Homework for
UTK – M351 – Algebra I
Spring 2007, Jochen Denzler, MWF 10:10–11:00, Ayres 205

Problem 42:
In the ring $\mathbb{Z}[i]$, find a greatest common divisor of $a = 16 + 2i$ and $b = 14 + 31i$, using repeated division with remainder in analogy to Problem 25.

(Note that I said: **a** GCD, with the indefinite article. If g is a GCD, then $-g$, ig and $-ig$ also are correct solutions. The option of selecting 'the positive one' is not available here.)

Problem 43:
Give the isomorphism $\theta : \mathbb{Z}_{12} \to \mathbb{Z}_3 \oplus \mathbb{Z}_4$ afforded by the chinese remainder theorem explicitly (i.e., table all values). — Likewise for $\theta : \mathbb{Z}_{10} \to \mathbb{Z}_2 \oplus \mathbb{Z}_5$.

Also show that there cannot be an isomorphism $\mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$. To do this, observe, for instance, the number of solutions to the equation $x + x = 0$ in either ring. Come up with at least one other equation (using multiplication) that has different numbers of solutions in either ring. (Doing so amounts to giving a second proof that there cannot be an isomorphism $\mathbb{Z}_4 \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$). Include a formally sufficient proof of the last statement in the following note, such as to make rigorous why the number of solutions to an equation involving only ring operations can be used to show that two rings are not isomorphic.

Note: How would one typically show that two rings are isomorphic? Easy in principle: one exhibts a mapping explicitly and shows that it is 1-1, onto, and a homomorphism. This does not mean that the task is always easy in practice. — But how does one show that two rings are NOT *isomorphic? Not so easy in principle. One has to show that no 1-1 onto map watsoever can be a homomorphism. Between two rings with just four lousy elements, there would be 24 bijective maps already to check for homomorphism properties. This problem shows a more feasible approach: Find properties that are preserved under isomorphisms: If a certain equation in one ring R has exactly n solutions $x_1, \ldots, x_n$, then it has exactly n solutions in any other ring S that is isomorphic to R; if $\theta : R \to S$ is a ring isomorphism, then the solution to that equation in S are $\theta(x_1), \ldots, \theta(x_n)$.*

Problem 44:
Use modular arithmetic to show that the following determinant is not 0:

$$\begin{vmatrix} 1 & 3 & 5 & 0 & 2 & 4 \\ 5 & 2 & 1 & 2 & 4 & 2 \\ 10 & 5 & 3 & 7 & 1 & 0 \\ -5 & 5 & 15 & 11 & -7 & 10 \\ 15 & 0 & -5 & 20 & 5 & 3 \\ 0 & -10 & 5 & 10 & 3 & 5 \end{vmatrix}$$

Problem 45:
How many zeros exactly are at the end of the decimal representation of the number 93!, written out in digits? Only count the contingent zeros at the end, after the last non-zero digits. For instance, for the number 350102100000, you would count five zeros.

Problem 46:
Find all numbers n such that $\varphi(n) = 12$. Show that there are no numbers n such that $\varphi(n) = 14$.

Problem 47:
Let's try the ring $\mathbb{Z}[\sqrt{-5}]$ for a change: another subring of $\mathbb{C}$; it consists of all the numbers $a+b\sqrt{-5}$ with $a, b \in \mathbb{Z}$.

First show that the only numbers dividing the identity 1 in this ring are $+1$ and -1: you have to find all integers a, b, c, d such that $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$.

Now show that 3 has no divisors but ± 3 and ± 1 of 3 in this ring. Show the analog for the numbers 2 and $1 \pm \sqrt{-5}$. In other words, all of these numbers are irreducible in the ring $\mathbb{Z}[\sqrt{-5}]$.

(Remember: irreducible means that the number cannot be factored further except by introducing units (= divisors of 1) as factors.)

Hint: The task to find all integers a, b, c, d such that $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$ (or 3 etc) is simplified a lot if you first multiply this equation with its complex conjugate. If you still get stuck, hand it in as pingpong hwk.

Problem 48:
Show that in the ring $\mathbb{Z}[\sqrt{-5}]$, the number 6 can be written as a product of irreducible factors in two essentially different ways. (Refer to previous problem for raw material).

Problem 49:
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 $(ab)_n = \sum_{i=0}^{n} a_i b_{n-i} = a_0b_n + a_1b_{n-1} + \ldots + a_{n-1}b_1 + a_nb_0$.

(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 50:
In the ring $\mathbb{Z}[[X]]$, show that the element $a = (1, 1, 1, 1, \ldots)$ is invertible and give its inverse.

Problem 51:
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 52:
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 53:
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 $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ when no confusion arises. Calculate $(1 + 2X)^3$ in the ring $\mathbb{Z}_3[X]$.

Comments:
The usual symbol for the ring $Seq_0(R)$ 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 $Seq(R)$ 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 54:
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 55:
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 56:
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 57:
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 56 is the integer -6, whereas in problem 57, the 'same' -6 is a shorthand for the element $\overline{-6}_{13} = \overline{7}_{13} \in \mathbb{Z}_{13}$. But it's nevertheless common language usage to consider the 'same' polynomial in different rings.

Problem 58:
In the ring $\mathbb{Z}[X]$, show that the ideal $(2, X) := \{2p + qX \mid p, q \in \mathbb{Z}[X]\}$ is *not* principal, i.e., it is *not* of the form $(g) := \{gp \mid p \in \mathbb{Z}[X]\}$. Show that the polynomials 2 and X do have a gcd, but that this gcd cannot be obtained as a linear combination of 2 and X.

Problem 59:
In the ring $\mathbb{Z}[\sqrt{-5}]$, show that the ideal $(1 + \sqrt{-5}, 3) := \{(1 + \sqrt{-5})a + 3b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}$ is *not* principal, i.e., it is *not* of the form $(g) := \{gp \mid p \in \mathbb{Z}[\sqrt{-5}]\}$. Show that the numbers $1 + \sqrt{-5}$ and 3 do have a gcd, but that this gcd cannot be obtained as a linear combination of $1 + \sqrt{-5}$ and 3.

Problem 60:
In the ring $2\mathbb{Z}$ of even integers (which lacks a 1), show that the numbers 4 and 6 do not have a common divisor. *The definitions in class concerning princial ideals are not meant to carry over to rings without a 1, but would need to be modified. So no questions pertaining to ideals are asked for this example.*

Problem 61:
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 62:
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 $\mathbb{R}[X]$ (two quadratic factors; show that this is a complete factorization), and a complete factorization in $\mathbb{C}[X]$ by further factoring the real quadratics.

Also give three different incomplete factorizations (product of two quadratics) in $\mathbb{C}[X]$ (for later use) by grouping the linear terms in two pairs in 3 different ways.

Problem 63:
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 $1, 2, 3, \ldots, 14$, since $15 \equiv -14$, $16 \equiv -13$,....

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 $\mathbb{C}[X]$) found in problem 62 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 64:
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 (and not even an integral domain).

Problem 65:
In $\mathbb{Z}_2[X]$, consider the ideal I of all multiples of the irreducible polynomial $X^3 + X + 1$. Denoting the equivalence class $\bar{X}_I$ 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 $\mathbb{Z}_2[X]/I$.