Bsp für Körpererweiterung:

Es ist $\sqrt[3]{2} \in \mathbb{R} \setminus \mathbb{Q}$.

Also hat $f(X) := X^3 - 2 \in \mathbb{Q}[X]$

keine Nullstelle in $\mathbb{Q}$.

Also ist $X^3 - 2 \in \mathbb{Q}[X]$

irreduzibel, denn gäbe es eine

nichttriviale Zerlegung von $X^3 - 2$

in zwei Faktoren in $\mathbb{Q}[X]$,

dann wäre einer dieser Faktoren

von Grad 1 und es gäbe

eine Nullstelle in $\mathbb{Q}$, was nicht

so ist.

Aber natürlich ist $f(\sqrt[3]{2})$

$= (\sqrt[3]{2})^3 - 2 = 0.$

Daher ist das Minimalpolynom

$$f(X) = \mu_{\sqrt[3]{2},\mathbb{Q}}(X)$$

gefunden; vgl. Bem. 184.

Da $\sqrt[3]{2}$ algebraisch ist über $\mathbb{Q}$, ist

$$\mathbb{Q}[\sqrt[3]{2}] = \{ g(\sqrt[3]{2}) : g(X) \in \mathbb{Q}[X] \}$$

$$\| $$

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ \frac{g(\sqrt[3]{2})}{h(\sqrt[3]{2})} : g(X), h(X) \in \mathbb{Q}[X], h(\sqrt[3]{2}) \neq 0 \right\}$$

Es ist

$$\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$$

eine Körpererweiterung.

Da $\deg\left(\mu_{\sqrt[3]{2},\mathbb{Q}}(X)\right) = \deg(X^3-2) = 3$,

ist eine $\mathbb{Q}$-lineare Basis von

$\mathbb{Q}(\sqrt[3]{2})$ gegeben durch

$$\left(\left(\sqrt[3]{2}\right)^0, \left(\sqrt[3]{2}\right)^1, \left(\sqrt[3]{2}\right)^2\right)$$

Somit ist

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ a_0 + a_1\sqrt[3]{2} + a_2\left(\sqrt[3]{2}\right)^2 : a_0, a_1, a_2 \in \mathbb{Q} \right\},$$

und die Koeffizienten a_0, a_1, a_2 sind jeweils eindeutig bestimmt.

Es ist auch der Grad der Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ dadurch bestimmt: ...

... Es gilt

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

$$\overset{\text{def.}}{=} \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = 3$$

Wir rechnen in $\mathbb{Q}(\sqrt[3]{2})$.

Wir wollen $c := 1 + \sqrt[3]{2} - 2(\sqrt[3]{2})^2$ invertieren. Dafür bilden wir das Minimalpolynom von c über $\mathbb{Q}$.

Es gilt

$$c^2 = \left(1 + \sqrt[3]{2} - 2(\sqrt[3]{2})^2\right)^2$$

$$= \ldots$$

$$\ldots = 1 + \left(\sqrt[3]{2}\right)^2 + 4\left(\sqrt[3]{2}\right)^4$$

$$+ 2\sqrt[3]{2} - 4\left(\sqrt[3]{2}\right)^2$$

$$- 4\left(\sqrt[3]{2}\right)^3$$

$$= -7 + 10\sqrt[3]{2} - 3\left(\sqrt[3]{2}\right)^2$$

Es gilt

$$c^3 = \left(-7 + 10\sqrt[3]{2} - 3\left(\sqrt[3]{2}\right)^2\right)$$

$$\cdot\left(1 + \sqrt[3]{2} - 2\left(\sqrt[3]{2}\right)^2\right)$$

$$= -7 - 7\sqrt[3]{2} + 14\left(\sqrt[3]{2}\right)^2$$

$$-40 + 10\sqrt[3]{2} + 10\left(\sqrt[3]{2}\right)^2$$

$$-6 + 12\sqrt[3]{2} - 3\left(\sqrt[3]{2}\right)^2$$

$$= -53 + 15\sqrt[3]{2} + 21\left(\sqrt[3]{2}\right)^2$$

Es ist (c^0, c^1, c^2) $\mathbb{Q}$-l.u.

Suchen wir $a_0, a_1, a_2 \in \mathbb{Q}$

mit

$$c^3 = a_0 + a_1 c + a_2 c^2 .$$

LGS:

$$\begin{array}{l} (\sqrt[3]{2})^0: \\ (\sqrt[3]{2})^1: \\ (\sqrt[3]{2})^2: \\ \quad\ (a_0) \end{array} \left(\begin{array}{ccc|c} 1 & 1 & -7 & -53 \\ 0 & 1 & 10 & 15 \\ 0 & -2 & -3 & 21 \end{array}\right) \begin{array}{c} \\ \\ \\ (a_1) \end{array} \quad (a_2)$$

$$\rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & -17 & -68 \\ 0 & 1 & 10 & 15 \\ 0 & 0 & 17 & 51 \end{array}\right)$$

$$\rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & -17 \\ 0 & 1 & 0 & -15 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

Somit

$$c^3 = -17 - 15c + 3c^2 .$$

Da (c^0, c^1, c^2) $\mathbb{Q}$-l.u. ist,

ist

$$X^3 - 3X^2 + 15X + 17 \in \mathbb{Q}[X]$$

das Polynom kleinsten Grades

mit Nullstelle c. Dank Bem 184

folgt

$$\mu_{c,\mathbb{Q}}(X) = X^3 - 3X^2 + 15X + 17$$

Ferner ist

$$c^3 - 3c^2 + 15c = -17,$$

also $c^2 - 3c + 15 = -\frac{17}{c}$,

also ...

$$\dots \quad \frac{1}{c} = -\frac{1}{17}\left(c^2 - 3c + 15\right)$$

$$= -\frac{1}{17}\Big(-7 + 10\sqrt[3]{2} - 3\left(\sqrt[3]{2}\right)^2$$

$$-3 - 3\sqrt[3]{2} + 6\left(\sqrt[3]{2}\right)^2$$

$$+15\Big)$$

$$= -\frac{1}{17}\left(5 + 7\sqrt[3]{2} + 3\left(\sqrt[3]{2}\right)^2\right)$$

Bsp für Konstruktion eines endlichen Körpers.

Wir wollen einen Körper mit 8 Elementen konstruieren.

Es ist $8 = 2^3$.

Es ist

$$X^3 + X + 1 \in \mathbb{F}_2[X]$$

irreduzibel: wäre es zerlegbar in einen Faktor vom Grad 2 und einen Faktor vom Grad 1, dann hätte es eine Nullstelle in $\mathbb{F}_2[X]$. Die hat es aber nicht.

Sei $\mathbb{F}_8 := \mathbb{F}_2[X] / (X^3 + X + 1)$.

Sei $\beta := X + (X^3 + X + 1)$,

Dann ist

$$\mathbb{F}_8 = \mathbb{F}_2(\beta) = \mathbb{F}_2[\beta].$$

Es ist $\mu_{\beta,\mathbb{F}_2}(X) = X^3 + X + 1$,

Es ist $0 = \mu_{\beta,\mathbb{F}_2}(\beta) = \beta^3 + \beta + 1$,

Also ist $\boxed{\beta^3 = \beta + 1.}$

Wegen $\operatorname{char}(\mathbb{F}_2) = 2$ ist

auch $\boxed{2 \cdot \beta = 0}$

$= 3 - 1$

Schließlich ist $(\beta^0, \beta^1, \beta^2)$

eine $\mathbb{F}_2$-lineare Basis

von $\mathbb{F}_8$.

Also

$$\mathbb{F}_8 = \{ a_0 + a_1\beta + a_2\beta^2 : a_0, a_1, a_2 \in \mathbb{F}_2 \}$$

$$= \{ 0, 1, \beta, 1+\beta, \beta^2, 1+\beta^2, \beta+\beta^2, 1+\beta+\beta^2 \}$$

Also

$(+)$	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
0	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
1	1	0	$1+\beta$	β	$1+\beta^2$	β^2	$1+\beta+\beta^2$	$\beta+\beta^2$
β	β	$1+\beta$	0	1	$\beta+\beta^2$	$1+\beta+\beta^2$	β^2	$1+\beta^2$
$1+\beta$	$1+\beta$	β	1	0	$1+\beta+\beta^2$	$\beta+\beta^2$	$1+\beta^2$	β^2
β^2	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$	0	1	β	$1+\beta$
$1+\beta^2$	$1+\beta^2$	β^2	$1+\beta+\beta^2$	$\beta+\beta^2$	1	0	$1+\beta$	β
$\beta+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$	β^2	$1+\beta^2$	β	$1+\beta$	0	1
$1+\beta+\beta^2$	$1+\beta+\beta^2$	$\beta+\beta^2$	$1+\beta^2$	β^2	$1+\beta$	β	1	0

Und

$(\cdot)$	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
0	0	0	0	0	0	0	0	0
1	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
β	0	β	β^2	$\beta+\beta^2$	$1+\beta$	1	$1+\beta+\beta^2$	$1+\beta^2$
$1+\beta$	0	$1+\beta$	$\beta+\beta^2$	$1+\beta^2$	$1+\beta+\beta^2$	β^2	1	β
β^2	0	β^2	$1+\beta$	$1+\beta+\beta^2$	$\beta+\beta^2$	β	$1+\beta^2$	1
$1+\beta^2$	0	$1+\beta^2$	1	β^2	β	$1+\beta+\beta^2$	$1+\beta$	$\beta+\beta^2$
$\beta+\beta^2$	0	$\beta+\beta^2$	$1+\beta+\beta^2$	1	$1+\beta^2$	$1+\beta$	β	β^2
$1+\beta+\beta^2$	0	$1+\beta+\beta^2$	$1+\beta^2$	β	1	$\beta+\beta^2$	β^2	$1+\beta$

Man kann aus der Multiplikationstafel die jeweiligen Inversen ablesen. Z.B. $\beta^{-1} = 1+\beta^2$

Vorsicht: $\mathbb{F}_8 \neq \mathbb{Z}/(8)$.