Algebraic Geometry, PS 3

Bryden Cais

October 16, 2002

Exercise 1.

Exercise 2. Let $A = \mathbb{Z}/(6)$. Consider the ideal $2A$. If $x \in A \setminus 2A$ then x is odd. It follows that the ideal $(x, 2A)$ is all of A (one way to see this is that $2 \in 2A$ and since x is odd, we have integers a, b mod 6 such that $2a + x = 1$). Thus $2A$ is maximal. For the ideal $3A$, if $y \in A \setminus 3A$ then $y = 1, 2, 4$ or 5. If $y = 1$ or 5, y is a unit in $\mathbb{Z}/(6)$. Otherwise, we have $3 - 2 = 4 - 3 = 1$ so that in any case $(3A, y)$ is the unit ideal. Hence $3A$ is maximal. Since if $x \notin 2A, 3A$ we have $x = 1$ or 5 (modulo 6) we see that any such x is a unit. It follows that $2A, 3A$ ore the only maximal ideals of A. Now consider the localization A_{2A}. This consists of all fractions a/b with $a, b \in A$ and $b \notin 2A$ under the equivalence $a/b \sim c/d$ iff there exists $s \in A \setminus 2A$ with $s(ad - bc) = 0$ in A. Set $s = 3$. Then we have $a/b \sim c/d$ iff $ad \equiv bc \mod 2$. Since b, d are odd, we see that

$$0 \sim \frac{2}{*} \sim \frac{4}{*}$$

and

$$\frac{1}{*} \sim \frac{3}{*} \sim \frac{5}{*},$$

where $*$ denotes any element of $A \setminus 2A$. Thus, A_{2A} has two elements and is clearly isomorphic to $\mathbb{Z}/(2)$ since the numerator of $a/b + a/b$ is even and hence the sum is equivalent to 0. A similar analysis applies to the localization A_{3A}. In this case, we choose $s = 2$ and find that $a/b \sim c/d$ iff

$$ad \equiv cd \mod (3).$$

Now observe that $-a, b - a, 2b - a$ are three consecutive terms in arithmetic progression so that one of them is divisible by 3. It follows that $a/b \sim 0, 1$ or 2. Since $3 \sim 0$ we see that $A_{3A} \simeq \mathbb{Z}/(3)$. Now let P be a projective A module of rank 1. Then we know that P_{2A}, P_{3A} are free A_{2A}, A_{3A} (resp.) modules of rank 1, so pick $x \in P_{2A}, y \in P_{3A}$ such that

$$P_{2A} = A_{2A}x$$
$$P_{3A} = A_{3A}y.$$

By clearing denominators, we may assume that $x, y \in P$. We now claim that $P = A(x + y)$ and that $x + y$ is not a zero divisor. It then follows that $P \simeq A$. But how to show this claim??

Exercise 3. Set
$$A = \mathbb{C}[T_1, T_2]/(T_1^2 - T_2(T_2-1)(T_2-2))$$
and let t_1, t_2 be the images of T_1, T_2 under the quotient map. Let $I = (t_1, t_2)$. We show that for any maximal ideal $\mathfrak{M} \subset A$ the localization $I_{\mathfrak{M}}$ is a free $A_{\mathfrak{M}}$ module of rank 1. First, the maximal ideals of A are in bijective correspondence to the maximal ideals of $\mathbb{C}[T_1, T_2]$ containing the principal ideal $T_1^2 - T_2(T_2-1)(T_2-2)$. Since every maximal ideal of $\mathbb{C}[T_1, T_2]$ has the form $(T_1 - \alpha, T_2 - \beta)$, we see that the maximal ideals of A are precisely the ideals
$$\mathfrak{M}_{\alpha,\beta} = (t_1 - \alpha, t_2 - \beta)$$
where $(T_1, T_2) = (\alpha, \beta)$ is a root of $T_1^2 - T_2(T_2-1)(T_2-2)$. Suppose $(\alpha, \beta) \neq (0, 0)$. Then there exists some $f \in I$ with $f \notin \mathfrak{M}_{\alpha,\beta}$ (since $I = \mathfrak{M}_{0,0}, \mathfrak{M}_{\alpha,\beta}$ are distinct maximal ideals). It follows that $I_{\mathfrak{M}_{\alpha,\beta}}$ contains 1 and is therefore equal to $A_{\mathfrak{M}_{\alpha,\beta}}$, that is, is free of rank 1. Now consider I_I. Since I is the ideal of all $f \in A$ with no constant term, we find that any $f \in A_I$ with a nonzero constant term is invertible. In particular, $(t_2-1)(t_2-2)$ is invertible. It follows that
$$\frac{t_1}{(t_2-1)(t_2-2)} t_1 = t_2$$
with $\frac{t_1}{(t_2-1)(t_2-2)} \in A_I$. From this, we see that $I_I = (t_1, t_2)I_= A_I t_1 + A_I t_2 = A_I t_1$ since $A_I t_2 \subset A_I t_1$. Now the elliptic curve $T_1^2 - T_2(T_2-1)(T_2-2)$ has distinct roots and is therefore irreducible. It follows that A is an integral domain and hence that t_1 in particular is not a zero divisor. Therefore, $I_I = A_I t_1$ is free of rank one (sending $t_1 \mapsto 1$ gives a surjective homomorphism from I_I to A_I; injectivity follows from the fact that t_1 is not a zero divisor). Therefore, since the localization of I at every maximal ideal of A is free of rank 1, we see that I is a projective A module of rank 1. Now we must show that I is not free, or equivalently that I is not a principal ideal.

Exercise 4. Suppose that I is a homogenous ideal of $k[T]$ such that $m_+^s \subset I$ for some s. Let $F \in k[T]$. Then for any $G \in m_+^s$ we have $GF \in m_+^s \subset I$ so that $F \in I^{sat}$. Thus, $I^{sat} = k[T]$. For the second part of the question, I am convinced that there is a typo and that it cannot be "Proposition 1." But then what proposition is it supposed to be?

Exercise 5. Let $I = (T_0^2, T_0 T_1) \subset k[T_0, T_1]$. Then since $m_+ = (T_0, T_1)$ we have $T_0 G \in I$ for any $G \in m_+$. Thus, $T_0 \in I^{sat}$ so that $I \subset (T_0) \subset I^{sat}$. We claim that $I^{sat} = (T_0)$. For suppose that $FG \in (T_0)$ for all $G \in m_+^s$ for some s. In particular, $T_1^s F \in (T_0)$ so that F is divisible by T_0 and hence $F \in (T_0)$. It follows that (T_0) is saturated and that $I^{sat} = (T_0)$.

Exercise 6. We first homogenize the equations to find that the projective closure is given by the equations
$$Z_2 Z_0 - Z_1^2, Z_3 Z_0^2 - Z_1^3.$$

The solution set can be parameterized. Indeed, if $Z_0 = 0$ then we must have $Z_1 = 0$ also, whence we obtain the points

$$(0,0,1,t)$$

and

$$(0,0,0,1)$$

for any $t \in k$. Otherwise, $Z_0 \neq 0$ whence we obtain the parameterization

$$(1,t,t^2,t^3)$$

for any $t \in k$. Thus, the projective closure is

$$\{(1,t,t^2,t^3) : t \in k\} \cup \{(0,0,1,t) : t \in k\} \cup (0,0,0,1).$$

Exercise 7. If F is a homogenous polynomail free of multiple factors then $(F) = (F)^{sat}$. We know that the set of solutions of F in $\mathbb{P}^n_k(K)$ is irreducible if and only if the corresponding coordinate ring is an integral domain. But the coordinate ring is

$$A = k[T]/(F)^{sat} = k[T]/(F),$$

and is therefore an integral domain if and only f F is irreducible.

Exercise 8. Clearly, P has only simple roots in $\bar{k}$ iff P, P' have no common roots. By exercise 9 this is the case iff $\text{Res}(P', P) \neq 0$ (since the resultant is a product over all pairwise differences of the roots of P and P'). Let us now compute $\text{Res}(P, P')$ in the case where P is of degree less than 4.

1. $\deg(P) = 2$: Set $P(Z) = a_0Z^2 + a_1Z + a_2$ so that $P'(Z) = 2a_0Z + a_1$. We then have

$$\begin{aligned}\text{Res}(P, P') &= \begin{vmatrix} a_0 & a_1 & a_2 \\ 2a_0 & a_1 & 0 \\ 0 & 2a_0 & a_1 \end{vmatrix} \\ &= -a_0(a_1^2 - 4a_2a_0).\end{aligned}$$

2. $\deg(P) = 3$: Set $P(Z) = a_0Z^3 + a_1Z^2 + a_2Z + a_3$ so that $P'(Z) = 3a_0Z^2 + 2a_1Z + a_2$. We then have

$$\begin{aligned}\text{Res}(P, P') &= \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ 3a_0 & 2a_1 & a_2 & 0 & 0 \\ 0 & 3a_0 & 2a_1 & a_2 & 0 \\ 0 & 0 & 3a_0 & 2a_1 & a_2 \end{vmatrix} \\ &= 27a_3^2a_0^3 + (-18a_3a_2a_1 + 4a_2^3)a_0^2 + (4a_3a_1^3 - a_2^2a_1^2)a_0.\end{aligned}$$

3. $\deg(P) = 4$: Set $P(Z) = a_0Z^4 + a_1Z^3 + a_2Z^2 + a_3Z + a_4$ so that $P^{'}(Z) = 4a_0Z^3 + 3a_1Z^2 + 2a_2Z + a_3$. Proceeding as above (and using `PARI`), we have

$$\begin{aligned}\mathrm{Res}(P, P^{'}) &= \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & a_4 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 \\ 4a_0 & 3a_1 & 2a_2 & a_3 & 0 & 0 & 0 \\ 0 & 4a_0 & 3a_1 & 2a_2 & a_3 & 0 & 0 \\ 0 & 0 & 4a_0 & 3a_1 & 2a_2 & a_3 & 0 \\ 0 & 0 & 0 & 4a_0 & 3a_1 & 2a_2 & a_3 \end{vmatrix} \\ &= 256a_4^3a_0^4 + (-192a_4^2a_3a_1 + (-128a_4^2a_2^2 + 144a_4a_3^2a_2 - 27a_3^4))a_0^3 + ((144a_4^2a_2 - 6a_4a_3^2)a_1^2 \\ &+ (-80a_4a_3a_2^2 + 18a_3^3a_2)a_1 + (16a_4a_2^4 - 4a_3^2a_2^3))a_0^2 + (-27a_4^2a_1^4 + (18a_4a_3a_2 - 4a_3^3)a_1^3 \\ &+ (-4a_4a_2^3 + a_3^2a_2^2)a_1^2)a_0.\end{aligned}$$

Exercise 9. Let

$$\begin{aligned} P &= a_0(Z - \alpha_1)\cdots(Z - \alpha_n) = a_0Z^n + a_1Z^{n-1} + \cdots + a_n, \\ Q &= b_0(Z - \beta_1)\cdots(Z - \beta_m) = b_0Z^m + b_1Z^{m-1} + \cdots + b_m. \end{aligned}$$

Let $V(X_1, X_2, \ldots, X_r)$ denote the matrix

$$\begin{pmatrix} 1 & X_1 & \cdots & X_1^r \\ 1 & X_2 & \cdots & X_2^r \\ \vdots & \vdots & \cdots & \vdots \\ 1 & X_r & \cdots & X_r^r \end{pmatrix},$$

set $M = V(\beta_m, \cdots, \beta_1, \alpha_n, \cdots, \alpha_1)$ and

$$R = \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_{m-1} & \ddots & b_0 \\ a_n & \ddots & a_1 & b_m & \ddots & \vdots \\ & \ddots & \vdots & & \ddots & b_{m-1} \\ & & a_n & & & b_m \end{pmatrix}.$$

We first show that $\det(V(X_1, \ldots, X_r)) = \prod_{1 \le i < j \le r}(X_i - X_j)$. To see this, for $1 \le j \le r - 1$, subtract X_1 times the j^{th} column from the $(j + 1)^{\text{st}}$ column of the matrix $V(X_1, \ldots, X_r)$. These operations do not alter the determinant, and we find that

$$\det(V(X_1,\dots,X_r)) = \prod_{2\le i\le r}(X_i - X_1)\,\det(V(X_2,\dots,X_r)).$$

Induction then gives the proposed formula. We now compute the determinant of MR in two different ways. It is not difficult to see that

$$\begin{pmatrix} 1 & \beta_m & \cdots & \beta_m^{m+n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \beta_1 & \cdots & \beta_1^{m+n-1} \\ 1 & \alpha_n & \cdots & \alpha_n^{m+n-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha_1 & \cdots & \alpha_1^{m+n-1} \end{pmatrix} \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_0 & b_{m-1} & \ddots & b_0 \\ a_n & \ddots & a_1 & b_m & \ddots & \vdots \\ & \ddots & \vdots & & \ddots & b_{m-1} \\ & & a_n & & & b_m \end{pmatrix}$$

$$= \begin{pmatrix} P(\beta_m) & \cdots & P(\beta_m)\beta_m^{m-1} & & & \\ \vdots & \cdots & \vdots & & & \\ P(\beta_1) & \cdots & P(\beta_1)\beta_1^{m-1} & & & \\ & & & Q(\alpha_n) & \cdots & Q(\alpha_n)\alpha_n^{n-1} \\ & & & \vdots & \cdots & \vdots \\ & & & Q(\alpha_1) & \cdots & Q(\alpha_1)\alpha_1^{n-1} \end{pmatrix},$$

and hence that

$$\det(MR) = \det(V(\beta_m,\dots,\beta_1)V(\alpha_n,\dots,\alpha_1)) \prod_{1\le j\le m} P(\beta_j) \prod_{1\le i\le n} Q(\alpha_i).$$

On the other hand,

$$\begin{aligned} \det(MR) &= \det(M)\,\det(R^T) \\ &= \det(V(\beta_m,\dots,\beta_1,\alpha_n,\dots,\alpha_1))\,\mathrm{Res}(P,Q), \end{aligned}$$

where R^T denotes the transpose of R. Now, using our formula for the determinant of $V(X_1,\dots,X_r)$, we see that

$$\begin{aligned} &\det(V(\beta_m,\dots,\beta_1,\alpha_n,\dots,\alpha_1)) \\ &\quad= \det(V(\beta_m,\dots,\beta_1))\det(V(\alpha_n,\dots,\alpha_1)) \prod_{1\le i\le n}\prod_{1\le j\le m}(\alpha_i - \beta_j) \\ &\quad= \det(V(\beta_m,\dots,\beta_1))\det(V(\alpha_n,\dots,\alpha_1)) \frac{1}{b_0^n} \prod_{1\le i\le n} Q(\alpha_i). \end{aligned}$$

It thus follows that

$$\operatorname{Res}(P,Q) = b_0^n\, P(\beta_1)\cdots P(\beta_m).$$

Notice that $\operatorname{Res}(P,Q) = (-1)^{mn}\operatorname{Res}(Q,P)$ since to swap the roles of the a_i's and the b_j's in the defining determinant of the resultant requires a bubble sort involving mn flips of columns. Thus, we also have

$$\operatorname{Res}(P,Q) = (-1)^{mn} a_0^m\, Q(\alpha_1)\cdots Q(\alpha_n).$$

Exercise 10. Let X be the cubic curve defined projectively by $T_1^2T_0 - T_2^2 - T_0^3 = 0$. Except for the point at infinity, $(0,1,0)$, all points on $X(\mathbb{C})$ lie in $\mathbb{A}^1_{\mathbb{C}}$ (where we take the copy of $\mathbb{A}^1_{\mathbb{C}} \subset \mathbb{P}^1_{\mathbb{C}}$ given by $T_0 = 1$. We thus proceed to determine explicit formulae for the group law on the affine curve X' given by $y^2 = x^3 + 1$. Let $P_0 = (x_0, y_0), P_1 = (x_1, y_1)$ be any two *distinct* points on X'. Then line through these points intersects X at a third point whose x coordinate is the third root of

$$\left(\frac{y_1 - y_0}{x_1 - x_0}(x - x_0) + y_0\right)^2 = x^3 + 1.$$

Call this root x_2. Then since x_0, x_1 are also roots, we know that

$$\left(\frac{y_1 - y_0}{x_1 - x_0}\right)^2 = x_0 + x_1 + x_2.$$

Similarly, y_2 is given by

$$y_2 = \frac{y_1 - y_0}{x_1 - x_0}(x_2 - x_0) + y_0.$$

Taking the point $(0,1,0)$ as the zero element, we find that the sum $P_0 + P_1$ on X is the point $P_2 = (x_2, -y_2)$. Observe that

$$\begin{aligned}
x_2 &= \left(\frac{y_1 - y_0}{x_1 - x_0}\right)^2 - x_0 - x_1 \\
&= \left(\frac{x_1^3 - x_0^3}{(x_1 - x_0)(y_1 + y_0)}\right)^2 - x_0 - x_1 \\
&= \left(\frac{x_0^2 + x_0x_1 + x_1^2}{y_1 + y_0}\right)^2 - x_0 - x_1,
\end{aligned}$$

so that if $P_0 = P_1$ we have $2P_0 = (x_2, -y_2)$, where

$$x_2 = \left(\frac{3x_0^2}{2y_0}\right)^2 - 2x_0,$$

and

$$y_2 = \left(\frac{3x_0^2}{2y_0}\right)(x_2 - x_0) + y_0.$$

All of these formulae make sense except when $x_0 = x_1$ but $P_0 \neq P_1$ (in which case the sum $P_0 + P_1$ is seen to be the point at infinity) and when $y_0 = 0$, when x_0 is a cube root of -1 whence the sum $2P_0$ is again the point at infinity.

Exercise 11. Using our formulae above, we can determine explicit formulae for $3P$ when P is a point on X. Let $P = (x, y)$. It is not difficult to see from the formulae that the points of order 3 in $X(C)$ correspond to those points P with $2P = -P$, i.e. those points P with

$$\left(\frac{3x^2}{2y}\right)^2 - 3x = 0.$$

This gives

$$x^4 + 4x = 0,$$

or $x = 0, -\sqrt[3]{4}, \rho\sqrt[3]{4}, -\rho\sqrt[3]{4}$, where $\rho = e^{\pi i/3}$ is a cube root of -1. For each of these four values of x there are two corresponding values of y, giving 8 points of order exactly 3. Since the point at infinity O also satisfies $3O = O$, we see that there are nine points in $X(C)$ satisfying $3P = O$. They are

$$\begin{aligned}
O &= (0, 1, 0) \\
\pm P_1 &= (1, \pm 1, 0) \\
\pm P_2 &= (1, \pm i\sqrt{3}, -\sqrt[3]{4}) \\
\pm P_3 &= (1, \pm i\sqrt{3}, \rho\sqrt[3]{4}) \\
\pm P_4 &= (1, \pm i\sqrt{3}, -\rho\sqrt[3]{4}).
\end{aligned}$$

Now let us determine the inflection points of X in $\mathbb{C}$. A point (T_0, T_1, T_2) is an inflection point of X if and only if

$$\begin{vmatrix} -6T_0 & 2T_1 & 0 \\ 2T_1 & 2T_0 & 0 \\ 0 & 0 & 6T_2 \end{vmatrix} = -24T_2(3T_0^2 + T_1^2) = 0.$$

These are the points on X with $T_2 = 0$ or $T_1 = \pm i\sqrt{3}T_0$. It is easy to see that these are precisely the 9 points listed above. Of course, a more intuitive way to think about this problem is that the points of order 3 are those points P such that the tangent line at P has third point of intersection P (this is just the requirement that $2P = -P$). But this is equivalent to requiring that the tangent line at

P intersect X with multiplicity 3 (the maximum multiplicity, according to Bezout's theorem), i.e. that P be an inflection point of X.

Now it can be seen that any line containing two of the eight points of order 3 contains a third, and hence that this is an example of a configuration of 8 points not satisfying the assumption of Lemma 1.

Exercise 12. Let X be the curve given by $T_1^2T_0 - T_2^3$. For any field K, define the map $f : X(K) \setminus (1,0,0) \to K$ by

$$(T_0, T_1, T_2) \mapsto \frac{T_2}{T_1}.$$

Observe that this is a well defined map since $T_1 = 0$ iff $T_2 = 0$ and we are excluding the point $(1,0,0)$; in addition, the value of f is independent of the homogenous coordinates chosen. We now show that f induces an isomorphism of the group structure on $X(K)$ with the additive group K^+. Recall that X is *rational*, that is, we have the parameterization $(1, t^3, t^2)$ (excluding the point at infinity). Thus, let $P = (1, \alpha^3, \alpha^2), Q = (1, \beta^3, \beta^2)$ be any two points of $X(K)$. Let us determine $P+Q$. Passing to affine coordinates by setting $y = T_1/T_0, x = T_2/T_0$ and writing $y = mx+b$ for the line (in affine coordinates) passing through P, Q, we see that α^2, β^2 are both roots of $(mx+b)^2 = x^3$ and that the third root, γ is the x coordinate of the sum $P+Q$. Then we have $\alpha^2 + \beta^2 + \gamma = m^2$. By now this process is standard, and we find that the x coordinate of $P+Q$ is given by:

$$\begin{aligned}\left(\frac{\alpha^3-\beta^3}{\alpha^2-\beta^2}\right)^2 - (\alpha^2+\beta^2) &= \frac{\alpha^6+\beta^6-2\alpha^3\beta^3-(\alpha^2-\beta^2)(\alpha^4-\beta^4)}{(\alpha^2-\beta^2)^2} \\ &= \frac{\alpha^2\beta^2(\alpha-\beta)^2}{(\alpha^2-\beta^2)^2} \\ &= \left(\frac{\alpha\beta}{\alpha+\beta}\right)^2.\end{aligned}$$

It then follows that the y coordinate of $P+Q$ is given by

$$\left(\frac{\alpha\beta}{\alpha+\beta}\right)^3.$$

Therefore, in homogenous coordinates, we have

$$P+Q = \left(1, \left(\frac{\alpha\beta}{\alpha+\beta}\right)^3, \left(\frac{\alpha\beta}{\alpha+\beta}\right)^2\right)$$

if $\alpha \neq -\beta$ (that is, if $P \neq -Q$) and $P+Q = (0,1,0)$ if $P = -Q$. Now we have

$$f(0,1,0) = 0$$

and

$$
\begin{aligned}
f(P+Q) &= f\left(1, \left(\frac{\alpha\beta}{\alpha+\beta}\right)^3, \left(\frac{\alpha\beta}{\alpha+\beta}\right)^2\right) \\
&= \frac{\left(\frac{\alpha\beta}{\alpha+\beta}\right)^2}{\left(\frac{\alpha\beta}{\alpha+\beta}\right)^3} \\
&= \frac{\alpha+\beta}{\alpha\beta} \\
&= f(P) + f(Q),
\end{aligned}
$$

so that f is indeed a group homomorphism. We have already seen that f is bijective, so we are done.

Exercise 13. This is similar to the above. Let X be given in projective coordinates by $T_1^2 T_0 - T_2^2(T_2 + T_0)$. For any field K, define the map $f : X(K) \setminus (1,0,0) \to K$ by

$$
(T_0, T_1, T_2) \mapsto \frac{T_1 - T_2}{T_1 + T_2}.
$$

As before, it is not difficult to see that this is a well defined map and that $f(0,1,0) = 1 \in K^*$. We claim that f induces an isomorphism of the group structure on $X(K)$ with the multiplicative group K^*. As above, X is parameterized by $(1, t(t^2-1), t^2-1)$ (excluding the point at infinity). Thus, let $P = (1, \alpha(\alpha^2-1), \alpha^2-1), Q = (1, \beta(\beta^2-1), \beta^2-1)$ be any two points of $X(K)$. Observe first that

$$
\begin{aligned}
f(P) &= \frac{\alpha-1}{\alpha+1} \\
f(Q) &= \frac{\beta-1}{\beta+1}.
\end{aligned}
$$

Let us determine $P+Q$. Proceeding as above, set $y = T_1/T_0, x = T_2/T_0$ and write $y = mx + b$ for the line (in affine coordinates) passing through P, Q. Then we see that α^2-1, β^2-1 are both roots of $(mx+b)^2 = x^3 + x^2$ and that the third root, γ is the x coordinate of the sum $P+Q$. Then we have $\alpha^2 + \beta^2 + \gamma - 2 = m^2 - 1$. By now this process is standard, and we find that the x coordinate of $P+Q$ is given by:

$$
\begin{aligned}
\left(\frac{\alpha(\alpha^2-1) - \beta(\beta^2-1)}{\alpha^2-\beta^2}\right)^2 - (\alpha^2+\beta^2-1) &= \left(\frac{\alpha^2+\beta^2+\alpha\beta-1}{\alpha+\beta}\right)^2 - (\alpha^2+\beta^2-1) \\
&= \frac{\alpha^2\beta^2 - \alpha^2 - \beta^2 + 1}{(\alpha+\beta)^2} \\
&= \left(\frac{\alpha\beta+1}{\alpha+\beta}\right)^2 - 1.
\end{aligned}
$$

We therefore see that

$$P+Q=\left(1,\frac{\alpha\beta+1}{\alpha+\beta}\left(\left(\frac{\alpha\beta+1}{\alpha+\beta}\right)^2-1\right),\left(\frac{\alpha\beta+1}{\alpha+\beta}\right)^2-1\right),$$

so that

$$f(P+Q)=\frac{\alpha\beta-\alpha-\beta+1}{\alpha\beta+\alpha+\beta+1}=\frac{(\alpha-1)(\beta-1)}{(\alpha+1)(\beta+1)}=f(P)f(Q).$$

Thus f is a homomorphism. The fact that f is bijective follows from the rationality of our curve and the definition of f.