Math 351:03 — Fall 1999
MW4 SEC-217
Prof. Bumby

Workshop 7, Introduction to rings.

15. Let R be any commutative ring. Let

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$$

with entry-wise addition and the usual formula for matrix multiplication. This can be shown to be a ring either by direct verification of all axioms or by identifying $M_2(R)$ as R module homomorphisms of the module of all *column vectors* of length 2 with entries in R. We assume this has been done.

(a) Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$\Delta = ad - bc$. If Δ^{-1} exists in R, find a formula for M^{-1}.

(b) If $M = M^{-1}$, show that $(1 + \Delta)b = (1 + \Delta)c = 0$ and $(1 - \Delta^2)a = (1 - \Delta^2)d = 0$.

(c) If $R = \mathbb{Z}$, show that there are infinitely many solutions of $M = M^{-1}$. In particular, find a solution with $a = 7$ and another solution with $b = 7$.

16. As part of showing that problem 4 of Section 4.3 (which you are doing as a homework exercise) leads to a solution of problem 5 of that section, show the following properties of a ring R in which $x^3 = x$ for all $x \in R$.

(a) For any x, if $e = x^2$, then $e^2 = e$.

(b) If $x^2 = 0$ in R, then $x = 0$.

(c) Use the result of problem 4 to show that, if $e^2 = e$ and x is any element of R, then $ex = xe$. Combining this with (a), gives that every square of an element of R commutes with all elements of R.

(d) Supply reasons for the chain of equations

$$xy = (xy)^3 = xy(xy)^2 = x(xy)^2y = x^2yxy^2 = yx^3y^2 = y^3x^3 = yx.$$

This shows that any two elements of R commute.

17. Let O be the set of rational numbers that can be written with an odd denominator. We will find all ideals of O. There is always an ideal consisting only of zero. Having note this, we let I be an ideal that contains a nonzero element.

(a) Show that I contains a positive integer. Let n be the smallest positive integer in I.

(b) If I contains an odd integer, show that $1 \in I$, and hence $I = O$.

(c) Show that n is always a power of 2.

(d) Show that $I = nO$.

(e) Show that every ideal other than O itself is contained in $2O$.

. . . continued on other side

18. Consider the ring $G = \mathbb{Z}[i]$ whose elements are

$$\{a + bi : a, b \in \mathbb{Z}\}$$

with $i^2 = -1$. The operations could be defined by considering this as a subring of $\mathbb{C}$ or defined directly.

(a) Show that, if an ideal I of G contains $a + bi$, then $a^2 + b^2 \in I$. If not both a and b are zero, this quantity is a positive integer, so every nonzero ideal contains a positive integer. Let n be the smallest positive integer in I. Note that we also have $ni \in I$, so I contains an element with a nonzero coefficient of i.

(b) If I is an ideal of G, let

$$\tau(I) = \left\{ b : (\exists a) \left[a + bi \in I \right] \right\}.$$

Show that $\tau(I)$ is an ideal of $\mathbb{Z}$.

(c) Every nonzero ideal of $\mathbb{Z}$ consists of all multiples of the smallest positive integer in the ideal. Suppose that $\tau(I)$ consists of the multiples of c. Then, show that

$$\left[a + bi \in I \right] \implies \left[c|a \& c|b \right]$$

where $c|a$ means "c divides a". This allows I to be written as a product of c and an ideal J with $\tau(J) = \mathbb{Z}$.

(d) If $\tau(I) = \mathbb{Z}$, then there is an integer u such that $u + i \in I$.

(e) With n from (a) and u from (d),

$$I = \{nx + (u + i)y : x, y \in \mathbb{Z}\}.$$

We shall say that I is *generated by* n and $u + i$ in this case. Show that $n|(u^2 + 1)$. Write $u^2 + 1 = nn'$.

(f) Show that $I \cdot (-u + i) = n \cdot I'$ where I' is the ideal generated by n' and $u - i$.

(g) If I is generated by n and $u + i$, then u can be replaced by anything congruent to it modulo n, so we may assume $|u| \leq n/2$. With n' constructed as in (e), this gives

$$n' \leq \frac{n^2 + 4}{4n}.$$

Show that $0 \leq n' \leq n/2$ if $n \geq 2$. Thus, repeating this construction will lead to an ideal that contains 1, which must be all of G.

(h) This construction is the inductive step in showing that all ideal of G consist of the multiples of a single element. Rather than giving this general proof. Illustrate the method by finding this element in the case when $n = 65$ and $u = 18$.

End workshop 7