Solution for Homework 4

Xiangcan Li

March 22, 2021

Exercise 2.3.3 Let $f = x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2$ and $g = 4x^4 + 16$. Find $\gcd(f, g)$ and express it as $uf + vg$.

$$\begin{aligned} x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2 &= \Big(\frac{1}{4}x + \frac{1}{2}\Big)(4x^4 + 16) + (2x^3 - x^2 - 6x - 10) \\ 4x^4 + 16 &= (2x^3 - x^2 - 6x - 10)(2x + 1) + (13x^2 + 26x + 26) \\ 2x^3 - x^2 - 6x - 10 &= (13x^2 + 26x + 26)\Big(\frac{2}{13}x - \frac{5}{13}\Big). \end{aligned}$$

Hence, the greatest common divisor is $\frac{1}{13} \times (13x^2 + 26x + 26) = x^2 + 2x + 2$.
Then we have

$$\begin{aligned} x^2 + 2x + 2 &= \frac{1}{13}\Big(4x^4 + 16 - (2x^3 - x^2 - 6x - 10)(2x + 1)\Big) \\ &= \frac{1}{13}\Big(4x^4 + 16 - (x^5 + 2x^4 + 2x^3 - x^2 - 2x - 2 - \Big(\frac{1}{4}x + \frac{1}{2}\Big)(4x^4 + 16))(2x + 1)\Big) \\ &= \frac{1}{13}\Big(g - (f - \Big(\frac{1}{4}x + \frac{1}{2}\Big)g)(2x + 1)\Big) \\ &= \frac{1}{13}\Big(g + (2x + 1)\Big(\frac{1}{4}x + \frac{1}{2}\Big)g - (2x + 1)f\Big) \\ &= \Big(-\frac{2}{13}x - \frac{1}{13}\Big)f + \Big(\frac{1}{26}x^2 + \frac{5}{52}x + \frac{3}{26}\Big) \end{aligned}$$

Hence, $\gcd(f, g) = x^2 + 2x + 2 = \Big(-\frac{2}{13}x - \frac{1}{13}\Big)f + \Big(\frac{1}{26}x^2 + \frac{5}{52}x + \frac{3}{26}\Big)g$.

Exercise 2.3.5 Prove that a polynomial $f \in \mathbb{F}[x]$ of degree 3 is irreducible in $\mathbb{F}[x]$ if it does not have a root in $\mathbb{F}$.

For all $f \in \mathbb{F}$ and $\alpha \in \mathbb{F}$, there exists a polynomial $q \in \mathbb{F}$ so that $f = (x - \alpha)q + f(\alpha)$. Assume f does not have a root, then $f(\alpha) \neq 0$ for all $\alpha \in \mathbb{F}$. Hence, if we write $f = uv$, then neither $\deg(u)$ and $\deg(v)$ can be 1.

Write $f = uv$, where $= \deg(f) = 3$. Without loss of generality, suppose $\deg(u) > \deg(v)$. There are two cases.

- $\deg = 2$ and $\deg(v) = 1$. This is impossible since neither $\deg(u)$ and $\deg(v)$ can be 1.
- $\deg = 3$ and $\deg(v) = 0$.

We conclude the only to write $f = uv$ is to let either u or v be a unit. Hence, a polynomial $f \in \mathbb{F}[x]$ of degree 3 is irreducible in $\mathbb{F}[x]$ if it does not have a root in $\mathbb{F}$.

Exercise Come up with a polynomial $g \in Q[x]$ that has no roots in Q but is not irreducible.

Let $g(x) = (x^2+4x+5)(x^2+2x+3)$. Since $x^2+4x+4+1 = (x+2)^2+1 > 0$ and $x^2+2x+3 = (x+1)^2+2 > 0$, $g(x) > 0$. Then $g(x) = 0$ does not have a solution. However, since $g(x)$ can be written as a product of two polynomials with degree 2, respectively, $g(x)$ is not irreducible.

Exercise 2.3.6 Consider the polynomial $f(x) = x^3 - x + 2 \in \mathbb{Z}_5[x]$ (more precisely, $f(x) = [1]x^3 - [1]x + [2]$). Prove that f is irreducible in $\mathbb{Z}_5[x]$.

$f(0) = 0^3 - 0 + 2 = 2 \neq 0$
$f(1) = 1^3 - 1 + 2 = 2 \neq 0$
$f(2) = 2^3 - 2 + 2 = 3 \neq 0$
$f(3) = 3^3 - 3 + 2 = 1 \neq 0$
$f(4) = 4^3 - 4 + 2 = 2 \neq 0$
Hence, $f(x) = x^3 - x + 2$ has no root in $\mathbb{Z}_5[x]$.
By **Exercise 2.3.5**, f is irreducible in $\mathbb{Z}_5[x]$.

Exercise Consider the polynomial $p(x) = 3x^3 + 2x^2 + 4x + 2 \in \mathbb{Z}_7[x]$ (more precisely, $f(x) = [3]x^3 + [2]x2 + [4]x + [2]$). Prove that f is not irreducible in $\mathbb{Z}_7[x]$.

$f(0) = 3 \cdot 0^3 + 2 \cdot 0^2 + 4 \cdot 0 + 2 = 2$
$f(1) = 3 \cdot 1^3 + 2 \cdot 1^2 + 4 \cdot 1 + 2 = 4$
$f(2) = 3 \cdot 2^3 + 2 \cdot 2^2 + 4 \cdot 2 + 2 = 0$
Hence, 2 is a root.
By **Exercise 2.3.5**, a polynomial $f \in \mathbb{F}[x]$ of degree 3 is irreducible in $\mathbb{F}[x]$ if it does not have a root in $\mathbb{F}$. Then the contrapositive statement is a polynomial $f \in \mathbb{F}[x]$ of degree 3 is not irreducible in $\mathbb{F}[x]$ if it has a root in $\mathbb{F}$.
We conclude f is not irreducible in $\mathbb{Z}_7[x]$.

Exercise 2.5.1 Suppose $T : \mathbb{R}_n \to \mathbb{R}_n$ is a linear transformation. Prove that T is an isometry if and only if $T(\mathbf{v}) \cdot T(\mathbf{w}) = \mathbf{v} \cdot \mathbf{w}$. Recall that an isometry is a bijection that preserves distance

Since T is a linear transformation, there exists a matrix $A \in M_{n\times n}$ so that $T = T_A : \mathbb{R}^n \to \mathbb{R}^n$ is given by matrix multiplication $T_A(\mathbf{v}) = A\mathbf{v}$.
$\Longrightarrow$: If T is an isometry, then $|T(\mathbf{x}) - T(\mathbf{y})| = |\mathbf{x} - \mathbf{y}|$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$.
Then we have

$$\begin{aligned}
|A\mathbf{x} - A\mathbf{y}| = |\mathbf{x} - \mathbf{y}| &\implies |A\mathbf{x} - A\mathbf{y}|^2 = |\mathbf{x} - \mathbf{y}|^2 \\
&\implies (A\mathbf{x} - A\mathbf{y}) \cdot (A\mathbf{x} - A\mathbf{y}) = (\mathbf{x} - \mathbf{y}) \cdot (\mathbf{x} - \mathbf{y}) \\
&\implies (A\mathbf{x} - A\mathbf{y})^t (A\mathbf{x} - A\mathbf{y}) = (\mathbf{x} - \mathbf{y})^t (\mathbf{x} - \mathbf{y}) \\
&\implies \big(A(\mathbf{x} - \mathbf{y})\big)^t \big(A(\mathbf{x} - \mathbf{y})\big) = (\mathbf{x} - \mathbf{y})^t (\mathbf{x} - \mathbf{y}) \\
&\implies \big((\mathbf{x} - \mathbf{y})^t A^t\big) \big(A(\mathbf{x} - \mathbf{y})\big) = (\mathbf{x} - \mathbf{y})^t (\mathbf{x} - \mathbf{y}) \\
&\implies (\mathbf{x} - \mathbf{y})^t (A^t A)(\mathbf{x} - \mathbf{y}) = (\mathbf{x} - \mathbf{y})^t (\mathbf{x} - \mathbf{y}) \\
&\implies A^t A = I.
\end{aligned}$$

Hence, we have

$$\begin{aligned}
T(\mathbf{w}) \cdot T(\mathbf{v}) &= A\mathbf{w} \cdot A\mathbf{v} \\
&= (A\mathbf{w})^t A\mathbf{v} \\
&= \mathbf{w}^t A^t A\mathbf{v} \\
&= \mathbf{w}^t \mathbf{v} \\
&= \mathbf{v} \cdot \mathbf{w}.
\end{aligned}$$

$\Longleftarrow$: We have

$$T(\mathbf{w}) \cdot T(\mathbf{v}) = \mathbf{v} \cdot \mathbf{w} = \mathbf{w}^t \mathbf{v},$$

and

$$\begin{aligned}
T(\mathbf{w}) \cdot T(\mathbf{v}) &= A\mathbf{w} \cdot A\mathbf{v} \\
&= (A\mathbf{w})^t A\mathbf{v} \\
&= \mathbf{w}^t A^t A\mathbf{v}.
\end{aligned}$$

Then $\mathbf{w}^t\mathbf{v} = \mathbf{w}^t A^t A\mathbf{v}$. Hence, $A^t A = I$.

Note that $T(\mathbf{v}) = \mathbf{w} \implies A\mathbf{v} = \mathbf{w} \implies A^t A\mathbf{v} = A^t\mathbf{w} \implies \mathbf{v} = A^t\mathbf{w}$. Hence, for all $\mathbf{w} \in \mathbb{R}^n$, there exists $\mathbf{v} = A^t\mathbf{w} \in \mathbb{R}^n$ such that $T(\mathbf{v}) = \mathbf{w}$. Then T is surjective.

$T(\mathbf{v}) = T(\mathbf{w}) \implies A\mathbf{v} = A\mathbf{w} \implies A^t A\mathbf{v} = A^t A\mathbf{w} \implies \mathbf{v} = \mathbf{w}$. Hence, T is injective.

We conclude that T is a bijection.

Also,

$$\begin{aligned}
|\mathbf{x} - \mathbf{y}| &= \sqrt{(\mathbf{x} - \mathbf{y})^t(\mathbf{x} - \mathbf{y})} \\
&= \sqrt{(\mathbf{x} - \mathbf{y})^t(A^t A)(\mathbf{x} - \mathbf{y})} \\
&= \sqrt{\big((\mathbf{x} - \mathbf{y})^t A^t\big)\big(A(\mathbf{x} - \mathbf{y})\big)} \\
&= \sqrt{(A\mathbf{x} - A\mathbf{y})^t(A\mathbf{x} - A\mathbf{y})} \\
&= |A\mathbf{x} - A\mathbf{y}|.
\end{aligned}$$

We conclude that T is an isometry.

Hence, T is an isometry if and only if $T(\mathbf{v}) \cdot T(\mathbf{w}) = \mathbf{v} \cdot \mathbf{w}$.