Martin Schlichenmaier
Université du Luxembourg

Mathematical Foundations

Solution hints

This concerns only Problem 1 of Exercise sheet 2.

The ring of polynomials $(\mathbb{K}[X], +, \cdot)$ over a field $\mathbb{K}$ behaves algebraically very much like the ring of integers $\mathbb{Z}$. In particular, one has the notion of divisibility, one has the (extended) division algorithm of Euclid to determine the greatest common divisor, etc.

The group of units (i.e. the elements which are invertible with respect to the multiplication) is given by the non-zero elements of the field (and is denoted by $\mathbb{K}^*$).

Two polynomials $f, g \in \mathbb{K}[X]$ are associated if and only if there is a $r \in \mathbb{K}$, $r \neq 0$ such that $f = r \cdot g$. A polynomial is called normalized if the highest non-vanishing coefficient (i.e. the coefficient of the term with the highest degree in the variable X) is equal to 1.

We fix a polynomial f. 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 $g - h = q \cdot f$. 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.

Solution: Everything works similar as for the ring $\mathbb{Z}$. For $g, g' \in \bar{g}$ and $h, h' \in \bar{h}$,

$$g' = g + k \cdot f, \qquad h' = h + l \cdot f, \quad \text{with} \quad l, k \in \mathbb{K}[X]$$

Hence,

$$g' + h' = (g + h) + (k + l) \cdot f,$$
$$g' \cdot h' = (g + k \cdot f) \cdot (h + l \cdot f) = g \cdot h + (h \cdot k + g \cdot l + k \cdot l \cdot f) \cdot f.$$

In particular, $g + h \sim g' + h'$ and $g \cdot h \sim g' \cdot h'$ and the operations are well-defined on R. That R is ring, follows from the fact that the operations are coming from $\mathbb{K}[X]$, and $\mathbb{K}[X]$ is 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 $\deg h < n$.

Solution:
Given g, make division with remainder by f. This yields $g = k \cdot f + h$ with $k, h \in \mathbb{K}[X]$ and either $h \equiv 0$ or $\deg h < n$. Now $g \sim h$ as their difference is divisible by f. In other words, $\bar{g} = \bar{h}$.

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

Solution:
First note that $\mathbb{K}[X]$ is a vector space and the ideal (f) is a vector subspace. Hence as quotient $\mathbb{K}[X]/(f)$ is also a vector space. Of course, one could show this directly as one has the operation of adding the classes of polynomials and multiplying them with scalars.
Following (b) every element in $\mathbb{K}[X]/(f)$ can be represented by either the zero polynomial or a polynomial of degree $< n$. In particular, the vector space will be generated by the residue classes of the monomials $X^i, i = 0, 1, \ldots, n-1$. It will be a basis if the residue classes are linearly independent. Assume that

$$a_0\overline{X^0} + a_1\overline{X^1} + a_2\overline{X^2} + \cdots + a_{n-1}\overline{X^{n-1}} = \overline{0}$$

is a linear combination of the zero element. This relation is true if and only if

$$a_0X^0 + a_1X^1 + a_2X^2 + \cdots + a_{n-1}X^{n-1} = k \cdot f$$

with a polynomial k. On the r.h.s. there is either the zero polynomial or a polynomial of degree $\geq n$ and on the l.h.s. there is either the zero polynomial or a polynomial of degree $< n$. The only solution is the zero polynomial. In particular all $a_i = 0$. Hence, the generating set is linearly independent, and as such a basis. In particular the dimension of R is n.

(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 $\bar{g} \cdot \bar{h} = \bar{1}$.

Solution:
(Again like in the case $\mathbb{Z}$.) As the $gcd(f, g) = 1$ the extended Euclid algorithm gives a presentation

$$1 = k \cdot f + l \cdot g, \quad \text{with} \quad k, l \in \mathbb{K}[X].$$

If we pass to the residue classes

$$\overline{1} = \overline{k} \cdot \overline{f} + \overline{l} \cdot \overline{g} = \overline{k} \cdot \overline{0} + \overline{l} \cdot \overline{g} = \overline{l} \cdot \overline{g}.$$

(e) A polynomial f is called irreducible if f cannot 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 $\mathbb{F}_p$.)

Solution
First note that $\mathbb{K}[X]/(f)$ is a field if and only if every element different from the zero element is invertible. Note that "zero" here means the zero class. And the polynomials representing the zero class are exactly those polynomials which are multiples of f.
If f is not irreducible it can be written as $f = g \cdot h$ with polynomials g, h of degree between 1 and $n-1$. In particular, $\overline{0} = \overline{g} \cdot \overline{h}$. From the degree it follows that both $\overline{g}$ and $\overline{h}$ are not equal to $\overline{0}$. Hence these elements are non-trivial zero-divisors. But in a field it is not possible to have non-trivial zero-divisors. Hence, R is not a field.
Now let f be irreducible. One has to show that every non-zero element is invertible. Let $\overline{g} \neq \overline{0}$, hence g is not a multiple of f. Let $d = gcd(f, g)$. As gcd d has to divide f. But f is irreducible and hence has as only divisors (up to associated elements) 1 and f itself. As d has also to divide g and g is not a multiple of f, only $d = 1$ is possible. From part (d) it follows that $\overline{g}$ is invertible. Hence R is a field.

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