Aufgabe (23).

(a) *Bestimmen Sie die Minimalpolynome aller Zahlen aus $\mathbb{Q}[i] \setminus \mathbb{Q}$. Sie gehen alle durch Substitution aus $x^2 + 1$ hervor.*

(b) *Zeigen Sie: Der Grad eines Primpolynomes aus $\mathbb{Q}[x]$, das eine Nullstelle in einer n-dimensionalen Körpererweiterung von $\mathbb{Q}$ besitzt, ist ein Teiler von n.*

Zu (a). Das Polynom $p := x^2 + 1$ ist das Minimalpolynom von i über $\mathbb{Q}$ und somit irreduzibel. Sei $a + bi \in \mathbb{Q}[i] \setminus \mathbb{Q}$, wobei a und $b \in \mathbb{Q}$ seien und $b \neq 0$.[1] Der Einsetzhomomorphismus $\pi_{(x-a)/b} : \mathbb{Q}[x] \to \mathbb{Q}[x]$ ist sogar ein Automorphismus von $\mathbb{Q}[x]$, denn es existiert eine inverse Abbildung:

$$\pi_{(x-a)/b} \circ \pi_{bx+a} = \mathrm{id} = \pi_{bx+a} \circ \pi_{(x-a)/b}.$$

Irreduzible Elemente werden unter Automorphismen wieder auf irreduzible Elemente abgebildet. Auch die Multiplikation mit Einheiten ändert nichts an der Eigenschaft, irreduzibel zu sein. Also ist

$$q := b^2\, \pi_{(x-a)/b}(p) = b^2\, p(\frac{x-a}{b}) = b^2\, (\frac{1}{b^2}x^2 - 2\frac{a}{b}x + \frac{a^2}{b^2} + 1) = x^2 - 2ab\, x + a^2 + b^2$$

ebenfalls irreduzibel. Weiterhin gilt

$$q(a + bi) = b^2\, p(\frac{a + bi - a}{b}) = b^2\, p(i) = 0.$$

Da also q irreduzibel ist, $a + bi$ als Nullstelle besitzt und offensichtlich normiert ist, ist q das Minimalpolynom von $a + bi$ über $\mathbb{Q}$.

Zu (b). Seien $\mathbb{Q} \lhd L$ eine n-dimensionale Körpererweiterung von $\mathbb{Q}$ und $p \in \mathbb{Q}[x]$ ein Primpolynom[2] mit einer Nullstelle $\alpha \in L$. Damit ist α algebraisch über $\mathbb{Q}$, und es gilt

$$\mathbb{Q} \lhd \mathbb{Q}[\alpha] \lhd L.$$

Das Minimalpolynom von α über $\mathbb{Q}$ ist p.

Der Grad der Körpererweiterung $\mathbb{Q} \lhd \mathbb{Q}[\alpha]$ ist nach Beobachtung 6 in § 11 gleich dem Grad des Minimalpolynomes von α und somit gleich dem Grad von p. Nach der Dimensionsformel § 11 Satz 13 folgt nun

$$n = [L : \mathbb{Q}] = [\, L : \mathbb{Q}[\alpha]\,] \cdot \underbrace{[\, \mathbb{Q}[\alpha] : \mathbb{Q}\,]}_{=\deg p},$$

und $\deg p$ ist ein Teiler von n.

[1] Alle Zahlen aus $\mathbb{Q}[i] \setminus \mathbb{Q}$ lassen sich so darstellen, da $(1, i)$ eine $\mathbb{Q}$-Basis von $\mathbb{Q}[i] \setminus \mathbb{Q}$ ist.

[2] In der Vorlesung wurden „Primpolynome“ als normierte Primelemente eines Polynomringes eingeführt.