ALG Ü10

345 + 346!) zz: $\mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\}$ ist euklidisch vermittels der euklidischen Bewertung $H(z) := |z|^2$

Def Integritätsbereich R heißt euklidischer Ring $\Leftrightarrow \forall a \in R\setminus\{0\}, b \in R\ \exists q, r \in R: b = aq + r$ mit $r = 0 \vee H(r) < H(a)$

Dass $\mathbb{Z}[i]$ abgeschlossen bzgl. $+, \cdot, 0, 1, -$ ist, ist klar. $\Rightarrow$ Ring mit 1

Dass $\mathbb{Z}[i]$ kommutativ ist ebenso. Die Nullteilerfreiheit vererbt sich von den komplexen Zahlen, in die $\mathbb{Z}[i]$ eingebettet ist. $\Rightarrow$ Integritätsbereich

Sei $a \in \mathbb{Z}\setminus\{0\}$, $b \in \mathbb{Z}$ bel. $\Rightarrow \exists \tilde{q} \in \mathbb{C}: b = a \cdot \tilde{q}$

$q := \lfloor \tilde{q} \rfloor$ wobei $\lfloor . \rfloor : \mathbb{C} \to \mathbb{Z}[i]$ $x+iy \mapsto \lfloor x \rfloor + i \lfloor y \rfloor$ mit runden zur nächsten ganzen Zahl

$\lfloor . \rfloor : \mathbb{R} \to \mathbb{Z}$
$42{,}6 \mapsto 43$
$42{,}4 \mapsto 42$
$42{,}5 \mapsto 42$
$\vdots$

$a \cdot \tilde{q} - a \cdot q =: r \quad \Rightarrow b = a \cdot \tilde{q} = a \cdot q + r$ nun zz: $r \in \mathbb{Z}[i]$

$r = a \cdot \tilde{q} - a \cdot q = b - a \cdot q$ mit $a, b, q \in \mathbb{Z}[i] \Rightarrow r \in \mathbb{Z}[i]$

$$H(r) = |r|^2 = |a \cdot \tilde{q} - a \cdot q|^2 = |a(\tilde{q} - q)|^2 = |a|^2 \cdot |\tilde{q} - q|^2 = H(a)\, |\tilde{q} - q|^2$$

$\tilde{q} - q = x + iy$ mit $x, y \in [0, \frac{1}{2}] \Rightarrow |\tilde{q} - q|^2 = \sqrt{x^2+y^2}^{\,2} = x^2 + y^2 \in [0, \frac{1}{2}]$

$\Rightarrow H(r) = H(a)\,(x^2+y^2) < H(a)$

zz: $p = a^2 + b^2 = (a+ib)(a-ib) \in \mathbb{P}$, $a, b \in \mathbb{N} \Rightarrow a+ib, a-ib$ ... prim in $\mathbb{Z}[i]$

Wir wissen prim $\Leftrightarrow$ irreduzibel. Sei $x, y \in \mathbb{Z}[i]$ bel. mit $a + ib = x \cdot y$.

$\Rightarrow a - ib = \bar{x} \cdot \bar{y} \quad \Rightarrow p = x \cdot y \cdot \bar{x} \cdot \bar{y} = x\bar{x} \cdot y\bar{y} = |x|^2 \cdot |y|^2 \Rightarrow |x|^2 = 1 \vee |y|^2 = 1$
da p irreduzibel in $\mathbb{Z}$

Nur $\underbrace{\{1, -1, i, -i\}}_{= E(\mathbb{Z}[i])}$ liegen in $\mathbb{Z}[i]$ und haben $|x| = 1$.

$\Rightarrow$ Das Produkt $x \cdot y$ ist trivial also ist $a+ib$ (und genauso $a-ib$) irreduzibel also prim in $\mathbb{Z}[i]$.

zz: ges: Primfaktorzerlegung von $27+6i$ und $-3+4i$ in $\mathbb{Z}[i]$.

$$27 + 6i = 3(9 + 2i) = 3(1+4i)(1-2i)$$

Da $1^2 + 4^2 = 17$ und $1^2 + 2^2 = 5$ prim sind gilt nach oben, dass $1+4i$ und $1-2i$ in $\mathbb{Z}[i]$ prim sind.

$-3 + 4i = (1+2i)^2$ nach oben ebenso eine Primfaktorzerlegung in $\mathbb{Z}[i]$.

(Werte gefunden durch ausprobieren und mit einem Python Skript.)

ALG Ü10

353) Eisensteinsches Kriterium

R... faktorieller Ring $f=\sum_{i=0}^{n} a_i x^i \in R[x]$ mit Grad ≥ 1 ... primitives Polynom
$p \in R$... irreduzibel mit $p \nmid a_n$, $p | a_i$ für $i \in \{0,...,n-1\}$ und $p^2 \nmid a_0$
$\Rightarrow f$ ist irreduzibel in $R[x]$

Indirekt angenommen f ist reduzibel in $R[x]$.

$\Rightarrow \exists q, r \in R[x]$ mit $0 < grad(q), grad(r) < n$ und $f = q \cdot r$

$$q = \sum_{i=0}^{m} b_i x^i \qquad r = \sum_{i=0}^{l} c_i x^i$$

*

$$h: R[x] \longrightarrow R[x]/pR[x] \qquad \text{"mod } p\text{"}$$

$$\sum_{i=0}^{k} d_i x^i \longmapsto \sum_{i=0}^{k} (d_i x^i) + pR[x] \cong \sum_{i=0}^{k} (d_i + pR) x^i$$

$h(q) \cdot h(r) = h(q \cdot r) = h(f) = a_n x^n + pR[x]$, da alle anderen Koeffizienten von p geteilt werden.

△ $\Rightarrow \exists j,k: 0 < j,k < n \wedge h(q) = \tilde{b}_j x^j + pR[x] \wedge h(r) = \tilde{c}_k x^k + pR[x]$

Also sind alle anderen Koeffizienten von p geteilt, insbesondere $p | b_0 \wedge p | c_0$

$\Rightarrow a_0 = b_0 \cdot c_0$ ergibt $p^2 | a_0$ ↯

---

* Da $pR[x] = \langle p \rangle_{Ideal}$ ein Primideal ist (p... irreduzibel und weil in faktoriellem Ring damit prim) folgt $R[x]/pR[x]$... Integritätsbereich.

△ $h(q) \cdot h(r) = (q + pR[x])(r + pR[x]) = qr + pR[x] = a_n x^n + pR[x]$

Angenommen $h(q)$ oder $h(r)$ ist kein "Monom" $z x^\alpha + pR[x]$.

o.B.d.A. $\exists \alpha, \beta \in \{1,...,m\}: p \nmid b_\alpha \wedge p \nmid b_\beta \qquad \exists \gamma \in \{1,...,l\}: p \nmid c_\gamma$

$$\Rightarrow q \cdot r = \Big(b_\alpha x^\alpha + b_\beta x^\beta + \sum_{\substack{i=0 \\ i \neq \alpha \\ i \neq \beta}}^{m} b_i x^i\Big)\Big(c_\gamma x^\gamma + \sum_{\substack{i=0 \\ i \neq \gamma}}^{l} c_i x^i\Big) = b_\alpha c_\gamma x^{\alpha+\gamma} + b_\beta c_\gamma x^{\beta+\gamma} + \dots \neq a_n x^n$$

□

ALG Ü10

353) Eisensteinsches Kriterium

R... faktorieller Ring $f=\sum_{i=0}^{n} a_i x^i \in R[x]$ $grad(f)\geq 1$ f... primitives Polynom

$p\in R$... irreduzibel $p\nmid a_n$ $p\mid a_i$ für $i\in\{0,\dots,n-1\}$ $p^2\nmid a_0$

$\Rightarrow f$ ist irreduzibel in $R[x]$

Indirekt Angenommen f ist reduzibel in $R[x]$

$\Rightarrow \exists q,r\in R[x]$ mit $f=q\cdot r$ und $0<grad(q), grad(r)$, da f primitives Polynom ist sowie $grad(q), grad(r)<n$, damit $grad(f)=n$

$q(x)=\sum_{i=0}^{m} b_i x^i$ $r(x)=\sum_{j=0}^{l} c_j x^j$

$\Rightarrow a_0=b_0\cdot c_0$

1. Fall $p\mid b_0 \wedge p\mid c_0 \Rightarrow p^2\mid a_0$ ↯

2. Fall $p\mid b_0 \wedge p\nmid c_0 \Rightarrow \exists k\in\{1,\dots,m\}: p\nmid b_k$, da sonst $\forall k\in\{0,\dots,m\}: p\mid b_k$

$\Rightarrow p\mid q \Rightarrow p\mid f$ ↯ zu $p\nmid a_n$

Sei k mit dieser Eigenschaft minimal also $\forall i\in\{0,\dots,k-1\}: p\mid b_i \wedge p\nmid b_k$

$\Rightarrow a_k=\sum_{i=0}^{k} b_i c_{k-i} = \sum_{i=0}^{k-1} b_i c_{k-i} + b_k c_0$

$p\mid \sum_{i=0}^{k-1} b_i c_{k-i}$, da $\forall i\in\{0,\dots,k-1\}: p\mid b_i$ $p\mid a_k$ da $\forall i\in\{0,\dots,n-1\}: p\mid a_i$ und $k\in\{1,\dots,m\}$; $m=grad(q)<n$

$\Rightarrow p\mid b_k c_0$ ↯ da $p\nmid b_k$ und $p\nmid c_0$

3. Fall $p\nmid b_0 \wedge p\mid c_0$ analog

4. Fall $p\nmid b_0 \wedge p\nmid c_0 \Rightarrow p\nmid a_0$ $(a_0=b_0\cdot c_0)$ ↯

$\Rightarrow f$ ist irreduzibel in $R[x]$

□

ALG Ü10

357!) zz: K ... Körper $\quad f \in K[x] \quad grad(f) \in \{2,3\}$

f ... irreduzibel $\Leftrightarrow$ f hat keine Nullstelle in K

($\Rightarrow$) zz: f hat Nullstelle x_0 in K $\Rightarrow$ f ... reduzibel

$$f(x_0)=0 \overset{\text{Prop 5.3.3.1}}{\Longleftrightarrow} (x-x_0) \mid f(x)$$

$$\Rightarrow \exists g \in K[x]: f(x) = (x-x_0)\cdot g(x) \quad \Rightarrow f \text{ ... reduzibel}$$

$grad(g) \in \{1,2\}$

($\Leftarrow$) ① $grad(f) = 2$

zz: f ... reduzibel $\Rightarrow$ f hat eine Nullstelle in K

f ... reduzibel $\Rightarrow \exists\, q, r \in K[x]: f = q \cdot r \wedge grad(q), grad(r) = 1$

$\Rightarrow q = b_1 x + b_0 = b_1 \left(x + \frac{b_0}{b_1}\right) \quad b_1 \neq 0$, da $grad(q) = 1$

$\overset{\text{Prop 5.3.3.1}}{\Longrightarrow} -\frac{b_0}{b_1}$ ist Nullstelle von q also auch von f und liegt in K

② $grad(f) = 3$

f ... reduzibel $\Rightarrow \exists\, q, r \in K[x]: f = q \cdot r \wedge grad(q) = 1, grad(r) = 2$

$\Rightarrow$ wie oben q hat Nullstelle x_0 in K $\Rightarrow f(x_0) = 0$

ges: alle irreduziblen Polynome vom Grad höchstens 4 über $\mathbb{Z}_2$.

Für die ($\Rightarrow$) Richtung haben wir nicht verwendet, dass der grad 2 oder 3 sein muss.

Alle Polynome in denen nur x, x^2, x^3 und x^4 vorkommen haben die Nullstelle 0 und alle mit gerade vielen Summanden die Nullstelle 1.

grad 0: $\quad$ 0 ... reduzibel $\quad$ 1 ... Einheit

grad 1: $\quad x$ ... Einheit $\quad x+1$ ... irreduzibel

grad 2+3: nach oben sind irreduzibel: $x^2+x+1,\ x^3+x+1,\ x^3+x^2+1$,

grad 4: Polynome ohne Nullstellen sind: $\{x^4+x+1,\ x^4+x^2+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1\} = M$

$\forall m \in M: x \nmid m$; $(x+1)(x^3+x+1) = x^4+x^3+x^2+1 \notin M$; $(x+1)(x^3+x^2+1) = x^4+x^2+x+1 \notin M$

$(x^2+x+1)^2 = x^4+x^2+1 \in M \quad \Rightarrow x^4+x+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1$ ... irreduzibel

ALG Ü10

365) Gradsatz $K \leq E \leq L$ ... Körper zz: $[L:K] = [L:E] \cdot [E:K]$

Sei $(a_i)_{i \in I}$ eine Basis von E über K und $(b_j)_{j \in J}$ eine Basis von L über E.

zz: $(a_i b_j)_{(i,j) \in I \times J}$ ... Basis von L über K

Sei $l \in L$ bel. $\Rightarrow \exists (y_j)_{j \in J}$ in E mit $l = \sum_{j \in J} y_j b_j$, da $(b_j)_{j \in J}$ Basis.

$\forall j \in J$ $\exists (x_i)_{i \in I}$ in K mit $y_j = \sum_{i \in I} x_i a_i$, da $(a_i)_{i \in I}$ Basis von E über K.

$\Rightarrow l = \sum_{j \in J} (\sum_{i \in I} x_i a_i) b_j = \sum_{j \in J} (\sum_{i \in I} x_i a_i b_j) = \sum_{(i,j) \in I \times J} x_i a_i b_j$

$\Rightarrow (a_i b_j)_{(i,j) \in I \times J}$ erzeugt ganz L

Sei $(z_{i,j})_{(i,j) \in I \times J}$ in K mit $\sum_{(i,j) \in I \times J} z_{i,j} \cdot a_i b_j = 0$ bel.

$0 = \sum_{(i,j) \in I \times J} z_{i,j} \cdot a_i \cdot b_j = \sum_{j \in J} \underbrace{(\sum_{i \in I} z_{i,j} a_i)}_{\in E} b_j$, da $(b_j)_{j \in J}$ eine Basis ist muss

$\forall j \in J: \sum_{i \in I} \underbrace{z_{i,j}}_{\in K} a_i = 0$ gelten, da auch $(a_i)_{i \in I}$ eine Basis ist muss

$\forall j \in J$ $\forall i \in I$: $z_{i,j} = 0$ gelten. $\Rightarrow (a_i b_j)_{(i,j) \in I \times J}$ ist linear unabhängig.

$\Rightarrow (a_i b_j)_{(i,j) \in I \times J}$ ist eine Basis von L über K

$\Rightarrow [L:E] \cdot [E:K] = \dim((b_j)_{j \in J}) \cdot \dim((a_i)_{i \in I}) = \dim((a_i b_j)_{(i,j) \in I \times J}) = [L:K]$

$\square$

ALG Ü10

368) $p \in \mathbb{P}$ $\quad g(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x-1}$

zz: $g(x)$ ist in $\mathbb{Z}[x]$ irreduzibel

$$r(x) = g(x+1) = \frac{(x+1)^p - 1}{x} = \frac{\left(\sum_{k=0}^{p} \binom{p}{k} x^k\right) - 1}{x} = \frac{\sum_{k=1}^{p} \binom{p}{k} x^k}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}$$

$$= \sum_{k=0}^{p-1} \binom{p}{k+1} x^k = \sum_{k=0}^{p-1} \frac{p!}{(k+1)!(p-k-1)!} x^k = \underbrace{\frac{p!}{(p-1)!}}_{k=0} + \frac{p!}{2!(p-2)!} x + \dots + \underbrace{\frac{p!}{p!} x^{p-1}}_{k=p-1}$$

$$= p + p\left(\sum_{k=1}^{p-2} \frac{(p-1)!}{(k+1)!(p-k-1)!} x^k\right) + x^{p-1}$$

Eisensteinsches Kriterium $\quad R$ ... faktorieller Ring $\quad f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit grad ≥ 1 ... primitiv

$p \in R$ ... irreduzibel ; $p \nmid a_n$, $p \mid a_i$ für $i = 0, \dots, n-1$, $p^2 \nmid a_0$

$\Rightarrow f$ ... irreduzibel in $R[x]$

$p \geq 2$, da $p \in \mathbb{P}$

$\mathbb{Z}$ ... faktorieller Ring $\quad r \in \mathbb{Z}[x] \quad$ grad$(r) = p - 1 \geq 1$ ... primitiv

p ... prim also auch irreduzibel $\quad p \nmid \underset{a_{p-1}}{\underset{\parallel}{1}} \quad p \mid a_i$ für $i = 0, \dots, p-2$; $\quad p^2 \nmid \underset{a_0}{\underset{\parallel}{p}}$

$\Rightarrow r$ ... irreduzibel in $\mathbb{Z}[x]$

Sei $s, t \in \mathbb{Z}[x] : s(x) \cdot t(x) = g(x)$

$\Rightarrow s(x+1) \cdot t(x+1) = g(x+1) = r(x)$. $\quad \Rightarrow s(x+1) \in E(\mathbb{Z}[x]) \vee t(x+1) \in E(\mathbb{Z}[x])$

$E(\mathbb{Z}[x]) = \{1\}$ $\quad$ o.B.d.A. $s(x+1) = 1 \quad \Rightarrow s(x) = 1 \in E(\mathbb{Z}[x])$

$\Rightarrow g(x)$ ist irreduzibel

ALG Ü10

372!) ges: Minimalpolynom von $\sqrt{3}+i$ über $\mathbb{Q}$

$m(x)$ ... Minimalpolynom von $\alpha \iff m(\alpha)=0 \wedge m\neq 0 \wedge m$ ... normiert $\wedge$
m hat minimalen Grad

Grad 0: offenbar nur 0, das ist aber ausgeschlossen ↯

Grad 1: $p(x)=x+a$, da p normiert sein soll

$p(\sqrt{3}+i)=\sqrt{3}+i+a=0 \Rightarrow a=-\sqrt{3}-i\notin\mathbb{Q}$ ↯

Grad 2: $p(x)=x^2+ax+b$

$p(\sqrt{3}+i)=3+2\sqrt{3}i-1+a\sqrt{3}+ai+b=0 \Rightarrow 2\sqrt{3}+a=0 \Rightarrow a=-2\sqrt{3}\notin\mathbb{Q}$ ↯

Grad 3: $p(x)=x^3+ax^2+bx+c$

$p(\sqrt{3}+i)=8i+a(3+2\sqrt{3}i-1)+b(\sqrt{3}+i)+c=8i+3a+2\sqrt{3}ai-a+b\sqrt{3}+bi+c=0$

$\Rightarrow 8+2\sqrt{3}a+b=0 \wedge 3a-a+b\sqrt{3}+c=0$

$\Rightarrow b=-8-2\sqrt{3}a \wedge b=\frac{1}{\sqrt{3}}(-2a-c) \Rightarrow -8\sqrt{3}-6a=-2a-c$

$\Rightarrow 4a=-8\sqrt{3}+c \Rightarrow a=-2\sqrt{3}+\frac{c}{4}\notin\mathbb{Q}$ wenn $c\in\mathbb{Q}$ ↯

Grad 4: $p(x)=x^4+ax^3+bx^2+cx+d$

$p(\sqrt{3}+i)=-8+8\sqrt{3}i+a(8i)+b(2+2\sqrt{3}i)+c(\sqrt{3}+i)+d$

$=-8+2b+\sqrt{3}c+d+i(8\sqrt{3}+8a+2\sqrt{3}b+c)=0$

$\Rightarrow -8+2b+\sqrt{3}c+d=0 \wedge 8\sqrt{3}+8a+2\sqrt{3}b+c=0$

$\Rightarrow c=\frac{1}{\sqrt{3}}(8-2b-d)\in\mathbb{Q} \iff c=0 \wedge 8-2b-d=0$

$\Rightarrow 8-2b-d=0 \quad \wedge 8\sqrt{3}+8a+2\sqrt{3}b=0$

$\Rightarrow a=\frac{1}{8}(-8\sqrt{3}-2\sqrt{3}b)=-\sqrt{3}-\frac{1}{4}\sqrt{3}b=\sqrt{3}(-1-\frac{1}{4}b)\in\mathbb{Q} \iff a=0$

$\Rightarrow 8-2b-d=0 \wedge 8\sqrt{3}+2\sqrt{3}b=0 \Rightarrow 4+b=0 \Rightarrow b=-4$

$\Rightarrow 8+8-d=0 \Rightarrow d=16$

$p(x)=x^4-4x^2+16$ ist das Minimalpolynom von $\sqrt{3}+i$ über $\mathbb{Q}$

Prüfung $p(\sqrt{3}+i)=-8+8\sqrt{3}i-4(3+2\sqrt{3}i-1)+16=8+8\sqrt{3}i-12-8\sqrt{3}i+4=0$ ✓

ALG Ü10

373) ges: Grad von $\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$ über $\mathbb{Q}$

Da $\frac{\sqrt{6}\sqrt{10}}{2} = \frac{\sqrt{2}\sqrt{3}\sqrt{2}\sqrt{5}}{2} = \sqrt{3}\sqrt{5} = \sqrt{15}$ gilt

$$\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}) = \left\{ \frac{a+b\sqrt{6}+c\sqrt{10}+d\sqrt{15}+e\sqrt{6}\sqrt{10}+f\sqrt{6}\sqrt{15}+g\sqrt{10}\sqrt{15}+h\sqrt{6}\sqrt{10}\sqrt{15}}{a'+b'\sqrt{6}+c'\sqrt{10}+d'\sqrt{15}+e'\sqrt{6}\sqrt{10}+f'\sqrt{6}\sqrt{15}+g'\sqrt{10}\sqrt{15}+h'\sqrt{6}\sqrt{10}\sqrt{15}}, \right.$$
$$a,a',b,b',c,c',d,d',e,e',f,f',g,g',h,h' \in \mathbb{Q},$$
$$\left. (a',b',c',d',e',f',g',h') \neq (0,0,0,0,0,0,0,0) \right\}$$

$$= \left\{ \frac{a+b\sqrt{6}+c\sqrt{10}+e\sqrt{6}\sqrt{10}}{a'+b'\sqrt{6}+c'\sqrt{10}+e'\sqrt{6}\sqrt{10}}, a,a',b,b',c,c',e,e' \in \mathbb{Q}, (a',b',c',e') \neq (0,0,0,0) \right\}$$

$= \mathbb{Q}(\sqrt{6},\sqrt{10})$ Da $\mathbb{Q} \leq \mathbb{Q}(\sqrt{6})$, $\sqrt{6} \in \mathbb{Q}(\sqrt{6})$ ... algebraisch über $\mathbb{Q}$

(nämlich x^2-6) $\xrightarrow{\text{Satz } 6.1.3.4.(2)}$ $\mathbb{Q}(\sqrt{6}) = \mathbb{Q}[\sqrt{6}]$

$B_1 := \{1, \sqrt{6}\}$ ist l.u. da $\sqrt{6} \notin \mathbb{Q}$ und erzeugt $\mathbb{Q}[\sqrt{6}] = \mathbb{Q}(\sqrt{6})$.

$\Rightarrow B_1$ ist Basis von $\mathbb{Q}(\sqrt{6})$ über $\mathbb{Q}$

$$\mathbb{Q}(\sqrt{6}) \leq \mathbb{Q}(\sqrt{6},\sqrt{10}) = \left\{ \frac{a+b\sqrt{6}+c\sqrt{10}+d\sqrt{60}}{a'+b'\sqrt{6}+c'\sqrt{10}+d'\sqrt{60}} \,\middle|\, \begin{array}{l} a,a',b,b',c,c',d,d' \in \mathbb{Q}, \\ (a',b',c',d') \neq (0,0,0,0) \end{array} \right\}$$

$$= \left\{ \frac{x+y\sqrt{10}}{x'+y'\sqrt{10}} \,\middle|\, x,y,x',y' \in \mathbb{Q}(\sqrt{6}), (x',y') \neq (0,0) \right\} = (\mathbb{Q}(\sqrt{6}))(\sqrt{10})$$

$\sqrt{10} \in \mathbb{Q}(\sqrt{6})(\sqrt{10})$ ... algebraisch über $\mathbb{Q}(\sqrt{6})$ (nämlich x^2-10)

$\xrightarrow{6.1.3.4.(2)}$ $\mathbb{Q}(\sqrt{6})(\sqrt{10}) = \mathbb{Q}(\sqrt{6})[\sqrt{10}]$

$B_2 := \{1, \sqrt{10}\}$ erzeugt $\mathbb{Q}(\sqrt{6})[\sqrt{10}] = \mathbb{Q}(\sqrt{6},\sqrt{10})$

Sei $x = a+b\sqrt{6} \in \mathbb{Q}[\sqrt{6}] = \mathbb{Q}(\sqrt{6})$ mit $1 \cdot x = \sqrt{10}$ bel.

$\Rightarrow \sqrt{2}\sqrt{5} = \sqrt{10} = a+b\sqrt{6} = a+b\sqrt{2}\sqrt{3}$

$\Leftrightarrow \sqrt{5} = \frac{1}{\sqrt{2}}a + b\sqrt{3} = \frac{a}{2}\frac{2}{\sqrt{2}} + b\sqrt{3} = \frac{a}{2}\sqrt{\frac{4}{2}} + b\sqrt{3} = \frac{a}{2}\sqrt{2} + b\sqrt{3}$ ↯, da

$\sqrt{5} \notin \sqrt{2}\,\mathbb{Q} + \sqrt{3}\,\mathbb{Q}$ $\Rightarrow B_2$ ... l.u. $\rightarrow B_2$ ... Basis von $\mathbb{Q}(\sqrt{6},\sqrt{10})$ über $\mathbb{Q}(\sqrt{6})$

$\Rightarrow [\mathbb{Q}(\sqrt{6},\sqrt{10}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{6},\sqrt{10}) : \mathbb{Q}(\sqrt{6})] \cdot [\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 2 \cdot 2 = 4$

$\quad \| $

$[\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15}) : \mathbb{Q}]$ nach Gradsatz und

$B := B_1 \cdot B_2 = \{1, \sqrt{6}, \sqrt{10}, \sqrt{60}\}$ ist Basis von $\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15})$ über $\mathbb{Q}$

$(\sqrt{2}\sqrt{2}\sqrt{3}\sqrt{5} = 2\sqrt{15})$