Spivak Chapter Problem Set 1 Chapter 28

Jack Ceroni [*]

September 2020

Contents

1 Chapter 28

1.1 Problem 5

Lemma 1. *For any field, we have:*

$$\underbrace{(e + \cdots + e)}_{m \text{ times}} \cdot \underbrace{(e + \cdots + e)}_{n \text{ times}} = \underbrace{(e + \cdots + e)}_{mn \text{ times}}$$

for all natural numbers n and m.

Proof. Pick ome arbitrary natural number m. We proceed by induction. Clearly, the lemma is true in the case of $n = 1$. Let us assume the case of n. Consider the case of $n + 1$. We have:

$$\underbrace{(e + \cdots + e)}_{m \text{ times}} \cdot \underbrace{(e + \cdots + e)}_{n+1 \text{ times}} = \underbrace{(e + \cdots + e)}_{m \text{ times}} \cdot \left[\underbrace{(e + \cdots + e)}_{n \text{ times}} + e\right]$$

Now, we use the distributive property of fields and the definition of the identity, along with the assumtpion that the lemma holds true in the case of n to get:

$$\Rightarrow \left[\underbrace{(e + \cdots + e)}_{mn \text{ times}} + e \cdot \underbrace{(e + \cdots + e)}_{m \text{ times}}\right] = \left[\underbrace{(e + \cdots + e)}_{mn \text{ times}} + \underbrace{(e + \cdots + e)}_{m \text{ times}}\right] = \underbrace{(e + \cdots + e)}_{m(n+1) \text{ times}}$$

So the lemma is proved.

□

Theorem 1. *If in some field F we have:*

$$\underbrace{e + \cdots + e}_{n \text{ times}} = 0$$

then the smallest n for which this is true is prime.

Proof. Assume that n isn't prime. It follows that we can write n as a product of at least two whole numbers less than n and greater than 1. Thus, $n = ab$. By the previous lemma, we have:

[*]jackceroni@gmail.com

$$\underbrace{e + \cdots + e}_{n \text{ times}} = \underbrace{(e + \cdots + e)}_{a \text{ times}} \cdot \underbrace{(e + \cdots + e)}_{b \text{ times}} = 0$$

In a field, we know that $a \cdot 0 = a$, as 0 is the element of the field such that $a + 0 = a$. We then have (by distribution) that $(a \cdot a) + (a \cdot 0) = (a \cdot a) = (a \cdot a) + 0$. By left cancellation, we have $a \cdot 0 = 0$. Assume that both the right-hand sums of e (for a and b) are non-zero. It follows that they have inverses. Let us denote the two sums by A and B. It follows that:

$$e = A^{-1}AB^{-1}B = (A^{-1}B^{-1}) \cdot (AB) = (A^{-1}B^{-1}) \cdot 0 = 0$$

which is a contradiction to the definition of a field, as the additive and multiplicative identities must be different. Thus, at least one of these sums is equal to 0 it follows that either a or b is a whole number less than n such that:

$$\underbrace{e + \cdots + e}_{a \text{ or } b \text{ times}} = 0$$

which is a contradiction. Thus, n must be prime.

□

1.2 Problem 6

Lemma 2. *For some field F with a finite number of elements, there exist distinct natural numbers m and n such that:*

$$\underbrace{e + \cdots + e}_{m \textit{ times}} = \underbrace{e + \cdots + e}_{n \textit{ times}}$$

Proof. Let $|F| = k$ be the cardinality of the set defining the field (which we know is some finite natural number, k). Let:

$$E(n) = \underbrace{e + \cdots + e}_{n \text{ times}}$$

Now, consider the set $\{E(1),\ E(2),\ ...,\ E(k),\ E(k+1)\}$. It follows that there must exist two elements of this set that are equal, or else we would have a subset of F that contains $k + 1$ **distinct** elements, a clear contradiction. Hence, there exist m and n such that:

$$\underbrace{e + \cdots + e}_{m \text{ times}} = \underbrace{e + \cdots + e}_{n \text{ times}}$$

□

Theorem 2. *In a field F with a finite number of elements, there exists some natural number r such that:*

$$\underbrace{e + \cdots + e}_{r \textit{ times}} = 0$$

Proof. By the previous lemma, we know there exist m and n such that $E(m) = E(n)$. Without loss of generality, let $n < m$ (the two numbers are distinct, so one is larger than the other). We have:

$$0 + \underbrace{e + \cdots + e}_{n \text{ times}} = \underbrace{e + \cdots + e}_{m \text{ times}} = \underbrace{e + \cdots + e}_{m - n \text{ times}} + \underbrace{e + \cdots + e}_{n \text{ times}}$$

So by right cancellation, we have:

$$\underbrace{e + \cdots + e}_{m - n \text{ times}} = 0$$

It follows that $r = m - n$ and the theorem is proved. □