbar,* wenn (in $\mathbb{Z}_7$)

$$10^0\cdot\alpha_0+10^1\cdot\alpha_1+10^2\cdot\alpha_2+10^3\cdot\alpha_3+10^4\cdot\alpha_4+10^5\cdot\alpha_5+...+$$
$$10^{6k}\cdot\alpha_{6k}+10^{6k+1}\cdot\alpha_{6k+1}+10^{6k+2}\cdot\alpha_{6k+2}+10^{6k+3}\cdot\alpha_{6k+3}+10^{6k+4}\cdot\alpha_{6k+4}+$$
$$10^{6k+5}\cdot\alpha_{6k+5}+... \overset{\text{in } \mathbb{Z}_7}{=} \alpha_0+3\alpha_1+2\alpha_2-\alpha_3-3\alpha_4-2\alpha_5$$
$$+...+\alpha_{6k}+3\alpha_{6k+1}+2\alpha_{6k+2}-\alpha_{6k+3}-3\alpha_{6k+4}-2\alpha_{6k+5}+...$$

gleich Null (in $\mathbb{Z}_7$) ist; also wenn das, was rechts steht, durch 7 teilbar ist.

Zu Hause:

Teilbarkeitsregel für 13 und 37. Hinweis: $37 \mid 999 = 1000 - 1$, $13 \mid 999999 = 10^7 - 1$.

Mit diesen Methoden kann man mehrere Zahlentheoretische Aufgaben lösen

BspAufgabe: Z.z.: $27 \mid 10^n + 18n - 1$. **Umformulieren:** Z.z.: $[10^n + 18n - 1] = [0]$ in $\mathbb{Z}_{27}$

Ausrechnen in $\mathbb{Z}_{27}$:

k	$[10^k]$ in $\mathbb{Z}_{27}$
0	$[1]$
1	$[10]$
2	$[100] = [4 \cdot 27 - 8] = [-8]$
3	$[10] \overset{\text{mod } 7}{\cdot} [-8] = [-81 + 1] = [1]$
$\vdots$	$\vdots$
$3k$	$[1]$
$3k+1$	$[10]$
$3k+2$	$[-8]$
$\vdots$	$\vdots$

Für $n = 3k$ ist $[10^{3k} + 18 \cdot 3 \cdot k - 1] = [1 + 0 - 1] = [0]$,

Für $n = 3k + 1$ ist

$[10^{3k+1} + 18 \cdot (3 \cdot k + 1) - 1] = [10 + 18 - 1] = [27] = [0]$,

Für $n = 3k + 2$ ist

$[10^{3k+2} + 18 \cdot (3 \cdot k + 2) - 1] = [-8 + 18 \cdot 2 - 1] = [27] = [0]$. □

Def. 5 *Seien* $a, b \in \mathbb{Z}$. *Grösster gemeinsamer Teiler von* a, b *(Bezeichnung:* $ggT(a,b)$ *) ist die grösste Zahl* $m \in \mathbb{N}$ *s.d.* $m \vdots a$ *und* $m \vdots b$. $ggT(a,b)$ *existiert g.d.w.* $(a,b) \neq (0,0)$. *Ist* $ggT(a,b) = 1$, *so heißen* a *und* b *teilerfremd.*

Satz 3 *Seien* $a, b \in \mathbb{Z}$, $(a,b) \neq (0,0)$. *Dann gilt: Es gibt* $n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a,b)$.

Wir beweisen zuerst die folgende

Hilfsaussage: $ggT(a,b) = ggT(a-b,b)$. $\quad (*)$

Tatsächlich, $\begin{array}{c} x \vdots a \\ k_1 x = a \end{array}$ und $\begin{array}{c} x \vdots b \\ k_2 x = b \end{array} \Rightarrow \begin{array}{c} x \vdots a-b \\ (k_1 - k_2)x = a - b, \end{array}$

also die Menge

$A := \{\text{alle gem. Teiler von } a, b\}$ ist eine Teilmenge von

$B := \{\text{alle gem. Teiler von } a-b, b\}$ (d.h., $A \subseteq B$).

Analog gilt:

$\begin{array}{c} x \vdots a \\ k_1 x = a - b \end{array}$ und $\begin{array}{c} x \vdots a-b \\ k_2 x = b \end{array} \Rightarrow \begin{array}{c} x \vdots b \\ (k_1 - k_2)x = b, \end{array}$

also die Menge

$A := \{\text{alle gem. Teiler von } a, b\}$ enthält alle Elemente von

$B := \{\text{alle gem. Teiler von } a-b, b\}$ (d.h., $A \supseteq B$).

Also, $A = B$, und die grössten Elemente der Mengen sind ebenfalls gleich.

Wied. – Satz 3 *Seien* $a, b \in \mathbb{Z}$, $(a, b) \neq (0, 0)$. *Dann gilt: Es gibt* $n, m \in \mathbb{Z}$ *s.d.* $na + mb = ggT(a, b)$.

Beweis des Satzes: OBdA ist $a > 0$, $b > 0$. Induktion in $N := a + b$.

IA Falls $N = a + b = 2$, ist der Satz offensichtlich.

IV Angenommen für alle $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, $a + b \leq N$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

IS Z.z.: Für alle $a, b \in \mathbb{Z}$, $a > 0$ $b > 0$, $a + b = N + 1$ gibt es n, m s.d. $na + bm = ggT(a, b)$.

Ist $a = b$, so ist die Aussage offensichtlich: $1 \cdot a + 0 \cdot b = ggT(a, b)$.

Angenommen, $a \neq b$, oBdA sei $a > b$. Nach (IV) und Hilfsaussage gibt es n, m_1 s.d. $n \cdot (a - b) + m_1 \cdot b = ggT(a - b, b) \overset{(*)}{=} ggT(a, b)$. Also,

$$na + \underbrace{(m_1 - n)}_{m} b = ggT(a, b),$$

□

Def. 6 Ein kommutativer Ring $(\mathbb{K}, \cdot, +)$ heißt ein Körper, falls $(\mathbb{K} \setminus \{0\}, \cdot)$ eine Gruppe ist, wobei 0 das neutrale Element in $(\mathbb{K}, +)$ ist.

Bemerkung. Die Gruppe $(\mathbb{K} \setminus \{0\}, \cdot)$ ist automatische abel'sch, weil „$\cdot$“ kommutativ ist.

Bsp. $(\mathbb{Q}, \cdot, +)$, $(\mathbb{R}, \cdot, +)$, $(\mathbb{C}, \cdot, +)$ sind Körper.

Sazt 4 $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist g.d. ein Körper, wenn q eine Primzahl ist.

Beweis $\Longleftarrow$**:** Angenommen: q ist eine Primzahl. Z.z.: $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein Körper. $(\mathbb{Z}_q, \overset{\text{mod } q}{\cdot}, \overset{\text{mod } q}{+})$ ist ein kommutativer Ring. Z.z.: $(\mathbb{Z}_q \setminus \{[0]\}, \overset{\text{mod } q}{\cdot})$ ist eine Gruppe.
(G1) ist nach Definition des Rings erfüllt, siehe (R2).
(G2) [1] ist ein neutrales Element bzgl. $\overset{\text{mod } q}{\cdot}$.
(G3) Z.z. Für jeden $[a] \neq [0]$ gibt es ein n mit $[n \cdot a] = [1]$. Da q eine Primzahl ist, ist $ggT(q, a) \in \{1, q\}$. Ist $ggT(q, a) = q$, so $q \vdots a$, also $[a] = [0]$. Ist $ggT(q, a) = 1$, so gibt es nach Satz 3 die Zahlen n, m mit $1 = m \cdot q + n \cdot a$. Dann $1 = [m \cdot q + n \cdot a] = [n \cdot a]$ (d.h., n ist ein inverses Element zu a). Offensichtlich, ist $[n] \neq 0$. (G3) ist bewiesen.
Daraus folgt auch, dass die Operation „ $\cdot$ “ wohldefiniert ist: wenn $[a] \neq 0$ und $[b] \neq 0$ sind, ist $[a] \cdot [b]$ ebenfalls nicht 0. In der Tat, wir nehmen n mit $[n] \cdot [a] = [0]$. Ist $[a] \cdot [b] = [0]$, so ist $\underbrace{[n] \cdot [a]}_{[1]} \cdot [b] = [n] \cdot [0]$; daraus folgt dass $[b] = [0]$ was uns ein Widerspruch gibt. □

Beweis $\Longrightarrow$**.** Z.z.: ist $\mathbb{K}$ eine Körper, so ist q eine Primzahl. Sei $q = m \cdot n$, wobei $n \neq q$,. Dann ist $[q] = [m \cdot n]$, also $[0] = [m] \overset{\text{mod } q}{\cdot} [n]$. Dann gilt: $[0] \overset{\text{Lemma 4}}{=} [0] \overset{\text{mod } q}{\cdot} ([n]^{-1}) = [m] \overset{\text{mod } q}{\cdot} [n] \overset{\text{mod } q}{\cdot} ([n]^{-1}) = [m]$, also $[m] = 0$, also $m = q$. □

Def. 7 *Sei* $(\mathbb{K}, \cdot, +)$ *ein Körper. Ein Unterkörper des Körpers* $\mathbb{K}$ *ist eine nicht leere Teilmenge* $\mathbb{K}' \subseteq \mathbb{K}$*, die abgeschlossen bzgl. Addition, Multiplikation, und Invertieren in* $(\mathbb{K}, +)$ *und* $(\mathbb{K} \setminus \{0\}, \cdot)$ *ist.*

Satz 5 *Unterkörper ist ein Körper (bzgl. der induzierten Operationen.)*

Beweis. $\mathbb{K}'$ ist eine Untergruppe der Gruppe $(\mathbb{K}, +) \overset{\text{Satz 2}}{\Longrightarrow}$ ist eine Gruppe. Da die Gruppe $(\mathbb{K}, +)$ abe'sch ist, ist auch $\mathbb{K}'$ abel'sch.
$\mathbb{K}' \setminus \{0\}$ ist eine Untergruppe der Gruppe $(\mathbb{K} \setminus \{0\}, \cdot) \overset{\text{Satz 2}}{\Longrightarrow}$ ist eine abel'sche Gruppe. □

Def 8. *Seien* $(\mathbb{K}_1, \cdot_1, +_1)$ und $(\mathbb{K}_2, \cdot_2, +_2)$ Körper. Eine Bijektion $\phi : \mathbb{K}_1 \to \mathbb{K}_2$ heißt ein Isomorphismus, falls für alle $a, b \in \mathbb{K}_1$ gilt:
$\phi(a \cdot_1 b) = \phi(a) \cdot_2 \phi(b)$,
$\phi(a +_1 b) = \phi(a) +_2 \phi(b)$.

Bemerkung *Körperisomorphismus ist eine Äquivalenzrelation auf der Menge aller Körper.*

Def 9. *Ein Körper* $(\mathbb{H}, \cdot, +)$ *heißt eine Körpererweiterung des Körpers* $(\mathbb{K}, \cdot, +)$*, falls* $\mathbb{H}$ *einen Unterkörper hat, der zu* $\mathbb{K}$ *isomorph ist.*

Bsp. Jede Körper ist eine Körpererweiterung von sich selbst.
$(\mathbb{R}, \cdot, +)$ ist eine Körpererweiterung von $(\mathbb{Q}, \cdot, +)$.
$(\mathbb{C}, \cdot, +)$ ist eine Körpererweiterung von $(\mathbb{R}, \cdot, +)$.

Satz 6 *Jeder Körper ist eine Körpererweiterung von* $\mathbb{Z}_q$ *oder von* $\mathbb{Q}$ (Ohne Beweis).

Satz 7 und Def. 10 *Sei $\mathbb{K} \subset \mathbb{R}$ ein Unterkörper des $(\mathbb{R}, +, \cdot)$. Ist $s \in \mathbb{K}$, $s > 0$, so ist $\mathbb{K}(\sqrt{s})$ definiert als Menge aller Zahlen der Form*

$$a + b\sqrt{s} \qquad \text{mit } a, b \in \mathbb{K}.$$

$\mathbb{K}(\sqrt{s})$ ist ein Unterkörper von $\mathbb{R}$. Ist $\sqrt{s} \notin \mathbb{K}$, so heißt $\mathbb{K}(\sqrt{s})$ eine quadratische Erweiterung von $\mathbb{K}$.
Ein Körper $\mathbb{K}$ heißt iterierte quadratische Erweiterung von $\mathbb{Q}$, wenn es eine Folge $\mathbb{Q} = \mathbb{K}_0, \mathbb{K}_1, \ldots, \mathbb{K}_n = \mathbb{K}$ mit $n \in \mathbb{N}_0$ gibt, so daß $\mathbb{K}_j$ eine quadratische Erweiterung von $\mathbb{K}_{j-1}$ ist, $j = 1, \ldots, n$.

Beweis. Sei $s \in \mathbb{K}$, $\sqrt{s} \notin \mathbb{K}$. Z.z.: $\mathbb{K}(\sqrt{s})$ ist ein Körper, d.h.,
(i) $\mathbb{K}(\sqrt{s})$ ist abgeschlossen bzgl. Addition und Subtraktion (=Invertieren bzgl. „+“) und
(ii) $\mathbb{K}(\sqrt{s}) \setminus \{0\}$ ist abgeschlossen bzgl. Multiplikation und Division (=Invertieren bzgl. „$\cdot$“).

(i) ist offensichtlich: ist $x_1 = a_1 + b_1\sqrt{s}$ und $x_2 = a_2 + b_2\sqrt{s}$, so ist $x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt{s} \in \mathbb{K}(\sqrt{s})$. Analog gilt:
$x_1 - x_2 = (a_1 - a_2) + (b_1 - b_2)\sqrt{s} \in \mathbb{K}(\sqrt{s})$.
(ii) (Multiplikation) Ist $x_1 = a_1 + b_1\sqrt{s}$ und $x_2 = a_2 + b_2\sqrt{s}$, so ist
$x_1 x_2 = (a_1 + b_1\sqrt{s})(a_2 + b_2\sqrt{s}) = a_1 a_2 + b_1 b_2 s + (a_2 b_1 + a_1 b_2)\sqrt{s} \in \mathbb{K}(\sqrt{s})$.

$\mathbb{K}(\sqrt{s})$ ist abgeschlossen bzgl. Division

Sei $a + b\sqrt{s} \neq 0$. Dann ist auch $a - b\sqrt{s} \neq 0$ (denn andernfalls wäre $(a + b\sqrt{s}) - (a - b\sqrt{s}) \neq 0$, also $b\sqrt{s} \neq 0$, folglich $b \neq 0$ und daher $\sqrt{s} = a/b$, im Widerspruch zu $\sqrt{s} \notin \mathbb{K}$),und deswegen $(a + b\sqrt{s})(a - b\sqrt{s}) = a^2 - b^2 s \neq 0$.
Es folgt

$$\frac{1}{a + b\sqrt{s}} = \frac{a - b\sqrt{s}}{(a + b\sqrt{s})(a - b\sqrt{s})} = \frac{a}{a^2 - b^2 s} - \frac{b}{a^2 - b^2 s}\sqrt{s},$$

und dies ist in $\mathbb{K}(\sqrt{s})$. Also ist $\mathbb{K}(\sqrt{s})$ auch gegenüber der Division durch Zahlen $\neq 0$ abgeschlossen und daher ein Unterkörper von $\mathbb{R}$. □

Bemerkung Man kann sich $\mathbb{C}$ als eine quadratische Erweiterung von $\mathbb{R}$ mit $s = -1$ vorstellen. Insbesondere ist die Operation invertieren $\frac{1}{x+iy} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x-iy}{x^2+y^2}$ wie oben in Bsp. mit dem beliebigen s.

Rechnen Sie bitte selbst:

Schreiben Sie $\frac{(1+2\sqrt{2})(3-4\sqrt{2})}{5+6\sqrt{2}}$ in der Form $a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$.

Rechnen Sie bitte selbst:

Jetzt sei $\mathbb{K} = \mathbb{Q}(\sqrt{2})$; d.h., $\mathbb{K} := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
Wir betrachten $\mathbb{K}(\sqrt{3})$.
Schreiben Sie $\frac{((1+2\sqrt{2})+(1-2\sqrt{2})\sqrt{3})\cdot((2-\sqrt{2}))}{1+\sqrt{2}+\sqrt{3}}$ in der Form $a + b\sqrt{3}$ mit $a, b \in \mathbb{K}$.