Marcelo Leszynski
Rootfinding Research Prerequisites
07/13/20

Assignment 1.5
Exercises: 1, 2, 3, 4, 5, 6, 7, 10, 11, 12

Exercise 1.5.1

Proof. Let $f \in \mathbb{C}[x]$ be a polynomial of degree $n > 0$. We wish to show that f can be written in the form $f = c(x - a_1) \ldots (x - a_n)$, where $c, a_1, \ldots, a_n \in \mathbb{C}$ and $c \neq 0$.

We begin by noting that f has some root $r_1 \in \mathbb{C}$ by Theorem 1.1.7. This allows us to rewrite $f = f_1(x - a_1)$ for some $f_1 \in \mathbb{C}[x]$. By Corollary 1.5.3, we know that f_1 has a degree of up to $n - 1$. We can proceed similarly by acknowledging that f_1 has a root $r_2 \in \mathbb{C}$ such that $f_1 = f_2(x - r_2)$ for some $f_2 \in \mathbb{C}[x]$ of degree $n - 2$. We repeat this process n times to get $f_1, \ldots, f_{n-1}$ with $f_{n-1} = cx + d$ having degree 1. Then $c \neq 0$, so $f_{n-1} = c(x - r_n)$ for $r_n = -d/c$. We now have the following

$$\begin{aligned} f &= f_1(x - r_1) = f_2(x - r_2)(x - r_1) = \ldots \\ &= f_{n-1}(x - r_{n-1}) \ldots (x - r_1) \\ &= c(x - r_n)(x - r_{n-1}) \ldots (x - r_1) \\ &= c(x - r_1) \ldots (x - r_n) \end{aligned}$$

as desired. □

Exercise 1.5.2

Proof. Let A be the matrix pictured in the problem. If we suppose that the determinant $\det(A) = 0$, then there exists some vector $\vec{v} \in k^n$ such that $A\vec{v} = \vec{0}$ with $\vec{v} \neq \vec{0}$.

Let $\vec{v} = \langle c_0, \ldots, c_{n-1} \rangle^T$. Next, define a polynomial that represents a row of A as $p(x) = c_{n-1}x^{n-1} + \ldots + c_0$. Since the degree of $p(x)$ is at most $n - 1$, it can have up to $n - 1$ distinct roots. Observe that $\det(A) = 0$ implies that $p(a_i) = c_{n-1}a_i^{n-1} + \ldots + c_0 = 0$ for all $1 \leq i \leq n, i \in \mathbb{N}$. Thus we have n distinct roots resulting from distinct a_i values, which contradicts our previous finding. Therefore, we can conclude by contradiction that $\det(A) \neq 0$. □

Exercise 1.5.3

Proof. We wish to show that $I = \langle x, y \rangle \subseteq k[x, y]$ is not a principal ideal. In other words, I cannot be generated by one element. We proceed with a proof by contradiction.

Suppose, by way of contradiction, that $\langle x, y \rangle = \langle g \rangle$ for some $g \in k[x, y]$. Then g divides x, or in other words, $x = fg$ for some $f \in k[x, y]$. Rewriting $f = \sum_i f_i(y)x^i$ and $g = \sum_j g_j(y)x^j$, we have that

$$x = fg = \left(\sum_i f_i(y)x^i \right) \left(\sum_j g_j(y)x^j \right) = \sum_t \left(\sum_{i+j=t} f_i(y)g_j(y) \right) x^t.$$

There are only two cases where this is possible.

Case 1: $f = c$ and $g = dx$ with $c, d \in k$ satisfying $cd = 1$. This implies that $y \in \langle x, y \rangle = \langle dx \rangle$ is divisible by x, which is impossible.

Case 2: $f = cx$ and $g = d$ with $c, d \in k$ satisfying $cd = 1$. This implies that $\langle x, y \rangle = \langle d \rangle$. This is impossible since $1 \notin \langle x, y \rangle$.

$\square$

Exercise 1.5.4

Proof. Assume that $h = \gcd(f, g)$. Then, by Proposition 1.5.6, h is a generator of $\langle f, g \rangle$. That is, $\langle h \rangle = \langle f, g \rangle$. Note that $h = 1 \cdot h \in \langle h \rangle = \langle f, g \rangle$, which implies that $h = Af + Bg$ for some $A, B \in k[x]$ by definition of the ideal $\langle f, g \rangle$. $\square$

Exercise 1.5.5

Proof. Let $f, g \in k[x]$. We wish to show that $\langle f - qg, g \rangle = \langle f, g \rangle$ for any $q \in k[x]$.

($\subseteq$):

$$f - qg = 1 \cdot f + (-q) \cdot g \in \langle f, g \rangle$$
$$g = 0 \cdot f + 1 \cdot g \in \langle f, g \rangle$$

so $\langle f - qg, g \rangle \subseteq \langle f, g \rangle$.

($\supseteq$):

$$f = 1 \cdot (f - qg) + q \cdot g \in \langle f - qg, g \rangle$$
$$g = 0 \cdot (f - qg) + 1 \cdot g \in \langle f - qg, g \rangle$$

so $\langle f, g \rangle \subseteq \langle f - qg, g \rangle$.

Therefore, $\langle f - qg, g \rangle = \langle f, g \rangle$ as desired. $\square$

Exercise 1.5.6

Proof. Let $f_1, \ldots, f_s \in k[x]$ and let $h = \gcd(f_2, \ldots, f_s)$. We wish to show that $\langle f_1, h \rangle = \langle f_1, f_2, \ldots, f_s \rangle$.

($\subseteq$): By Proposition 1.5.6, we know that h is a generator of $\langle f_2, \ldots, f_s \rangle$, i.e., $\langle h \rangle = \langle f_2, \ldots, f_s \rangle \subseteq \langle f_1, f_2, \ldots, f_s \rangle$. We observe that $f_1 \in \langle f_1, f_2, \ldots, f_s \rangle$. Thus $\langle f_1, h \rangle \subseteq \langle f_1, f_2, \ldots, f_s \rangle$.

($\supseteq$): Note that $f_1 \in \langle f_1, h \rangle$ and that, for $2 \leq i \leq s$, $f_i \in \langle f_2, \ldots, f_s \rangle = \langle h \rangle \subseteq \langle f_1, h \rangle$. Thus $\langle f_1, f_2, \ldots, f_s \rangle \subseteq \langle f_1, h \rangle$.

Therefore, $\langle f_1, h \rangle = \langle f_1, f_2, \ldots, f_s \rangle$. $\square$

Exercise 1.5.7 The algorithm is as follows:

Input: $f_1, \ldots, f_s \in k[x], s \geq 2$
Output: $h = \gcd(f_1, \ldots, f_s)$

$h := f_s$
FOR $i = s - 1$ TO 1 DO {
$h := \gcd(f_i, h)$
}
RETURN h

Exercise 1.5.10 The algorithm is as follows:

Input: $f, g \in k[x]$
Output: $h = \gcd(f, g), A, B \in k[x]$ with $Af + Bg = h$

$h := f$
$s := g$
$A := 1$
$B := 0$
$C := 0$
$D := 1$
WHILE $s \neq 0$ DO {
$r :=$ remainder(h, s)
$q :=$ quotient(h, s)
$h := s$
$s := r$
TempA $:= A$
TempB $:= B$
$A := C$
$B := D$
$C :=$ TempA $- q * C$
$D :=$ TempB $- q * D$
}
RETURN h, A, B

Exercise 1.5.11

(1.5.11a): Let $f \in \mathbb{C}[x]$ be nonzero. We wish to show that $V(f) = \emptyset$ if and only if f is constant and will proceed by proving the contrapositive statements $V(f) \neq \emptyset \Leftrightarrow f$ is nonconstant.

($\Rightarrow$): Assume $V(f) \neq \emptyset$, so there exists some $a \in V(f)$. This implies that $f(a) = 0$ so f must be nonconstant since we assumed f to be nonzero.

($\Leftarrow$): Assume f is nonconstant. Then, by Theorem 1.1.7, there exists some root $a \in \mathbb{C}$ which implies $a \in V(f)$ so $V(f) \neq \emptyset$.

Therefore, $V(f) = \emptyset$ if and only if f is constant.

(1.5.11b): Let $f_1, \dots, f_s \in \mathbb{C}[x]$. We wish to show that

$$V(f_1, \dots, f_s) = \emptyset \Leftrightarrow \gcd(f_1, \dots, f_s) = 1.$$

($\Rightarrow$): Let $f = \gcd(f_1, \dots, f_s)$. Then f is a generator for $\langle f_1, \dots, f_s \rangle$ such that $\langle f \rangle = \langle f_1, \dots, f_s \rangle$. Proposition 1.4.4 then gives that $V(f_1, \dots, f_s) = V(f) = \emptyset$. This implies that f is a constant, and it follows that $f = 1$ since any other nonzero value implies that $V(f_1, \dots, f_2) \neq \emptyset$.

($\Leftarrow$): Let $f = \gcd(f_1, \dots, f_s) = 1$. It follows that f is a generator for $\langle f_1, \dots, f_s \rangle$, i.e., $\langle f \rangle = \langle f_1, \dots f_s \rangle$. Note that $V(f) = \emptyset$ since f is a constant. Proposition 1.4.4 then gives that $V(f) = V(f_1, \dots, f_s) = \emptyset$.

Therefore, $V(f_1, \dots, f_s) = \emptyset$ if and only if $\gcd(f_1, \dots, f_s) = 1$.

(1.5.11c): Given an arbitrary set of polynomials $f_1, \dots, f_s \in \mathbb{C}[x]$, compute the gcd $f = \gcd(f_1, \dots, f_s)$. If $f = 1$, then $V(f_1, \dots, f_s) = \emptyset$. If $f \neq 1$, then $V(f_1, \dots, f_s) \neq \emptyset$. This is true because of the biconditional that was proven in Exercise 1.5.11b.

Exercise 1.5.12

(1.5.12a): $V(f) = \{a_1, \dots, a_l\}$ follows by definition of $f = c(x - a_1)^{r_1} \dots (x - a_l)^{r_l}$.

(1.5.12b): Let $f_{red} = c(x - a_1) \dots (x - a_l)$. We wish to show that $I(V(f)) = \langle f_{red} \rangle$.

($\subseteq$): Let $g \in I(V(f))$, i.e., g vanishes at $\{a_1, \dots, a_l\}$. This means that g has at least l roots labeled $a_1, \dots, a_l, a_{l+1}, \dots, a_m$ where $m \geq l$. Since we are over $\mathbb{C}$, we have that

$$g = d(x - a_1)^{s_1} \dots (x - a_l)^{s_l} (x - a_{l+1})^{s_{l+1}} \dots (x - a_m)^{s_m}$$

with $d \in \mathbb{C}$ such that $d \neq 0$ and $s_i \geq 1$ for all $1 \leq i \leq m$. Hence, g is a multiple of $(x - a_1) \dots (x - a_l)$ and thus it is a multiple of $f_{red} = c(x - a_1) \dots (x - a_l)$ (since $c \neq 0$). Thus $g \in \langle f_{red} \rangle$. Since g is arbitrary, we have shown that $I(V(f)) \subseteq \langle f_{red} \rangle$.

($\supseteq$): Note that f_{red} vanishes on $\{a_1, \dots, a_l\} = V(f)$. Thus $f_{red} \in I(V(f))$ and so $\langle f_{red} \rangle \subseteq I(V(f))$.

Therefore, we conclude that $I(V(f)) = \langle f_{red} \rangle$ as desired.