Marcelo Leszynski
Rootfinding Research Prerequisites
10/07/20

Assignment 5.2
Exercises: 1, 2, 3, 5, 8, 13, 16

Exercise 5.2.1 To determine wheter $f \equiv g \mod I$, first compute a Grobner basis G for $I = \langle f_1, \cdots, f_s \rangle$, then check to see if $\overline{f-g}^G = 0$. If yes, then $f \equiv g \mod I$. Else, $f \not\equiv g \mod I$.

Exercise 5.2.2

Proof. We begin by defining a map Φ mapping ϕ to the equivalence class of $[f]$ congruent modulo $\mathbf{I}(V)$. In other words, we have that f represents ϕ. Likewise, we define a map Ψ that maps the equivalence class $[g]$ congruent module $\mathbf{I}(V)$ to the polynomial function $\psi : V \to k$ represented by g. Using Proposition 5.1.2, these two maps are well defined. Thus, we suppose that ϕ is represented by f and have that

$$\Psi(\Phi(\phi)) = \Psi([f])$$

is equal to the polynomial function represented by $f = \phi$, and that

$$\Phi(\Psi([f])) = [f]$$

is equal to Ψ of the polynomial function represented by f.

It follows that Φ and Ψ are inverses of each other, so the distinct polynomial functions ϕ are in one-to-one correspondence with the equivalence classes of polynomials under congruence module $\mathbf{I}(V)$ as desired. □

Exercise 5.2.3

Proof. Let I be an ideal such that $I \in k[x_1, \ldots, x_n]$. Let $[f], [g], [h] \in k[x_1, \ldots, x_n]/I$. Using the fact that $k[x_1, \ldots, x_n]$ is a commutative ring, we have that

$([f] + [g]) + [h] = [(f + g) + h] = [f + (g + h)] = [f] + ([g] + [h])$	associativity (+)
$[f] + [g] = [f + g] = [g + f] = [g] + [f]$	commutativity (+)
$[f] \cdot [g] = [f \cdot g] = [g \cdot f] = [g] \cdot [f]$	commutativity (*)
$[f] \cdot ([g] + [h]) = [f \cdot (g + h)] = [f] \cdot [g] + [f] \cdot [h]$	distributivity
$[f] + [0] = [f + 0] = [f]$	additive ident.
$[f] \cdot [1] = [f \cdot 1] = [f]$	multiplicative ident.
$[f] + [-f] = [f + (-f)] = [0]$	additive inverse

□

Exercise 5.2.5

(5.2.5a): Using the division algorithm in $\mathbb{R}[x]$, we have that $f = q(x^2+1) + r$ for some $q, r \in \mathbb{R}[x]$ where $r = 0$ or $\deg(r) < 2$ is unique. Thus we can write $r = ax + b$ for some $a, b \in \mathbb{R}$. Since $f - r = q(x^2+1) \in I = \langle x^2+1 \rangle$, r satisfies the desired conditions of congruence.

(5.2.5b): We define addition and multiplication in $\mathbb{R}[x]/\langle x^2+1 \rangle$ as follows:

$$[ax+b] + [cx+d] = [(a+c)x + (b+d)],$$

$$[ax+b] \cdot [cx+d] = [(ax+b)(cx+d)] = [acx^2 + (ad+bc)x + bd] = [(ad+bc)x + (bd-ac)].$$

(5.2.5c): We can observe that $\mathbb{R}[x]/\langle x^2+1 \rangle$ is ring isomorphic to $\mathbb{C}$ by noting that $[x^2+1] = [0]$ in $\mathbb{R}[x]\langle x^2+1 \rangle$, so we have $[x^2] + [1] = 0$, which implies that $[x^2] = [-1]$. Thus $[x]$ is the square root of -1.

Exercise 5.2.8

(5.2.8a):

Proof. We have that Φ is onto, so for any $s \in S$, there exists some $r \in R$ such that $\Phi(r) = s$. It follows that

$$s = \Phi(r) = \Phi(1r) = \Phi(1)\Phi(r) = s\Phi(1).$$

Thus, when $s = 1$, we have that $\Phi(1) = 1$ and the identity in R is mapped to the identity in S by Φ. □

(5.2.8b):

Proof. For any $r \in R$, we have that $\Phi(r^{-1})$ is a multiplicative inverse for $\Phi(r)$ since

$$\Phi(r)\Phi(r^{-1}) = \Phi(rr^{-1}) = \Phi(1) = 1.$$

□

(5.2.8c): We have shown that S contains the identity along with a multiplicative inverse. To show commutativity, we have that, for some $s_1, s_2 \in S$ such that $\Phi(r_1) = s_1$ and $\Phi(r_2) = s_2$,

$$s_1 s_2 = \Phi(r_1)\Phi(r_2) = \Phi(r_1 r_2) = \Phi(r_2 r_1) = \Phi(r_2)\Phi(r_1) = s_2 s_1.$$

Exercise 5.2.13

(5.2.13a): Note that $0 \in \Phi^{-1}(J)$ since $\Phi(0) = \Phi(0) + \Phi(0) = 0$, Next, we suppose that $\Phi(r_1) = s_1 \in J, \Phi(r_2) = s_2 \in J$. It follows that

$$\Phi(r_1 + r_2) = \Phi(r_1) + \Phi(r_2) = s_1 + s_2,$$

which implies $r_1 + r_2 \in \Phi^{-1}(J)$, since $s_1 + s_2 \in J$. It also follows that

$$\Phi(r_1 r_2) = \Phi(r_1)\Phi(r_2) = \Phi(r_1)s_2,$$

which implies $r_1 r_2 \in \Phi^{-1}(J)$, since $\Phi(r_1)s_2 \in J$.

(5.2.13b): For any ideal $I \in R$, we must show $\Phi(I)$ is an ideal in S. We know that $0 \in \Phi(I)$, so it suffices to show closure under addition and multiplication. Let $s_1, s_2 \in \Phi(I)$ such that $\Phi(r_1) = s_1, \Phi(r_2) = s_2$ for some $r_1, r_2 \in I$. We have that

$$r_1 + r_2 \in I, \Phi(r_1 + r_2) = \Phi(r_1) + \Phi(r_2) = s_1 + s_2 \Rightarrow s_1 + s_2 \in \Phi(I).$$

Similarly, we have that

$$\Phi(r_1 r_2) = \Phi(r_1)\Phi(r_2) = s_1 s_2 \Rightarrow s_1 s_2 \in \Phi(I)$$

since $r_1 r_2 \in I$.

Since we know that Φ is bijective, we have that

$$\Phi \circ \Phi^{-1}(J) = J, \Phi^{-1} \circ \Phi(I) = I$$

for ideals $I \in R$ and $J \in S$.

Exercise 5.2.16

(5.2.16a): $0 \in \ker(\Phi)$ by Exercise 5.2.13a. Assume $r_1, r_2 \in \ker(\Phi)$. Then $\Phi(r_1 + r_2) = \Phi(r_1) + \Phi(r_2) = 0 + 0$, so $r_1 + r_2 \in \ker(\Phi)$. We also have that, for some $r \in k[x_1, \ldots, x_n]$, $\Phi(r r_1) = \Phi(r)\Phi(r_1) = \Phi(r) \cdot 0 = 0$, so $r \cdot r_1 \in \ker(\Phi)$. Therefore, $\ker(\Phi)$ is an ideal.

(5.2.16b): Assume that $r \equiv r' \mod \ker(\Phi)$ such that $[r] = [r']$ with $r - r' \in \ker(\Phi)$. Since $\Phi(r) - \Phi(r') = \Phi(r - r') = 0$, it follows that

$$v([r]) = \Phi(r) = \Phi(r') = v([r']).$$

Therefore, the mapping v is well-defined.

(5.2.16c): Let $[r_1], [r_2] \in k[x_1, \ldots, x_n]/\ker(\Phi)$. We then have that

$v([r_1] + [r_2]) = v([r_1 + r_2]) = \Phi(r_1 + r_2) = \Phi(r_1) + \Phi(r_2) = v([r_1]) + v([r_2]),$
$v([r_1][r_2]) = v([r_1 r_2]) = \Phi(r_1 r_2) = \Phi(r_1)\Phi(r_2) = v([r_1])v([r_2]),$
$v([1]) = \Phi(1) = 1$ by Exercies 5.2.8a

(5.2.16d): Let $[r_1], [r_2] \in k[x_1, \ldots, x_n]/\ker(\Phi)$ and assume that $v([r_1]) = v([r_2])$. It follows that $\Phi(r_1) = \Phi(r_2)$, which implies that $\Phi(r_1 - r_2) = 0$, i.e., $r_1 - r_2 \in \ker(\Phi)$. Therefore, $[r_1] = [r_2]$. Thus v is one-to-one, and v being onto follows from the fact that $v([r]) = \Phi(r)$ and Φ is an onto mapping.