

Solutions to Assignment #4

Reminder: Midterm is in Haines A18.

Errata: In Handout J, J-8(b), the card numbers are A, 2, 3, 4, not A, 1, 2, 3. The reference should be to G-8, not G-9.

p. I 9, solution to E-5: line 3 should say $t_1 = t_2$.

p. L 1, solution to p. 15, Ex. 2: line 4 should say $1 - i / ((1 + i)(1 - i)) = (1 - i) / 2 = \frac{1}{2} - \frac{1}{2}i$.

Solutions:

First, a comment on a situation that often arises.

Recall that an implication $P \Rightarrow Q$ is equivalent to the “contrapositive” form $\text{not } Q \Rightarrow \text{not } P$, in which P and Q are negated and switched. The contrapositive of the contrapositive is the original implication. Notice that the contrapositive is *equivalent* to the original; it is not the same as the opposite implication $Q \Rightarrow P$ (the “converse”).

Often a statement to be proved will have the form $a \neq b \Rightarrow c \neq d$. It is often simpler and clearer to prove the contrapositive: $c = d \Rightarrow a = b$.

For example, if you are asked to prove that a function f is one-to-one, which says $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, it is often better to prove the contrapositive form $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Other examples occur in the solutions below to problems about Latin squares.

Using the contrapositive is so frequent that in simple situations you can use it without calling attention to it.

The contrapositive can also be viewed as a version of proof by contradiction.

p. 66, Ex. 6. The row-reduced echelon form is
$$\begin{bmatrix} 1 & 7 & 0 & 3 & 0 \\ 0 & 0 & 1 & 5 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

(a) A basis for V consists of the nonzero rows of the row-reduced echelon form. As the text does, let's call the three nonzero rows ρ_1, ρ_2, ρ_3 (rho's).

(b) The elements of V are vectors of the form $c_1\rho_1 + c_2\rho_2 + c_3\rho_3$.

(c) For $(x_1, \dots, x_5) \in V$, using the fact that we can see a pattern like the identity matrix in the first, third, and fifth entries of ρ_1, ρ_2, ρ_3 when compared, we see that the coefficients needed are $c_1 = x_1, c_2 = x_3, c_3 = x_5$.

Ex. 7. Let's write $[A|Y]$ for the augmented matrix. We know that row-reducing the augmented matrix doesn't change the solutions, so we can work with its row-reduced echelon form $[E|Z]$. There are only two possibilities: (i) The last row of $[E|Z]$ looks like $(0, \dots, 0, 1)$. In that case there is an equation $0 = 1$ and the system (row-reduced or not) cannot be solved. (ii) The rows of $[E|Z]$ all look like $(0, \dots, 0, 1, \dots, z_i)$ (perhaps with no 0's to start but at least with the 1). In this case we can solve for the pivot variables in terms of non-pivot variables and constants, and there are solutions.

p. 73, Ex. 1. (b) and (e) are linear transformations, since each output coordinate is a linear combination of input coordinate values.

(a), (c), and (e) all fail the condition that $T(rv) = rT(v)$, for example if $r = 3$ and x_1 is any nonzero value.

Ex's 2 and 3 are not on Midterm #1, although you do need to know the similar concepts for matrices. (For matrices we didn't talk about the range, but rather the column space, which turns out to be the same thing.) These problems are based on reading, to prepare for the discussion in class.

Ex. 2. Let $n = \dim V$. For the zero transformation, the range is $\{\mathbf{0}\}$, the rank is 0, the null space is V , and the nullity is n . For the identity transformation, the range is V , the rank is n , the null space is $\{\mathbf{0}\}$, and the nullity is 0.

Ex. 3. For Example 2: Let's stick to $F = \mathbb{R}$; I think the problem is harder than intended otherwise. Notice that V is the space of all polynomial functions, not just polynomials up to some degree. The range is V and the null space is the subspace of constant functions.

For Example 5: Notice that $T(f)$, or Tf , has the property that $(Tf)(0) = 0$ and also Tf has a continuous derivative, as mentioned in the text. The range consists of all functions with these two properties. To see this, let g be such a function and consider $h = T(g')$, which is given by $h(x) = \int_0^x g'(t)dt = g(x) - g(0) = g(x)$, by a version of the fundamental theorem of calculus. Thus $g = T(g')$ and is in the range. The null space consists of all functions f with $Tf = 0$, which says $\int_0^x f(t)dt = 0$ for all x . Taking the derivative of both sides we get $f(x) = 0$, again by a version of the fundamental theorem of calculus. Therefore the null space consists only of the 0 function.

For Problem J-1: In §2, row-reduce M to get $E = \begin{bmatrix} 1 & 2 & 0 & -1 & 0 \\ 0 & 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$,

as shown in §3. A basis for the row space consists of the three nonzero rows of M .

In §5, make a matrix M whose columns are the given vectors. The linear relations between the columns are given by the null space, so the possible coefficients (r, s, t, u, v) are linear combinations of the basis vectors from §3, namely $(-2, 1, 0, 0, 0)$ and $(1, 0, -3, 1, 0)$ (where they were columns, but here we can write rows if we want to).

In §7, based on the explanation we make A with the given vectors as columns and find a basis for the null space of A^t , which is the same as the matrix in §4 (called M there, but that's a different M from this problem). Then we transpose back. The basis is the same as shown in §3, so our answer is

$$M = \begin{bmatrix} -2 & 1 & 0 & 0 & 0 \\ 1 & 0 & -3 & 1 & 0 \end{bmatrix}.$$

For Problem J-2:

For §8: Following the suggestion, let's put the two lists together as columns of a matrix. Then the problem is like §6, so one basis consists the first, third, and fifth of these vectors.

If you find the basis by instead making a matrix with these five vectors as rows, when you row reduce you get the identity matrix. This means that the rows generate all of \mathbb{R}^3 , and the basis is the standard basis.

For §9: As mentioned, the idea is that when you throw two sets of equations together, the set of solutions in common is the intersection of their respective solution sets.

For the vectors $(1, 2, 1)$, $(2, 4, 2)$, $(1, 3, 3)$, putting them as the rows of a matrix and looking for a basis for the null space we get a single basis vector. Any scaled version of it will do; the simplest seems to be $(3, -2, 1)$. We can check that this vector is indeed in the null space.

For the vectors $(2, 7, 8)$, $(3, 8, 8)$, putting them as the rows of a matrix we get a basis vector proportional to $(-8, 8, -5)$, so let's use that one. We take our two null-space bases together as the rows of a matrix, whose null space should be the intersection we desire. A basis for the null space is a single vector proportional to $(2, 7, 8)$.

Although the problem doesn't ask us to, we could check that our answer is in the span of both of the original spanning sets. For W_1 we get $(2, 7, 8) = -(1, 2, 1) + 3(1, 3, 3)$. For W_2 , $(2, 7, 8)$ is already one of the spanning vectors in the second subspace.

For Problem J-3:

(a) For uniformity, let's write all vectors as column vectors and then for a row vector write the transpose of a column vector. Direction " \Leftarrow ": If $M = vw^t$ then row i is the i -th entry of v times the vector w^t . Since all rows are

proportional, the row space is spanned by w^t alone. Therefore the rank of M is 1.

Direction “ \Rightarrow ”: Since M is nonzero it has some row that is a nonzero row vector; call it v^t . Since v^t is a nonzero vector in a 1-dimensional space (the row space), it spans the row space and every vector in the space is a scalar times v^t , in fact a unique scalar since v^t is nonzero. Let r_i be the scalar for row i and let $w = (r_1, \dots, r_m)^t$, where m is the number of rows of M . Then $M = wv^t$.

(b) The key observation is that elementary row operations preserve the property that the rows are arithmetic progressions. You can do this directly, but a nicer way is to point out that the differences of consecutive columns are all the same and that this is a linear relation between columns and so is preserved by row operations.

What matrices in row-reduced echelon form have the property that their rows are in arithmetic progression? One possible row is $1, 0, -1, -2, \dots$. Another is $0, 1, 2, 3, \dots$. Also possible is $0, 0, \dots$. But that’s all, since all rows have 1 as their first nonzero entry, if any. So the rank can’t be more than 2.

For Problem J-4: (a) In this problem there are two numberings—the numbers used to name the fingers and the numbers of the terms in the sequence. The sequence repeats every 8, so we can work modulo 8. Since 8 divides 1,000,000 evenly, it’s tempting to say the 0-th term is the same as the millionth, but since there was no 0-th term in this problem we look at the 8th term, which is finger number 2 (index finger).

(b) This problem really asks what number from 0 to 9 is congruent to $7^{1,000,000}$ modulo 10. Working base 10, we simply ignore all digits but the last. 7^2 ends in 9, 7^4 ends the same as 9^2 , which is 1, and since $7^{1,000,000} = (7^4)^{250,000} \equiv 1^{250,000} \pmod{10}$, the answer is 1.

(c) See answers to (a) and (b).

For Problem J-5:

(a) We know $V \cong F^2$, so V has the same number of elements as F^2 , namely 4. In general, if F is the 2-element field then F^n will have 2^n elements.

(b) For any field F , if W_1, W_2 are distinct 2-dimensional subspaces of F^3 , then $W_1 + W_2$ is larger than either, so must be the whole space, so is of dimension 3. Then the equation $\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = \dim W_1 + \dim W_2$ becomes $3 + ? = 2 + 2$, so the intersection must have dimension 1.

(c) If W_1 and W_2 are distinct 1-dimensional subspaces, then their intersection is $\{\mathbf{0}\}$, so the equation $\dim(W_1 + W_2) + \dim(W_1 \cap W_2) = \dim W_1 + \dim W_2$

shows that their sum has dimension 2. Therefore W_1 and W_2 are contained in just one 2-dimensional subspace.

(d) As suggested, let the 1-dimensional subspaces be the plants and the 2-dimensional subspaces determine blocks (so the block for W of dimension 2 consists of the 1-dimensional subspaces contained in W). Then by (c), any two plants have exactly one block in common, and by (b), any two blocks have exactly one plant in common. This much would work over any field. For $\text{GF}(2)$, the solution to Problem G-4 shows precisely how to make the actual design. For each block we get three plants in it, since there are three 1-dimensional subspaces in each 2-dimensional vector space over $\text{GF}(2)$.

For Problem J-6:

$-x = x$ for all $x \in F$. For addition and multiplication we get

$$\begin{array}{c|cccc}
 + & 0 & 1 & \alpha & \beta \\
 \hline
 0 & 0 & 1 & \alpha & \beta \\
 1 & 1 & 0 & \beta & \alpha \\
 \alpha & \alpha & \beta & 0 & 1 \\
 \beta & \beta & \alpha & 1 & 0
 \end{array}
 \quad \text{and} \quad
 \begin{array}{c|cccc}
 \cdot & 0 & 1 & \alpha & \beta \\
 \hline
 0 & 0 & 0 & 0 & 0 \\
 1 & 0 & 1 & \alpha & \beta \\
 \alpha & 0 & \alpha & \beta & 1 \\
 \beta & 0 & \beta & 1 & \alpha
 \end{array}$$

Therefore F is closed under addition and multiplication. It does turn out that multiplication is commutative, even though for other 2×2 matrices it might not be.

(b) To see that F is a field: Additively, F is a vector subspace of the vector space of 2×2 matrices over $\text{GF}(2)$, so the laws involving addition, negation, and 0 hold. Multiplicatively, the associative law is true for matrices in general, F is commutative as we saw, and the multiplication table shows that each nonzero element of F has a multiplicative inverse. The distributive law is true for matrices in general.

(c) The characteristic is 2, since $1 + 1 = 0$.

(d) Yes, $\{0, 1\} \subseteq F$ has exactly the same operation tables as Z_2 .

For Problem J-7: In the addition table, consider the column for any element c and rows for elements r_1 and r_2 . If the corresponding two entries in the column are the same, that says $r_1 + c = r_2 + c$. We are tempted to cancel the c 's, and in fact that is ok since field have additive inverses. Then $r_1 = r_2$. This shows that two *different* rows cannot have equal entries in a column. Since the operation is commutative, each row also has distinct entries. Thus the table is a Latin square.

For the multiplication table, again we are asking whether $r_1c = r_2c \Rightarrow r_1 = r_2$. The answer is yes, since in a field nonzero elements have multiplicative inverses and so we can cancel the c . Again the operation is commutative so the rows also have distinct entries. Thus the table is a Latin square.

For Problem J-8: (a) There are two things to show: That each table $T(r)$ is a Latin square and that any two tables are orthogonal.

To see that each row of $T(r)$ has distinct entries, look at an arbitrary column j and rows i, i' . Suppose that $T(r)_{ij} = T(r)_{i'j}$. This says $x_i + rx_j = x_{i'} + rx_j$. Canceling the common term we get $x_i = x_{i'}$, so there is no repeated entry in the column.

We can't just say "similarly, ..." for the rows, since the definition of $T(r)$ is not symmetrical for rows and columns! So look at an arbitrary row i and columns j, j' . Suppose that $T(r)_{ij} = T(r)_{ij'}$. This says $x_i + rx_j = x_i + rx_{j'}$. Canceling the common term we get $rx_j = rx_{j'}$. Since $r \neq 0$ we can also cancel r and we get $x_j = x_{j'}$. Therefore there is no repeated entry in the row. This finishes the proof that $T(r)$ is a Latin square, for any r .

Now consider two squares $T(r)$ and $T(r')$. Are they orthogonal? This means that there are no two positions with the same pair of entries. In other words, if $(T(r)_{ij}, T(r')_{ij}) = (T(r)_{i'j'}, T(r')_{i'j'})$, must $i = i'$ and $j = j'$? Let's see:

$$\text{This says } \begin{cases} x_i + rx_j = x_{i'} + rx_{j'} \\ x_i + r'x_j = x_{i'} + r'x_{j'} \end{cases}$$

$$\text{Putting everything on the left in each equation we get } \begin{cases} (x_i - x_{i'}) + r(x_j - x_{j'}) = 0 \\ (x_i - x_{i'}) + r'(x_j - x_{j'}) = 0 \end{cases}$$

Subtracting and simplifying, we get $(r - r')(x_j - x_{j'}) = 0$. Since $r - r' \neq 0$, we can cancel that factor and get $x_j - x_{j'} = 0$, so $x_j = x_{j'}$. Then in the first equation of the last pair we get $x_i - x_{i'} = 0$, so that $x_i = x_{i'}$, and we are done.

(b) Using the order $\text{GF}(4) = \{0, 1, \alpha, \beta\}$, the tables are

$$\begin{bmatrix} 0 & 1 & \alpha & \beta \\ 1 & 0 & \beta & \alpha \\ \alpha & \beta & 0 & 1 \\ \beta & \alpha & 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & \alpha & \beta & 1 \\ 1 & \beta & \alpha & 0 \\ \alpha & 0 & 1 & \beta \\ \beta & 1 & 0 & \alpha \end{bmatrix} \quad \begin{bmatrix} 0 & \beta & 1 & \alpha \\ 1 & \alpha & 0 & \beta \\ \alpha & 1 & \beta & 0 \\ \beta & 0 & \alpha & 1 \end{bmatrix}$$

Using the equivalences suggested in the problem and superimposing the tables, we get the cards

ASr	2Ds	3Cg	4Hb
2Hg	ACb	4Dr	3Ss
3Db	4Sg	AHs	2Cr
4Cs	3Hr	2Sb	ADg

Here colors are lower case; S is spades and s is silver.