Assignment #4

Quiz 4 in discussion section, **Tuesday, October 23:** The same kind of problem as last week, except use the opposite method from the one you used for Quiz 3. If you did the problem directly, do it by an isomorphism, and vice versa.

Midterm #1 will be Friday, October 26, in a different room: **Haines A18**

Reading. Read §3.1.

Assignment due in lecture **Wednesday, October 24** (shorter because of the midterm)

where	Do but don't hand in	Hand in
p. 66	Ex. 6	Ex. 7
p. 73	Ex.'s 1, 2, 3	
J	J-1, J-4	J-2, J-3, J-5, J-6, J-7, J-8

Problem J-1. On Handout H, solve the problems from §2, §5, and §7.

Problem J-2. On Handout H, solve the problems from §8 and §9.

Problem J-3. (a) Show that a nonzero matrix M has rank 1 if and only if it is the matrix product of a column vector times a row vector.

(b) If M is a matrix each of whose rows is a finite arithmetic progression, show that M has rank at most 2. (Suggestion: Use column relations as discussed in lecture.)

Discussion. In (a), "nonzero matrix" means "not the zero matrix", so it's OK if some entries are 0, but not all. In contrast to this problem, notice that for a row vector times a column vector, the product doesn't make sense unless they are have the same length, and then the product is the same as their dot product. For a column vector times a row vector they don't have to be the same length and the product is a larger matrix. "If and only if" is $\Leftrightarrow$; prove each direction separately.

In (b), the finite arithmetic progresson with n terms, initial term a, and difference d means the finite sequence $a, a+d, a+2d, a+3d, \ldots a+(n-1)d$.

To gain an understanding of each of (a) and (b), on your own try examples with numbers first.

Problem J-4. (a) Number the fingers on your right hand 1 through 5 with your thumb as 1. Suppose you count back and forth starting 1, 2, 3, 4, 5, 4, 3, 2, 1, 2, ... Which finger gets the millionth count in this list?

(b) What is the last digit of $7^{1,000,000}$ (base 10)?

(c) What do (a) and (b) have to do with congruences?

Problem J-5. (a) In a previous problem you have found that for $F = \mathrm{GF}(2)$, F^2 has three 1-dimensional subspaces. If V is *any* two-dimensional vector space over GF(2), how many 1-dimensional subspaces does it have, and why?

(b) Similarly, in a previous problem you have found that for $F = GF(2)$, F^3 has seven one-dimensional subspaces and seven two-dimensional subspaces.

Using Theorem 6, p. 46, relating the dimensions of the sum and intersection of two subspaces to the dimensions of the subspaces, show that any two 2-dimensional subspaces intersect in a 1-dimensional subspace.

(c) Also, for two given 1-dimensional subspaces, how many 2-dimensional subspaces contain both? (Reason directly or by the same theorem as in (b).)

(d) Putting together (a), (b), (c), solve Problem G-9 again by using the 1-dimensional subspaces of F^3 for plants and the 2-dimensional subspaces to determine blocks.

Problem J-6. This problem shows one way to construct GF(4) concretely. Consider the following four matrices over GF(2):

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \alpha = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ \beta = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Here the symbols $0, 1$ are used for two different things (elements of GF(2) and matrices), but it should always be clear which is meant.

Let $F = \{0, 1, \alpha, \beta\}$.

(a) F is contained in the set of all 2×2 matrices over GF(2). Show that F is closed under matrix addition, negation, and multiplication, by making addition and multiplication tables using $0, 1, \alpha, \beta$ for entries. (What about negation? Does $\alpha\beta = \beta\alpha$?)

(b) Show that F is a field. (To save effort, you may quote any laws you know about operations on matrices.)

(c) What is the characteristic of F?

(d) Is $\{0, 1\}$ a subfield of F? If so, is this subfield isomorphic to $\mathbb{Z}_2$?

Note. $\beta = 1 + \alpha$, so we can just write $F = \{0, 1, \alpha, 1 + \alpha\}$. In the end it is best to think about F this way and forget it came from matrices, just as $\mathbb{C}$ can be made from matrices but we don't think of it that way.

Problem J-7. A "Latin square" is an $n \times n$ table whose entries are n different symbols each repeated n times, arranged so that no row or column has a repeated symbol. For example, in Problem G-9, the card numbers made a Latin square, and so did the suits.

(a) Show that in any finite field the addition table makes a Latin square.

(b) Show that in any finite field the multiplication table for non-zero elements makes a Latin square.

As one example, you made addition and multiplication tables for GF(4) in Problem 6. As another example, $\mathrm{GF}(5) = \mathbb{Z}_5$ has tables

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

and

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Method: In both parts, use field properties rather than trying to describe the table precisely. You can refer to rows and columns by field elements, e.g., "row r" where r is an arbitrary element of F.

Problem J-8. Two Latin squares are said to be "orthogonal" if when one is laid on top of the other all possible pairs occur. For example, your solution to Problem G-8 showed that it's possible to have two orthogonal 4×4 Latin squares, one made from the card numbers and the other made from the suits.

(a) Show that if F is a finite field with n elements, you can make $n-1$ Latin squares, each $n \times n$, so that any two are orthogonal.

Method: Let $F = \{x_1, x_1, \ldots, x_n\}$; one of these elements is 0 and another is 1, but that doesn't even matter. For each nonzero $r \in F$, make a table $T(r)$ by saying that $T(r)_{ij}$ is $x_i + r x_j$ for $i, j = 0, \ldots, n-1$. Then show that these tables have the desired properties.

(b) Using $F = \mathrm{GF}(4)$, show that you can do even better than G-8: Show how to take four different decks of cards (say with red, green, blue, and silver backs, just to identify them) and make one 4×4 arrangement of sixteen cards using Ace, 2, 3, 4 so that in each row and column, no number, suit, or deck is repeated, and also each of the sixteen possible pairs of number and suit occurs, each of the sixteen possible pairs of number and deck occurs, and each of the sixteen possible pairs of suit and deck occurs.

Method: From (a), superimposing the three resulting Latin squares you will get triples of field elements that need to be turned into a card number, suit, and deck. For uniformity, let's say for the first Latin square $0, 1, \alpha, \beta$ become respectively Ace, 2, 3, 4; for the second, $0, 1, \alpha, \beta$ become Spades, Hearts, Diamonds, Clubs; and for the third they become red, green, blue, silver.

Note. The problems on card arrangements and designs with blocks are part of the subject of combinatorics.