Math 341 - Fall 2019
Homework 1 - Fields: Definition and Examples
Due: Friday 09/13/2019

Remark. Answers should be written in the following format:
A) Result.
B) If possible the name of the method you used.
C) The computation or proof that justify what you wrote in Part A.

1. **Definition.**

   (a) Write down the definition of a field. This definition was given in class, so just write it down again.

   For what follow, suppose $(\mathbb{F}, +, \cdot, 0, 1)$ is a field (i.e., it satisfies all the axioms you wrote in Part (a) above). Let us denote it shortly by $\mathbb{F}$.

   (b) Show that:

      1. If $a \in \mathbb{F}$ satisfies $a + b = b$, for every $b \in \mathbb{F}$, then $a = 0$.
      2. If $a \in \mathbb{F}$ satisfies $a \cdot b = b$, for every $b \in \mathbb{F}$, then $a = 1$.

   (c) Show that $0 \cdot a = 0$, for every $a \in \mathbb{F}$.

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. **The Complex Numbers**.

The complex numbers are the set $\mathbb{C}$ of elements of the form $a + bi$, where $a, b \in \mathbb{R}$, and i is a symbol. We equip $\mathbb{C}$ with addition and multiplication as follows:

(i) Addition: $(a + bi) + (c + di) \stackrel{\text{def}}{=} (a + c) + (b + d)i$.

(ii) Multiplication $(a + bi) \cdot (c + di) \stackrel{\text{def}}{=} (ac - bd) + (ad + bc)i$ (or simpler, just multiply as in the real numbers and use the property $i^2 = -1$).

Let us denote by 0 the element $0 + 0i$, and by 1 the element $1 + 0i$.

It turns out that $(\mathbb{C}, +, \cdot, 0, 1)$ is a field. It is called the field of complex numbers, and will be denoted by $\mathbb{C}$.

Suppose $z = a + bi \neq 0$ is an element of $\mathbb{C}$. We know that all non-zero elements of a field must have a multiplicative inverse. In this problem you will prove this (and compute the inverse) 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) Find all the complex numbers z that satisfies $z^4 = -1$.

Remarks

- You are very much encouraged to work with other students. However, submit your work alone.
- The Lecturer will be happy to help you with the homework. Please visit the office hours if you want.

Good Luck!