

Problem 1.

- (i) Suppose P is not an inflection point on the curve E . This means that the tangent line to E on P meets the curve in a third point Q where $Q \neq P$. Now again if we draw the tangent line to E on Q , if it meets the curve in Q 3 times, it means that Q is an inflection point and this case was solved in class. So assume that Q also is not an inflection point, which means that the tangent line on Q meets the curve in a third point R , where $R \neq Q$ and $R \neq P$. Now consider the matrix:

$$M_\alpha = \begin{bmatrix} P_x & Q_x & R_x \\ P_y & Q_y & R_y \\ P_z & Q_z & R_z \end{bmatrix}$$

Since these three points are not on the same line, then they are linearly independent. This means that $\det(M_\alpha) \neq 0$. Then suppose $\alpha = M_\alpha^{-1}$. Now it is easy to see that α maps P and Q and R respectively to $[1; 0; 0]$, $[0; 1; 0]$ and $[0; 0; 1]$. Suppose that E after transformation with M_α has the form:

$$G(u, v, w) = ku^3 + lu^2v + muv^2 + nv^3 + pu^2w + quvw + rv^2w + suw^2 + tvw^2 + fw^3 = 0$$

Now since $G(1, 0, 0) = G(0, 1, 0) = G(0, 0, 1) = 0$, then we have $k = n = f = 0$. Now the line tangent to P and passing through Q is now the line that is tangent to $[1; 0; 0]$ and passing through $[0; 1; 0]$. It is easy to see that this line is $W = 0$. Now consider intersections of this line and G :

$$\begin{aligned} G(u, v, 0) &= lu^2v + muv^2 = 0 \\ &= uv(lu + mv) = 0 \end{aligned}$$

Now note that uv has roots $[1; 0; 0]$ and $[0; 1; 0]$. The third root is also $[1; 0; 0]$. Therefore $lu + mv$ has root $[1; 0; 0]$:

$$l \cdot 1 + 0 = 0 \implies l = 0$$

Also since $[0; 1; 0]$ is not its root, then :

$$l \cdot 0 + m \cdot 1 \neq 0 \implies m \neq 0$$

Also the tangent line to Q which goes through R is now transformed to line tangent to $[0; 1; 0]$ and goes through $[0; 0; 1]$. It is not hard to see that this line is $U = 0$. Now if we see the intersections of this line with the curve, we get three points, $[0; 1; 0]$ two times, and $[0; 0; 1]$ one time. This means that $[0; 1; 0]$ is root of the below equation 2 times, and $[0; 0; 1]$ is the root of it one time:

$$\begin{aligned} G(0, v, w) &= rv^2w + tvw^2 = 0 \\ &= vw(rv + tw) = 0 \end{aligned}$$

Now vw has roots $[0; 1; 0]$ and $[0; 0; 1]$, thus $[0; 1; 0]$ is root of $rv + tw$, and $[0; 0; 1]$ is not, we have:

$$\begin{aligned} r \cdot 1 + t \cdot 0 &= 0 \implies r = 0 \\ r \cdot 0 + t \cdot 1 &\neq 0 \implies t \neq 0 \end{aligned}$$

This gives us the form:

$$G(u, v, w) = muv^2 + pu^2w + quvw + suw^2 + tvw^2 = 0$$

Now here if we do the substitution $(u, v, w) \rightarrow (K^2, LN, KN)$, we have:

$$mK^2L^2N^2 + pk^5N + qk^3LN^2 + sK^4N^2 + tK^2LN^3 = 0$$

And here dividing by K^2N , we get:

$$\begin{aligned} mL^2N + pK^3 + qKLN + sK^2N + tLN^2 &= 0 \\ mL^2N + qKLN + tLN^2 &= -pK^3 - sK^2N \end{aligned}$$

Dehomogenizing in L we get:

$$mL^2 + (qK + t)L = -pK^3 - sK^2$$

Now replace L with $(L - \frac{1}{2}(qK + t))$ we get:

$$L^2 = \text{cubic in } K.$$

The cubic in K might not have leading coefficient 1, but we can adjust that by replacing K and L by λK and $\lambda^2 L$, where λ is the leading coefficient of the cubic. So we do finally get an equation in Weierstrass form.

(ii)

Problem 2.

$C(x, y, z)$ is a projective curve of degree 3:

$$ax^3 + bx^2y + cx^2z + dxy^2 + exz^2 + fy^3 + gy^2z + hyz^2 + iz^3 + jxyz = 0$$

First note that \mathcal{O} is on the curve, then $C(0, 1, 0) = fy^3 = 0$. Thus $f = 0$. Since the line $z = 0$ intersects with the curve 3 times in \mathcal{O} , then:

$$C(x, y, 0) = ax^3 + bx^2y + dxy^2 = x(ax^2 + bxy + dy^2) = 0$$

has the root $[0; 1; 0]$, 3 times. x has one root $[0; 1; 0]$. Now since $[0; 1; 0]$ is the root of $ax^2 + bxy + dy^2$, then we have: $d(1)^2 = 0$, which suggests that $d = 0$.

$$C(x, y, 0) = ax^3 + bx^2y = x^2(ax + by) = 0$$

Since x^2 has two roots, then $ax + by$ has one root, $[0; 1; 0]$. This means that $b(1) = 0$ and $b = 0$. Rewriting $C(x, y, z)$ we have:

$$C(x, y, z) = ax^3 + cx^2z + exz^2 + gy^2z + hyz^2 + iz^3 + jxyz = 0$$

Dividing by g and then replacing x with $x/\sqrt[3]{a}$ we get:

$$y^2z + h'yz^2 + j'xyz = x^3 + c'x^2z + e'xz^2 + i'z^3$$

Which is in Weierstrass form. Note that since \mathbb{C} is algebraically closed, then $\sqrt[3]{a}$ is also in \mathbb{C} , and transformations are all valid.

Problem 3.

First we have to show that the curve is smooth. We Homogenize the equation:

$$y^2z + xyz - x^3 - z^3 = 0$$

Then we calculate all partial derivatives:

$$\frac{\partial F}{\partial x} = -3x^2 + yz \quad \frac{\partial F}{\partial y} = 2yz + xz \quad \frac{\partial F}{\partial z} = -3z^2 + y^2 + xy$$

Since we want to find the answers in \mathbb{F}_2 , then we have:

$$\frac{\partial F}{\partial x} = x^2 + yz \quad \frac{\partial F}{\partial y} = yz + xz \quad \frac{\partial F}{\partial z} = z^2 + y^2 + xy$$

If a point is singular, then it vanishes in all three derivatives:

$$\left. \begin{array}{l} x^2 + yz = 0 \\ yz + xz = 0 \end{array} \right\} \implies x^2 - xz = 0 \implies x(x - z) = 0$$

Then we have two cases:

a) $x = 0$

Then since $x^2 + yz = 0$, we get $yz = 0$. Now either $y = 0$ or $z = 0$, WLOG suppose that $y = 0$. Then since $z^2 + y^2 + xy = 0$, we have $z^2 = 0$ and $z = 0$, but this point $(0, 0, 0)$ is not on the plane.

b) $x = 1, x = z$

In this case note that $x^2 + yz = 0$, then $1 + y = 0$, which means that $y = 1$. But then we have $z^2 + y^2 + xy = 1$, and therefore this point is non-singular. Thus all points on this curve are non-singular and the curve is smooth. Also since the point $(1, 1, 1)$ is on the curve, then this curve is indeed an elliptic curve.

Now we have to show that the point $(1, 1, 1)$ is of order 4. Only points on this curve are: $\mathcal{O} = [0; 1; 0], [1; 0; 1], [0; 1; 1], [1; 1; 1]$. So we only need to show that $P = (1, 1, 1)$ is not of order 2. For this we find $2P$.

$$\begin{aligned}\frac{\partial F}{\partial x}(P) &= -3x^2 + y = (x^2 + y)(P) = 2 = 0 \\ \frac{\partial F}{\partial y}(P) &= (2y + x)(P) = x(P) = 1\end{aligned}$$

Thus the tangent line to P is $1(y - 1) = 0$ or simply $y = 1$. For us to find the third point we find the roots of:

$$1 + x = x^3 + 1$$

This equation has 0 as its roots once and 1 as its roots twice. Thus the third intersection of the line and the curve is $(1, 1)$. In other words $P * P = P$. To find $P + P$ we need to find $P * \mathcal{O}$. Consider the equation in homogenized form:

$$y^2z + xyz = x^3 + z^3$$

Suppose the line $ax + by + cz = 0$ is passing through P and \mathcal{O} . Then $b = 0$ and $a = c$, or $x = z$. Substitution gives us:

$$\begin{aligned}y^2x + x^2y &= x^3 + x^3 = 2x^3 = 0 \\ \implies xy(y + x) &= 0\end{aligned}$$

If $x = z = 0$, then gives us the root $\mathcal{O} = [0; 1; 0]$. If $x = z = 1$, then gives us the roots $[1; 0; 1]$ and $[1; 1; 1]$. Therefore we have $P + P = P * \mathcal{O} = [1; 0; 1] \neq \mathcal{O}$. Then P is not of order 2. Therefore P has order 4.

Problem 4.

- (i) Note that $v(1 \times 1) = v(1) + v(1)$, thus $v(1) = 0$, hence $v(1) = v(-1) + v(-1)$, resulting $v(-1) = 0$. Now we can write $v(-n) = v(-1) + v(n)$, which gives us $v(n) = v(-n)$. Suppose that $v(x) < v(y)$. We can write:

$$v(x + y) = v(x) + v(1 + \frac{y}{x})$$

Since $v(x + y) \geq \min\{v(x), v(y)\} = v(x)$, we have $v(1 + \frac{y}{x}) \geq 0$. Now we have:

$$0 = v(1) = v(1 + \frac{y}{x} - \frac{y}{x}) \geq \min\{v(1 + \frac{y}{x}), v(-\frac{y}{x})\}$$

Since $v(-\frac{y}{x}) = v(\frac{y}{x}) = v(y) + v(\frac{1}{x}) = v(y) - v(x) > 0$, then we have $v(1 + \frac{y}{x}) = 0$, which gives us $v(x + y) = v(x)$.

- (ii) Since the sum is finite, WLOG suppose that $a_1 = \min\{a_i\}_{1 \leq i \leq n}$. Then for any a_i , either $v(a_1) = v(a_i)$, and we are done, then assume otherwise, using the first part, we have:

$$\begin{aligned} & \forall i, v(a_1) \neq v(a_i) \\ \implies & \forall i, v(a_1 + a_i) = \min\{a_1, a_i\} = a_1 \end{aligned}$$

Now note that:

$$\begin{aligned} & v(a_1 + a_2) = v(a_1) \\ v(a_1 + a_2) = v(a_1) \neq v(a_2) & \implies v(a_1 + a_2 + a_3) = \min\{v(a_1 + a_2), v(a_3)\} = v(a_1) \\ & \vdots \\ v(a_1 + \dots + a_{n-2}) = v(a_1) \neq v(a_{n-1}) & \implies \\ & v(a_1 + \dots + a_{n-1}) = \min\{v(a_1 + \dots + a_{n-2}), v(a_{n-1})\} \\ & = \min\{v(a_1), v(a_{n-1})\} = v(a_1) \end{aligned}$$

Note that $0 = v(1) = v(-1 \times -1) = v(-1) + v(-1)$, hence $v(-1) = 0$. Then we have:

$$v(-n) = v(-1) + v(n) = v(n)$$

Now note that $a_1 + a_2 + \dots + a_{n-1} = -a_n$, This means that $v(a_1 + \dots + a_{n-1}) = v(a_n)$ therefore $v(a_1) = v(a_n)$. Which gives us a contradiction since we assumed there is no i such that $v(a_1) = v(a_i)$.

Problem 5.

- (i) First we show that $1_F \in R_v$. For this we show that $v(1) = v(1) + v(1)$, which means that $v(1) = 0$, then since $R_v = \{x \in F | v(x) \geq 0\}$. Thus $1_F \in R_v$.

$$0 = v(1) = v(a) + v(a^{-1})$$

This means that either $v(a) \geq 0$ or $v(a^{-1}) \geq 0$, therefore either $a \in R_v$ or $a^{-1} \in R_v$.

- (ii) Suppose that there exists some $x \in J$ such that $x \notin I$. If such element does not exist, then we have $J \subseteq I$ and we are done. Now Let $y \in I$. For any element of $k \in R_v$, we have $ky \in I$. This means that $ky \neq x$ for any $k \in R_v$. Now consider the element $xy^{-1} \in F$. If it were to have this element in R_v , then we would have $xy^{-1}y = x \in I$, which can not happen, thus $xy^{-1} \notin R_v$, and by part i, we have $(xy^{-1})^{-1} = yx^{-1} \in R_v$. Then we have $yx^{-1}x = y \in J$. Since y was an arbitrary element of I , we conclude that $I \subseteq J$.
- (iii) To show that this ring is a local, we first prove that it has a maximal ideal. Consider the ideal $I = \{x \in F | v(x) > 0\}$. To show that this is an ideal we have to show that for any $x, y \in I$ and $r \in R_v$ we have $rx - y \in I$.

$$v(rx - y) \geq \min\{v(rx), v(-y)\} = \min\{v(r) + v(x), v(y)\}$$

Since both $x, y \in I$, we have $v(x), v(y) > 0$. Thus $v(rx - y) > 0$, and $rx - y \in I$. Now we show that an element x in R_v is unit iff $v(x) = 0$.

$$\begin{aligned} v(x) = 0 &\implies v(1) = v(x) + v(x^{-1}) \implies v(x^{-1}) = 0 \implies x^{-1} \in R_v \\ x^{-1} \in R_v &\implies v(x^{-1}) \geq 0 \implies v(1) = v(x) + v(x^{-1}) = 0 \implies v(x^{-1}) = v(x) = 0 \end{aligned}$$

Now this means that I is the ideal of all non-unit elements of R_v . I is maximal since adding any other element, means adding 1 to the ideal, hence the ideal is R_v . To show that this maximal ideal is unique, suppose we have some other J that is ideal. It is obvious that J can not contain any unit element, since it constructs R_v , then $J \subset I$. This gives us a contradiction as there is only R_v itself over J . Thus R_v has only one maximal ideal, and is local. Next we have to show that if it is a noetherian ring, then it is PID. Each ideal is finitely generated. Let $I = \langle a_1, a_2, \dots, a_n \rangle$. And let a_1 be the element with the smallest valuation. We show that $I = \langle a_1 \rangle$. For this we have to show that there exists some element b_i such that $b_i a_1 = a_i$ for each $2 \leq i \leq n$. Let $b_i = a_i a_1^{-1}$. We only have to show that $b_i \in R_v$, for this note that:

$$v(b_i) = v(a_i) + v(a_1^{-1}) = v(a_i) - v(a_1) \geq 0$$

The last part is followed by the fact that we chose a_1 to have the minimum v among all a_i s. This shows that $b_i \in R_v$, and thus $I = \langle a_1 \rangle$, and since I was an arbitrary ideal, then R_v is a PID.

Problem 6.

- (i) First note that $| \cdot |_p$ is non-archimedean, we show that if $|x|_p \neq |y|_p$ then $|x + y|_p = \max\{|x|_p, |y|_p\}$. WLOG suppose that $|x|_p > |y|_p$. we can write:

$$|x + y|_p \leq \max\{|x|_p, |y|_p\} = |x|_p$$

We can also write:

$$|x|_p = |x + y - y|_p \geq \max\{|x + y|_p, |-y|_p\}$$

Now note that $|-y|_p = |y|_p$, and since we had $|x|_p > |y|_p$, then we have that $\max\{|x + y|_p, |-y|_p\} = |x + y|_p$. Then we have $|x|_p = |x + y|_p$ and the claim is proven. Now suppose that we have a, b, c , three numbers each representing one vertex of the triangle, then sides of this triangle have lengths: $|a - b|_p, |b - c|_p, |a - c|_p$. If $|a - b|_p = |b - c|_p$, then we are done. Otherwise, by the fact proven above, we have that $|a - c|_p = |a - b + b - c|_p$, and since $|a - b|_p \neq |b - c|_p$, then $|a - c|_p = \max\{|a - b|_p, |b - c|_p\}$, which gives us two equal sides of the triangle, and we are done!

(ii)

(iii)

Problem 7.

(i)

(ii)