Math 55a: Honors Abstract Algebra

Homework Assignment #1 (1 September 2010):
Linear algebra I: vector space basics; introduction to convolution rings

$$\ast$$

—Axler, page 1 [why?]

This problem set is due Friday, September 10, at the beginning of class.

We start with some basic problems from Chapter 1 of the Axler textbook, on vector spaces and their subsets, intersections, and sums.

1.–6.[1] Solve problems 4 through 14 on pages 19 and 20 of the Axler textbook. (In problem 4, and problems 8 through 13, V is a vector space over an arbitrary field $\mathbf{F}$.) Which if any of these basic results would fail if $\mathbf{F}$ were replaced by $\mathbf{Z}$?

One way to study and use a mathematical structure is via constructions of new examples from known ones. The remaining problems of this problem set illustrate this with a construction that we shall return to several times this year.

Fix a ring A (with unity, but for now not assumed commutative). We construct a new ring S_A as follows. The elements of S_A are sequences $a = (a_0, a_1, a_2, \ldots)$ with each $a_n \in A$. Addition is "termwise": the sum of a and $b = (b_0, b_1, b_2, \ldots)$ is the sequence $a + b$ whose n-th term is $a_n + b_n$ for each $n = 0, 1, 2, \ldots$. The product is <u>not</u> termwise, though: we multiply sequences a and b by *convolving* them, forming the sequence $a * b$ whose n-th term is

$$\sum_{i=0}^{n} a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0$$

for each $n = 0, 1, 2, \ldots$. (This sequence $a * b$ is thus called the *convolution* of a and b.) Let $S_A^0 \subset S_A$ consist of the sequences a for which there exists some N such that $a_n = 0$ for all $n > N$.[2]

NB: At least in the case that A is commutative you may recognize one if not both of S_A and S_A^0 by another name. Giving this alternative name or notation for S_A or S_A^0 does not by itself constitute a solution of the problems 7–9, though it might give you a sense of where these rings come from. This "convolution" approach also leads to generalizations and applications that might seem unnatural starting from the more familiar picture of S_A and S_A^0.

7. Prove that S_A and S_A^0, with these definitions of the sum and product, are indeed rings. (Be sure to check everything that requires checking!) Find an isomorphic copy of A in S_A^0, and thus also

[1] These 11 problems, plus the question about "vector spaces over $\mathbf{Z}$", are sufficiently small and straightforward compared to our usual fare that I'm counting each as the equivalent of only half of a problem.

[2] These can also be called "sequences of finite support": the "support" of a sequence a is $\{n : a_n \neq 0\}$. Note that an infinite sequence $(a_n)_{n=0}^{\infty}$ with terms in A is entirely equivalent to a function $n \mapsto a_n$ from the nonnegative integers to A; the choice of whether to refer to a sequence as a function depends on context. The same notion of "support" is used for any function $f : X \to Y$ for which Y contains a zero element: the support is $\{x : f(x) \neq 0\}$.

in S_A. ("Isomorphic" means that your copy should come with a bijection to A that respects the ring structure, i.e. takes 0 to 0, 1 to 1, and likewise for sums, additive inverses, and products.)

8. Prove that S_A and S_A^0 are commutative if and only if A is, and are [integral] domains (i.e. have no zero divisors other than 0 itself) if and only if A is.

9. Suppose now that A is a field. Show that neither S_A nor S_A^0 is a field, but give (and prove) a simple description of the invertible elements of each of these two rings.

10. What goes wrong when you try to extend $*$ to a ring operation on the "two-sided sequences" $(a_n)_{n=-\infty}^{\infty}$? Find a subset $\overline{S}_A$ of the two-sided sequences that is closed under termwise addition and has an operation $*$ such that:

    - i) For every $a \in S_A$ the sequence $\overline{a}$ defined by[3]
    $$\overline{a}_n := \begin{cases} a_n, & \text{if } n \geq 0; \\ 0, & \text{if } n < 0 \end{cases}$$
    is contained in $\overline{S}_A$;
    - ii) $(\overline{S}_A, 0, 1, +, *)$ is a ring containing S_A (for suitable elements "0" and "1" of $\overline{S}_A$);
    - iii) if A is a field then so is $\overline{S}_A$.

Note that in (ii) of the last problem you should show that the map $S_A \to \overline{S}_A$, $a \mapsto \overline{a}$ is a ring homomorphism. Since it is clear that $\overline{a} + \overline{b} = \overline{a+b}$ for all $a, b \in S_A$, this means that you should verify that this map also takes the multiplicative identity of S_A to the multiplicative identity of $\overline{S}_A$, and satisfies $\overline{a} * \overline{b} = \overline{a * b}$ for all $a, b \in S_A$. Cf. the parenthetical remark on "isomorphic" in problem 7.

Finally, a topical computational application:

11. The following mathematical model is sometimes used (for instance by www.fivethirtyeight.com) in predicting the results of Presidential elections in the United States. Let $n_1, \ldots, n_{51}$ be the numbers of Electoral College (EC) votes assigned to the 50 States and the District of Columbia; these are positive integers with $\sum_{i=1}^{51} n_i = 538$ (hence the URL). These are distributed among two candidates, call them P and Q. For each i there are nonnegative probabilities p_i, q_i, estimated by extensive polling, with $p_i + q_i = 1$ such that the i-th block of votes goes to P with probability p_i and to Q with probability q_i. The 51 events are assumed independent. Thus for each subset $S \subseteq \{1, 2, \ldots, 51\}$ the model assumes that the probability that the i-th block goes to P if and only if $i \in S$ is $\prod_{i \in S} p_i \cdot \prod_{i \notin S} q_i$. In this case P gets $\sum_{i \in S} n_i$ EC-votes and Q gets $\sum_{i \notin S} n_i$ EC-votes. We want to compute, for each $k = 0, 1, 2, \ldots, 538$, the probability that P wins exactly k votes.

    The direct method of trying all possible S is impractical (why?). Instead FiveThirtyEight uses a pseduorandom number generator to assign each i to S or the complement of S with probabilities p_i, q_i respectively, calculates and records k, and repeats tens of thousands of times to estimate the probabilities. What does problem 7 suggest should be done instead of this "Monte Carlo" approximation?

(Yes, a couple of states have other possible outcomes, and Nebraska actually split its EC vote in the 2008 election. The answer to problem 11 easily generalizes to accommodate this possibility as long as we still assume all 51 contributions to k remain independent.)

[3] The definition of $\overline{a}$ has the equivalent statement: if we regard a as a function from $\{0, 1, 2, \ldots\}$ to A, then $\overline{a}$ is the "extension by zero" of a to a function from $\mathbf{Z}$ to A.