MAT 240F – Assignment #1

Problem #1: Suppose that F is a field with 3 distinct elements $\{0, 1, a\}$. Prove that

$$1 + 1 = a, \quad a + 1 = 0, \quad a \cdot a = 1.$$

- We cannot have $a+1 = 1$, since the cancellation property would give $a = 0$. We cannot have $a + 1 = a$, since the cancellation property would give $1 = 0$. Hence, we must have $a + 1 = 0$.
- We cannot have $1 + 1 = 1$, since the cancellation property would give $0 = 1$. We cannot have $1 + 1 = 0$, since adding a to both sides would give

$$\begin{aligned} & a + (1 + 1) = a + 0 & \\ \Rightarrow \quad & (a + 1) + 1 = a & \text{using } F2 \text{ and } F3 \\ \Rightarrow \quad & 0 + 1 = a & \text{since } a + 1 = 0 \\ \Rightarrow \quad & 1 = a & \text{using } F1 \text{ and } F3. \end{aligned}$$

  which is impossible. Hence, the only remaining possibility is $1 + 1 = a$.
- By F3, the element a has a multiplicative inverse a^{-1}. This inverse cannot be 1 or 0, since

$$a \cdot 1 = a \neq 1, \quad a \cdot 0 = 0 \neq 1.$$

  The only possibility is $a^{-1} = a$. That is, $a \cdot a = 1$.

Problem #2: Let F be any field. Show that if $1 + 1 + 1 + 1 = 0$ in F, then $1 + 1 = 0$. Indicate clearly which properties of fields you are using. (Hint: consider $(1 + 1) \cdot (1 + 1)$.)

We have

$$\begin{aligned} (1 + 1) \cdot (1 + 1) &= (1 + 1) \cdot 1 + (1 + 1) \cdot 1 & \text{by F5} \\ &= (1 + 1) + (1 + 1) & \text{by F1 and F3} \\ &= 1 + 1 + 1 + 1 & \text{using F2 to drop parentheses} \\ &= 0 & \text{by assumption.} \end{aligned}$$

But $a \cdot b = 0$ implies $a = 0$ or $b = 0$. Hence $1 + 1 = 0$.

Problem #3: For the field $\mathbb{Z}_7 = \{0, 1, \ldots, 6\}$, list the multiplicative inverses of all non-zero elements. That is, find $1^{-1}, \quad 2^{-1}, \quad \ldots, \quad 6^{-1}$ as elements of $\mathbb{Z}_7$. (Note: If preferred, you may write the elements of $\mathbb{Z}_7$ with square brackets, as in class.)

We have

$$[1]^{-1} = [1],\ [2]^{-1} = [4],\ [3]^{-1} = [5],\ [4]^{-1} = [2],\ [5]^{-1} = [3],\ [6]^{-1} = [6],$$

since

$$\begin{aligned} &[1] \cdot [1] = [1], \\ &[2] \cdot [4] = [8] = [1], \\ &[3] \cdot [5] = [15] = [1], \\ &[6] \cdot [6] = [36] = [1] \end{aligned}$$

Problem #4: Find the last digit of the number $((7^7)^7)^7$.

Working modulo 10, we have that

$$[7]^7 = [-3]^7 = [-3] \cdot [-3]^6 = [-3] \cdot [9]^3 = [-3] \cdot [-1]^3 = [3].$$

Hence

$$([7]^7)^7 = [3]^7 = [3] \cdot [3]^6 = [3] \cdot [9]^3 = [3] \cdot [-1]^3 = [-3] = [7]$$

and finally

$$(([7]^7)^7)^7 = [7]^7 = [3],$$

by the first line. Hence, the final digit is a 3.

Problem #5: Let F be a field, and $a \in F$ an element with the property $a \cdot a = 1$. Using only the field axioms, and properties proved from it, show that

$$a = 1 \quad \text{or} \quad a = -1.$$

At each step, indicate clearly which properties you are using.

We have

$$\begin{aligned} a \cdot a = 1 &\Rightarrow a \cdot a - 1 = 0 && \text{adding } -1 \text{ to both sides, and using } F4 \\ &\Rightarrow a \cdot a - 1 \cdot 1 = 0 && \text{by F3} \\ &\Rightarrow (a-1) \cdot (a+1) = 0 && \text{by formula } a^2 - b^2 = (a-b)(a+b) \\ &\Rightarrow a = 1 \text{ or } a = -1 && \text{since } ab = 0 \text{ implies } a = 0 \text{ or } b = 0. \end{aligned}$$