An Exploration of the Group Law on an Elliptic Curve

Tanuj Nayak

Abstract

Given its abstract nature, group theory is a branch of mathematics that has been found to have many important applications. One such application forms the basis of our modern Elliptic Curve Cryptography. This application is based on the axiom that all the points on an algebraic elliptic curve form an abelian group with the point at infinity being the identity element. This one axiom can be explored further to branch out many interesting implications which this paper explores. For example, it can be shown that choosing any point on the curve as the identity element with the same group operation results in isomorphic groups along the same curve.

Applications can be extended to geometry as well, simplifying proofs of what would otherwise be complicated theorems. For example, the application of the group law on elliptic curves allows us to derive a simple proof of Pappus's hexagon theorem and Pascal's Theorem. It bypasses the long traditional synthetic geometrical proofs of both theorems. Furthermore, application of the group law of elliptic curves along a conic section gives us an interesting rule of constructing a tangent to any conic section at a point with only the aid of a straight-edge ruler.

Furthermore, this paper explores the geometric and algebraic properties of an elliptic curve's subgroups.

(212 words)

Contents

Introduction 4

Groups 4

Elliptic Curves 6

Group Law on Elliptic Curves 7

Another Take on the Identity O 14

Pappus' Theorem 18

Tangent to a Conic 20

Subgroups of the Cubic Curve Group 21

Order 2 22

Order 3 22

Playing More With Flexes 23

Rational Points 24

Conclusion 28

Introduction

Given its abstract nature, group theory is a branch of mathematics that has been found to have many important applications. From rigid motions to cryptography to crystallography, groups can be found almost everywhere. Being a frequent online shopper, I tend to rely on the safety of online transactions a lot. To find out how secure these transactions are, I decided to research them and found out that a lot of the involved cryptographic systems are based on the fact that the points on an elliptic algebraic curve form a group by themselves. To follow through, I became interested in further exploring on the group law on the algebraic cubic curve. So in my exploration, I have discovered many more implications of the group law on the cubic curve such as in algebraic geometry.

Groups

First of all, in order to explore the notion of the group law on the cubic curve we must introduce the concept of a group itself. A group is basically a well-defined set of objects with a defined binary operation associated with this group. This binary operation must have a specific set of properties. Namely, this operation must be closed and associative. Also, the group must be structured in such a way that it contains an identity element and also has an inverse within the group for each element.

Closure

A group operation is said to be closed if the following condition is satisfied for the operation:

If the domain of a group operation is restricted to the set of elements within the group, then its range is also restricted to the same set.

For example, if we take a set of elements to be $\{1,2,3,4,5,6\}$ and associate the defined operation $x \otimes y = x * y$ with this we will find that this function is actually not closed within this set. This can be seen by the fact that $3 \otimes 4 = 12$ lies outside this set. However, the same function can be said to be closed within the set $\{-1,1\}$ as all possible function values $-1 \otimes -1 = 1, 1 \otimes -1 = -1, 1 \otimes 1 = 1$ lie within the same set.

Associativity

An operation $\otimes$ is said to be associative if $x \otimes (y \otimes z) = (x \otimes y) \otimes z$ for all x, y, z within a set. For example, if we define $x \otimes y$ to be the geometric mean of x and y where x and y are real numbers, we will find that $x \otimes (y \otimes z) \neq (x \otimes y) \otimes z$ as $\sqrt{x\sqrt{yz}} \neq \sqrt[3]{xyz}$ for some reals x, y and z. However, we find that the operation of normal addition (+) is associative.

Identity and Inversion

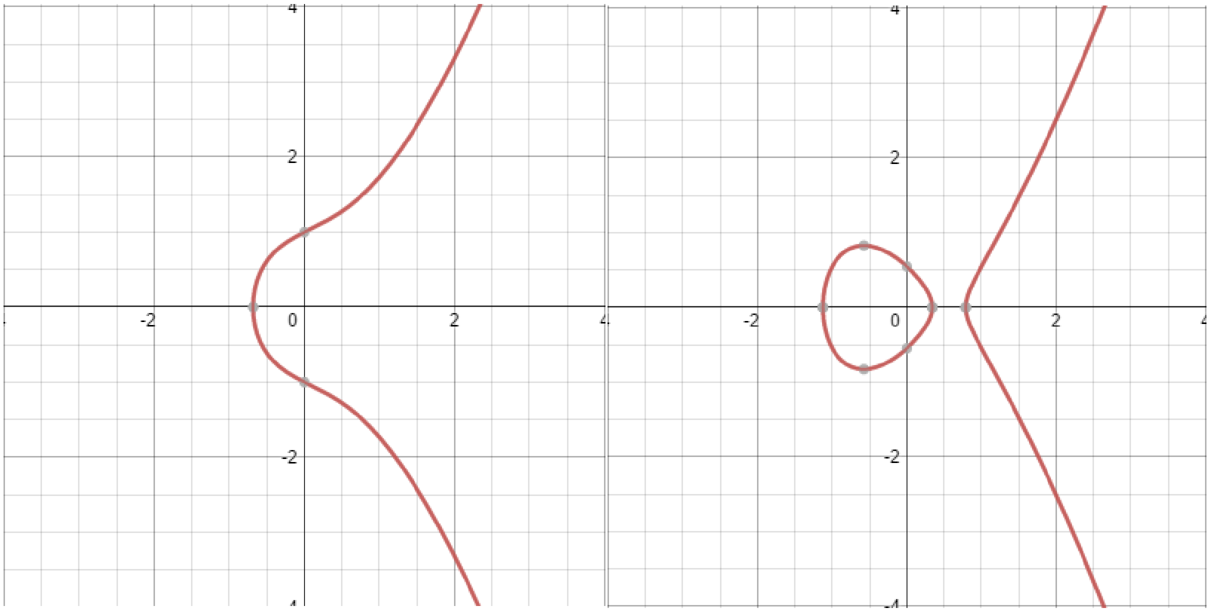
Every group has a special identity element. Let us say that this identity element is O. So this identity element O is defined such that $O \otimes x = x \otimes O = x$ for any x within the group. For example, 1 is the identity element for the group of integers in normal multiplication (·).

An operation $\otimes$ is said to be invertible within a set if each element k has an element within the same set k^{-1} such that $k \otimes k^{-1} = O$ where O is the identity of the operation within the set. In this case, k^{-1} and k are said to be each other's inverses.

Given all these fundamental properties of a group it is a common mistake to assume that all groups are commutative. This assumption however is not necessarily true. For example, the set of invertible matrices in multiplication form a group. However, this operation is not commutative. Some groups can be commutative though, like the group of integers in addition. Such groups are said to be abelian groups. Interestingly enough, the set of points on an elliptic curve form an abelian group. This group is the subject of this exploration and will be elaborated upon shortly.

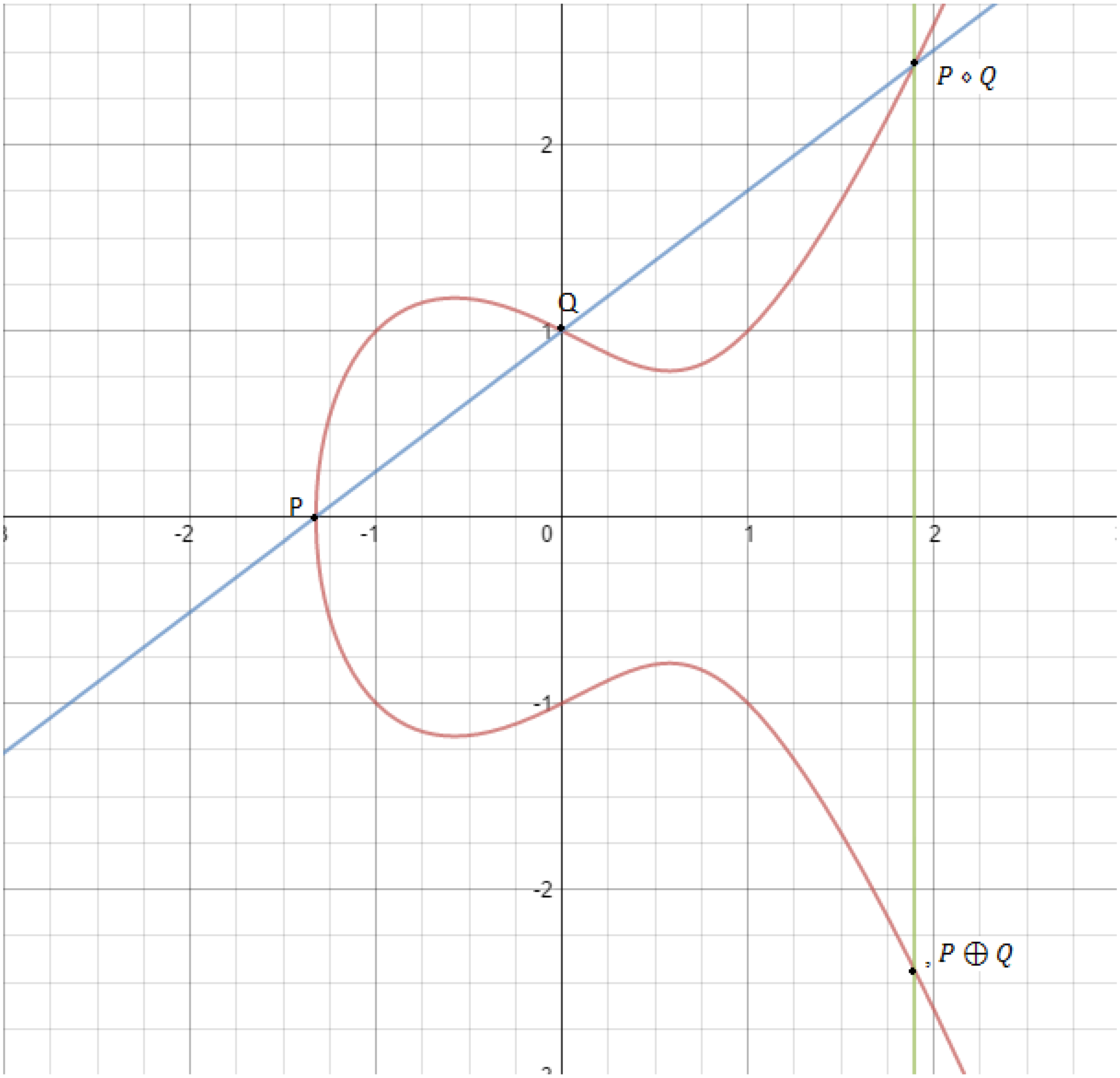
Elliptic Curves

Now that we have been introduced to the notion of groups, we must briefly do the same for elliptic curves before delving into the intriguing abelian group law behind it. Elliptic curves are algebraic plane curves which are described by the intersection of the $z = 0$ plane and the polynomial function $y^2 = x^3 + ax + b$. Furthermore, this curve must have no cusps and hence have a genus of one. To express the aforementioned restriction algebraically, we say that the curve's discriminant, $-16(4a^3 + 27b^2)$ is non-zero. Given below are examples of elliptic curve.

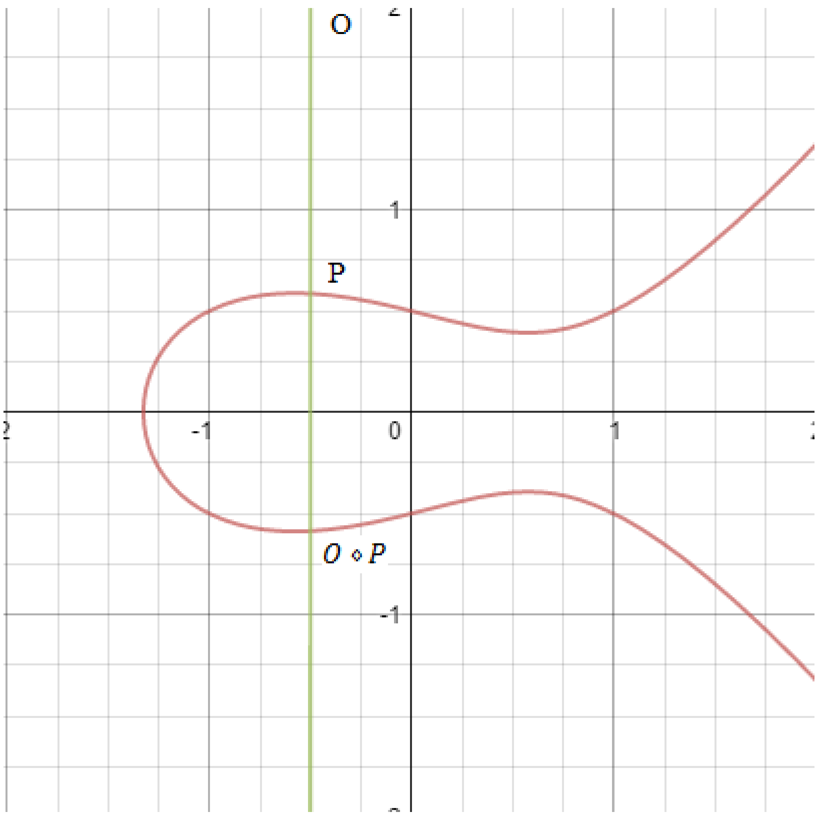


Group Law on Elliptic Curves

Now that we have introduced the concepts of groups and elliptic curves, let us examine the connection between the two. We see that all the points on any elliptic curve form an infinite abelian group. The rule associated with this group can be explained as follows. Let us take the point at infinity, O, on the curve such that every vertical line goes through this point. Let us define the operator ⋄ such that $P \diamond Q$ (with P and Q being points on a curve) is the third intersection point of the line joining P and Q with the curve. Now let us define $P \oplus Q$ to be equivalent to $O \diamond (P \diamond Q)$. In other words, $P \oplus Q$ is the second intersection of the vertical line at $P \diamond Q$ with the curve. This $\oplus$ operator is the group law of this curve. This law is illustrated in the following diagram:



We see that this operator upholds the properties of associativity, commutability, closure and inversion. Also, the identity of this group happens to be the point at infinity, O. This can be seen by the following: $O \oplus P = O \diamond (O \diamond P)$

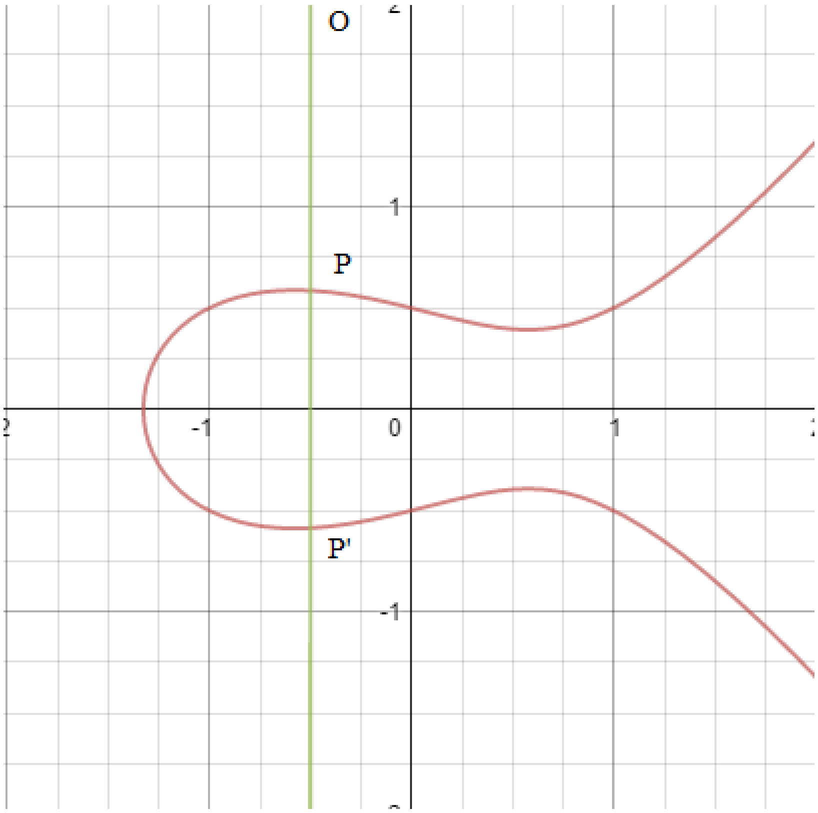


So we have that $O \diamond P$ is the third intersection point of the vertical line going through P with the curve by the definition of O. Due to this fact, $O \oplus P = O \diamond (O \diamond P)$ should lie on the same vertical line and should be equivalent to P. Hence, $O \oplus P$ returns P for any P on the curve, hence O serves as the identity of this group.

Closure also is very trivial by the definition of the group law.

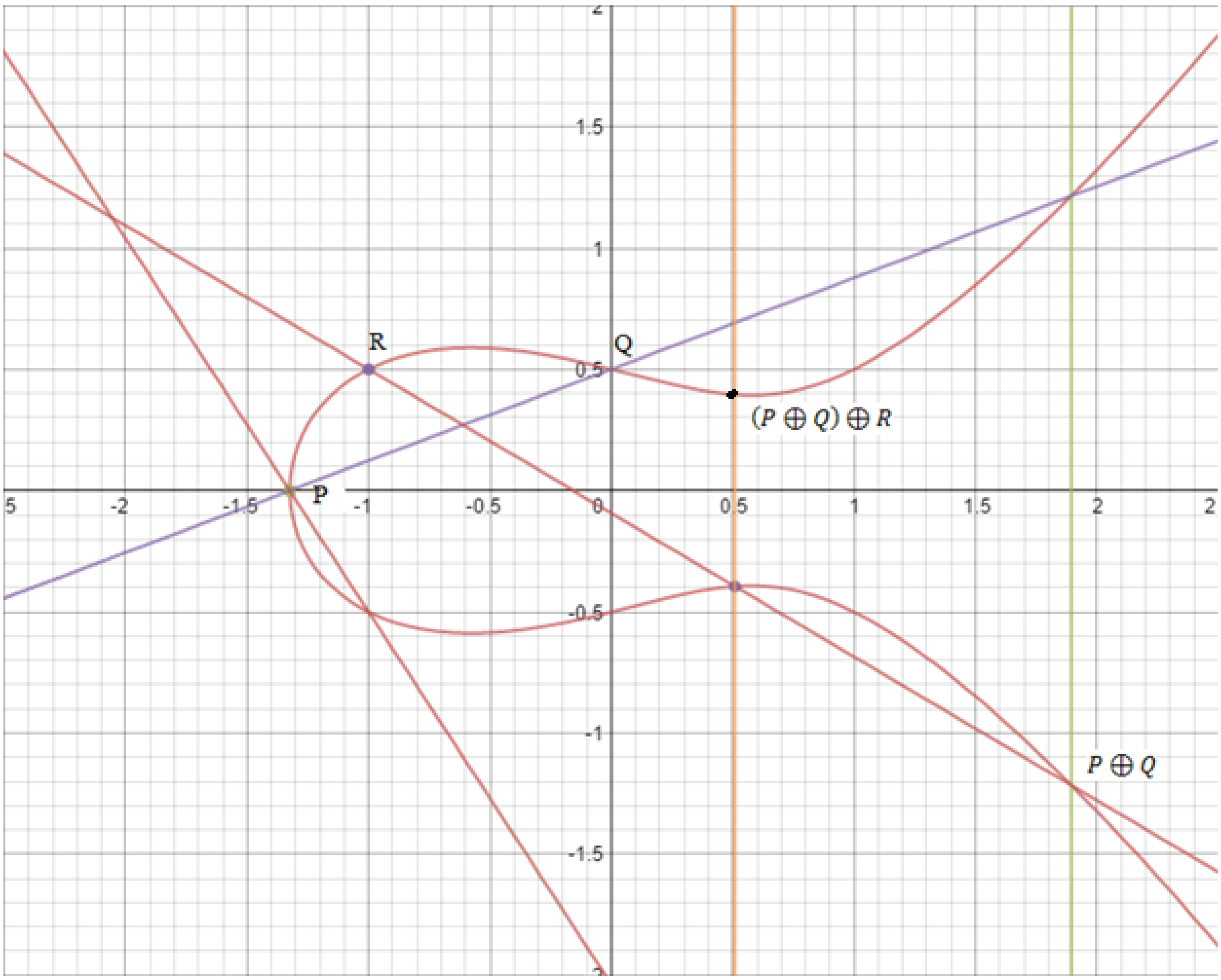
The commutability of this group is quite trivial, given the trivial property $Q \diamond P = P \diamond Q$. We have that $P \oplus Q = O \diamond (P \diamond Q) = O \diamond (Q \diamond P) = Q \oplus P$. $(P \oplus Q) \diamond R$

We also find that each point on the curve has an inverse. Since the general equation for an elliptic curve is $y^2 = x^3 + ax + b \Rightarrow \pm y = \sqrt{x^3 + ax + b}$, we know that for each point (x, y) on the curve, its reflection across the x axis $(x, -y)$is also on the curve. We also notice that the inverse of each point on the curve is the third intersection of the vertical line going through it with the cubic. In other words, the inverse of P is its vertical reflection due to the symmetry of the cubic curve. To prove this, let us take a point P on an elliptic cubic curve. Let us call its vertical reflection P'. Note that $P \diamond P' = O$ as P and P' lie on the same vertical line, leaving O to be the third point on this line as all vertical lines intersect at O. So we see that $P \oplus P' = O \diamond (P \diamond P') = O \diamond O = O$. Hence, P and its vertical reflection P' are indeed inverses of each other.

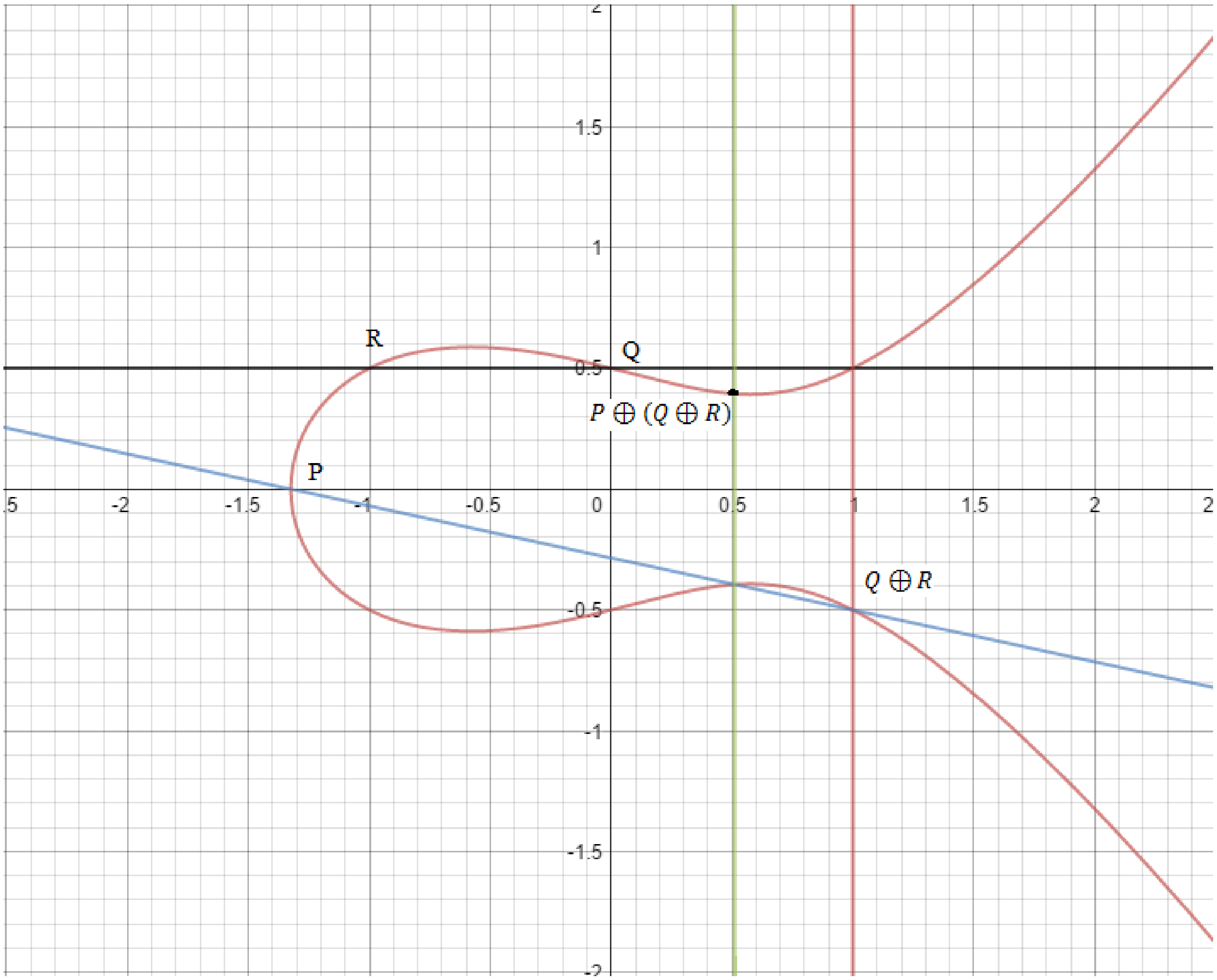


Associativity, however, is a rather difficult property to prove. We must prove that $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ for all points P, Q and R on the cubic curve. So let us illustrate $P \oplus$

$(Q \oplus R)$ and $(P \oplus Q) \oplus R$ on a diagram. Below we have illustrated $(P \oplus Q) \oplus R$.



Next, we have the illustration of $P \oplus (Q \oplus R)$:

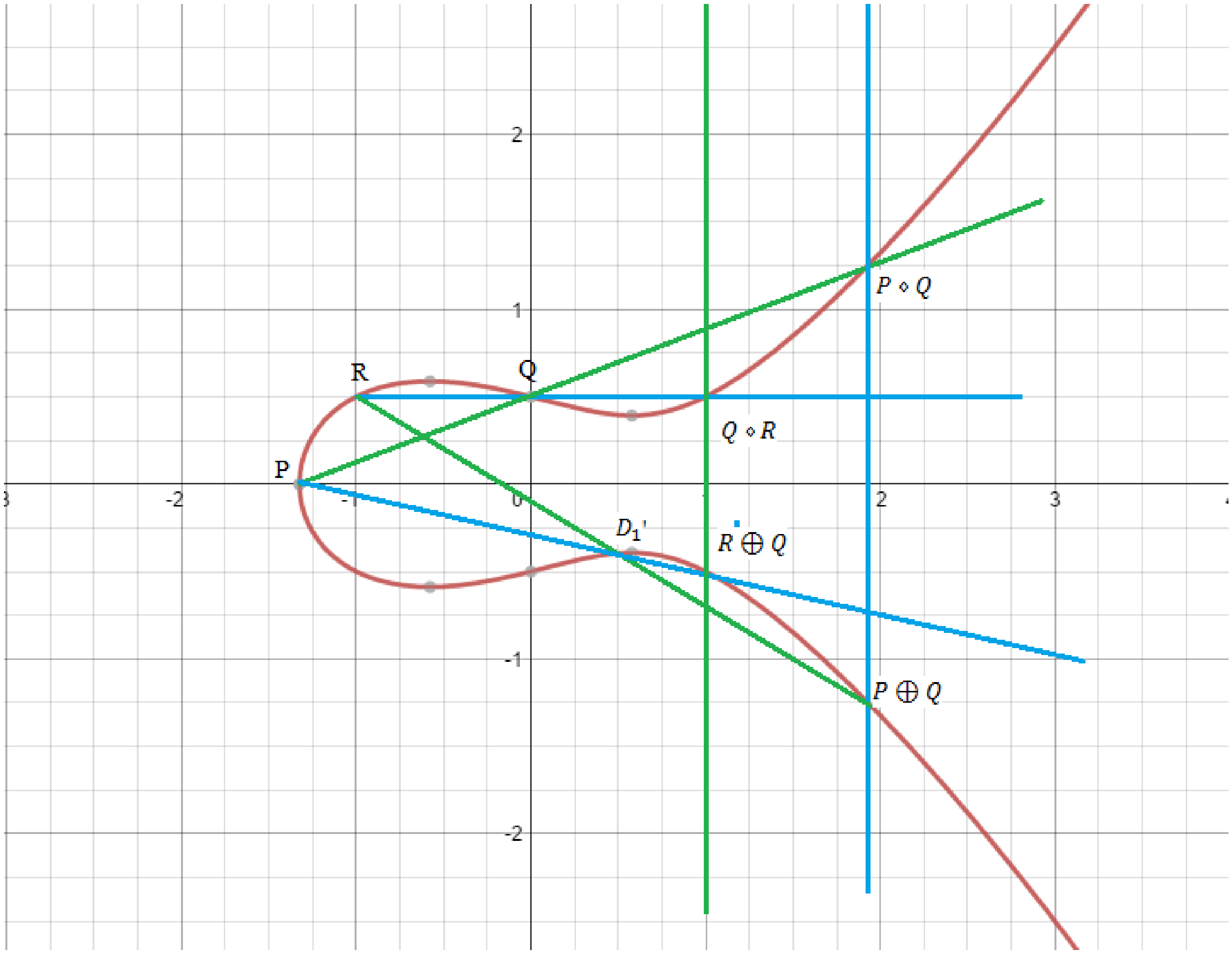


So to prove that $P \oplus (Q \oplus R)$ and $(P \oplus Q) \oplus R$ coincide we must use the Cayley Bacharach Theorem:

Cayley-Bacharach Theorem: Say that two cubic intersect at 9 points, $g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8$ and g_9. If a third cubic passes through eight of these points, then it must pass through the remaining ninth point as well.

Let us call the cubic curve which comprises of the group in question, C_1. For convenience, let us say $D_1 = P \oplus (Q \oplus R)$ and $D_2 = (P \oplus Q) \oplus R$. Let us also define the lines $L_1 =$

$\overline{QR(Q \diamond R)}, L_2 = \overline{O(P \oplus Q)(P \oplus Q)'}$ and $L_3 = \overline{PD_1{}'(Q \oplus R)}$ (the blue lines in the diagram below). The union of these three lines form a degenerate cubic C_2. Let us then define the lines $N_1 = \overline{R(P \oplus Q)D_2{}'}$, $N_2 = \overline{PQ(P \diamond Q)}$ and $N_3 = \overline{(Q \diamond R)O(R \oplus Q)}$, (the green lines below). We can form another degenerate cubic, C_3, with the union of these three lines.

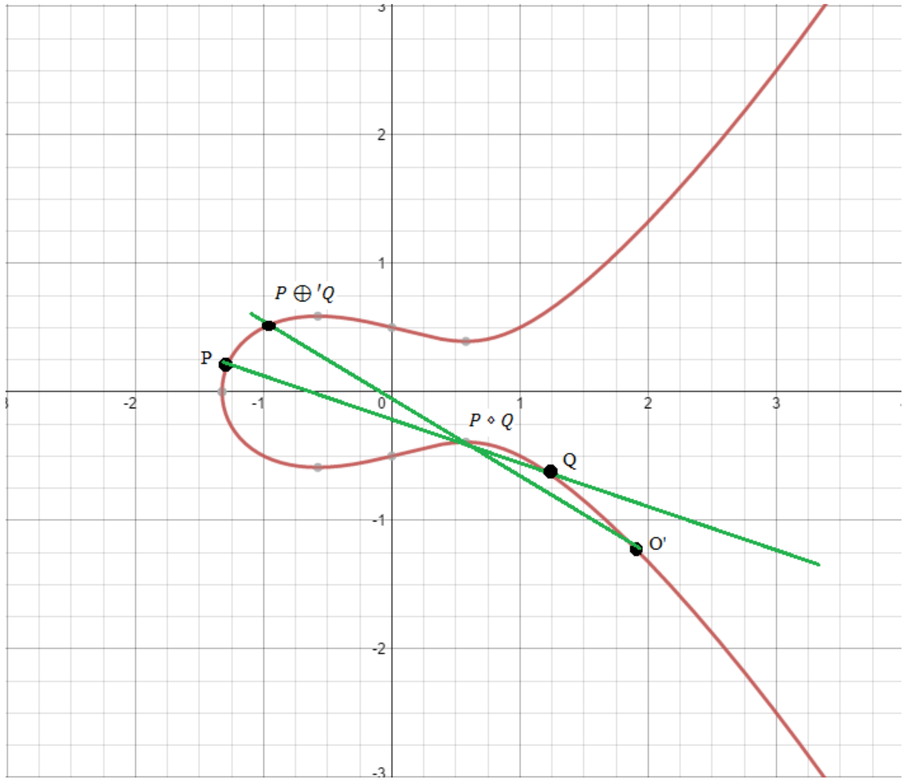


So we see that C_1 and C_2 intersect at nine points, $P, R, Q, Q \diamond R, P, D_1', R \oplus Q, P \oplus Q, P \diamond Q$ and O. We also see that C_3 trivially contains eight of these points, but not through $D_1{}'$. However, by the Cayley-Bacharach Theorem, C_3 must go through $D_1{}'$. We see that N_2 must contain $D_1{}'$ in order for this to happen. As $D_1{}'$ and D_2’ are both the third intersection points of N_2 with C_1, the others being $P \oplus Q$ and R, $D_1' = D_2{}'$. As $D_1{}'$ and $D_2{}'$ are inverses of D_1 and D_2, respectively, and

$D_1' = D_2{}'$ we also know that $D_1 = D_2$. Hence, we have also proven that $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.

Another Take on the Identity O

So far, we have seen that the group structure of an elliptic curve is heavily dependent on the location of the identity, O, at infinity. This is evident in the fact that $P \oplus Q$ is equivalent to $O \diamond (P \diamond Q)$, or in other words the third intersection point of O and $(P \diamond Q)$. By virtue of the location of O so far, $O \diamond (P \diamond Q)$ happens to be second intersection of the vertical line going through $P \diamond Q$ with the curve. So then it is tempting to question what happens when the identity point, O, is taken as a different point on the curve. So then we have to define a new group operation to account for this. Let us define this operation to be $\oplus\,'$. So we will define $\oplus\,'$ in a way similar to $\oplus$. So we have that $P \oplus 'Q$ is equal to $O' \diamond (P \diamond Q)$. This new operation is illustrated below:



Interestingly, this new operation tells us that $P \oplus' Q = O' - (P \oplus Q)$. To see why this is the case, we must first note that $P \diamond Q$ is equal to $-(P \oplus Q)$ where $-P$ is defined to be the inverse of P in the group $(C, \oplus)$. In other words, $-P$ is the third intersection point of the vertical line going through P or $-P = O \diamond P$. So going off of the notion that $P \oplus' Q = O' \diamond (P \diamond Q)$, we have that $P \oplus' Q = O' \diamond (-(P \oplus Q)) = -(O' \oplus -(P \oplus Q))$.

Now to continue further, we must convince ourselves that $-(P \oplus Q) = -P \oplus -Q$. To do this, we must use the following lemma:

Lemma statement: If $P, Q, R \in C$ are collinear, then we have that $P \oplus Q \oplus R = O$.

Proof: Since P, Q, R are collinear, we have that $Q \diamond R = P$. Hence, we have that $P \oplus Q \oplus R = P \oplus (Q \oplus R) = P \oplus O \diamond (Q \diamond R) = P \oplus O \diamond P = P \oplus -P = O$. So we have proven that $P \oplus Q \oplus R = O$.

So going off of the lemma we have that

$P \oplus Q \oplus R = O$

$\Rightarrow P \oplus Q = O \oplus -R$

$\Rightarrow P \oplus Q = \ -R$

$\Rightarrow -(P \oplus Q) = R$ (1)

We also have that

$P \oplus Q \oplus R = O$

$\Rightarrow P \oplus (Q \oplus R) = O$

$\Rightarrow Q \oplus R = -P$

$\Rightarrow R = -P \oplus -Q$ (2)

Substituting (1) into (2) results in

$$-(P \oplus Q) = -P \oplus -Q$$

QED

So continuing from the earlier result that

$$P \oplus' Q = -(O' \oplus -(P \oplus Q))$$

So we have that

$$P \oplus' Q = -\left(O' \oplus -(P \oplus Q)\right) = (P \oplus Q) \oplus -O'$$

This operation should hold the same properties of closure, commutability, identity and inversion. The inverse of P in this scenario would be $P \diamond O'$ instead of the usual $P \diamond O$. We also see that associativity holds by the same argument using the Cayley-Bacharach theorem. So seeing how this group operation holds with O' as the identity. It seems that we can now generate different groups on a single curve by choosing different identity points. However, we see that the set of elements within each of these groups remains the same no matter what we choose for the identity element. So it seems that we can perhaps find an isomorphism between the group of elements $(C,\oplus)$ with identity O and another group $(C,\oplus')$ with some other identity O'. Let us say that in this hypothetical isomorphism, each element P in $(C,\oplus)$ maps to $f(P)$ in the other group $(C,\oplus\,')$. So in order for this isomorphism to hold, the operation in both groups must be preserved by it. That means that for any two elements P and Q in $(C,\oplus)$, we must have that if $P \oplus Q = R$, then $f(P) \oplus' f(Q) = f(R)$. So we have that

$$f(R) = f(P \oplus Q) = f(P) \oplus f(Q) \oplus -O'$$

This statement happens to be true when $f(P) = O' \oplus -P$ giving us,

$$f(P) \oplus 'f(Q) = (O' \oplus -P) \oplus (O' \oplus -Q) \oplus -O'$$

$$= (O' \oplus O' \oplus -O') \oplus (-P \oplus -Q)$$

$$= O' \oplus -(P \oplus Q)$$

$$= f(P \oplus Q)$$

So we have found the possibility of the following isomorphic mapping β:

$$f: (G,\oplus) \mapsto (G,\oplus')$$

$$P \mapsto f(P) = O' \oplus -P$$

The final step to showing that $f(P)$ is actually an isomorphic mapping, we need to show that it is bijective. To do this, we need an inverse function $f^{-1}(P)$ which maps $f(P)$ to P. We have that

$$f\left(f^{-1}(P)\right) = P = O' \oplus -f^{-1}(P)$$

$$\Rightarrow f^{-1}(P) = O' \oplus -P$$

$$\Rightarrow f^{-1}(P) = O' \oplus -P$$

$$= f(P)$$

So we have a well-defined inverse function for $f(P)$ which interestingly enough is $f(P)$ is itself. So every point Q in the range of $f(P)$, maps back to the domain of $f(P)$ by virtue of the well-defined inverse function $f^{-1}(P)$. Hence, $f(P)$ is a bijective mapping. Therefore, it is also an isomorphism from $(G,\oplus)$ to $(G,\oplus')$.

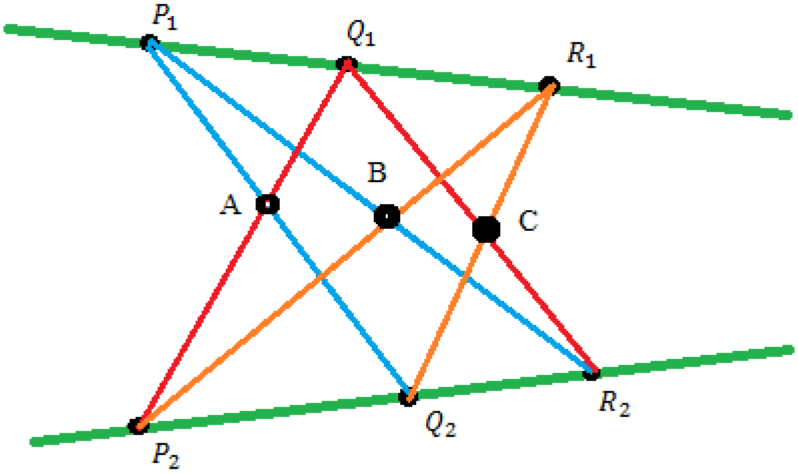
In effect, we have found that all the seemingly different groups defined by the different identity points on a cubic curve are actually all isomorphic to each other. Hence, the group structure on the cubic curve is actually independent of the chosen identity point.

This fact, along with the associativity property of cubic curves gives rise to many other interesting theorems.

Pappus' Theorem

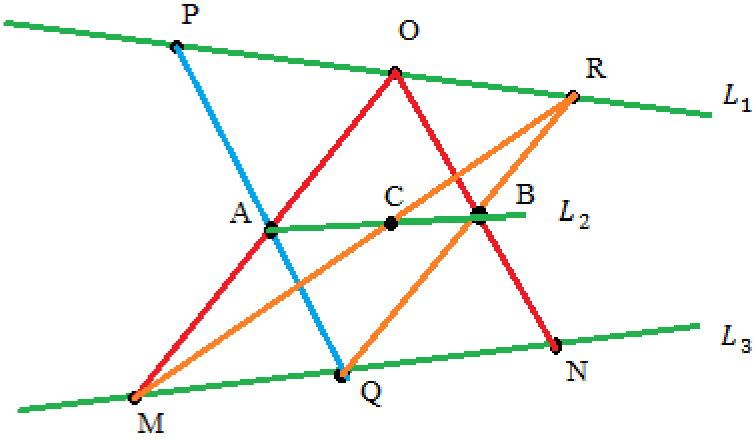
Being an ardent math competitor, I tend to apply Pappus' theorem at times to the Olympiad problems I have to solve. Interestingly, there is a deep connection between the elliptic curve group law and this theorem. The theorem is stated as follows:

Let L_1 and L_2 be two lines in a plane. Let P_1, Q_1 and R_1 be points on L_1 and P_2, Q_2 and R_2 be points on L_2. Let, $A = \overline{P_1Q_2} \cap \overline{Q_1P_2}, B = \overline{P_1R_2} \cap \overline{R_1P_2}$ and $C = \overline{Q_1R_2} \cap \overline{R_1Q_2}$. Then we have that A, B and C are collinear.



This theorem is generally proven through general Euclidean geometry. However, we can readily apply the group structure of cubic curves to prove this. We start off by defining $P = P_1,\ O = Q_1,$

$R = R_1$ and $Q = Q_2$ from the above diagram. We also set $M = P_2$ and $N = R_2$ We also say that $A = \overline{PQ} \cap \overline{OM}$ and $B = \overline{QR} \cap \overline{ON}$. Let us say that $L_1 = \overline{POR}$, $L_2 = \overline{AB}$ and $L_3 = \overline{MQN}$. We can take the union of L_1, L_2 and L_3 to be a degenerate cubic curve. Let us also say that $M \diamond R$ or $C = \overline{MR} \cap L_2$. So we have the following diagram so far:



So in since we have taken the union of all the green lines to be one degenerate cubic, we have that $P, O, R, A, C, B, M, Q, N$ are elements of the group in this cubic. Also, let us take the identity of this group to be O. So we see that $A = P \diamond Q = -(P \oplus Q)$. Hence, we see that $M = O \diamond (P \diamond Q) = P \oplus Q$. Similarly, $N = Q \oplus R$.

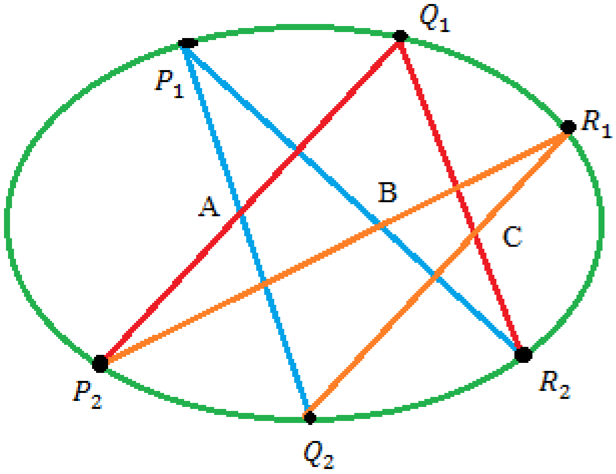
In order to complete the proof of Pappus's theorem, we want to prove that $\overline{PN} \cap \overline{MR}$ lies on L_2. To do this, it is sufficient to show that $\overline{PN} \cap \overline{MR} = \overline{PN} \cap L_2 = C$.

Moving on, we see that $C = M \diamond R = (P \oplus Q) \diamond R = -((P \oplus Q) \oplus R)$. Also, $\overline{PN} \cap L_2 = P \diamond N = -(P \oplus N) = -\big(P \oplus (Q \oplus R)\big) = -\big((P \oplus Q) \oplus R\big) = C$ by virtue of the associativity property of the group operation on a cubic. So we have proven that $\overline{PN} \cap L_2 = C$, proving Pappus's Theorem.

To me, this proof using elliptic curves is a very beautiful one. This seems especially true when compared to the primal and tedious synthetic geometry proof.

A similar argument can be used to prove Pascal's theorem which is stated as follows.

Let T be a conic in a plane. Let P_1, Q_1, R_1, P_2, Q_2 and R_2 be points on T. Let, $A = \overline{P_1Q_2} \cap \overline{Q_1P_2}, B = \overline{P_1R_2} \cap \overline{R_1P_2}$ and $C = \overline{Q_1R_2} \cap \overline{R_1Q_2}$. Then we have that A, B and C are collinear.

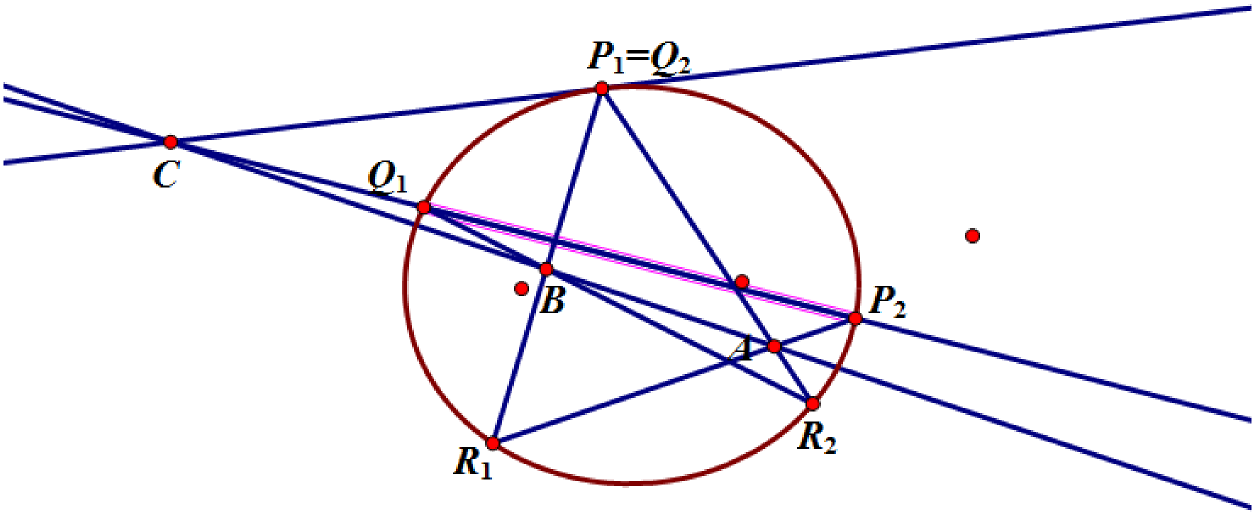


The proof for this is almost identical to the one I have shown for Pappus's except we form the cubic curve group through the union of the conic T and $\overline{AC}$. Interestingly, this theorem leads to two profound lemmas.

Tangent to a Conic

In the setup of Pascal's theorem, let P_1 and Q_2 coincide. So then we get the following diagram:

So this leads us to deduce a handy rule for constructing a tangent to a conic at a point:



We see that $\overline{P_2Q_1}, \overline{AB}$ and $\overline{P_1Q_2}$ (the tangent at P_1) all concur at C. Hence, we can construct $\overline{P_1Q_2}$ if C and P_1 are known. C is simply found by the intersection of lines $\overline{P_2Q_1}$ and $\overline{AB}$. As this holds for any inscribed pentagram with a vertex being the required point of tangency, we have a rule for constructing a tangent to a conic at a point.

Subgroups of the Cubic Curve Group

Since we have a group structure on the elliptic curve, it is not unnatural to explore its non-trivial subgroups.

Order 2

The most basic non-trivial group would consist of two elements, namely the identity element, O and another element P such that $2P$ or $P \oplus P$ is equal to O. Now let us investigate these such elements. Assuming such elements exist, we have that

$$P \oplus P = O$$

$$(P \diamond P) \diamond O = O$$

This implies that $P \diamond P = O$ since O is the only element, M, on a cubic such that $M \diamond O = O$. Hence, we have that if an element, P, is part of a subgroup of order 2 and is not the identity of the cubic curve, then $P \diamond P = O$. In other words, if an element, P, is in a subgroup of order 2 then its tangent to the given cubic intersects it at the identity, O. We can reverse the same] proof to show the converse of the statement to hold true to conclude that a point on a cubic is part of an order 2 subgroup if and only if the tangent to the curve at that point intersects it at the identity.

Order 3

The next smallest non-trivial subgroup of a cubic curve would be one of order 3. It would consist of a set in the form $\{O, M, 2M\}$ where $3M = O$ just like a generic order 3 subgroup. So we have that:

$$3M = M \oplus M \oplus M = O$$

We can manipulate this equation to obtain a useful result:

$$M \oplus M \oplus M \oplus (-M) = O \oplus (-M)$$

$$M \oplus M = -M$$

$$O \diamond (M \diamond M) = O \diamond M$$

From this equation, we deduce that $M \diamond M = M$. Hence, the tangent to the given cubic at M intersects the cubic only at M. In other words, M is a flex to the cubic. So we have proven that if M is in a subgroup of order 3 on a cubic C, then it is an flex point on C. We can prove the converse of this statement by reversing the proof given that $M \diamond M = M$ for all flex points M on a cubic C to conclude that a point M on C is a flex point if and only if it is contained in a subgroup of order 3.

Playing More With Flexes

So given the statement that P is a flex point if and only if $3P = O$, we can actually show that all the flex points in a cubic curve are actually closed under a single subgroup. Suppose we have two flex points P and Q, then we can actually use the abelian nature of the cubic curve group to show that $P \oplus Q$ is also a flex. We have that

$$3(P \oplus Q) = P \oplus Q \oplus P \oplus Q \oplus P \oplus Q$$

$$= P \oplus P \oplus P \oplus Q \oplus Q \oplus Q$$

$$= 3P \oplus 3Q$$

$$= O \oplus O$$

$$= O$$

Hence, as $3(P \oplus Q) = O$, we have that $P \oplus Q$ is a flex point.

Rational Points

As I will discuss later a widely-used method of cryptography, works using this group structure of elliptic curves. However, as we have computers working with this algorithm, the numbers involved in the cryptosystem are most likely all rational ones. If only rational points are worked with when using an elliptic curve for a cryptosystem, then surely all the rational points in the elliptic curve must be closed under the group operation for the curve, forming a subgroup. We can confirm this by proving the algebraic closure of the rational points in a curve's group operation. Before going about this, we must first recall that for any two points P and Q on an elliptic curve with identity O, $P \oplus Q$ is equivalent to $(P \diamond Q) \diamond O$. If we just prove that the operation $\diamond$ is algebraically closed among all the ration points on the curve, then the closure of the $\oplus$ in the same set immediately follows. So let us define an elliptic curve, C, in its generic form as $y = x^3 + ax + b$. Let us also define two points with rational coordinates on this curve $P\left(\frac{d_1}{e_1}, \frac{d_2}{e_2}\right)$ and $Q\left(\frac{m_1}{n_1}, \frac{m_2}{n_2}\right)$ where $d_!, d_2, e_1, e_2, m_1, n_1, m_2, n_2$ are all integers.

The line joining P and Q has a slope of $\frac{\frac{m_2}{n_2} - \frac{d_2}{e_2}}{\frac{m_1}{n_1} - \frac{d_1}{e_1}}$

$$= \frac{(m_2 e_2 - d_2 n_2) n_1 e_1}{(m_1 e_1 - n_1 d_1) n_2 e_2}$$

$$= \frac{h}{j}$$

Where $h = (m_2 e_2 - d_2 n_2) n_1 e_1$and $j = (m_1 e_1 - n_1 d_1) n_2 e_2$. Notice how the slope here is also rational. Now the final equation of the line $\overline{PQ}$ would be solved as follows using the point-slope formula:

$$\frac{y-\frac{d_2}{e_2}}{x-\frac{d_1}{e_1}}=\frac{h}{j}$$

$$y=\frac{hx}{j}-\frac{d_1}{e_1}\frac{h}{j}+\frac{d_2}{e_2}$$

Which turns out to in the form of

$$y=\frac{h}{j}x+\frac{r}{s}$$

For some integers r and s. Now when we equate this equation with that of C to solve for their intersection points, we obtain:

$$y^2=x^3+ax+b=\left(\frac{h}{j}x+\frac{r}{s}\right)^2$$

$$x^3-\frac{h^2}{j^2}x^2+\left(a-2\frac{hr}{js}\right)x+\left(b-\frac{r^2}{s^2}\right)=0$$

We already know that the x-coordinates of P and Q are roots of this equation as they are given intersection points of the line $\overline{PQ}$ and C. Let us say that the third intersection point is $P \diamond Q = R(w,z)$. Hence, w is the third root of the above equation. By Vieta's formulas we know that the sum of the roots of the above equation is the additive inverse of the coefficient of x^2 in the equation. In other words, the sum of the roots is $\frac{h^2}{j^2}$. So we have that

$$w+\frac{m_1}{n_1}+\frac{d_1}{e_1}=\frac{h^2}{j^2}$$

We can solve for w from this:

$$w = \frac{h^2}{j^2} - \frac{m_1}{n_1} - \frac{d_1}{e_1}$$

$$w = \frac{h^2 n_1 e_1 - j^2 m_1 e_1 - j^2 d_1 n_1}{j^2 n_1 e_1}$$

$$= \frac{t}{u}$$

Where t is the integer $h^2 n_1 e_1 - j^2 m_1 e_1 - j^2 d_1 n_1$ and u is the integer $j^2 n_1 e_1$. Note that we have expressed w as a quotient of two integers, showing that is rational. From this value of w we can solve for the y-coordinate of R, z as follows:

$$z = \frac{h}{j} w + \frac{r}{s}$$

$$= \frac{g}{f}$$

Where g is the integer $hws + jr$ and f is the integer js. Note that we have expressed z as a quotient of two integers, showing that is also rational. So we have found the third intersection point R to have rational coordinates $w = \frac{t}{u}$ and $z = \frac{g}{f}$.

So we proved that the third intersection of line $\overline{PQ}$ with C has rational coordinates. In effect, we proved that $P \diamond Q$ yields a point with rational coordinates if P and Q have rational coordinates. Therefore, the operator $\diamond$ is algebraically closed under rational points.

As $P \diamond Q$ yields a rational point if P and Q are rational, $P \oplus Q = (P \diamond Q) \diamond O$ will also yield a rational if P, Q and O are all rational. Hence, $P \oplus Q$ is indeed algebraically closed in the rational points on an elliptic curve.

In order to completely prove the claim that all the rational points on an elliptic curve form a subgroup, we must also show that that each element in the set of rational points on the curve has an inverse. As we discussed earlier, the inverse of an element P on an elliptic is simply $O \diamond P$. As the operator $\diamond$ is closed in the set of rational points, each rational point P also has an inverse $O \diamond P$ that is rational. Hence, we have shown that the set of rational points on an elliptic curve does indeed form a subgroup in the operation, $\oplus$.

As I mentioned earlier, this rational subgroup of elliptic curves happens to be the basis of increasingly popular elliptic curve cryptosystems. The most basic of them is called the Diffie-Hellman Key Exchange Protocol.

In such a cryptosystem, there publicly exists an elliptic curve C and a publicly known point P on the curve. The identity of the group of points on C is usually taken to be the point at infinity. Suppose Billy wants to send an encrypted message to Bob through this cryptosystem. Billy and Bob will first confer that they wish to exchange a message. Bob has a randomly generated number k_A which he multiplies with P to yield k_AP (P added to itself using the standard group operation, $\oplus$, k_A times). He sends this result to Billy. After receiving this value, Billy maps his message to some point, M, on C using a commonly agreed upon mapping. Then he uses his randomly generated private key k_B to generate the values k_Bk_AP and k_BP. Finally, he sends Bob the points k_BP and $M \oplus k_Bk_AP$. Now, Bob can evaluate k_Bk_AP by multiplying his private key with the received point k_BP. To retrieve the message M he can simply add the inverse of k_Bk_AP with the received point $M \oplus k_Bk_AP$.

Notice how third-party knowledge of k_Bk_AP enables a middle-man to eavesdrop on the exchanged message. Although, P is publicly known k_Bk_A cannot be determined as easily as there is no quick and efficient method of “dividing” two points. In other words, we can easily add a point, P, to itself n times to obtain nP but we can’t easily find n given nP and P. This property is what makes this cryptosystem so useful.

Conclusion

When I first heard about cubic polynomials, I merely thought that they would be regular functions which I encounter in my math class exercises and only serve to fill my math homework packets. However, my discovery of the abelian group structure on these polynomials opened this idea up to so many applications from geometry all the way to cryptography. Not only did this group structure yield many applications of elliptic cubic curves but it yielded many interesting properties about elliptics themselves.

Apart from teaching me about the versatility of elliptic curves, this investigation served as an example of how interconnected math can be within its various branches and with the real world no matter how obscure a concept may seem. It really encouraged me to look beyond solving problems from math competitions and schoolwork and to look for deeper connections across the various branches of mathematics. In retrospect, successful mathematical advances were mostly made by people looking for these connections. For example, René Descartes’s Cartesian plane linked algebra and geometry, forming a foundation that is irreplaceable today. I hope to break out of my shell of problem solving and further delve into finding useful and interesting connections in the future.