Exercise sheet 9

The content of the marked exercises **(*)** should be known for the exam.

1. **(*)** Let K be a field.

1. Suppose that $P \in K[X]$ is a non-zero polynomial of degree d. Prove that P has at most d roots in K. [*Hint:* Exercise 2.3 from Exercise sheet 8].
2. Is the previous point also true if K is just supposed to be a division ring? [*Hint:* Exercise 1 from Exercise sheet 6].
3. Now suppose that K is an infinite field, and that $P \in K[X]$ is such that $P(\alpha) = 0$ for every $\alpha \in K$. Prove: $P = 0$ in $K[X]$.
4. Still supposing that K is an infinite field, show that if $P \in K[X_1, \ldots, X_n]$ is such that for every $(\alpha_1, \ldots, \alpha_n) \in K^n$ one has $P(\alpha_1, \ldots, \alpha_n) = 0$, then $P = 0$ in $K[X_1, \ldots, X_n]$.

2. Let $p \in \mathbb{Z}$ be a positive prime number.

1. Prove that there exists a unique ring map $\mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$ sending $X \mapsto X$, and that it is surjective. For $f \in \mathbb{Z}[X]$, we denote by $\bar{f}$ its image via this map.
2. Let $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ be such that $p | a_i$ for $i \in \{0, \ldots, n-1\}$ and $p \nmid a_n$. Prove that $\bar{f}$ is a monomial in $\mathbb{Z}/p\mathbb{Z}[X]$, and deduce that if $f = gh$ in $\mathbb{Z}[X]$ with g and h non-constant polynomials, then $p^2 | a_0$ [Hint: $\mathbb{Z}/p\mathbb{Z}$ is a field, hence $\mathbb{Z}/p\mathbb{Z}[X]$ is a principal ideal domain].
3. Conclude: if $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ is such that $p^2 \nmid a_0$, $p \nmid a_n$, $p | a_i$ for $i \in \{0, \ldots, n-1\}$ and the coefficients $a_0, \ldots, a_n$ are coprime, then f is an irreducible polynomial in $\mathbb{Z}[X]$. (This is known as Eisenstein's Criterion).
4. For $n \in \mathbb{Z}_{>1}$, we denote by W_n the set of primitive n-th roots of unity, and define the n-th cyclotomic polynomial
$$\Phi_n(t) := \prod_{\zeta \in W_n} (X - \zeta) \in \mathbb{C}[X].$$
For $n = p$ a prime number, show that $\Phi_p(X) \in \mathbb{Z}[X]$, and that it is irreducible over $\mathbb{Z}[X]$. [*Hint:* First, find $(X-1)\Phi_p(X)$. Then take also in account the polynomial $Q(X) = \phi_p(X+1)$]

Please turn over!

3. Let $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

1. Show that R is a ring, and determine $R^\times$. [*Hint:* Suppose that $\alpha \in R^\times$. What can we say about $|\alpha|^2$?]
2. Show that $2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ are two non-equivalent factorizations of $6 \in R$, so that R is not a UFD.
3. Prove that the ideal $\mathfrak{m} = (2, 1 + i\sqrt{5}) \subseteq R$ is maximal but not principal. [*Hint:* Compute $R/\mathfrak{m}$ and deduce that $\mathfrak{m}$ is maximal. Working by contradiction and using irreducibility of 2, you can prove that $\mathfrak{m}$ is not principal.]

Due to: 20 November 2014, 3 pm.