HW4

MTH 643

Due: 3 June 2026

Instructions

As always, your answer will be graded on the quality of presentation as well as the correct answer. To get a good score: write your answer neatly, use complete sentences, and *justify your work*.

1. Suppose that $(B, C, D) \in \mathbb{Z} \times \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ and $B^2 - 4C$ is not a square. Consider the equation

$$X^2 + BXY + CY^2 = DZ^2. \tag{\dagger}$$

and suppose $(a_0, b_0, c_0) \in \mathbb{Z} \times \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is a solution to Eq. (†) with $c_0 \neq 0$.

   (a) Let $f(x) = x^2 - Bx + C$. Prove that $f(x)$ is irreducible over $\mathbb{Q}$.

   (b) Let $K \subseteq \mathbb{C}$ be the splitting field for $f(x)$, and let $\alpha \in K$ be a root of $f(x)$. Prove that $B - \alpha$ is the other root of $f(x)$.

   (c) Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and let σ be the generator for G, so in particular $\sigma(\alpha) = B - \alpha$. For all $(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, write $\beta_{(a,b,c)} = \frac{a+b\alpha}{c}$. Prove: for all $\mathbf{v} \in \mathbb{Z} \times \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$,

$$\mathbf{v} \text{ is a solution to Eq. (†)} \qquad \text{if and only if} \qquad \beta_{\mathbf{v}} \cdot \sigma(\beta_{\mathbf{v}}) = D.$$

   (d) Let $\beta_0 = \beta_{(a_0,b_0,c_0)}$. Prove: for all $\mathbf{v} \in \mathbb{Z} \times \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$,

$$\mathbf{v} \text{ is a solution to Eq. (†)} \qquad \text{if and only if} \qquad \frac{\beta_{\mathbf{v}}}{\beta_0} \cdot \sigma\left(\frac{\beta_{\mathbf{v}}}{\beta_0}\right) = 1.$$

   (e) Use Hilbert's Theorem 90 to prove: for all $\mathbf{v} \in \mathbb{Z} \times \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$,

$$\mathbf{v} \text{ is a solution to Eq. (†)} \qquad \text{if and only if} \qquad \text{there exist } m, n \in \mathbb{Z} \text{ such that } \beta_{\mathbf{v}} = \beta_0 \left(\frac{m + Bn - n\alpha}{m + n\alpha}\right).$$