Thu May 1 18:27:53 2003 : can you post solutions to 7.6.2, 8.1.6, and 8.2.4? thanks

Problem 2 of §7.6: I'll take it as given that R is a commutative ring (Exercise 15 of §1) and that we know about idempotents (Exercise 1 of §7.6). We can try to do this exercise by induction on the number of elements of R. It might be informative to know going in that the order of R is a power of 2: This follows from the observation that $2a = 0$ for all $a \in R$, which we can prove by writing $4a = 4a^2 = (a + a)^2 = a + a$. Since $2a = 0$ for all $a \in R$, R is naturally a vector space over the field $\mathbf{Z}/2\mathbf{Z}$, so it's isomorphic to $(\mathbf{Z}/2\mathbf{Z})^n$ (for some n) as an additive group. In the induction that we contemplate, we can start with the case where R has 2 elements, in which case it's clear that $R \approx \mathbf{Z}/2\mathbf{Z}$ as a ring. Now suppose that R has more than 2 elements, and pick $e \in R$ different from 0, 1. Then e is an idempotent, so R is the product of Re and $R(1 - e)$ by Exercise #1. Both factors are non-zero; indeed, they contain the non-zero elements e and $1-e$, respectively. Hence each factor has fewer elements than R. By induction, each factor is isomorphic as a ring to a product of copies of $\mathbf{Z}/2\mathbf{Z}$, so the same statement is true for R.

Problem 6 of §8.1: We are given relatively positive integers a and b and wish to study the set of integers of the form $an+bm$ with n and m non-negative. We're supposed to be able to get all integers greater than $ab-a-b$ and not $ab-a-b$. (No information is requested on integers smaller than $ab - a - b$.) Equivalently, we can study the set of integers $an+bm$ with n and m *positive*; these are gotten by adding $a+b$ to the integers $an+bm$ with n and m non-negative. This second way of doing things seems promising because translating $ab - a - b$ up by $a + b$ turns it into the simpler-looking ab. We have to show that ab is not of the form $an + bm$ (with n and m positive) but that integers bigger than ab are of this form.

If $an + bm = ab$, then b divides an, so it divides n because it's prime to a. Thus n is a multiple of b. Similarly m is a multiple of a. Since we are requiring n and m to be positive, an is at least as big as ab, and so is bm. Hence $an + bm$ is at least $2ab$ and can't be ab.

Assume now that d is bigger than ab. Because a and b are relatively prime, there are integers x and y so that $ax + by = 1$. Clearly one of ax, by is positive and the other is negative. Let's assume that ax is positive and by is negative. After changing the sign of y, we have $1 = ax - by$ with $x, y > 0$. For every integer t, we have

$$\begin{aligned} d = d \cdot 1 = d(ax - by) &= dax - tab + tab - dby \\ &= a(dx - tb) + b(ta - dy). \end{aligned}$$

We need the existence of t so that $dx - tb$ and $ta - dy$ are both positive, i.e., so that $dy/a < t < dx/b$. The interval $(\frac{dy}{a}, \frac{dx}{b})$ has length $d(x/b - y/a) = d/ab > 1$. Accordingly, it does contain an integer in its interior. Conclusion: we can find t and stamp our envelope.

Problem 4 of §8.2: Let a and b be non-zero elements of R and let d be a greatest common divisor of a and b. Because d is a common divisor, (d) contains (a) and b, so (d) contains the ideal (a, b). The condition that d may be written $ra+sb$ means that, conversely, (d) is contained in (a, b). It follows that if I is an ideal of R that is generated by at most two elements, then I is generated by at most one element. Using induction, we can deduce from this that if I is generated by n elements $a_1, \ldots, a_n$, then I is actually principal. For example, suppose that $n = 3$; let's say that I is generated by a, b and c. Then I is the smallest ideal containing (a, b) and c, so it's the smallest ideal containing d and c if d is the gcd of a and b. We can therefore conclude that R is a PID once we know that every ideal of I is generated by a finite number of elements. (It's easy to make examples of ideals in integral domains that are *not* generated by a finite number of elements, so we should watch out here. For an explicit example, take the integral domain to be the ring of polynomials in variables $x_1, x_2, \ldots$ over a field and consider the ideal generated by all of the variables x_i.) The finite generation of ideals follows from the second condition. Arguing by contradiction, let's assume that I is an ideal of R that cannot be generated by a finite set of its elements. Take a non-zero a_1 in I. Then $(a_1) \subset I$, and the inclusion is strict. Take an a_2 in the complement of (a_1) in I. We get $(a_1) \subset (a_1, a_2) \subset I$, with strict inclusions. Continuing in this manner, we get $(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots \subset I$. Now each of the ideals $(a_1, a_2, \cdots, a_n)$ is principal by what we already know; let $(a_1, a_2, \cdots, a_n) = (r_n)$. Then r_2 divides r_1, r_3 divides r_2, and so on. The quotients r_n/r_{n+1} are non-units because the inclusions are strict. This is in contradiction with **(ii)**, which says that there's an N so that r_N/r_n is a unit for $n \geq N$.