Sheet 3

1)(i) Let $l_i \subseteq \mathbb{C}^3$ be the 1-dimensional subspace corresponding to P_i, $i \in \{1,\dots,4\}$. Then $\mathbb{C}^3 = l_1 \oplus l_2 \oplus l_3$. Now pick $v_4 \in l_4 \setminus \{0\}$ and let $v_1 \in l_1, v_2 \in l_2, v_3 \in l_3$ be the unique vectors with $v_4 = v_1 + v_2 + v_3$. Then (v_1, v_2, v_3) is a basis of $\mathbb{C}^3$ which gives the required coordinate system. The only choice we had was the choice of v_4, so that gives the uniqueness up to multiplication by a single scalar.

(ii) A conic $q = AX^2 + BY^2 + CZ^2 + DXY + EYZ + FXZ$ passes through $P_1, \dots, P_5$ (using the coordinate system from (i)) iff $A = B = C = 0$, and $D + E + F = 0$ and $abD + bcE + acF = 0$.
We can think of these conics as forming a subspace determined by two equations in a three dimensional space (the "(D,E,F)-space")
If $P_5 \notin \{P_1, \dots, P_4\}$, then these two equations are linearly independent and our space of conics is one-dimensional, in accordance with Cor 2 to Bezout's Theorem (Lecture 5).

2) Let $P = \sum_{m,n \geq 0} a_{mn} x^m y^n$ be a polynomial that vanishes on the affine curve $C = \{y^2 = x^3\}$. We have $P \equiv \sum_{m \geq 0} b_m x^m + \sum_{m \geq 0} c_m x^m y \mod (y^2 - x^3)$
Evaluating at $(x,y) = (t^2, t^3)$ we get $0 = \sum_{m \geq 0} b_m t^{2m} + \sum_{m \geq 0} c_m t^{2m+3}$, since P and anything divisible by $y^2 - x^3$ vanishes on C.
Since terms in the first sum are all of even degree and the terms in the second sum are all of odd degree we get $b_m = c_m = 0 \; \forall_{m \geq 0}$.
So $P \equiv 0 \mod (y^2 - x^3)$. Notice the similarity with the proof of the lemma in Lecture 4.

3) We may assume, after a change of coordinates, that $p = (a,b) = (0,0) = \underline{0}$.
(i) Then $f = \frac{\partial f}{\partial x}(\underline{0}) x + \frac{\partial f}{\partial y}(\underline{0}) y + g$, where g is a linear combination of monomials of degree ≥ 2 in x and y (i.e. monomials $x^i y^j$ with $i + j \geq 2$).
Now let L' be a line through $p = \underline{0}$. Pick $\underline{v} \in L' \setminus \{\underline{0}\}$. Then $t \mapsto t\underline{v}$ is a linear parameterisation of L and we have
$f(t\underline{v}) = t\left(\frac{\partial f}{\partial x}(\underline{0}) v_1 + \frac{\partial f}{\partial y}(\underline{0}) v_2\right) + g(t\underline{v})$. Since $t^2 \mid g(t\underline{v})$ we see that $P = \underline{0}$ is a multiple root of $f|_{L'}$ iff $\frac{\partial f}{\partial x}(\underline{0}) v_1 + \frac{\partial f}{\partial y} v_2 = 0$ iff $\underline{v}$ lies on the tangent line L iff $L = L'$.

(ii) Let $q(t)=(a(t),b(t))\in C$ be a differentiable parameterisation of C at $p=\underline{0}$ with $q(0)=\underline{0}$ and $\frac{dq}{dt}(0)=\left(\frac{da}{dt}(0),\frac{db}{dt}(0)\right)\neq(0,0)$. Since $f(a(t),b(t))\equiv 0$, we obtain $0=\frac{d}{dt}f(a(t),b(t))\Big|_{t=0}=\frac{\partial f}{\partial x}(\underline{0})\frac{da}{dt}(0)+\frac{\partial f}{\partial y}\frac{db}{dt}(0)$.

So $\frac{dq}{dt}(0)=\left(\frac{da}{dt}(0),\frac{db}{dt}(0)\right)$ is a nonzero vector on the tangent line L of C at $p=\underline{0}$. The equation for the line passing through p and $q(t)$ is $b(t)x-a(t)y=0$, or, if we want a nonzero limit equation: $\frac{b(t)}{t}x-\frac{a(t)}{t}y=0$. If we take the limit $t\to 0$, we get $\frac{db}{dt}(0)x-\frac{da}{dt}(0)y$. Clearly $\frac{dq}{dt}(0)=\left(\frac{da}{dt}(0),\frac{db}{dt}(0)\right)$ lies on this line, so this line is the tangent line L of C at $p=\underline{0}$

4(i) The projectivization is given by $F=Y^2Z-X(X-Z)(X+Z)=Y^2Z-X^3+XZ^2=0$. The point p_∞ at infinity, which is obtained by putting $Z=0$, has homogeneous coordinates $(0,1,0)$.

(ii) We have $dF=(-3X^2+Z^2)dX+2YZdY+(Y^2+2XZ)dZ$.
So a point is a singular point of $\tilde{C}$ iff it satisfies the equations

$$\begin{cases} Y^2Z-X^3+XZ^2=0\\ -3X^2+Z^2=0\\ 2YZ=0\\ Y^2+2XZ=0\end{cases}$$

By considering the cases $Y=0$ & $Z=0$ (from $2YZ=0$) we easily see that there is no nonzero solution. So $\tilde{C}$ is smooth.

(iii) The tangent line of $\tilde{C}$ at p_∞ has equation $Z=0$ (i.e. it is the line at infinity of $\mathbb{P}^2$). Since $F|_{\{Z=0\}}=-X^3$, p_∞ is an inflection point. Now we choose p_∞ to be the unit element, then the group law on $\tilde{C}$ is determined by $P_1+P_2+P_3=0 \Leftrightarrow P_1,P_2,P_3$ are collinear with the usual convention when some of the P_i coincide.
So we have $p+p=0 \Leftrightarrow 0=p_\infty$ lies on the tangent line of $\tilde{C}$ at p. $\forall p\in C$
These points are determined by the equations

$$\begin{cases} Y^2Z-X^3+XZ^2=0\\ 2YZ=0\end{cases} \Leftrightarrow \begin{cases} X(X-Z)(X+Z)=0\\ Y=0 \text{ or } Z=0\end{cases}$$

The solutions are $(0,0,1),(1,0,1),(1,0,-1)$ and $p_\infty=(0,1,0)$.
The first three of these are the points of order 2.