Homework 2 for
UTK – M351 – Algebra I
Spring 2004, Jochen Denzler, MWF 10:10–11:00, Ayres 111

Problem 3:
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 4:
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 5:
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 6:
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 7:
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 8:
Suppose, in a ring, the extra property $a \cdot a = a$ is verified for *every* a. (We had two examples where this happened: Ex. 3.4 on p. 7 of the book, and the example in the previous problem). 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 9:
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 10: *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 7, 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 11:
Show that in a ring with identity that has more than one element, the multiplicative identity is automatically different from the additive identity.

Problem 12:
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 13:
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 10a 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 14:
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 15:
Why can a similar substitution of the *additive* identity not happen?

Problem 16:
Here is another example of an ordered ring: Let R be the ring of polynomials $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ with real coefficients. The operations are the usual ones you know from calculus, so R is a subring of $C^0(\mathbb{R})$.

Show that the definition below of R^+ satisfies the axioms for an ordered ring:
(a) If $p \in R^+$ and $q \in R^+$, then $p + q \in R^+$
(b) If $p \in R^+$ and $q \in R^+$, then $p \cdot q \in R^+$
(c) Exactly one of the following three is true: $p = 0$, or $p \in R^+$, or $-p \in R^+$.

Def: $p \in R^+$, iff in the list of coefficients $\{a_0, a_1, \ldots, a_n\}$ of $p := a_0 + a_1x + \ldots + a_nx^n$, the first nonzero number is positive. If all coefficients are 0 or the first nonzero coefficient is negative, then $p \notin R^+$.

Order the following polynomials from smallest to largest. $p_1 = 1$, $p_2 = x^2$, $p_3 = x - x^2$, $p_4 = 1 - x$, $p_5 = 3x^3$, $p_6 = x + x^2$, $p_7 = x^2 + 25x^{11}$, $p_8 = 2x - x^4$, $p_9 = -x^4 + 3x^5$, $p_{10} = x^8$.

Problem 17:
The same ring can be ordered in a different way: In this problem define $p \in R^+$, iff in the list of coefficients $\{a_0, a_1, \ldots, a_n\}$ of $p := a_0 + a_1x + \ldots + a_nx^n$, the *last* nonzero number is positive.

Order the same polynomials as previously from smallest to largest, according to the new definition.

Comment: There are many more choices for an ordering; relying on calculus, you could choose any $x_0 \in \mathbb{R}$ and say $p \in R^+$, provided the first nonzero among $p(x_0)$, $p'(x_0)$, $p''(x_0)$, ldots, $p^{(n)}(x_0)$ is positive. — When we study polynomials in more detail later, we can do the same thing within a pure algebraic framework (not relying on calculus), but the punchline here is just to give you more illustrations of the concept of ordered rings.

Problem 18:
Prove: In a *commutative* ring R, it holds: $(ab)^n = a^nb^n$ for any $n \in \mathbb{N}$. and for any $a, b \in R$. (from p. 34 of textbook)

Problem 19:
In the ring $M_2(\mathbb{Z})$ (the ring of 2×2 matrices with integer entries), prove that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

(from p. 35 of textbook)

Problem 20:
Review the definition of 'multiple'; in the ring $\mathcal{P}(M)$ described in problem 7, what is nA for an integer n and a set $A \subseteq M$?

Format of the answer: If n is ________, then $nA =$________. If n is ________, then $nA =$________.