Aufgabe (33). *In $\mathbb{Q}[x,y,z]$ seien $f_1 = x^2 - 2$, $f_2 = y^2 - 3$ und $f_3 = x + y - z$. Sei $I = \langle f_1, f_2, f_3 \rangle_{\mathbb{Q}[x,y,z]}$ das von f_1, f_2, f_3 in $\mathbb{Q}[x,y,z]$ erzeugte Ideal. Zeigen Sie:*

$$I \cap \mathbb{Q}[z] = \langle g \rangle_{\mathbb{Q}[z]} \quad \textit{mit } g = \mathsf{MiPo}_{\mathbb{Q}}(\sqrt{2} + \sqrt{3})$$

Wiederholung. *Aus einer früheren Übungsaufgabe wissen wir*

$$g = \mathsf{MiPo}_{\mathbb{Q}}(\sqrt{2} + \sqrt{3}) = z^4 - 10z^2 + 1 \in \mathbb{Q}[z].$$

Wir zeigen zunächst, dass $g \in I$ gilt. Der Ring $R_z = \mathbb{Q}[x,y,z]$ lässt sich auch als Polynomring $(\mathbb{Q}[x,y])[z]$ in der Variablen z über $\mathbb{Q}[x,y]$ auffassen. Division in R_z von g mit Rest durch ein lineares Polynom $z - a$ ergibt wie üblich

$$g = u \cdot (z - a) + g(a) \ .$$

Im Spezialfall $a = x + y$ und $-f_3 = z - (x + y)$ bedeutet dies mit $r_3 = g(x + y)$ und $p_3 = -u$:

$$g = p_3 f_3 + r_3 \ .$$

Ausmultipliziert ergibt sich

$$r_3 = g(x+y) = (x+y)^4 - 10(x+y)^2 + 1 = y^4 + 4xy^3 + (6x^2 - 10)y^2 + (4x^3 - 20x)y + 1 - 10x^2 + x^4 \ .$$

In $R_y = (\mathbb{Q}[x,z])[y]$ kann nun r_3 durch $f_2 = y^2 - 3$ dividiert werden. Man erhält

$$r_3 = p_2 f_2 + r_2$$

mit $p_2 = (y^2 + 4xy + 6x^2 - 7)$ und $r_2 = (4x^3 - 8x)y - 20 + 8x^2 + x^4 = x^4 + 4x^3y + 8x^2 - 8xy - 20$.

Schließlich kann jetzt noch in $R_x = (\mathbb{Q}[y,z])[x]$ der Rest r_2 durch $f_1 = x^2 - 2$ dividiert werden. Man erhält

$$r_2 = p_1 f_1 + 0$$

mit $p_1 = x^2 + 4xy + 10$.

Insgesamt folgt

$$g = p_3 f_3 + p_2 f_2 + p_1 f_1 \in I.$$

Da $g \in I \cap \mathbb{Q}[z]$, ist auch $\langle g \rangle_{\mathbb{Q}[z]} \subseteq I \cap \mathbb{Q}[z]$. Da g als Minimalpolynom unzerlegbar ist, ist $\langle g \rangle_{\mathbb{Q}[z]}$ ein maximales Ideal in $\mathbb{Q}[z]$. Als Schnitt des Ideales I und des Unterrings $\mathbb{Q}[z]$ von $\mathbb{Q}[x,y,z]$ ist auch $I \cap \mathbb{Q}[z]$ ein Ideal von $\mathbb{Q}[z]$. Wegen der Maximalität von $\langle g \rangle_{\mathbb{Q}[z]}$ muss daher gelten

$$\langle g \rangle_{\mathbb{Q}[z]} = I \cap \mathbb{Q}[z] \text{ oder } I \cap \mathbb{Q}[z] = \mathbb{Q}[z].$$

Wir zeigen nun, dass $I \cap \mathbb{Q}[z] \neq \mathbb{Q}[z]$, indem wir zeigen, dass $1 \notin I$ gilt.

Angenommen, das wäre der Fall. Dann existierten Polynome q_1, q_2 und $q_3 \in \mathbb{Q}[x,y,z]$ mit $1 = q_1 f_1 + q_2 f_2 + q_3 f_3$. Offensichtlich ist das Tripel $v = (\sqrt{2}, \sqrt{3}, \sqrt{2} + \sqrt{3}) \in \mathbb{C}^3$ eine gemeinsame Nullstelle von f_1, f_2 und f_3. Dann ist aber auch

$$1(v) = (q_1 f_1 + q_2 f_2 + q_3 f_3)(v) = q_1(v) f_1(v) + q_2(v) f_2(v) + q_3(v) f_3(v) = 0.$$

Widerspruch! Also ist $1 \notin I$ und damit $I \cap \mathbb{Q}[z] \neq \mathbb{Q}[z]$.

Es folgt $\langle g \rangle_{\mathbb{Q}[z]} = I \cap \mathbb{Q}[z]$ wie behauptet.