Problem Sheet 6

1. Recall that in order to obtain a codeword of the *Reed-Solomon code*, the message is interpreted as a polynomial p of degree less than k over the finite field $\mathbb{F}$ with q elements. In turn, the polynomial p is evaluated at a fixed set of n distinct points $a_1, \ldots, a_n$ of the field $\mathbb{F}$, and the sequence of values is the corresponding codeword. Formally, the set $\mathbf{C}$ of codewords of the Reed-Solomon code is defined as follows:

$$\mathbf{C} = \left\{ \big(p(a_1), p(a_2), \ldots, p(a_n)\big) \;\middle|\; p \text{ is a polynomial over } \mathbb{F} \text{ of degree } < k \right\}.$$

Compute the minimal distance of the Reed-Solomon code.

2. Let $\mathbb{F}$ be a field and let $\mathbb{F}[X, Y]$ be the polynomial ring on two variables X and Y over the field $\mathbb{F}$. Since $\mathbb{F}[X, Y] = (\mathbb{F}[X])[Y]$, every element q of $\mathbb{F}[X, Y]$ can be viewed as a polynomial $q = q(Y)$ in the variable Y with coefficients in the ring $\mathbb{F}[X]$. Let $\beta \in \mathbb{F}[X]$. Prove that

$$q(\beta) = 0 \iff Y - \beta \text{ divides } q(Y).$$

3. In computational complexity theory, **BPP**, which stands for *bounded-error probabilistic polynomial time*, is the class of decision problems solvable by a probabilistic Turing machine in polynomial time, with an error probability of at most $1/3$ for all instances. That is, on any given run of the algorithm, it has a probability of at most $1/3$ of giving the wrong answer, whether the correct answer is **YES** or **NO**. Prove that the constant $1/3$ in this definition is irrelevant, as it can be any constant between 0 (inclusive) and $1/2$ (exclusive).