To answer question j) of exercice 1, one needs to prove that the space of polynomials $F \in \mathbb{C}[x,y]$ of degree at most $N-3$ injects in $\mathcal{M}(\widehat{X})$ by restriction to X. This results from the *irreducibility* of the polynomial P defining $X = P^{-1}(0)$, which itself results from the hypotheses made on P, and will be shown directly for $P = x^N + y^N - 1$.

Namely $F = 0$ on X implies by Hilbert's "Nullstellenstaz" that some power of F is divisible by P, hence that P divides F (recall that $\mathbb{C}[x,y]$ is a unique factorization domain).

To show that $P = x^N + y^N - 1$ is irreducible, consider it as a polynomial in y with coefficients in $\mathbb{C}[x]$. Then $P = y^N + (x^N - 1)$, so that $x-1$ divides all non-leading coefficients, and divides only once the "constant coefficient" $x^N - 1$. By Eisenstein's criterion, P is irreducible. Explicitly, if P isn't irreducible one can write

$$P = QR$$

with

$$Q = y^q + b_1(x)y^{q-1} + \cdots + b_q(x),$$
$$R = y^r + c_1(x)y^{r-1} + \cdots + c_r(x)$$

for polynomials $b_i, c_i \in \mathbb{C}[x]$ and $q + r = N$, $q, r \geq 1$. Restricting to $x = 1$ we obtain

$$P(1,y) = y^N = Q(1,y)R(1,y),$$

so that necessarily

$$Q(1,y) = y^q, \quad R(1,y) = y^r.$$

But then $b_q(1) = c_r(1) = 0$, so that the "constant coefficient"

$$b_q(x)c_r(x) = x^N - 1$$

is divisible by $(x-1)^2$, a contradiction.

In the general case one can show that P is irreducible as follows. Assume a non-trivial factorization $P = QR$ normalized as above. Then the homogeneneous components of maximal degrees Q_q and R_r verify $Q_q R_r = P_N$ and so are necessarily of the form

$$Q_q(x,y) = \prod_{1 \leq i \leq q} (y - \beta_i x), \quad R_r(x,y) = \prod_{1 \leq j \leq r} (y - \gamma_j x)$$

for a partition $\{\beta_1, \ldots, \beta_q\}, \{\gamma_1, \ldots, \gamma_r\}$ of $\{\alpha_1, \ldots, \alpha_N\}$.

Consider then the *resultant* of Q and R as polynomials in y, that we can define as the function $\rho(x)$ whose value for each x in $\mathbb{C}$ is the product

$$\rho(x) = \prod_{i=1}^{q} \prod_{j=1}^{r} (\beta_{i,x} - \gamma_{j,x})$$

where $Q(x,y) = \prod_{i=1}^q (y - \beta_{i,x})$ and $R(x,y) = \prod_{j=1}^r (y - \gamma_{j,x})$ (for arbitrary x there is no preferred indexation of the roots of $Q(x,\cdot)$ or $R(x,\cdot)$ this is just a notation).

It is equal to $\rho(x) = \prod_{i=1}^q R(x, \beta_{i,x}) = (-1)^{qr} \prod_{j=1}^r Q(x, \gamma_{j,x})$, and is a polynomial function of x by the elementary theory of symmetric functions. It vanishes at x iff $Q(x,\cdot)$, $R(x,\cdot)$ have a common root.

Obviously, we have for any x

$$P(x,y) = \prod_i (y - \beta_{i,x}) \prod_j (y - \gamma_{j,x}).$$

For large $|x| \geq R >> 1$, let $v = y/x$ and write

$$P(x,y)/x^N = p_N(v) + p_{N-1}(v)/x + \cdots + p_1(v)/x^{N-1} + p_0/x^N$$

so that $P(x,y)=0$ implies

$$|p_N(v)| = \prod_i |v-\lambda_i| \leq C(1+|v|^{N-1})/R,$$

and this forces $|p_N(v)| \leq C'/R$, for some C', since otherwise we find $(v_n)_n$ tending to ∞ with $|p_N(v_n)| = O(|v_n|^{N-1})$ which is absurd.

It is then clear that for $|x| \to \infty$, the sets $\{\beta_{i,x}/x\}_i$ and $\{\gamma_{j,x}/x\}_j$ tend respectively to $\{\beta_i\}_i$ and $\{\gamma_j\}_j$ so that $\rho(x) = \prod_{i,j}(\alpha_i - \beta_j)x^{qr} + o(|x|^{qr})$ for large $|x|$, hence that the polynomial ρ is of degree qr.

In particular ρ has a root x_0, and by definition there is y_0 suct that $Q(x_0,y_0) = R(x_0,y_0) = 0$. Then P and its partial derivatives vanish at (x_0,y_0), contradicting the hypothesis.

This proof can also be adapted to show that X is *connected*, an all important fact which is necessary for the conclusions, already for question h (the genus is defined only for compact connected Riemann surfaces X, and $\mathcal{M}(\widehat{X})$ is not a field if X is disconnected).

Namely let $X = X_0 \cup X_1$ with X_0, X_1 disjoint non-empty open and closed subspaces. Then X_0 and X_1 are Riemann surfaces, and the restrictions f_0, f_1 of the first projection map on X_0 and X_1 are holomorphic and proper.

Then one can repeat the above proof with $(x,\beta_{i,x})_i$ (resp. $(x,\gamma_{j,x})_j$) defined as the points (x,y) of $f_0^{-1}(x)$ (resp. $f_1^{-1}(x)$), repeated with multiplicities equal to their ramification indices $e_{f_0}(x,y)$ (resp. $e_{f_1}(x,y)$). We know that the sum of these multiplicities is locally constant, hence constant, denoted by q (resp. r), with $q+r=N$. One can then define a function $\rho(x)$ by the same formula, and this is now a priori only a holomorphic function of $x \in \mathbb{C}$. Indeed, for x outside of the branch points of f_0, f_1, one can choose locally the $\beta_{i,x}$, $\gamma_{j,x}$ holomorphic in x, at the branch points ρ is holomorphic by the removable singularity theorem.

Moreover the function ρ has no zero since X_0, X_1 are disjoint.

Continuing as above, for $|x| \to \infty$, the sets $\{\beta_{i,x}/x\}_i$ and $\{\gamma_{j,x}/x\}_j$ tend to a partition of $\{\alpha_1,\dots,\alpha_N\}$, and one concludes in the same way that $\rho(x) \equiv cx^{qr}$, $c \in \mathbb{C}^*$. But this implies that ρ is a polynomial function of degree qr, and this is a contradiction, since it has no zero.

The connectedness of the Fermat curve X defined by $x^N + y^N = 1$ is easier to see directly, for example connecting any point (x,y) in a dense subset of X to a point $(\lambda,0) \in \mu_N \times \{0\}$ with a curve $t \mapsto (x_t, ty)$, $t \in [0,1]$ in X (e.g. by solving a differential equation in t), and then $(\lambda,0)$ to $(0,1)$ by the curve $t \mapsto ((1-t^N)^{1/N}\lambda, t)$, $t \in [0,1]$.