Marcelo Leszynski
Rootfinding Research Prerequisites
05/10/20

Section 1.1
Exercises: 1, 2, 5, 6

Exercise 1.1.1 F_2 is a field since it meets the following criteria (not checking the associative and distributive properties):

Additive Identity: 0 satisfies the additive identity property since $1+0 = 1$ and $0+0 = 0$.

Multiplicative Identity: 1 satisfies the multiplicative identity property since $1 \cdot 0 = 0$ and $1 \cdot 1 = 1$.

Additive Inverse: 0 satisfies the additive inverse property for 0 since $0+0 = 0$. Likewise, 1 satisfies the additive inverse property for 1 since $1 + 1 = 0$.

Multiplicative Inverse: The only nonzero element in F_2 is 1, which has a multiplicative inverse of 1 since $1 \cdot 1 = 1$.

Therefore, F_2 is a field.

Exercise 1.1.2

(a) Notice that, for all $f \in F_2$, we have that $f^2 + f = f + f = 0$. thus, given the polynomial $g(x, y) = x^2y + y^2x \in F_2[x, y]$, we have that

$$\begin{aligned}
g(x,y) &= x^2y + y^2x \\
&= x^2y + xy + y^2x + xy && \text{adding zero} \\
&= (x^2 + x)y + (y^2 + y)x \\
&= 0(y) + 0(x) \\
&= 0 + 0 = 0
\end{aligned}$$

as desired. This does not contradict proposition 5 because, in this instance, the field $k = F_2$ is not infinite.

(b) Define $g(x, y, z) = x^2yz + xy^2z + xyz^2 + xyz$. Then, similarly to 1.1.2a, we have that

$$\begin{aligned}
g(x,y,z) &= x^2yz + xy^2z + xyz^2 + xyz \\
&= x^2yz + xy^2z + xyz^2 + xyz + 4xyz && \text{adding zero} \\
&= (x^2yz + xyz) + (xy^2z + xyz) + (xyz^2 + xyz) + (xyz + xyz) && \text{regrouping} \\
&= (x^2 + x)yz + (y^2 + y)xz + (z^2 + z)xy + (xyz + xyz) \\
&= 0(yz) + 0(xz) + 0(xy) + 0 \\
&= 0 + 0 + 0 + 0 = 0
\end{aligned}$$

as desired.

(c) Continuing our pattern from parts (a) and (b), we can construct $g(x_1, \ldots, x_n) \in F_2[x_1, \ldots, x_n]$ as follows:

$$g(x_1, \ldots, x_n) = (x_1^2 + x_1)x_2 \ldots x_n + (x_2^2 + x_2)x_1 \cdot x_3 \ldots x_n + \ldots + (x_n^2 + x_n)x_1 \ldots x_{n-1}$$

Exercise 1.1.5

(a) $f(x, y, z) = (y^2z)x^5 - (y^3)x^4 + (z)x^2 + (y + 2)x + (y^5 - y^3z - 5z + 3)$

(b) $f(x, y, z) = y^5 + (-x^4 - z)y^3 + (x^5z)y^2 + (x)y + (2x - 5z + 3)$

(c) $f(x, y, z) = (x^5y^2 + x^2 - y^3 - 5)z + (-x^4y^3 + y^5 + xy + 2x + 3)$

Exercise 1.1.6

(a)

Proof. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and assume that f vanishes at every point of $\mathbb{Z}^n$. We wish to show that f is the zero polynomial and proceed by induction on n.

Base case: Suppose that $n = 1$. Then, since $f(a) = 0$ for all $a \in \mathbb{Z}$, it is obvious that there are an infinite number of roots, which can only occur when $f = 0$ is the zero polynomial.

Inductive step: Assuming the base case and letting $n > 1$, we rewrite f as

$$f = \sum_{i=0}^{N} g_i(x_1, \ldots, x_{n-1})x_n^i$$

by collecting powers of x_n. Note that $g_i(a_1, \ldots, a_{n-1}) = 0$ for all i. Thus, by induction, we have that $g_i \in \mathbb{C}[x_1, \ldots, x_{n-1}]$ gives the zero function, which implies that f is the zero polynomial in $\mathbb{C}[x_1, \ldots, x_n]$. □

(b) Let $f \in \mathbb{C}[x_1 \ldots x_n]$ and let M be the largest power of any variable that appears in f. Let $\mathbb{Z}^n_{M+1}$ be the set of points of $\mathbb{Z}^n$, all coordinates of which lie between 1 and $M + 1$ inclusive.

Proof. We wish to show that if f vanishes at all points of $\mathbb{Z}^n_{M+1}$, then f is the zero polynomial. We begin by assuming that f vanishes at all points of $\mathbb{Z}^n_{M+1}$ and work by induction on n.

Base case: Suppose that $n = 1$. Then f is a polynomial in one variable with a maximum degree of M. If we have that $f(1) = f(2) = \ldots = f(M) = f(M + 1) = 0$, we can conclude that f must have at least $M + 1$ distinct roots. Since the number of distinct roots is greater than the degree of the polynomial, it must be that the polynomial is the zero polynomial $f = 0$.

Inductive step: Assuming the base case and letting $n > 1$, we rewrite f as

$$f = \sum_{i=0}^{M} g_i(x_1, \ldots, x_{n-1})x_n^i$$

with $g_i \in \mathbb{C}[x_1, \ldots, x_{n-1}]$. We know then that, for any $(a_1, \ldots, a_{n-1}) \in \mathbb{Z}^{n-1}_{M+1}$, we have

$$f(a_1, \ldots, a_{n-1}, x_n) = \sum_{i=0}^{M} g_i(a_1, \ldots, a_n - 1)x_n^i.$$

We see that $g_i(a_1, \ldots, a_{n-1}) = 0$ for all $i = 0, \ldots, M$. Now we have that g_i is the zero polynomial by induction, which implies that f is also the zero polynomial. □