Chapter 1, Geometry, Algebra, and Algorithms

§5. Polynomials of One Variable.

---

§1.5.1.

Prove: If k is an algebraically closed field and $f \in k[x]$ is a nonzero polynomial, then f can be written in the form $f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$, where $c, a_1, a_2, \ldots, a_n \in \mathbb{C}$ and $c \neq 0$.

Proof. By induction on the degree of f, using the fact that in an algebraically closed field k each nonzero polynomial h has a factorization of the form $h(x) = (x-a)g(x)$, where $a \in k$ and $g(x)$ is a nonzero polynomial.

---

§1.5.2.

Consider the Vandermonde determinant

$$\text{Vandermonde}(a_1, a_2, \ldots, a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix}.$$

We will show how to evaluate Vandermonde$(a_1, \ldots, a_n)$ when $a_1, \ldots, a_n \in k$, where k is an arbitrary field. Starting with the rightmost column, add to it $-a_1$ times the column that preceeds it. Then do the same with the $n-1$-st column and continue in this manner moving to the left through the columns until this procedure terminates when $-a_1$ times the first column is added to the second. At this stage the only nonzero entry in the first row is the initial 1. Expand by minors along the first row. For each k, $2 \leq k \leq n$, factor $a_k - a_1$ out of the $(k-1)$-st column of the remaining $(n-1) \times (n-1)$-determinant to get the relation

$$\text{Vandermonde}(a_1, \ldots, a_n) = (a_2 - a_1)(a_3 - a_1)\cdots(a_n - a_1) \cdot \text{Vandermonde}(a_2, \ldots, a_n).$$

If this expansion is continued in the same manner we eventually arrive at the identity

$$\text{Vandermonde}(a_1, a_2, \ldots, a_n) = \prod_{1 \leq i < j \leq n} (a_j - a_i).$$

It follows from this that Vandermonde$(a_1, a_2, \ldots, a_n) \neq 0$ when the a_i's are distinct.

---

§1.5.3.

The fact that every ideal of $k[x]$ is principal (generated by one element) is special to the case of polynomials in one variable. In this exercise we will see why. Namely, consider the ideal $I = \langle x, y \rangle \subset k[x, y]$. Prove that I is not a principal ideal.

Proof. Suppose $I = k[x, y] \cdot f(x, y)$. Then $x = h(x, y)f(x, y)$ and $y = w(x, y)f(x, y)$; so f divides x and f divides y. However, the only divisors of x are the polynomials of the form ax or a where $0 \neq a \in k$. Similarly for y. Since f cannot have both of the forms ax and by, it must be that $f(x, y) = a \neq 0$ is a nonzero constant. Then, however, $f(x, y) \cdot k[x, y] = k[x, y] \neq \langle x, y \rangle$, which contradicts the assumption that $f(x, y) \cdot k[x, y] = \langle x, y \rangle$.

---

§1.5.4.

If h is the GCD of $f, g \in k[x]$, prove that there are polynomials $A, B \in k[x]$ such that $Af + Bg = h$.

Proof. We will make free use of the fact that $k[x]$ is a principal ideal domain. Let $q \in k[x]$ generate the ideal $\langle f, g\rangle$; so $\langle f, g\rangle = q \cdot k[x]$. In particular, $q \in \langle f, g\rangle$; so there are polynomials $F, G \in k[x]$ for which $q = Ff + Gg$, since $\langle f, g\rangle$ consists of such combinations of f and g. First note that $f \in \langle f, g\rangle = q \cdot k[x]$; so q divides f. Similarly, q divides g. Next note that h divides f and h divides g. It follows that h divides $Ff + Gg = q$ and we have $q = Wh$ for some $0 \neq W \in k[x]$. Since h is the greatest common divisor of f and g, the polynomial W must be a constant, for otherwise $Wh = q$ would be a greater common divisor. But in this case $W^{-1} \in k$ and $h = w^{-1}q = (W^{-1}F)f + (W^{-1}G)g$ showing that $A = W^{-1}F$ and $B = W^{-1}G$ will satisfy $Af + Bg = h$. We have also shown that $\langle f, g\rangle = h \cdot k[x]$.

---

§1.5.5.

If $f, g \in k[x]$, show that $\langle f - qg, g\rangle = \langle f, g\rangle$ for any q in $k[x]$.

Proof. ($\subset$): This is clear because both $f - qg$ and g are in the ideal $\langle f, g\rangle$.

($\supset$): $f = (f - qg) + qg$ shows $f \in \langle f - qg, g\rangle$ and it is trivial that $g \in \langle f - qg, g\rangle$. So these equations establish the stated inclusion.

---

§1.5.6.

Given $f_1, \ldots, f_s \in k[x]$, let $h = GCD(f_2, \ldots, f_s)$. Then use the equality $\langle h\rangle = \langle f_2, \ldots, f_s\rangle$ to show that $\langle f_1, h\rangle = \langle f_1, f_2, \ldots, f_s\rangle$.

Solution. ($\subset$): This is trivial because $h \in \langle h\rangle = \langle f_2, \ldots, f_s\rangle \subset \langle f_1, f_2, \ldots, f_s\rangle$.

($\supset$): It suffices to show $f_2 \in \langle f_1, h\rangle$. But $f_2 \in \langle f_2, \ldots, f_s\rangle = \langle h\rangle \subset \langle f_1, h\rangle$.

---

§1.5.7.

If you are allowed to compute the GCD of only two polynomials at a time (which is true for most computer algebra systems), give pseudocode for an algorithm that computes the GCD of polynomials $f_1, \ldots, f_s \in k[x]$, where $s > 2$. Prove that your algorithm works.

Solution. Use the fact that $GCD(f_1, \ldots, f_s) = GCD\big(f_s, GCD(f_1, \ldots, f_{s-1})\big)$.

Proof. If h divides $f_1, \ldots, f_s$, then h divides $GCD(f_1, \ldots, f_{s-1})$ and h divides f_s. So any divisor of the "left side" divides the "right side". If g divides the "right side", g divides f_s and g divides $GCD(f_1, \ldots, f_{s-1})$. This means g divides each of the polynomials $f_1, \ldots, f_s$ and so divides $GCD(f_1, \ldots, f_s)$. Thus any divisor of the "right side" divides the "left side". The two sides agree to within a unit of $k[x]$.

---

§1.5.8.

Use a computer algebra system to compute the following GCD's.

(a) $GCD(x^4 + x^2 + 1,\ x^4 - x^2 - 2x - 1,\ x^3 - 1)$.

Solution. We use Mathematica 3.01. The command

In[1]= PolynomialGCD[x^4+x^2+1,x^4-x^2-2*x-1,x^3-1]

Gives the output

Out[1]= $1 + x + x^2$

(b) $GCD(x^3 + 2x^2 - x - 2,\ x^3 - 2x^2 - x + 2,\ x^3 - x^2 - 4x + 4)$.

Solution. The Mathematica command sequence

In[2]=PolynomialGCD[x^3+2x^2-x-2,x^3-2*x^2-x+2,x^3-x^2-4*x+4]

Out[2]= $-1 + x$.

---

§**1.5.9.**

Use the method described in the text to decide whether

$$x^2 - 4 \in \langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4,\ x^3 - 2x^2 - x + 2\rangle$$

Solution. The Mathematica command sequence

In[3]=PolynomialGCD[x^3+x^2-4*x-4,x^3-x^2-4*x+4,x^3-2*x^2-x+2]

Yields the output

Out[3]= $-2 + x$.

Since $x^2 - 4$ is a multiple of $x - 2$, it is true that

$$x^2 - 4 \in \langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4,\ x^3 - 2x^2 - x + 2\rangle$$

---

§**1.5.10.**

Give pseudocode for an algorithm that has input $f, g \in k[x]$ and output $h, A, B \in k[x]$, where $h = GCD(f, g)$ and $Af + Bg = h$.

Hint: The idea is to add variables A, B, C, D to the algorithm so that $Af + Bg = h$ and $Cf + Dg = s$ remain true at every step of the algorithm. Note the initial values of A, B, C, D are $1, 0, 0, 1$, respectively. You may find it useful to let quotient(f, g) denote the quotient of f on division by g, i.e., if the division algorithm yields $f = qg + r$, then $q =$ quotient(f, g).

Solution.

---

§**1.5.11.**

In this exercise we will study the one-variable case of the *consistency problem* from §1.2. Given $f_1, \ldots, f_s \in k[x]$. this asks if there is an algorithm to decide whether $\mathbf{V}(f_1, \ldots, f_s)$ is nonempty. We will see the answer is yes when k is algebraically closed.

(a) Let $f \in k[x]$ be a nonzero polynomial. Then since k is algebraically closed, f has a root in k unless $\deg f = 0$, i.e., unless f is constant. That is $\mathbf{V}(f) = \emptyset$ if and only if $\deg f = 0$. Remember: The zero polynomial has degree -1.

(b) If $f_1, \ldots, f_s \in k[x]$, prove $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$ if and only if $GCD(f_1, \ldots, f_s) = 1$.

Proof. ($\Rightarrow$): Suppose $g = GCD(f_1, \ldots, f_s)$. If $\deg g > 0$, and k is algebraically closed, let $\zeta \in k$ be a root of g. Then since g divides each f_i, $f_i(\zeta) = 0$, $1 \le i \le s$. As a consequence $\zeta \in \mathbf{V}(f_1, \ldots, f_s) \neq \emptyset$.

($\Leftarrow$): If $\xi \in \mathbf{V}(f_1, \ldots, f_s)$, then $x - \xi$ divides each f_i, $1 \le i \le s$, and hence $x - \xi$ divides $GCC(f_1, \ldots, f_s)$; so $GCD(f_1, \ldots, f_s) \neq 1$.

---

§**1.5.12.**

This exercise will study the one-variable case of the *Nullstellensatz problem* from §1.4, which asks for the relation between $\mathbf{I}\big(\mathbf{V}(f_1, \ldots, f_s)\big)$ and $\langle f_1, \ldots, f_s\rangle$ when $f_1, \ldots, f_s \in \mathbb{C}[x]$. By using GCD's we can reduce to the case of a single generator. So in this problem we will explicitly determine $\mathbf{I}(\mathbf{V}(f))$ when $f \in \mathbb{C}[x]$ is a nonconstant polynomial. Since we are working over the complex numbers, we know by Exercise 1.5.1 that f factors completely, i.e.,

$$f = c(x - a_1)^{r_1} \cdots (x - a_\ell)^{r_\ell},$$

where $a_1, \ldots, a_\ell \in \mathbb{C}$ are distinct and $c \in \mathbb{C} - \{0\}$. Define the polynomial

$$f_{red} = c(x - a_1) \cdots (x - a_\ell).$$

Note that f and f_{red} have the same roots but their *multiplicities* may differ. In particular, all roots of f_{red} have multiplicity one. It is common to call f_{red} the *reduced* or *square-free* part of f. To explain the latter name notice that f_{red} is the square-free factor of f of largest degree.

(a) Show that $\mathbf{V}(f) = \{a_1, \ldots, a_\ell\}$.

Solution. Both the inclusions $\supset$ and $\subset$ are elementary and clear.

(b) Show that $\mathbf{I}(\mathbf{V}(f)) = \langle f_{red} \rangle$.

Solution. ($\supset$): Every polynomial $x \mapsto f_{red}(x)\mathbb{C}[x]$ vanishes on $\{a_1, \ldots, a_\ell\}$. Since $f_{red} \cdot \mathbb{C}[x]$ is $\langle f_{red} \rangle$ this shows that $\mathbf{I}(\mathbf{V}(f)) \supset \langle f_{red} \rangle$.

($\subset$): $h \in \mathbf{I}(\mathbf{V}(f))$ implies that h vanishes on $\{a_1, \ldots, a_\ell\}$ and hence that f_{red} divides h. But this means that $h \in \langle f_{red} \rangle$.

Whereas part (b) describes $\mathbf{I}(\mathbf{V}(f))$, the answer is not completely satisfactory because we need to factor f completely to fine f_{red}. In Exercises 1.5.13, 1.5.14, 1.5.15 we will show how to determine f_{red} without any factoring.

---

§1.5.13.

In this exercise we will study the formal derivative of a polynomial $f = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{C}[x]$. The *formal derivative* is defined by the usual formulas from calculus: $f' = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1} + 0$. Prove that the following rules of differentiation apply:

$$(af)' = af', \qquad \text{when } a \in \mathbb{C}, \tag{1.5.13.a}$$

$$(f+g)' = f' + g', \tag{1.5.13.b}$$

$$(fg)' = f'g + fg'. \tag{1.5.13.c}$$

Solution. (1.5.13.a) and (1.5.13.b) are easily verified. To establish (1.5.13.c), note that because of (1.5.13.a) and (1.5.13.b), both sides of (1.5.13.c) are bilinear in (f, g). Accordingly, it suffices to establish (1.5.13.c) when $f = x^m$ and $g = x^k$. But then (1.5.13.c) reduces to

$$\begin{aligned}(fg)' &= \left(x^{k+m}\right)' \\ &= (m+k)\left(x^{k+m-1}\right) \\ &= mx^{m-1} \cdot x^k + x^m \cdot \left(kx^{k-1}\right). \\ &= f' \cdot g + f \cdot g'.\end{aligned}$$

---

§1.5.14.

In this exercise we will use the differentiation properties of Exercise 1.5.13 to compute $GCD(f, f')$ when $f \in \mathbb{C}[x]$.

(a) Suppose that $f = (x-a)^r h$ in $\mathbb{C}[x]$, where $h(a) \neq 0$. Prove that $f' = (x-a)^{r-1}h_1$, where $h_1 \in \mathbb{C}[x]$ does not vanish at a.

Proof. Computing directly,

$$\begin{aligned}f' &= r(x-a)^{r-1} \cdot h + (x-a)^r \cdot h' \\ &= (x-a)^{r-1}\big(r \cdot h + (x-a) \cdot h'\big).\end{aligned}$$

Putting $h_1 = r \cdot h + (x-a) \cdot h'$ and replacing x by a gives $h_1(a) = r \cdot h(a) \neq 0$.

(b) Let $f = c(x-a)^{r_1} \cdots (x-a_\ell)^{r_\ell}$. Prove that f' is a product $f' = (x-a_1)^{r_1-1} \cdots (x-a_\ell)^{r_\ell-1} \cdot H$, where $H \in \mathbb{C}[x]$ doesn't vanish at any of the points a_1, a_2, $\ldots$, a_ℓ.

Proof. Part (a) shows that $(x-a_t)^{r_t-1}$ is a factor of f' for each $1 \leq t \leq \ell$. So $f' = (x-a_1)^{r_1-1} \cdots (x-a_\ell)^{r_\ell-1} \cdot H(x)$, for some $H(x) \in \mathbb{C}[x]$. In the terminology of part (a), $h_1(x) = (x-a_2)^{r_2-1} \cdots (x-a_\ell)^{r_\ell-1}H(x)$. Since $h_1(a) \neq 0$, it follows that $H(a_1) \neq 0$. Similar arguments show that none of the terms $H(a_2), \ldots, H(a_\ell)$ is zero.

(c) Prove that $GCD(f,\, f') = (x-a_1)^{r_1-1}\cdots(x-a_\ell)^{r_\ell-1}$.

Proof. It is clear from part (b) that $GCD(f,\, f') = (x-a_1)^{r_1-1}\cdots(x-a_\ell)^{r_\ell-1}\cdot g$ for some $g \in \mathbb{c}[x]$ which divides the H of part (b). If $\deg g > 0$ then being a divisor of f, we must have $g(a_i) = 0$ for some $1 \le i \le \ell$, but being a divisor of H we must have $g(a_i) \neq 0$ for any $1 \le i \le \ell$. The only possibility is that $\deg g = 0$ or g is a constant. Since GCD is only defined to within a multiplicative constant we can take this constant to be $g = 1$.

---

§1.5.15.

This exercise is concerned with the square-free part f_{red} of a polynomial $f \in \mathbb{C}[x]$. c.f. Exercise 1.5.12.

(a) Use Exercise 1.5.14 to prove that f_{red} is given by

$$f_{red} = \frac{f}{GCD(f,\, f')}.$$

The virtue of this formula is that it allows us to find the square-free part without factoring f. This allows for much quicker computations.

Proof. If $f = c(x-a)^{r_1}\cdots(x-a_\ell)^{r_\ell}$ the above shows that $GCD(f,f') = c(x-a_1)^{r_1-1}\cdots(x-a_\ell)^{r_\ell-1}$.

$$f_{red} = (x-a)\cdots(x-a_\ell) = \frac{f}{GCD(f,f')}.$$

(b) Use a computer algebra system to find the square-free part of the polynomial

$$x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 2x^2 - x - 1.$$

Solution. The Mathematica command sequence

In[4]=**f=xˆ11-xˆ10+2*xˆ8-4*xˆ7+3*xˆ5-3*xˆ4+xˆ3+3*xˆ2-x-1;**
PolynomialQuotient[f,PolynomialGCD[f,D[f,x]],x]

Yields the output

Out[4]= $-1 - x + x^2 + x^5$.

As a check, adding the Mathematica command sequence

In[5]=**FactorSquareFree[f]**

yields

Out[5]=$(-1+x)^3(1+2x+x^2+x^3+x^4)^2$

To see what is going on we include the Mathematica sequence

In[6]=**Expand[(-1+x)*(1+2x+xˆ2+xˆ3+xˆ4)]**

Out[6]=$-1 - x - x^2 + x^5$.

Note. In this last input we omitted the multiplication symbol "*" in some spots.

---

§1.5.16.

Use Exercise 1.5.12 and 1.5.15 to describe (in words, not pseudocode) an algorithm whose input consists of polynomials $f_1, \ldots, f_s \in \mathbb{C}[x]$ and whose output consists of a basis of $\mathbf{I}\big(\mathbf{V}(f_1, \ldots, f_s)\big)$. It is much more difficult to construct such an algorithm when dealing with polynomials of more than one variable.

Solution. Compute

$$GCD\left(\frac{f_1}{GCD(f_1,\, f_1')}, \frac{f_2}{GCD(f_2,\, f_2')}, \ldots, \frac{f_s}{GCD(f_s,\, f_s')}\right).$$

---

§**1.5.17.**

Find a basis for the ideal $\mathbf{I}\big(\mathbf{V}(x^5 - 2x^4 + 2x^2 - x,\ x^5 - x^4 - 2x^3 + 2x^2 + x - 1)\big)$.

Solution. We offer the Mathematica 3.01 command sequence

```
In[7]= h1=x^5-2x^4+2x^2-x;
       h2=x^5-x^4-2x^3+2x^2+x-1;
       PolynomialGCD[PolynomialQuotient[h1,PolynomialGCD[h1,D[h1,x]],x],
       PolynomialQuotient[h2,PolynomialGCD[h2,D[h2,x]],x]]
```

Yields the output

Out[7]=$-1 + x^2$.

To see that this is correct consider the following:

```
In[8]=FactorSquareFree[h1]
```

Out[8]= $(-1 + x)^3 x(1 + x)$

(The implication being that $h1_{rad} = x(-1 + x^2)$.)

```
In[9]=FactorSquareFree[h2]
```

Out[9]= $(-1 + x)^3(1 + x)^2$

(The implication here being that $h2_{rad} = -1 + x^2$.)

These results agree, giving $\mathbf{I}\big(\mathbf{V}(x^5 - 2x^4 + 2x^2 - x,\ x^5 - x^4 - 2x^3 + 2x^2 + x - 1)\big) = \langle x^2 - 1\rangle$.