1 An Elliptic Curve

1.1 Question

The following is a plot of the curve E, given by $y^2 = x^3 - 2x$, on $\mathbb{R}^2$.

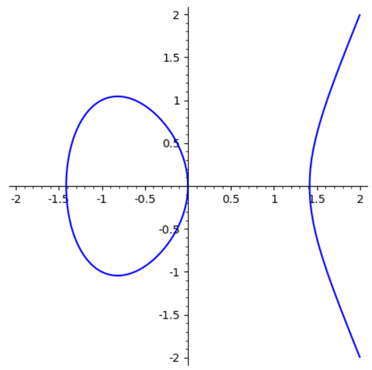

Figure 1: Curve E

Consider the set $E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q}^2 | y^2 = x^3 - 2x\}$.

Define the map $\star : E(\mathbb{Q}) \times E(\mathbb{Q}) \to E(\mathbb{Q}) \cup \{$ `TYPE ERROR`, `RANGE ERROR`$\}$ in the following manner:

- Given $P := (x_1, y_1)$ and $Q := (x_2, y_2) \in E(\mathbb{Q})$ as inputs.
- If $P \neq Q$ then let ℓ be the line joining P and Q and if $P = Q$ then let ℓ be the tangent to the curve E at the point P.
- If ℓ does not intersect the curve at a new point, output `RANGE ERROR`.
- If ℓ intersects the curve again at a new point S, but $S \notin E(\mathbb{Q})$, output `TYPE ERROR`.
- If ℓ intersects the curve again at a new point, say $S \in E(\mathbb{Q})$ with coordinates (x_3, y_3), then the value of $P \star Q$ is defined to be $(x_3, -y_3)$, a point named R.

Fill in the blanks:

For any choice of inputs in $E(\mathbb{Q})$, $\star$ will never result in a ___.

Is the following statement true?

$$P \star Q = Q \star P, \text{ for all } P, Q \in E(\mathbb{Q}).$$

Additionally, compute the value of $(-1, 1) \star (0, 0)$, $(2, 2) \star (2, 2)$, and $(2, 2) \star (-1, -1)$.

1.2 Answer

1.2.1 Assertion One

For any choice of inputs in $E(\mathbb{Q})$, $\star$ will never result in an `TYPE ERROR` : **TRUE**

`CASE ONE` : $x_1 \neq x_2$
Let $(x_1, y_1), (x_2, y_2) \in E(\mathbb{Q})$, the equation of the line ℓ that contains (x_1, y_1) and (x_2, y_2) is:

$$\ell := y = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1) + y_1$$

We can rewrite this equation into the $y = mx + c$ form by setting $m := \left(\frac{y_2 - y_1}{x_2 - x_1}\right)$ and $c := y_1 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)x_1$. Note that both m and c are rational numbers.

To compute the new intersection point, we can solve the following cubic:

$$(mx + c)^2 = x^3 - 2x$$

We already know two roots to this cubic, namely : x_1 and x_2.
Using Vieta's formula, we obtain a new rational root $m^2 - x_1 - x_2$.
Plugging this value back in the equation of ℓ, we find that $(x_1, y_1) \star (x_2, y_2) \in E(\mathbb{Q})$.

`CASE TWO` : $x_1 = x_2$ and $y_1 = y_2$
The line joining these two points is the tangent to the curve at (x_1, y_1).
The slope of the tangent can be computed by differentiating the curve with respect to x:

$$\ell := y = \left(\frac{3x_1^2 - 2}{2y_1}\right)(x - x_1) + y_1$$

If $y = 0$, the tangent has an infinite slope and thus it intersects the curve at 1 point alone. This results in a `RANGE ERROR`.
If not, we can use the earlier method to find a new rational root to the cubic polynomial.
Thus $(x_1, y_1) \star (x_1, y_1) \in E(\mathbb{Q})$

`CASE THREE` : $x_1 = x_2$ and $y_1 \neq y_2$
If $y_1 \neq y_2$ and (x_1, y_1), $(x_2, y_2) \in E(\mathbb{Q})$ then $y_1 = -y_2$.
Observe that the line ℓ joining these two points has an infinite slope and thus intersects the curve at 2 points alone, this results in a `RANGE ERROR`.

1.2.2 Assertion Two

It is not possible for $\star$ to produce a `RANGE ERROR` : **FALSE**

Consider $(-1, 1) \star (-1, -1)$, the line joining these two points will have an infinite slope. This is an instance of a `RANGE ERROR`.

1.2.3 Assertion Three

$$P \star Q = Q \star P, \text{ for all } P, Q \in E(\mathbb{Q}) : \textbf{TRUE}$$

Observe that the new point P depends on the line ℓ that joins the two points (x_1, y_1) and (x_2, y_2). The order in which the inputs are fed to $\star$ does not matter here, as the line ℓ will be identical.

1.2.4 Computation related

$$(-1, 1) \star (0, 0) = (2, 2)$$

The line ℓ joining $(-1, 1)$ and $(0, 0)$ is $y = -x$.
To find the next intersection point, we must solve the cubic $x^3 - x^2 - 2x = 0$.
Observe that this cubic factors into $x(x + 1)(x - 2)$ - the other root is 2.
Thus ℓ intersects the curve again at $(2, -2)$ and hence $(-1, 1) \star (0, 0) = (2, 2)$.

$$(2, 2) \star (2, 2) = \left(\frac{9}{4}, -\frac{21}{8}\right)$$

The line ℓ is the tangent to the curve E at $(2, 2)$.
The slope of the tangent can be computed using the earlier formula : $\frac{5}{2}$.
We can compute the new x-coordinate $\dfrac{25}{4} - 2 - 2 = \dfrac{9}{4}$. Thus the new point is $\left(\dfrac{9}{4}, -\dfrac{21}{8}\right)$

$$(2, 2) \star (-1, -1) = (0, 0)$$

The line ℓ joining $(-1, -1)$ and $(2, 2)$ is $y = x$.
The new x-coordinate is $1 - 2 - (-1) = 0$ and thus the new y-coordinate is 0.

1.3 Additional

- A video about Elliptic Curves and their connection to Fermat's Last Theorem.
- An animation that illustrates $\star$ on the curve $y^2 = x^3 - 4x + 1$ by John Voight, Dartmouth College.

2 Braid Group Actions

2.1 Questions

Let S_3 be the symmetric group on the symbols $\{1, 2, 3\}$.
Let $\mathbb{X} := S_3 \times S_3$ and define a group action $\alpha : \mathbb{Z} \times \mathbb{X} \to \mathbb{X}$ as $\alpha\Big(1, (g, h)\Big) \mapsto (h, h^{-1}gh)$.
Answer the following:

- $\alpha\Big(-1, (h, h^{-1}gh)\Big) = (a, b)$
- Let $p \in \mathbb{X}$ be $\Big((1, 2), (1, 3)\Big)$, What positive value of d satisfies $\mathrm{Stab}(p) = d\mathbb{Z}$?
- The largest orbit has the cardinality : ___

2.2 Answer

2.2.1 Compute related

We have $\alpha\Big(0, (g, h)\Big) = (g, h)$.
Recall that group actions are compatible with group operations.
Thus $\alpha\Big(-1 + 1, (g, h)\Big) = \alpha\Big(-1, \alpha\Big(1, (g, h)\Big)\Big)$

This evaluates to $\alpha\Big(-1, (h, h^{-1}gh)\Big) = (g, h)$.

2.2.2 Stabilizer

The orbit of $\Big((1, 2), (1, 3)\Big) = \Big\{\Big((1, 2), (1, 3)\Big), \Big((1, 3), (2, 3)\Big), \Big((2, 3), (1, 2)\Big)\Big\}$.
From orbit-stabilizer theorem, the index of the stabilizer is 3.

2.2.3 Fill in the blank

$$\text{The largest orbit has a cardinality of : } 4$$

On manually computing all orbits, we observe that orbits have sizes of $1, 2, 3$ and 4.
The orbit of $\Big((1, 3, 2), (1, 2)\Big)$ is:

$$\Big\{\Big((1, 3, 2), (1, 2)\Big), \Big((1, 2, 3), (1, 3)\Big), \Big((1, 2), (1, 2, 3)\Big), \Big((1, 3), (1, 3, 2)\Big)\Big\}$$

3 Direct Limit

3.1 Question

Let S_∞ be the set of all bijections $f : \mathbb{N} \to \mathbb{N}$.
Observe that S_∞ forms a group under composition.

Let U be any subset of $\mathbb{N}$ define $\texttt{Fix}(U) := \{f \in S_\infty \mid f(n) = n \text{ for all } n \in U\}$.
For each $n \in \mathbb{N}$, define $S_n := \texttt{Fix}\Big(\{j \in \mathbb{N} \mid j > n\}\Big)$

Which of the following are true:

- $\bigcup\limits_{n>0} S_n$ is a normal subgroup of S_∞
- For every $i \in \mathbb{N}$, $\texttt{Fix}\Big(\{i\}\Big)$ is a subgroup of S_∞
- For any two non-empty subsets U, V of $\mathbb{N}$, there exists a subset W of $\mathbb{N}$ such that: $\texttt{Fix}(U) \bigcap \texttt{Fix}(V) = \texttt{Fix}(W)$.
- For any two non-empty subsets U, V of $\mathbb{N}$, there exists a subset W of $\mathbb{N}$ such that: $\texttt{Fix}(U) \bigcup \texttt{Fix}(V) = \texttt{Fix}(W)$.

3.2 Answer

3.2.1 Key

- $\bigcup\limits_{n>0} S_n$ is a normal subgroup of S_∞. **TRUE**
- For every $i \in \mathbb{N}$, $\texttt{Fix}\Big(\{i\}\Big)$ is a subgroup of S_∞. **TRUE**
- For any two non-empty subsets U, V of $\mathbb{N}$, there exists a subset W of $\mathbb{N}$ such that: $\texttt{Fix}(U) \bigcap \texttt{Fix}(V) = \texttt{Fix}(W)$. **TRUE**
- For any two non-empty subsets U, V of $\mathbb{N}$, there exists a subset W of $\mathbb{N}$ such that: $\texttt{Fix}(U) \bigcup \texttt{Fix}(V) = \texttt{Fix}(W)$. **FALSE**

3.2.2 Normal subgroup

Claim : $\bigcup\limits_{n>0} S_n$ is a subgroup of S_∞

Let f, g be two bijections in $\bigcup\limits_{n>0} S_n$. Then $f \in S_{m_1}$ and $g \in S_{m_2}$ for some $m_1, m_2 \in \mathbb{N}$.
Without loss of generality, we may assume $m_1 \geq m_2$.
By construction, $f \circ g^{-1}(i) = i$ for all $i > m_1$. Hence $f \circ g^{-1} \in S_{m_1}$.

As a result $f \circ g^{-1} \in \bigcup\limits_{n>0} S_n$. Thus, $\bigcup\limits_{n>0} S_n$ satisfies the subgroup test.

Claim : $\bigcup\limits_{n>0} S_n$ is normal

It suffices to show $g \circ f \circ g^{-1} \in \bigcup\limits_{n>0} S_n$ for all $g \in S_\infty$ and $f \in \bigcup\limits_{n>0} S_n$.

Let g be any bijection in S_∞, we have $g \circ g^{-1}(i) = i$ for all $i \in \mathbb{N}$.

Let f be an element in $\bigcup\limits_{n>0} S_n$, then $f \in S_m$ for some $m \in \mathbb{N}$.
Since f is an element in S_m, $f(i) = i$ for all $i > m$.

As a result, $g \circ f \circ g^{-1}(i) = i$ for all $g^{-1}(i) > m$.

This means the finite set of values $\text{Disp}(f) := \{g(i) \mid 1 \leq i \leq m\}$ are mapped to another value.
Set $n_{fg} := \text{MAX}\Big(\text{Disp}(f)\Big) + 1$.

Thus $g \circ f \circ g^{-1} \in S_{n_{fg}}$ and hence $g \circ f \circ g^{-1} \in \bigcup\limits_{n>0} S_n$

3.2.3 A Fix to the subgroup problem

Let f, g be any two elements in $\texttt{Fix}\Big(\{i\}\Big)$.
Observe that, $f \circ g^{-1}(i) = f(i) = i$.
Thus $f \circ g^{-1} \in \texttt{Fix}\Big(\{i\}\Big)$.

3.2.4 Closure properties

Intersection

Let U, V be non-empty subsets of $\mathbb{N}$.
$\texttt{Fix}(U) \bigcap \texttt{Fix}(V) = \{f \in S_\infty \mid f(n) = n \text{ for all } n \in U\} \bigcap \{f \in S_\infty \mid f(n) = n \text{ for all } n \in V\}$.

Bijections that lie in the intersection must fix both U and V, thus:
$\texttt{Fix}(U) \bigcap \texttt{Fix}(V) = \{f \in S_\infty \mid f(n) = n \text{ for all } n \in U \cup V\}$.
Set $W := U \cup V$.

Union

Consider the instance $U := \{1\}$ and $V := \{2\}$.
$\texttt{Fix}(U)$ contains the bijection:

$$f(x) := \begin{cases} 1 & x = 1 \\ x+1 & x \text{ is even and } x > 1 \\ x-1 & x \text{ is odd and } x > 1 \end{cases}$$

$\texttt{Fix}(V)$ contains the bijection:

$$g(x) := \begin{cases} 3 & x = 1 \\ 2 & x = 2 \\ 1 & x = 3 \\ x+1 & x \text{ is even and } x > 3 \\ x-1 & x \text{ is odd and } x > 3 \end{cases}$$

Both f and g are bijections in the set $\texttt{Fix}(U) \cup \texttt{Fix}(V)$.

Suppose these exists a non-empty subset of $\mathbb{N}$ that is a candidate for W.
We note that f fixes 1 alone, no other elements are fixed.
Similarly, g fixes nothing but 2.
Thus W cannot contain any element in $\mathbb{N}$, else it will exclude f or g or both!

The only possible candidate for W is the empty set ϕ.
Observe that this bijection is not in $\texttt{Fix}(U) \cup \texttt{Fix}(V)$ but is in $\texttt{Fix}(\phi)$:

$$h(x) := \begin{cases} 2 & x = 1 \\ 1 & x = 2 \\ x & x \geq 3 \end{cases}$$

Thus, there is no subset of $\mathbb{N}$ that satisfies this statement.

3.3 Additional

If U is countably infinite, is it true that $\texttt{Fix}(U)$ is either finite or countably infinite?