Martin Schlichenmaier
Université du Luxembourg

Basic Algebraic Structures

Exercise sheet 2

1. Let $(\mathbb{K}[X], +, \cdot)$ be the ring of polynomials over the field $\mathbb{K}$ and $f \in \mathbb{K}[X]$. Denote by $(f) := \{g \cdot f \mid g \in \mathbb{K}[X]\}$ the "ideal" generated by the polynomial f. In complete formal agreement with the construction of the ring of residue classes we define for $g, h \in \mathbb{K}[X]$ that $g \sim h$ if and only if $g - h$ is divisible by f, or equivalently, there exists a polynomial q, such that $g - h = q \cdot g$. As usual we denote the equivalence class of g by $\bar{g}$ and the quotient set by $R := \mathbb{K}[X]/(f)$.

(a) Show that the following operations are well-defined

$$\bar{g} + \bar{h} := \overline{g + h}, \qquad \bar{g} \cdot \bar{h} := \overline{g \cdot h}.$$

From this it follows that the quotient $(R, +, \cdot)$ is again a ring.

(b) Let the degree of f be equal to n. Show that given g there exists always a h with $\bar{g} = \bar{h}$ such that either $h \equiv 0$ or that $\deg h < n$.

(c) Show that $\mathbb{K}[X]/(f)$ is a vector space over $\mathbb{K}$. What is its dimension?

(d) Let g be a polynomial such that $\gcd(f, g) = 1$ and let $\bar{g}$ its equivalence class. Show that there exists an $\bar{h}$ such that $\bar{g} \cdot \bar{h} = \bar{1}$.

(e) A polynomial f is called irreducible if f can not be written as product of two polynomials of degree ≥ 1. Show that $\mathbb{K}[X]/(f)$ is a field if and only if f is irreducible. (Check the proof in the construction of $\mathbb{F}_p$.)

2. (a) Calculate $gcd(X^4 - 1, X - 1)$.

(b) Calculate $gcd(3X^3 + 2X + 1, X^2 - 4X)$

3. (a) Let p be a prime number. Show that

$$X^p - X = \prod_{a \in \mathbb{F}_p} (X - a).$$

(b) Verify directly (over $\mathbb{F}_3$):

$$(X^3 - X) = X(X-1)(X-2).$$

(c) Does the polynomial $X^p - X + 1$ have any zeros in $\mathbb{F}_p$?

4. (a) As it is known from the lecture, $\mathbb{F}_7^*$ is a cyclic group. Determiner all generators.

(b) An element a of a field $\mathbb{K}$ is called a square if there exists $b \in \mathbb{K}$, such that $b^2 = a$. Determiner in $\mathbb{F}_7^*$ all squares.

5. Let $\mathbb{K}[X]$ be the ring of polynomials. The formal differentiation D is introduces as the map $D(X^n) = nX^{n-1}$ linearly extended to all polynomials, i.e.

$$f = \sum_{i=0}^{n} a_i X^i \quad \mapsto \quad D(f) = \sum_{i=0}^{n} i a_i X^{i-1}.$$

(a) Verify

$$D(f+g) = D(f) + D(g), \quad D(\alpha f) = \alpha D(f), \ \alpha \in \mathbb{K}$$
$$D(f \cdot g) = D(f)g + fD(g), \quad D(g^2) = 2gD(g).$$

Is $D(X^n) = 0$ for $n \geq 1$ possible?

(b) A polynomial f is called square-free if there does not exists a polynomial g of degree ≥ 1 such that g^2 divides f. Show that if $gcd(F, D(f)) = 1$ then f is square-free.

(c) Show that if α is a double zero of f, i.e. the polynomial f is divisible by $(X - \alpha)^2$, then α is also a zero of $D(f)$.

The web-page of the course:
`http://math.uni.lu/schlichenmaier/cours/mics`