Homework 2 for
UTK – M351 – Algebra I
Spring 2007, Jochen Denzler, MWF 10:10–11:00, Ayres 205

Problem 11:
Explore and discover...

Check each field axiom for validity in the following examples $(X, +, \cdot)$, and if not all are verifiied, decide whether they are rings, commutative rings, with or without unity. Here X is

(a) The set of integers, $\mathbb{Z}$ with the usual meanings of $+$ and $\cdot$ (also in the following examples with sets of numbers).

(a1) The set of odd integers

(a2) The set of even integers

(b) The set of rationals, $\mathbb{Q}$

(c) The set of 2×2 matrices with real entries (where $+$ and $\cdot$ denote addition and multiplication of matrices)

(c1) The set of 2×2 matrices of the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$.

(d) The set P of polynomials in the variable x, with rational coefficients.

(e) The set $\{E, O\}$, where the following rules define $+$ and $\cdot$: $E + E = E$, $E + O = O + E = O$, $O + O = E$. $E \cdot E = E$, $E \cdot O = O \cdot E = E$, $O \cdot O = O$.

(f) *You* invent this problem: The set $\{Z, I, T\}$ which made a commutative group with an operation $+$ in Example&Hwk #5. Together with definitions for a multiplication $\cdot$ that makes the set at least a ring. Check any further field axioms for validity in this example.

(g) Same task as before; but this time we want a set of *four* elements. You should now focus on which axioms we are losing, as compared to (e) and (f). Any hunch what feature of the numbers 2, 3, 4 is decisive?

Problem 12:
Let R be any ring (with operations $+$ and $\cdot$). Define the matrix ring $M_n(R)$ as the set of all $n \times n$ matrices whose entries are in R. The addition will be componentwise, and the multiplication will also be defined as in the usual matrix algebra course: $(AB)_{ik} = \sum_{j=1}^{n} A_{ij} B_{jk}$.

Show that $M_n(R)$ is a ring, and show that it has an identity provided R has.

Note: You should be able to handle the $\sum$ notation. If not, you may ask for help. I will accept a solution that only takes care of $n = 2$. But at least the stronger half of the students should attempt to do it for general n using the sum notation, or possibly a three-dots-substitute for $\sum$. Be aware that the $\sum$ notation for general n is shorter *than the pedestrian way for $n = 2$ only!*

Problem 13:
Let R be a ring (with operations $+$ and $\cdot$). We define operations on $R \times R$ as follows:

$$(x, y) + (u, v) := (x + u, y + v) \ , \quad (x, y) \cdot (u, v) := (xu - yv, xv + yu)$$

Here, as usual, $a - b$ stands for a plus the additive inverse of b.

Show that this defines a ring. We are going to denote $R \times R$, when adorned with *these* operations, as $R[i]$. (This is admittedly a strange name as of yet).

Problem 14:
Continuing the previous problem, show that $R[i]$ has an identity, if R has. Show also that $R[i]$ is commutative, if R is.

Assume that R is a field. Must $R[i]$ necessarily be a field? If not, what condition must be satisfied in R to guarantee that $R[i]$ is a field? *Some may find it convenient to attempt #6 before this second part of #5; try it in case you have difficulties at this moment.*

Problem 15:
Continuing the previous problem, let R be a commutative ring with identity 1. In $R[i]$, we'll denote the element $(0, 1)$ with the special symbol i. (You start getting an idea where $R[i]$ got its name from.) Calculate $i \cdot i$ (too easy. . .).

I claim that, for the case $R = \mathbb{R}$, the field of real numbers, you should be at least vaguely familiar with $\mathbb{R}[i]$ under a different name. Which one? Set up a complete translation dictionary (it has only a few lines) that translates the notation set up in Problem 4 into the more familiar one.

Show that $\mathbb{R}[i]$ is a field.

Problem 16:
I claimed in class that the power set $\mathcal{P}(M)$ (which is the set of all subsets of M), together with the operations $A + B := (A \setminus B) \cup (B \setminus A)$ and $A \cdot B := A \cap B$ is a commutative ring with identity. Prove the distributive law (as far as not done in class yet) and the associativity for $+$.

Problem 17:
Suppose, in a ring, the extra property $a \cdot a = a$ is verified for *every* a. (The previous problem is an example where this happens.) Show generally, that a ring satisfying that extra property is automatically commutative: Since this is a bit tricky, I give you the steps (the steps how I did it; I wouldn't claim with certainty that there cannot be another, shorter way):

(a) Show that $b + b = 0$ for every b. You do this by calculating $(b + b) \cdot (b + b)$ in two different ways.
(b) Show that $bcb = cbc$ for every b, c. You do this by calculating $(b \cdot c - c \cdot b) \cdot (b \cdot c - c \cdot b)$ in two different ways.
(c) Conclude $b \cdot c = c \cdot b$ from part (b) by appropriate multiplications and by again using $a \cdot a = a$.

Each step needs to be justified by explicit reference to the ring axioms (or to consequences thereof that were proved in class).

Problem 18:
Show: A ring with exactly 3 elements, $\{0, a, b\}$ must be commutative. *Hint: First show* $a + a = b$.

Problem 19:
In the ring $\mathbb{Z}$, find the gcd of 43728 and 15360 ('the' gcd: so make it a positive number), and express this gcd in the form $43728k + 15360\ell$ with integers k, ℓ.

Problem 20:
In this problem, we'll see that the division algorithm can be mimicked in the ring $\mathbb{Z}[i]$, which consists of the numbers $a + bi$ where $a, b \in \mathbb{Z}$ and i is the imaginary unit. You may view this ring either as a subring of $\mathbb{C}$, or as an instance of the class of rings constructed in Problem 5.

Given $a = a_1 + a_2 i \in \mathbb{Z}[i]$ and $b = b_1 + b_2 i \in \mathbb{Z}[i]$ with $b \neq 0$, we want to find $q = q_1 + q_2 i \in \mathbb{Z}[i]$ and $r = r_1 + r_2 i \in \mathbb{Z}[i]$ such that $a = qb + r$ and r "smaller" than b. We cannot require "$0 \leq r < b$" because we do not have an order in the ring $\mathbb{Z}[i]$; a statement "$0 \leq r < b$" would be meaningless. Instead we will use the absolute value of complex numbers and require that $|r|$ is smaller than $|b|$, or, equivalently: $r_1^2 + r_2^2 < b_1^2 + b_2^2$.

Given $a = a_1 + a_2 i \in \mathbb{Z}[i]$ and $b = b_1 + b_2 i \in \mathbb{Z}[i] \setminus \{0\}$, let $\vartheta = \vartheta_1 + i\vartheta_2 \in \mathbb{C}$ be the exact quotient $\vartheta = a/b$. Let q_1 be an integer closest possible to ϑ_1 (there may be several equally good choices) and let q_2 be an integer closest possible to ϑ_2. Let r be the remainder making $a = qb + r$ true

(a) To make sure you understand the principle, find q and r according to the prescription of the preceding paragraphs in the case $a = 517 + 213i$, $b = 11 + 25i$. Check that $r_1^2 + r_2^2$ is indeed less than $b_1^2 + b_2^2$.

(b) Write out explicitly what $a = \vartheta b$ means for a_1, a_2, b_1, b_2 and ϑ_1, ϑ_2. — Write out explicitly what $a = qb + r$ means for a_1, a_2, b_1, b_2, q_1, q_2, r_1, r_2. — What does your prescription about the choice of q imply about the size of $q_1 - \vartheta_1$, $q_2 - \vartheta_2$?

(c) Express r_1 and r_2 in terms of b_1, b_2, $q_1 - \vartheta_1$, $q_2 - \vartheta_2$ and conclude that $r_1^2 + r_2^2 < b_1^2 + b_2^2$.

Problem 21:
In many rings that are not fields, it can happen that $ab = 0$ for certain $a \neq 0$ and $b \neq 0$. The next problem gives a whole lot of examples, this one wants you merely to show:

In any ring, if $ab = 0$, but $a \neq 0$ and $b \neq 0$, then neither a nor b has a multiplicative inverse.

(Comment: Therefore, in fields this phenomenon $ab = 0$ with $a \neq 0$ and $b \neq 0$ cannot happen, because there, all nonzero elements have multiplicative inverses. The phenomenon also does not occur in the ring $\mathbb{Z}$, or, for that matter, in any ring that is subring of a field.)

Problem 22: *2pts each for* $(a), (b), (c) \cup (d), (e)$
Let me introduce a name: In a ring, whenever $a \neq 0$ and $b \neq 0$ satisfy $ab = 0$, then a and b are called *zero divisors*. In this problem, you'll find zero divisors in various rings:

(a) The ring $C^0[0, 1]$ of continuous, real-valued functions on the interval $[0, 1]$, with the usual addition and multiplication of functions. (The proof of the ring properties is straightforward, you are not required to write it out here.) Find a pair of zero divisors. *If you find this difficult, then the most likely source of your difficulty is that you are shying away from piecewise defined functions.*

(b) In the ring $M_2(\mathbb{Z}) = \mathbb{Z}^{2\times 2}$ of 2×2 matrices with integer entries, find a pair of zero divisors.

(c) In the direct sum $\mathbb{Z} \oplus \mathbb{Z}$, find a pair of zero divisors.

(d) In the ring $\mathcal{P}(M)$ described in Problem 16, where $M = \{\Box, \Diamond, \star, \triangle\}$, find a pair of zero divisors.

(e) Bonus problem: How many pairs of zero divisors does the commutative ring in (d) have, *not* counting pairs (A, B) and (B, A) as different?

Problem 23:
Show that in a ring with identity that has more than one element, the multiplicative identity is automatically different from the additive identity.

Problem 24:
In a ring with identity (not necessarily commutative!), assume that the elements a and b each have a multiplicative inverse; we'll call them a^{-1} and b^{-1} respectively. Show that ab has a multiplicative inverse as well, and give a 'formula' for it, in terms of a^{-1} and b^{-1}.

Problem 25:
Let A be any subset of $[0,1]$ (think of finitely many numbers between 0 and 1). Within the ring $C^0[0,1]$ (defined in 22a above), consider the set

$$C^0_A[0,1] := \{f \mid f(x) = 0 \ \text{ for all } \ x \in A\}$$

Show that $C^0_A[0,1]$ is a subring of $C^0[0,1]$. (Comment: The name $C^0_A[0,1]$ is an ad-hoc name given for this problem, unlike the name $C^0[0,1]$, which is generally understood in the mathematical community.)

Problem 26:
Warning / Surprise: If R is a ring with identity 1_R and S is a subring not containing the element 1_R, then S might still have an identity 1_S different from 1_R. In that case, by the uniqueness of the identity, 1_S could not serve as a multiplicative identity in R. In this problem, you'll see two examples:

(a) Take the ring $\mathbb{Z}\oplus\mathbb{Z}$. Give its multiplicative identity. Show that the ring $\mathbb{Z}\oplus\{0\} = \{(a,0) \mid a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \oplus \mathbb{Z}$. Show that it does have a multiplicative identity, and exhibit it.

(b) In the ring $\mathcal{P}(M)$, where $M = \{\Box, \Diamond, \star, \triangle\}$, what is the multiplicative identity? Show that $\mathcal{P}(N)$, where $N = \{\Box, \star, \triangle\}$, is a subring. What is its multiplicative identity?

Problem 27:
Why can a similar substitution of the *additive* identity not happen?

Problem 28:
Divisibility by 11: To find the remainder of a number when divided by 11, for an integer given in decimal notation, the following rule can be used with the digits: Add the digits from right to left, with *alternating sign*. Add/subtract multiples of 11 as needed or desired. The result (between 0 and 10) is the remainder of the given integer upon division by 11.

Example: $a = 357123946803$; We calculate $c = 3 - 0 + 8 - 6 + 4 - 9 + 3 - 2 + 1 - 7 + 5 - 3 = -3$ Add 11 to get 8 (between 0 and 10): The remainder of a when divided by 11 is therefore 8.

Prove this rule by writing up a claculation in the ring $\mathbb{Z}_{11}$

Problem 29:
Given an integer a, let $Q(a)$ be the sum of its digits. E.g., $Q(37491) = 3 + 7 + 4 + 9 + 1 = 24$. What is

$$Q(Q(Q(4444^{4444}))) \ ?$$

To answer the problem, give a rough estimate how large the number could be at most, and use a calculation in $\mathbb{Z}_9$ as a second piece of information.

Problem 30:
Show that 13 (which is a prime in $\mathbb{Z}$ of course) is *not* irreducible in the ring $\mathbb{Z}[i]$. In other words, find integers a, b, c, d such that $(a+bi)(c+di) = 13$, but neither of the numbers $a+bi$, $c+di$ should be 1, -1, i or $-i$.

Hint: such numbers are easier to guess (and finding one solution is good enough) than to find systematically; see if you can make $c + di = a - bi$.

Problem 31:
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 same for the numbers 2 and $1 \pm \sqrt{-5}$. In other words, all of these numbers are irreducible in the ring $\mathbb{Z}[\sqrt{-5}]$.

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 32:
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).