Math 55a: Honors Abstract Algebra
Homework 1

Lawrence Tyler Rush
<me@tylerlogic.com>

August 23, 2012

http://coursework.tylerlogic.com/math55a/homework01

I don't know exactly why this homework's numbers one through six are mapped to Axler's four through fourteen in chapter one (I assume for weighting... since those problems seem simpler than the rest), but I will make problems one through eleven of this homework map to four through fourteen of Axler's first chapter, and then continue on with homework problem seven being my twelve, eight being my thirteen, etc. The title of each problem should guide anyone perfectly.

1 Axler: Chapter 1, Problem 4

Let $a \in F$ and $v \in V$ such that $av = 0$. Assume by way of contradiction that both $a \neq 0$ and $v \neq 0$. Therefore, letting $v = (v_1, v_2, \ldots, v_n)$ we have that $av_j = 0$ for some $j \in 1, 2, \ldots, n$ where $v_j \neq 0$. However, this is a contradiction with the fact that F is a field since either a or v_j need to be zero but neither are. Thus we have that $a = 0$ or $v = 0$ is true.

Replacing $\mathbb{F}$ with $\mathbb{Z}$ This property will still hold for the integers.

2 Axler: Chapter 1, Problem 5

Keeping in mind that a subset of a vector space is a subspace if it is closed under vector addition and scalar multiplication and contains 0, we need only check these three things.

(a) Is $\{(x_1, x_2, x_3) \in F^3 : x_1 + 2x_2 + 3x_3 = 0\}$ a subspace of V?

Certainly the subset contains zero being that $0 + 2(0) + 3(0) = 0$. ✓
Letting (x, y, z) and (x', y', z') be in this subset, then we have that both $x + 2y + 3z = 0$ and $x' + 2y' + 3z' = 0$. This results in the following

$$(x + x') + 2(y + y') + 3(z + z') = x + x' + 2y + 2y' + 3z + 3z' = (x + 2y + 3z) + (x' + 2y' + 3z') = 0 + 0 = 0$$

and thus the subset is closed under addition. ✓
Futhermore, letting a be a scalar in F, we can see that

$$ax + 2(ay) + 3(az) = a(x + 2y + 3z) = a0 = 0$$

and therefore the subset is also closed under scalar multiplication. ✓
Hence we have that this subset defines a subspace of our vector space V.

(b) Is $\{(x_1, x_2, x_3) \in F^3 : x_1 + 2x_2 + 3x_3 = 4\}$ a subspace of V?

This is not a subspace since $0 + 2(0) + 3(0) \neq 4$ and hence the subset does not contain zero.

(c) Is $\{(x_1, x_2, x_3) \in F^3 : x_1 x_2 x_3 = 0\}$ a subspace of V?

This is not a subspace since we can see that $(1, 1, 0)$ and $(0, 0, 1)$ are in the subset, but yet $(1, 1, 0)+(0, 0, 1) = (1, 1, 1)$ would not be in the subset since $1(1)(1) \neq 0$, and thus there is no closure under addition.

(d) Is $\{(x_1, x_2, x_3) \in F^3 : x_1 = 5x_3\}$ a subspace of V?

Since $0 = 5(0)$, then zero is contained within this subset. ✓
Letting (x, y, z) and (x', y', z') be in the subset, we know that both $x = 5z$ and $x' = 5z'$, which means that the following equation holds.

$$(x, y, z) + (x'.y'.z') = (x + x', y + y', z + z') = (5z + 5z', y + y', z + z') = (5(z + z'), y + y', z + z')$$

Thus the subset is closed under addition. ✓
And finally, with the following equation, letting $a \in F^3$ we can see that the subset is also closed under scalar multiplication. ✓

$$a(x, y, z) = (ax, ay, az) = (a5z, ay, az) = (5(az), ay, az)$$

3 Axler: Chapter 1, Problem 6

The problem states that our subset needs to be nonempty, closed under addition, and closed under taking additive inverses, which informs us that the subset of our choosing must either not include zero or must fail to be closed under scalar multiplication. However, after a little thought about what it means to be closed under addition and taking additive inverses informs us about the fact that zero must also be in the set (the sum of an element and its inverse must be in the set, but what's that?). So we are left with finding a set where scalar multiplication is not closed. When we should multiply an element of a set by a scalar from a field to "break" out of the set, then a discrete set should come to mind. To that end, for our example we choose a set dealing with intgers, in fact, we will choose $\mathbb{Z}^2$, which is of course a subset of $\mathbb{R}^2$. However $(1, 1)$ is in the set, but $\frac{1}{2}(1, 1) = (\frac{1}{2}, \frac{1}{2})$ is not, and we now see the aforementioned "breaking" out of the set.

4 Axler: Chapter 1, Problem 7

Since we only need the subset to be closed under scalar multiplication, then we need a subset that is not closed under addition or is not closed under taking inverses. Note that multiplication of an element by $0 \in \mathbb{R}$ will result in the zero vector, so our subset will always by default contain that element. We know from our middle/high school mathematics experience (or at least I do) that the multiplication of two binomials needs to be "foiled", yielding those pesky middle terms. So we should be able to use this to our advantage. Like the subset in problem 2c above, we use an analogous set of $\{(x, y) \in \mathbb{R}^2 : xy = 0\}$ which is closed under scalar multiplication since $axay = a^2xy = 0$ when $xy = 0$ as it would for (x, y) in this set. However, we see that $(1, 0) + (0, 1) = (1, 1)$ which is not in the subset, and therefore the subset is not closed under addition.

5 Axler: Chapter 1, Problem 8

Well certainly an intersection any amount of subspaces of V will be a subset of V, so thus we only need the usual zero-addition-multiplication to be satisfied. Because we have that each of the sets in the intersection is a subspace of V, then they all contain the zero vector, and therefore, so does the intersection. Now let x be in the intersection of subspaces, which in turn means that x is in each of the individual subspaces and hence so is ax for any scalar a, which of course then means that the intersection contains ax as well, and thus we have the closure of scalar multiplication on the intersection. Also let y be a vector in the intersection. As with x above, y is also in each of the subspaces making up the intersection, and therefore, so is their sum, $x + y$. Thus the sum is also in the intersection, and the intersection is therefore closed under addition.

Replacing $\mathbb{F}$ with $\mathbb{Z}$ This property will still hold for the integers.

6 Axler: Chapter 1, Problem 9

Let U_1 and U_2 are subspaces of V for the following proofs.
($\rightarrow$)
Let $U_1 \cup U_2$ be a subspace of V. Then assume by way of contradiction that neither $U_1 \subseteq U_2$ nor $U_2 \subseteq U_1$. Thus there exist a u and u' such that $u \in U_1$, $u \notin U_2$ and $u' \in U_2$, $u' \notin U_1$, which means that both u and u' are in the union of U_1 and U_2. Hence since the union is a subspace of V, then $u + u'$ must also be in the union. However this would mean that the sum is also in U_1 or U_2, which in turn means, without loss of generality, that $u + u' \in U_1$. Because U_1 is a vector space, then both $-u \in U_1$ and $-u + u + u' = u' \in U_1$, but this contradicts the fact that u' is not in U_1, and therefore our by-way-of-contradiction assumption is false and hence we have that either U_1 is a subset of U_2, or vice versa.
($\leftarrow$)
Letting $U_1 \subseteq U_2$ then we would have that $U_1 \cup U_2 = U_2$ and thus the union is also a subspace of V.

Replacing $\mathbb{F}$ with $\mathbb{Z}$ This property will still hold for the integers.

7 Axler: Chapter 1, Problem 10

The subspace $U + U$ would simply be U due to the closure of addition on U which will demand that any element that can be constructed by the definition of the sum of vector spaces is already contained in U.

Replacing $\mathbb{F}$ with $\mathbb{Z}$ This property will still hold for the integers.

8 Axler: Chapter 1, Problem 11

The operation of addition on subspaces is both commutative and associative due to the fact that the addition operation of vectors has both properties as well. Its pretty easy to see that if $u_1 + u_2 \in U_1 + U_2$ then $u_1 + u_2 = u_2 + u_1 \in U_2 + U_1$ by the commutativity of addition, which gives us $U_1 + U_2 \subseteq U_2 + U_1$. We can similarly arrive at the converse relationship to prove equivalency, and therefore the commutativity of addition of subspaces. The proof for associativity is virtually the same as the previous proof for commutativity, but simply replacing the commutativity of vector addition with its property of association.

Replacing $\mathbb{F}$ with $\mathbb{Z}$ This property will still hold for the integers.

9 Axler: Chapter 1, Problem 12

As we saw earlier, the operation of addition on the subspaces of V will always have itself as an identity. Similarly, any subspace of U will be an identity for U, but note that U will not be an identity for the subspace, outside of the trivial subspace of U itself. So we can see that the identity is not actually unique. But this points us towards the more general idea that the addition operation of subspaces always "expands" the subspace addends. This is due to the fact that each addend contains the zero vector, and thus the sum of two subspaces will always have at least all the elements from the larger of the two (or more) subspaces.

Well we know that a subspace, U, has an inverse, U^{-1} if $U + U^{-1} = 0$ where 0 is the identity of course. However, as a result of what was previously discussed, there could potentially be many inverses of a subspace since there are multiple identities for a given subspace. If we were to choose one of the trivial identities, U itself, then any subspace of U would be the inverse of U. Although if we were to choose a subspace of U as the identity, then there would exist no subspace U^{-1} since it is impossible to add a subspace of U to U and have, as a result, a subspace of U. This is, of course, unless the subspace is U. This is simply again due to the closure of the subspace addition operation, and the "expansion" mentioned earlier in the problem; subspace adding will expand, or at the very least, result in nothing new.

Replacing $\mathbb{F}$ with $\mathbb{Z}$ This property will still hold for the integers.

10 Axler: Chapter 1, Problem 13

This seemingly looks so painfully true, but unfortunately it is not. One thing that stumped me and made me change thoughts is that for a given $u_1 \in U_1$ and $u_2 \in U_2$ there would exist $w, w' \in W$ such that

$$u_1 + w = u_2 + w'$$

but $w = w'$ did not necessarily need to be true. So I began to think of previous problems (above) and specifically thought about how adding a vector space and one of its subspaces would yield the first vector space, and then constructed the following counter-example from knowing that.

$$U_1 = \mathbb{Z}, U_2 = \mathbb{R}, W = \mathbb{C}$$

Replacing $\mathbb{F}$ with $\mathbb{Z}$ This property will still hold for the integers.

11 Axler: Chapter 1, Problem 14

Let U be the subspace of $\mathcal{P}(\mathbb{F})$ consisting of all polynomials of the following form.

$$p(z) = az^2 + bz^5 \tag{11.1}$$

Also let the subspace W of $\mathcal{P}(\mathbb{F})$ consist of all polynomials of the following form.

$$p(z) = c_0 + c_1 z + c_3 z^3 + c_4 z^4 + c_6 z^6 + \cdots + c_n z^n \tag{11.2}$$

From here it is easy to see that $\mathcal{P}(\mathbb{F}) = U + W$ since W basically "fills in" all the holes (being the powers of z) left by U to complete the set of polynomials over $\mathbb{F}$. Futhermore, since it is not possible for polynomials of the form in 11.1 to be equal to polynomials of the form in 11.2 unless zero, then we have that the intersection of U and W must be the set containing only $\{0\}$.

Sure this proof is slightly hand-wavy, but it is due to, in part, its innate simplicity, and also because I don't know of any theorem really that states that "two polynomials each with distinct powers of the input parameter can never be equal unless all coefficients are zero". If I knew of such a theorem, that is what I would have used.

12 Prove That S_A And S_A^0 Are Rings. Find The Bijection

In this proof, we let a, b, and c all be elements of S_A or S_A^0, context will define which one, and notation such as a_k will be an element of A which belongs to the sequence a at the k^{th} position.

Prove S_A is a ring. Both "Abelianism" and associativity of addition on this set are proven using the same old trick of combining the necessary elements using the definition of sum on S_A, then use the definition of sum on A, and the fact that A is a ring as well to shift around the terms of each element of S_A appropriately for proving associativity or commutativity, and then separate them again by using the inverse operation of sum on S_A. These, slightly annoying, but necessary manipulations follow first for commutativity, then associativity.

$$\begin{aligned}
a + b &= (a_0 + b_0, a_1 + b_1, \ldots) \\
&= (b_0 + a_0, b_1 + a_1, \ldots) \\
&= b + a \\
(a + b) + c &= (a_0 + b_0, a_1 + b_1, \ldots) + c \\
&= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, \ldots) \\
&= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), \ldots) \\
&= a + (b_0 + c_0, b_1 + c_1, \ldots) \\
&= a + (b + c)
\end{aligned}$$

In a similar pipeline of events as above, by the following eqautions, we can easily see that the additive identity of S_A is $(0, 0, \ldots)$ where $0 \in A$ is the identity, and also that $(a_0^{-1}, a_1^{-1}, \ldots)$ would be the inverse of $(a_0, a_1, \ldots)$.

$$\begin{aligned} a + (0, 0, \ldots) &= (a_0, a_1, \ldots) + (0, 0, \ldots) \\ &= (a_0 + 0.a_1 + 0. \ldots) \\ &= (a_0, a_1, \ldots) \\ &= a \\ a + (-a_0, -a_1, \ldots) &= (a_0, a_1, \ldots) + (-a_0, -a_1, \ldots) \\ &= (a_0 + (-a_0), a_1 + (-a_1), \ldots) \\ &= (0, 0, \ldots) \end{aligned}$$

The following set of equations reveal that $e = (1, 0, 0, \ldots)$ is the multiplicative identity of S_A.

$$\begin{aligned} (a_0, a_1, a_2, \ldots) * e &= \left(\sum_{i=0}^{0} a_i e_{0-i}, \sum_{i=0}^{1} a_i e_{1-i}, \sum_{i=0}^{2} a_i e_{2-i}, \ldots \right) \\ &= \left(a_0, a_1(1) + \sum_{i=0}^{0} a_i e_{1-i}, a_2(1) + \sum_{i=0}^{1} a_i e_{2-i}, \ldots \right) \\ &= \left(a_0, a_1 + \sum_{i=0}^{0} a_i(0), a_2 + \sum_{i=0}^{1} a_i(0), \ldots \right) \\ &= (a_0, a_1 + 0, a_2 + 0, \ldots) \\ &= (a_0, a_1, a_2, \ldots) \end{aligned}$$

The following set of equations shows that the product is associative on S_A by showing that each term of $a * (b * c)$ is equal to the corresponding term in $(a * b) * c$. There are a few key things to notice here. The first is a general thing about changing indicies. In a summation ($\sum$) there is always some fiddling that is allowed to be done with the indicies, as long as all of the combinations "hit" in the pre-fiddling from are the same as the post-fiddling form, and sometimes it is only the NUMBER of combinations that matter, but that is a discussion for another time. Nonetheless this property is only true for summations when the sum is a commutative operation, and since we are in the world of a ring, A, we are free to switch around indicies! So we take advantage of this in the changes from equation 12.4 to equation 12.5 and also from equation 12.6 to equation 12.7. The other thing to note is that the distributive law of A allowed us to go from equation 12.5 to equation 12.6.

$$(a * (b * c))_n = \sum_{j=0}^{n} a_j (bc)_{n-j} \tag{12.3}$$

$$= \sum_{j=0}^{n} a_j \sum_{i=0}^{n-j} b_i c_{(n-j)-i} \tag{12.4}$$

$$= \sum_{j=0}^{n} a_j \sum_{i=0}^{n-j} b_{(n-j)-i} c_i \tag{12.5}$$

$$= \sum_{j=0}^{n} \sum_{i=0}^{n-j} a_j b_{(n-j)-i} c_i \tag{12.6}$$

$$= \sum_{i=0}^{n} \sum_{j=0}^{n-i} a_j b_{(n-j)-i} c_i \tag{12.7}$$

$$= \sum_{i=0}^{n} \left(\sum_{j=0}^{n-i} a_j b_{(n-i)-j} \right) c_i \tag{12.8}$$

$$= \sum_{i=0}^{n} (a * b)_{n-i} c_i \tag{12.9}$$

$$= ((a * b) * c)_n \tag{12.10}$$

Like above, the following equations yield that each term of $a(b+c)$ is equal to the corresponding term in $ab+ac$. Giving to us that the distributive law holds for S_A, and thereby satisfying our final property to prove that S_A is a ring.

$$\begin{aligned}(a(b+c))_n &= \sum_{i=0}^{n} a_i(b+c)_{n-i} \\ &= \sum_{i=0}^{n} a_i(b_{n-i}+c_{n-i}) \\ &= \sum_{i=0}^{n} a_i b_{n-i} + a_i c_{n-i} \\ &= \left(\sum_{i=0}^{n} a_i b_{n-i}\right) + \left(\sum_{i=0}^{n} a_i c_{n-i}\right) \\ &= (ab+ac)_n\end{aligned}$$

Prove that S_A^0 is a ring. Here, like subspaces, we just need to check that S_A^0 contains both sum and product identities and is closed under both of the sum and product operations. Since the sum identity is all zeros, and the multiplicative identity is a one followed by all zeros, then they are both contained in S_A^0. The set is closed under addition since the addition of a and b is pairwise and the result, say r, will be such that $r_n = 0$ for all $n > max(n_a, n_b)$ where n_a and n_b are such that $a_i = 0$ and $b_j = 0$ for all $i > n_a$ and $j > n_b$.

Find an isomorphism from A to S_A^0. Here we need to find an isomorphism. I like to believe I have a knack for finding them, and it seems like that is really the only method. However, I can say that there are two things that seem to pop up time-after-time for me whenever I am tasked with finding a isomorphisms or, more generally, bijections. First, keep it simple. For some reasons a lot of isomorphisms that I have seen are not that complicated, and they always seem to "make sense". Second, there for some reason seems to be nice symmetries involved in a lot of isomorphisms/bijections, especially ones that can be shown pictorially.

Anyway, to get back to business, the mapping here is the following for $a \in A$.

$$\varphi(a) = (a, 0, 0, \ldots)$$

Instantly we can easily see that this mapping takes both the sum and product identities to the sum and product identities in S_A^0. Likewise the fact that additive inverses are taken to additive inverses are just as simple to see. Also by the following set of equations we have that this mapping preserves the sum structure of A in S_A^0

$$\begin{aligned}\varphi(a) + \varphi(b) &= (a, 0, 0, \ldots) + (b, 0, 0, \ldots) \\ &= (a+b, 0, 0, \ldots) \\ &= \varphi(a+b)\end{aligned}$$

and here, the product structure.

$$\begin{aligned}\varphi(a) * \varphi(b) &= (a, 0, 0, \ldots) * (b, 0, 0, \ldots) \\ &= (ab, a0 + 0b, a0 + 00 + 0b, a0 + 00 + 00 + 0b, \ldots) \\ &= (ab, 0, 0, \ldots) \\ &= \varphi(ab)\end{aligned}$$

Now assume that $\varphi(a) \neq \varphi(b)$. Therefore $(a, 0, 0, \ldots) \neq (b, 0, 0, \ldots)$, which guarentees us that $a \neq b$, and hence we know that our homomorphism is one-to-one. Since we are only trying to prove that there exists a set, inside of S_A^0 i.e. a subset, with structure identical to that of A, but not one in particular, then we don't care about the homomorphism being onto since the image of the mapping will simply act as our subset and mappings are, by definition, onto their own images. Hence we have that there is indeed a subset of S_A^0 that is isomorphic to A.

13 The Commutativity and "(Integral Domain)-ness" of S_A and S_A^0

Let the initial assumptions from the previous problems be the same for this problem.

(a) Prove S_A and S_A^0 are commutative iff A is too.

Let S_A and S_A^0 be commutative rings. Since we know that there exists a isomorphic version of A in these rings, as proven in the previous problems, then we can use that isomorphism to help us out. Thus the following equations give us that A is commutative.

$$\begin{aligned} xy &= \varphi^{-1}(\varphi(xy)) \\ &= \varphi^{-1}(\varphi(x)\varphi(y)) \\ &= \varphi^{-1}(\varphi(y)\varphi(x)) \\ &= \varphi^{-1}\left(\varphi(yx)\right) \\ &= yx \end{aligned}$$

Conversely, assume that A is a commutative ring. Then the following set of equations hold.

$$\begin{aligned} (a*b)_n &= \sum_{i=0}^{n} a_i b_{n-i} \\ &= \sum_{i=0}^{n} b_{n-i} a_i \\ &= \sum_{i=0}^{n} b_i a_{n-i} \\ &= (b*a)_n \end{aligned}$$

Hence we have that the n^{th} term of $a*b$ is equal to the n^{th} term of $b*a$, and thus both S_A and S_A^0 are commutative.

(b) Prove S_A and S_A^0 are integral domains iff A is too.

Assume that S_A is an integral domain. Thus for some $x, y \in A$ each of which are non-zero, we have that $\varphi(x)$ and $\varphi(y)$, where φ is the isomorphism from A into S_A, are both non-zero since only zero maps to zero. Therefore the product $\varphi(x)\varphi(y)$ is non-zero because S_A is an integral domain. This in turn means that $\varphi^{-1}(\varphi(x)\varphi(y))$ is also non-zero, again because only zero maps to zero. Hence, because we have that

$$xy = \varphi^{-1}(\varphi(xy)) = \varphi^{-1}(\varphi(x)\varphi(y))$$

then xy is also non-zero. Thus A is an integral domain.

Conversely, assume that A is an integral domain. Assume by way of contradiction that S_A is not an integral domain. Therefore there exists an $a, b \in S_A$ with $a \neq 0$ and $b \neq 0$ such that $ab = 0$. Let indicies j and k be such that $a_j \neq 0$ and $a_m = 0$ for all $m < j$. Allow the same for b and k as is for a and j, respectively. Without loss of generality, let j be less than k. Therefore, since the n^{th} term of ab is

$$\sum_{i=0}^{n} a_i b_{n-i} \tag{13.11}$$

then we have that $a_j b_k$ will be a term in the summation in $(ab)_{k+j}$. Because $a_0 = a_1 = \cdots = a_{j-1} = 0$ and $b_0 = b_1 = \cdots = b_{k-1} = 0$, then, given the indices of convolution (equation 13.11), $a_j b_k$ is the only term in the summation defining $(ab)_{k+j}$ where neither of the operands is zero. Thus we have that $(ab)_{k+j} = a_j b_k$, and since $ab = 0$ then a_j and b_k are zero divisors of A, since neither are zero, but this is a contradiction of the fact that A is an integral domain and thusly has no zero divisors. Hence S_A must be an integral domain. Note that this proof applies without change to S_A^0 as well.

14 Prove that if A is a field, than neither S_A nor S_A^0 are. Give a simple description of the invertible elements of each.

This one seems like it shouldn't be that hard. We have already shown that for any property of a field save for

multiplicative inverses, if A has such a property, than S_A and S_A^0 do as well, so we know that it is the multiplicative inverses that fail that neither S_A nor S_A^0 are a field when A is one. However, I just can't quite figure out the reason why.

15 "Two-sided" sequence consequence.

16 An electoral college computation example.

References

[1] Artin, Michael. *Algebra*. Prentice Hall. Upper Saddle River NJ: 1991.

[2] Axler, Sheldon. *Linear Algebra Done Right* 2nd Ed. Springer. New York NY: 1997.