Homework 4 for
UTK – M351 – Algebra I
Spring 2004, Jochen Denzler, MWF 10:10–11:00, Ayres 111

Problem 39:
Given a commutative ring R with identity, we consider the set $\mathrm{Seq}(R)$ consisting of all sequences $s = (s_0, s_1, s_2, s_3, \ldots)$ where each s_i is an element of R. For instance, with $R = \mathbb{Z}$, the following are elements of $\mathrm{Seq}(\mathbb{Z})$: $(0, 1, 4, 9, \ldots)$, or $(1, 0, -1, 0, 1, 0, -1, \ldots)$. Generally, we will denote by s_i the i^{th} entry in the sequence s, where we begin to count entries at number 0. We define the following operations on $\mathrm{Seq}(R)$:

The *sum* $a + b$ of two sequences is defined componentwise: $a + b = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$. The Cauchy product of two sequences is defined as follows:

$$ab = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots)$$

such that $(ab)_n = \sum_{i=0}^{n} a_ib_{n-i} = a_0b_n + a_1b_{n-1} + \ldots + a_{n-1}b_1 + a_nb_0$.

(a) Make sure that you understand the definition: To this end, calculate the Cauchy product ab of the sequence $a = (1, 1, 1, 1, 1, 1, \ldots)$ with $b = (0, 1, 2, 3, 4, 5, \ldots)$ in $\mathrm{Seq}(\mathbb{Z})$. Which number is the the entry $(ab)_{30}$?

(b) Now show that $\mathrm{Seq}(R)$ with these operations is a commutative ring.

We call this ring $R[[X]]$ (The ad-hoc name $\mathrm{Seq}(R)$ was just for the set.)

Problem 40:
In the ring $\mathbb{Z}[[X]]$, show that the element $a = (1, 1, 1, 1, \ldots)$ is invertible and give its inverse.

Problem 41:
We consider the subset $\mathrm{Seq}_0(R)$ of $\mathrm{Seq}(R)$, consisting of those sequences that have only finitely many non-zero entries. For instance, the sequence $(1, 2, 0, -7, 3, 0, 0, 0, 0, \ldots)$ is in $\mathrm{Seq}_0(\mathbb{Z})$. Such sequences can be written in abbreviated form as finite sequences by omitting the trailing zeros: $(1, 2, 0, -7, 3)$. Show that $\mathrm{Seq}_0(R)$ is a subring of $\mathrm{Seq}(R)$. In particular, to gain sufficient understanding concerning the closure of multiplication, calculate the Cauchy product of $(1, 2, 0, -7, 3)$ and $(2, -1, 4)$.

Problem 42:
In the ring $\mathrm{Seq}_0(R)$, we denote the element $(0, 1)$ as X. Calculate X^0, X^2, X^3 etc., and write $(1, 2, 0, -7, 3)$ as a linear combination of powers of X.

Problem 43:
From now on, we will take the liberty of writing the elements of $\mathbb{Z}_n$ as $0, 1, 2, \ldots, n-1$, rather than $[0], [1], [2], \ldots, [n-1]$ when no confusion arises. Calculate $(1 + 2X)^3$ in the ring $\mathbb{Z}_3[X]$.

Comments:
The usual symbol for the ring $\mathrm{Seq}_0(R)$ is $R[X]$, and this ring is called the polynomial ring with coefficients in R. Even though we can and will later plug in elements of R for the symbol X, as you would when viewing polynomials as functions of a variable, it is crucial that you do NOT view the ring of polynomials over R as a subring of the ring of functions from R to R. It MAY NOT BE one!!!

The usual symbol for the ring, consisting of the set $\mathrm{Seq}(R)$ and the addition and multiplication defined here, is $R[[X]]$, and it is called the "ring of formal power series with coefficients in R". (Name to be explained in lecture. Just take note here: unlike the power series you may have encountered at the end of Calculus II, you are NOT expected to plug anything in for X here, and therefore no convergence issues arise.) And one of the reasons I introduce this example is to stress the previous remark about polynomial rings, where plugging in ring elements for X is not part of the definition of $R[X]$ either.

Problem 44:
In the polynomial ring $\mathbb{Z}_6[X]$, find two polynomials p and q, such that $\deg(pq) < (\deg p) + (\deg q)$. Note that $\mathbb{Z}_6$ is not an integral domain; so the purpose of this problem is to show that the assumption that the coefficient ring be an integral domain is really needed for the degree formula to hold.

Problem 45:
In the ring $\mathbb{Z}[X]$ take the polynomials $a = X^3 + X^2 + 2X + 1$ and $b = 2X^2$. Show that it is not possible to find polynomials q and r in $\mathbb{Z}[X]$ such that $a = bq + r$ and $\deg r < \deg b$. If the coefficients are taken from a field, the euclidean algorithm asserts that such a division with remainder is possible. So this problem serves as an illustration that the requirement that the coefficient ring be a field is really needed for the euclidean algorithm.

Problem 46:
In the ring $\mathbb{Q}[X]$, find a GCD of $a = X^3 - 7X^2 + 3X + 3$ and $b = X^3 - 6X^2 + X + 7$. Also write the GCD thus obtained as a linear combination of a and b.

Problem 47:
In the ring $\mathbb{Z}_{13}[X]$, find a GCD of the "same" polynomials $a = X^3 - 7X^2 + 3X + 3$ and $b = X^3 - 6X^2 + X + 7$, and write the GCD thus obtained as a linear combination of a and b.

I put the word "same" in quotes, because this is an abuse of language. The coefficent -6 in b of problem 46 is the integer -6, whereas in problem 47, the 'same' -6 is a shorthand for the element $[-6]_{13} = [7]_{13} \in \mathbb{Z}_{13}$. But it's nevertheless common language usage to consider the 'same' polynomial in different rings.

Problem 48:
In a polynomial ring $R[X]$ (R is a commutative ring with 1), choose two polynomials p_1, p_2. Consider the set

$$I\langle p_1, p_2\rangle := \{r_1p_1 + r_2p_2 \mid r_1, r_2 \in R[X]\}$$

of all linear combinations of p_1 and p_2. (This is a set of common interest in algebra, but the notation I have used for it is different from the usual notation.)

Show that $I\langle p_1, p_2\rangle$ is a subring of $R[X]$ (it may not have a multiplicative identity, though).

Problem 49:
Continuing the previous problem, show that $I\langle p_1, p_2\rangle$ even is an *ideal.* — "Ideal" is a new concept for you, and here is the definition: A subring S of a commutative ring T is called an *ideal* if it has the property: For any $s \in S$ and any $t \in T$, it holds $st \in S$.

Rmk: The same set of problems 48, 49 could be done with any number of given polynomials $p_1, p_2, p_3, \ldots$, including the possibility of only a single polynomial.

Problem 50:
Give an example of a polynomial in $\mathbb{Q}[X]$ that is not prime (i.e. can be factored), but has no root in $\mathbb{Q}$. What is the smallest degree such a polynomial can have (explain why)?

Problem 51:
Show that the polynomial $p = X^2 + X + 1$ is irreducible in $\mathbb{Z}_2[X]$.

(Obviously p is not a constant polynomial, but:) show that the polynomial function $\mathbb{Z}_2 \to \mathbb{Z}_2, x \mapsto p(x)$ is a constant function.

Problem 52:
Show that the polynomial $p = X^4 + 1$ is irreducible in $\mathbb{Q}[X]$, but not in $\mathbb{R}[X]$ nor in $\mathbb{C}[X]$. Give a complete factorization in $\mathbb{R}[X]$, and a complete factorization in $\mathbb{C}[X]$.

Also give three different incomplete factorizations (product of two quadratics) in $\mathbb{C}[X]$ (for later use).

Problem 53:
In the fields $\mathbb{Z}_p$ for $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29$, find one solution of the equations $x^2 + 1 = 0$, $x^2 - 2 = 0$, $x^2 + 2 = 0$ each, or conclude that none exists. Basically that's trial and error, and I have filled in all but three of the "doesn't exist" cases, and a few of the existence cases, to save you work. Note also that in the example $p = 29$, to find solutions, I only needed to test $1, 2, 3, \dots, 14$, since $15 \equiv -14$, $16 \equiv -13, \dots$.

p	$x^2 + 1 = 0$	$x^2 - 2 = 0$	$x^2 + 2 = 0$
2	1	0	0
3	DNE	DNE	
5	2	DNE	DNE
7			DNE
11		DNE	
13			DNE
17			
19	DNE	DNE	6
23	DNE		DNE
29	12	DNE	DNE

Once this is accomplished, use the information, and wisdom gleaned from the very last part of the previous problem, to factor X^4+1 completely in $\mathbb{Z}_p[X]$ for the prime numbers $p = 2, 3, 5, 7, 11, 13, 17$ (and more of them, if you are bored, or want to get bored).

Background info: a simple result from the theory of quadratic residues (in elementary number theory), or in other terms, a simple argument about groups, which we have alas no time to go into, implies in particular: if p is an odd prime such that there is no element in $\mathbb{Z}_p$ whose square is -1, and also no element whose square is 2, then there does exist an element whose square is -2.

*Accepting this fact, you can conclude that at least one of the factorizations of X^4+1 into quadratics (in $\mathbb{Q}[X]$) found in problem 52 can serve as a model for factorization in $\mathbb{Z}_p[X]$; in other words: X^4+1 can be factored nontrivially in *every* $\mathbb{Z}_p[X]$.*

Problem 54:
We have seen that the mapping $F[X] \to \mathrm{Fct}(F \to F)$, which assigns to each polynomial the corresponding polynomial function $F \to F$ cannot be one-to-one, if the field F contains finitely many elements. (Simply because in this case there are still infinitely many polynomials, but only finitely many functions $F \to F$).

Now show conversely that, if F contains infinitely many elements, then the mapping $F[X] \to \mathrm{Fct}(F \to F)$ is indeed one-to-one.

Problem 55:
We have seen that a polynomial of degree n in $F[X]$ can have at most n roots in F (or any extension field of F). This assumed that F be a field. In contrast, consider the polynomial ring $\mathbb{Z}_{25}[X]$.

How many roots does the polynomial X^2 have in $\mathbb{Z}_{25}$?

Give several essentially different factorizations of X^2 in $\mathbb{Z}_{25}$, thus showing that the unique factorization property may fail in $R[X]$, if R is not a field.

Problem 56:
In $\mathbb{Z}_2[X]$, consider the ideal I of all multiples of the irreducible polynomial $X^3 + X + 1$. Denoting the equivalence class $[X]_I$ in $\mathbb{Z}_2[X]/I$ as j, list all elements of $\mathbb{Z}_2[X]/I$, and give their multiplication table. In particular, find the inverse of $1 + j$ in the field $\mathbb{Z}_2[X]/I$.