Solutions 1

P1.1 Let p be a prime integer and let $\mathbb{F}_p$ be a finite field with p elements. Demonstrate that $x^p - x$ is a nonzero polynomial in $\mathbb{F}_p[x]$ that vanishes at every point in $\mathbb{A}^1(\mathbb{F}_p)$.

Solution. We divide the solution into three steps.

- *For any integer j satisfying $0 < j < p$, the binomial coefficient $\binom{p}{j}$ is divisible by the prime p.*

  The binomial coefficient satisfies the equation $p! = j!\,(p-j)!\,\binom{p}{j}$ so p divides the product $j!\,(p-j)!\,\binom{p}{j}$. As p is prime, it must divide at least one of the three factors: $j!$, $(p-j)!$, or $\binom{p}{j}$. Because $0 < j < p$ and p is prime, we deduce that p does not divide $j!\,(p-j)!$. Therefore, the prime p divides $\binom{p}{j}$.

- *For any two integers a and b, we have $(a+b)^p \equiv a^p + b^p \mod p$.*

  The binomial theorem asserts that
  $$(a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j\, b^{p-j}\,.$$
  The first step shows that $\binom{p}{j} \equiv 0 \mod p$ for any integer j satisfying $0 < j < p$. It follows that $(a+b)^p \equiv a^p + b^p \mod p$.

- *For any nonnegative integer a, we have $a^p \equiv a \mod p$.*

  We proceed by induction on a. The cases $a = 0$ and $a = 1$ are trivial. The second step and the induction hypothesis give $(a+1)^p \equiv a^p + 1^p \equiv a + 1 \mod p$.

Since the nonnegative integers contain a complete set of representatives (also known as a transversal or a system of distinct representatives) for the quotient $\mathbb{F}_p = \mathbb{Z}/\langle p \rangle$, the third step implies that $a^p - a = 0$ for any element a in $\mathbb{F}_p$. Hence, the nonzero polynomial $x^p - x$ vanishes at every point in $\mathbb{F}_p$, so we have
$$x^p - x = x(x-1)(x-2)\cdots\big(x-(p-1)\big) \in \mathbb{F}_p[x]\,. \qquad \square$$

Alternative solution using group theory. Since the group $(\mathbb{F}_p)^\times$ of units consists of all the elements in $\mathbb{F}_p$ except for 0, it has order $p-1$. By the Lagrange Theorem, the order k of an element x in $(\mathbb{F}_p)^\times$ divides $p-1$, so $p-1 = km$ for some nonnegative integer m. Hence, we have $x^{p-1} \equiv x^{km} \equiv (x^k)^m \equiv 1^m = 1 \mod p$. In other words, the polynomial $x^{p-1} - 1$ vanishes at every nonzero point in $\mathbb{F}_p$. Since $x(x^{p-1} - 1) = x^p - x$, the nonzero polynomial $x^p - x$ in $\mathbb{F}_p[x]$ vanishes at every point of $\mathbb{A}^1(\mathbb{F}_p)$. $\square$

Remark. For more proofs, see
http://en.wikipedia.org/wiki/Proofs_of_Fermat's_little_theorem.

P1.2 Consider the curve, called a ***strophoid***, with the trigonometric parametrization given by $x = a\sin(\theta)$ and $y = a\tan(\theta)\,\big(1 + \sin(\theta)\big)$ where a is a constant and θ is a real parameter.

i. Find the implicit polynomial equation in x and y that describes the strophoid.
ii. Find a rational parametrization of the strophoid.

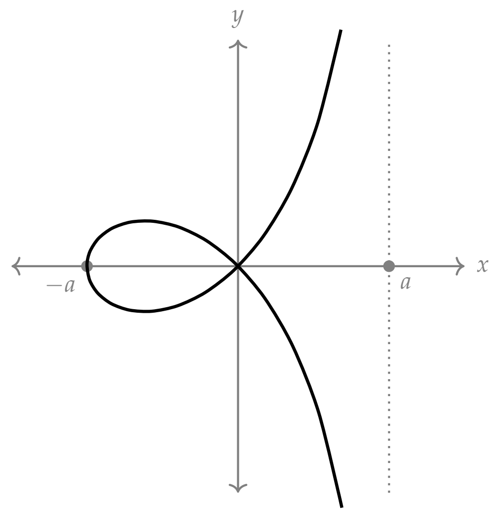

FIGURE 1. Real points on the strophoid

Solution.

i. Substituting $\sin(\theta) = x/a$ into the expression for y yields

$$y = a\frac{\sin(\theta)}{\cos(\theta)}\big(1+\sin(\theta)\big) = a\frac{x/a}{\cos(\theta)}\left(1+\frac{x}{a}\right) = \frac{x(x+a)}{a\cos(\theta)} \qquad \Rightarrow \qquad \cos(\theta) = \frac{x(x+a)}{ay}\,.$$

Since $\cos^2(\theta)+\sin^2(\theta) = 1$, we obtain

$$\begin{aligned}\left(\frac{x}{a}\right)^2 + \left(\frac{x(x+a)}{ay}\right)^2 = 1 \qquad &\Rightarrow \qquad x^2y^2 + x^2(x+a)^2 = a^2y^2\\ &\Rightarrow \qquad y^2(x^2-a^2)+x^2(x+a)^2 = 0\\ &\Rightarrow \qquad (x+a)\big(y^2(x-a)+x^2(x+a)\big) = 0\,.\end{aligned}$$

Since the vertical line $x = -a$ is not part of the stropoid, we conclude that the implicit equation is $y^2(x-a)+x^2(x+a) = 0$.

ii. Using the rational parametrization of the unit circle given by

$$t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right),$$

we obtain the following rational parametrization of the strophoid:

$$\begin{aligned} x &= a\sin(\theta) = a\frac{2t}{1+t^2}\\ y &= a\tan(\theta)\big(1+\sin(\theta)\big) = a\left(\frac{2t}{1-t^2}\right)\left(1+\frac{2t}{1+t^2}\right) = a\frac{2t(1+t)}{(1-t)(1+t^2)}\,.\end{aligned}$$

Thus, $t \mapsto \left(\frac{2at}{1+t^2}, \frac{2at(1+t)}{(1-t)(1+t^2)}\right)$ is a rational parametrization of the stropoid. □

P1.3 Prove that any nonempty open subset of an irreducible topological space is dense and irreducible (in the induced topology).

Solution. Let X be an irreducible topological space and consider a nonempty open subset U of X. Since U is open and nonempty in X, there exists a proper closed subset Y of X such that $U = X \setminus Y$. Writing $\overline{U}$ for the closure of U in X, we see that $X = \overline{U} \cup Y$. Since X is irreducible and Y is a proper subset, it follows that $\overline{U} = X$, so U is dense.

Suppose that Y_1 and Y_2 are two closed subsets of X such that

$$U = (U \cap Y_1) \cup (U \cap Y_2) = U \cap (Y_1 \cup Y_2)\,;$$

in other words, U is the union of two subsets each of which is closed in the induced topology. Since $\overline{U}$ is the intersection of all closed subsets containing U, it follows that $X = \overline{U} = Y_1 \cup Y_2$. Since X is irreducible, we may assume (up to relabelling the Y_i) that $X = Y_1$. Therefore, we conclude that $U = U \cap Y_1$ and U cannot be expressed as the union of two proper closed subsets. □

P1.4 Consider the map $\sigma \colon \mathbb{A}^3(\mathbb{Q}) \to \mathbb{A}^6(\mathbb{Q})$ defined by $\sigma(x_1, x_2, x_3) := (x_1^2, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2)$. Let $z_1, z_2, \dots, z_6$ denote the corresponding coordinates on $\mathbb{A}^6(\mathbb{Q})$.

i. Show that the image of the map σ satisfies the equations given by the 2-minors of the symmetric matrix

$$\Omega := \begin{bmatrix} z_1 & z_2 & z_3 \\ z_2 & z_4 & z_5 \\ z_3 & z_5 & z_6 \end{bmatrix}.$$

ii. Compute the dimension of the rational vector space V in $S := \mathbb{Q}[z_1, z_2, \dots, z_6]$ spanned by these 2-minors.

iii. Show that every homogeneous polynomial of degree 2 in the polynomial ring S vanishing on the image of σ is contained in V.

Solution.

i. We first observe that

$$\sigma^{-1}(\Omega) = \begin{bmatrix} x_1^2 & x_1x_2 & x_1x_3 \\ x_1x_2 & x_2^2 & x_2x_3 \\ x_1x_3 & x_2x_3 & x_3^2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}.$$

Since (3×3)-matrix $\sigma^{-1}(\Omega)$ is the product of matrices with rank 1, it has rank at most 1. In particular, the 2-minors of $\sigma^{-1}(\Omega)$ all vanish. In other words, the image σ satisfies the equations given by the 2-minors of the symmetric matrix Ω.

ii. Among the nine 2-minors of Ω, six are distinct, namely

$$z_1z_4 - z_2^2, \quad z_1z_5 - z_2z_3, \quad z_2z_5 - z_3z_4, \quad z_1z_6 - z_3^2, \quad z_2z_6 - z_3z_5, \quad z_4z_6 - z_5^2.$$

Since these equations have no monomials in common (and the monomials form a vector space basis for S), they are linearly independent. Therefore, the rational vector space V has dimension 6.

iii. The rational vector space S_2 of homogeneous quadratic polynomial functions on $\mathbb{A}^6(\mathbb{Q})$ has dimension $\binom{6+2-1}{2} = 21$ and the rational vector space R_4 of homogeneous quartic polynomial functions on $\mathbb{A}^3(\mathbb{Q})$ has dimension $\binom{3+4-1}{4} = 15$. The map σ induces a $\mathbb{Q}$-linear map $\sigma^\sharp \colon S_2 \to R_4$ such that

$$\begin{aligned}
z_1^2 &\mapsto x_1^4 & z_1z_2 &\mapsto x_1^3x_2 & z_1z_3 &\mapsto x_1^3x_2 \\
z_1z_4 &\mapsto x_1^2x_2^2 & z_1z_5 &\mapsto x_1^2x_2x_3 & z_1z_6 &\mapsto x_1^2x_2^2 \\
z_2^2 &\mapsto x_1^2x_2^2 & z_2z_3 &\mapsto x_1^2x_2x_3 & z_2z_4 &\mapsto x_1x_2^3 \\
z_2z_5 &\mapsto x_1x_2^2x_3 & z_2z_6 &\mapsto x_1x_2x_3^2 & z_3^2 &\mapsto x_1^2x_3^2 \\
z_3z_4 &\mapsto x_1x_2^2x_3 & z_3z_5 &\mapsto x_1x_2x_3^2 & z_3z_6 &\mapsto x_1x_3^3 \\
z_4^2 &\mapsto x_2^4 & z_4z_5 &\mapsto x_2^3x_3 & z_4z_6 &\mapsto x_2^2x_3^2 \\
z_5^2 &\mapsto x_2^2x_3^2 & z_5z_6 &\mapsto x_2x_3^3 & z_6^2 &\mapsto x_3^4 .
\end{aligned}$$

We see that linear map $\sigma^\sharp$ is surjective because all of the monomials of degree 4 lie in the image. The kernel of the linear map $\sigma^\sharp$ is the span of all polynomials sent to the zero function on $\mathbb{A}^3(\mathbb{Q})$. In other words, it is the collection of homogeneous quadratic polynomials that vanish on the image of the map σ, so $V \subseteq \operatorname{Ker}(\sigma^\sharp)$. Since $6 = \dim(V) \leqslant \dim \operatorname{Ker}(\sigma^\sharp) = \dim(S_2) - \dim(R_4) = 21 - 15 = 6$, we conclude that $V = \operatorname{Ker}(\sigma^\sharp)$. □

Remark. The dimension of the vector space of homogeneous polynomials having degree d in n variables is $\binom{n+d-1}{d}$. Since the monomials form a basis, it suffices to count them. Each monomial in n variables of degree d corresponds to a sequence of d stars and $n-1$ vertical bars separating the stars. For example, we have

$$x^4y^3z \leftrightarrow {*}{*}{*}{*} \,|\, {*}{*}{*} \,|\, {*} \quad \text{and} \quad xz^3 \leftrightarrow {*}\,||\,{*}{*}{*} \,.$$

The binomial coefficient $\binom{n+d-1}{d}$ counts the ways to choose d stars from $n+d-1$ symbols.

P1.5 Let d be a nonnegative integer.

i. Show that the polynomial $\binom{x}{d} := \frac{1}{d!}x(x-1)\cdots(x-d+1)$ in $\mathbb{Q}[x]$ takes integer values when evaluated at any integer.

ii. Show that every integer-valued polynomial in $\mathbb{Q}[x]$ of degree at most d can be written as a unique integer linear combination of the polynomials $\binom{x}{d}, \binom{x}{d-1}, \dots, \binom{x}{0}$.

Solution.

i. We proceed by induction on d. When $d = 0$ or $d = 1$, the assertion is trivial. Suppose that $\binom{x}{d}$ is an integer-valued polynomial. We have

$$\begin{aligned}
\binom{x+1}{d+1} - \binom{x}{d+1} &= \frac{(x+1)(x)\cdots(x-d+1)}{(d+1)!} - \frac{x(x-1)\cdots(x-d)}{(d+1)!} \\
&= \frac{x(x-1)\cdots(x-d+1)\big(x+1-(x-d)\big)}{(d+1)!} \\
&= \frac{x(x-1)\cdots(x-d+1)}{d!} = \binom{x}{d},
\end{aligned}$$

so the difference $\binom{m+1}{d+1} - \binom{m}{d+1}$ is an integer for any integer m. Since $\binom{0}{d+1} = 0$, it follows, via a induction on m, that the polynomial $\binom{x}{d+1}$ in $\mathbb{Q}[x]$ takes integer values when evaluated at any integer.

ii. Let f be an integer-valued polynomial in $\mathbb{Q}[x]$ of degree at most d. Since $\binom{x}{j}$ is a polynomial of degree j, we see that the list

$$\binom{x}{d}, \binom{x}{d-1}, \dots, \binom{x}{0}$$

forms a basis for the rational vector space of all polynomials having degree at most d. Hence, there exists unique rational numbers $c_d, c_{d-1}, \dots, c_0$ such that

$$f = c_d \binom{x}{d} + c_{d-1} \binom{x}{d-1} + \cdots + c_0 \binom{x}{0} .$$

It remains to prove that these rational coefficients are integers.

We proceed by induction on d. When $d = 0$, the polynomial $c_0 \binom{x}{0} = c_0$ is integer-valued, so the coefficient c_0 is an integer. For any positive integer d, the difference

$$f(x+1) - f(x) = \sum_{j=0}^{d} c_j \binom{x+1}{j} - \sum_{j=0}^{d} c_j \binom{x}{j} = \sum_{j=1}^{d} c_j \binom{x}{j-1}$$

is integer-valued. Hence, the induction hypothesis establishes that the coefficients $c_d, c_{d-1}, \dots, c_1$ are integers. Furthermore, the equation

$$c_0 = f(d) - \sum_{j=0}^{d} c_j \binom{d}{j}$$

shows that c_0 is also an integer. □