Math 341 - Fall 2014  
Homework 1 - Fields & Vector Spaces  
Due: 09/29/2014

Remark. Answers should be written in the following format:
A) Result.  
B) If possible the name of the method you used.  
C) The computation.

1. The Complex Numbers

Suppose \( z = a + bi \neq 0 \). We know that all non-zero elements of a field must have a multiplicative inverse. In this problem you will prove this in two ways.

(a) We would like to show that there exists some \( w = x + yi \) such that \( zw = (a + bi)(x + yi) = 1 \). Expand this expression and solve for \( x \) and \( y \) to show that a solution exists. Remember, \( 1 = 1 + 0i \). Hint: Since we know \( a + bi \neq 0 \) that means either \( a \neq 0 \) or \( b \neq 0 \). First try to do the problem assuming \( a \neq 0 \).

(b) To find the inverse another way we introduce the notion of the complex conjugate. If \( z = a + bi \) the complex conjugate \( \bar{z} = a - bi \). One important property of the complex conjugate is that \( z\bar{z} = a^2 + b^2 \in \mathbb{R} \). Use this fact to find a multiplicative inverse for \( z \).

(c) Recall that any complex number \( z \neq 0 \), can be written uniquely as \( r \cdot (\cos (\theta) + i \sin (\theta)) \) with \( r \) a positive real number, and \( 0 \leq \theta < 2\pi \). **De-Moivre’s Theorem** states that \( (\cos (\theta) + i \sin (\theta))^n = \cos (n\theta) + i \sin (n\theta) \) for every real number \( \theta \), and every integer \( n \). Use De-Moivre’s theorem to find all complex solutions to the following equations:

1. \( z^3 = 1 \).
2. \( z^4 = -1 \).

2. Finite Fields

Let \( p \) be a prime number. Then there is a field with exactly \( p \) elements. These fields are called the **finite fields** and are written \( \mathbb{F}_p \). We will construct these fields.

The elements of \( \mathbb{F}_p \) are the numbers \( \{0, 1, 2, \ldots, p - 1\} \). Addition is defined in the following way. In order to compute the sum \( x + y \in \mathbb{F}_p \), we first compute \( x + y = z \) as if \( x \) and \( y \) were ordinary integers. We then divide \( z \) by \( p \) obtaining a remainder \( r \in \mathbb{F}_p \). This number is our sum. For example: Let \( x = 5, y = 9, \) and \( p = 11 \). Then the ordinary sum of \( x \) and \( y \) is 14. The remainder after diving 14 by 11 is 3. So in \( \mathbb{F}_{11} \), \( 5 + 9 = 3 \).
Multiplication in \( \mathbb{F}_p \) is defined similarly. So to compute the product \( 5 \cdot 9 \) in \( \mathbb{F}_{11} \), we first compute the ordinary product which is 45. Dividing 45 by 11 we get a remainder of 1. So in \( \mathbb{F}_{11} \), \( 5 \cdot 9 = 1 \). So these two numbers are multiplicative inverses of one another.

(a) Write the addition and multiplication tables for \( \mathbb{F}_7 \). These tables should have the numbers \( 0, 1, \ldots, 6 \) along the top and the the left-hand side. On the interior of the table should be the corresponding sums and products. For instance in the multiplication table in the row corresponding to 2 and the column 3, you should have the number 6. Once you have done this, give the multiplicative inverses for all non-zero elements in \( \mathbb{F}_7 \).

(b) Compute \( 2^6 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \) in \( \mathbb{F}_7 \). **Fermat’s Little Theorem** states that if \( 0 \neq x \in \mathbb{F}_p \), then \( x^{p-1} = 1 \). Verify this for all non-zero elements in \( \mathbb{F}_7 \).

(c) We call an element \( y \in \mathbb{F}_p \) a quadratic residue if for some \( x \in \mathbb{F}_p \), \( x^2 = y \). Show that, if \( p \) is an odd prime, exactly half of the non-zero elements in \( \mathbb{F}_p \) are quadratic residues.

3. **Vector Spaces**

The definition for a vector space \( V \) over a field \( F \) appears in the book and will be given in class.

(a) Let \( F \) be any field. Show that \( F \) is a vector space over itself.

(b) Let \( \mathbb{F}_p^2 = \mathbb{F}_p \times \mathbb{F}_p \) be the set of ordered pairs \((x, y)\) where \( x, y \in \mathbb{F}_p \). Addition of two pairs is defined by coordinate, in other words \((x, y) + (x', y') = (x + x', y + y')\). Similarly these pairs can be multiplied by an element \( z \in \mathbb{F}_p \) in the following way, \( z \cdot (x, y) = (zx, zy) \). Show that \( \mathbb{F}_p^2 \) is a vector space over \( \mathbb{F}_p \).

Remember that the addition and multiplication you see is in \( \mathbb{F}_p \). For example, in \( \mathbb{F}_5^2 \), we have \((2, 4) + (3, 2) = (2+3, 4+2) = (0, 1)\), and \(3 \cdot (2, 4) = (3 \cdot 2, 3 \cdot 4) = (1, 2)\).

(c) The notion of a line that we are familiar with exists in these contexts though they appear slightly different. Draw a \( 7 \times 7 \) grid of points. Each point represents an element of \( \mathbb{F}_7^2 \), the bottom left point represents \((0, 0)\) and the point immediately to the right represents \((1, 0)\), and so forth. The line in \( \mathbb{F}_p^2 \) of slope \( a \) consists of all elements of the form \( x \cdot (1, a) \), where \( x \in \mathbb{F}_p \). Circle all the points on the \( 7 \times 7 \) grid that lie on the line of slope 2.

**Remarks**

- You are very much encouraged to work with other students. However, submit your work alone.

- The TA and the Lecturer will be happy to help you with the homework. Please visit the office hours.

**Good Luck!**