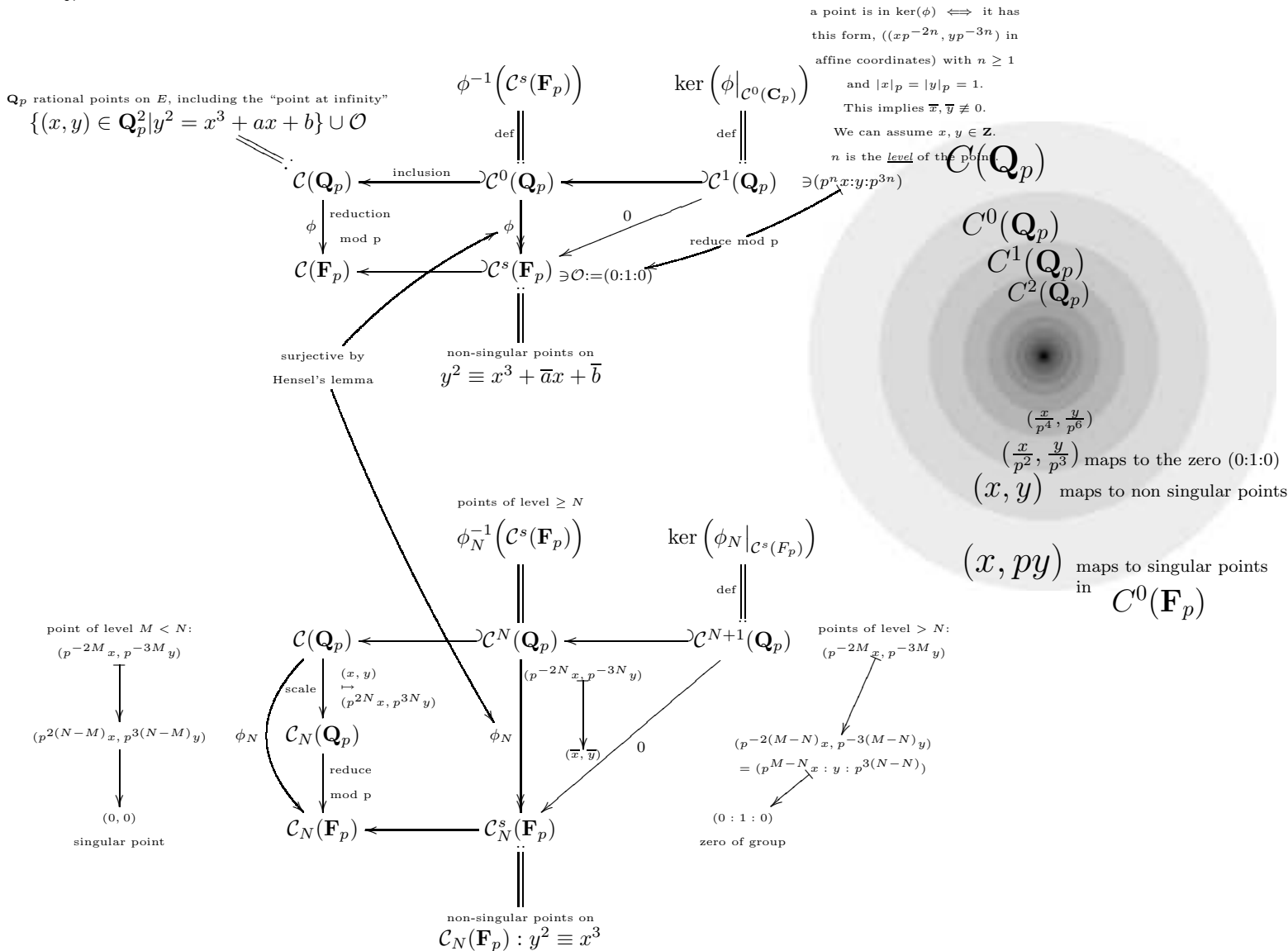


Let C be an elliptic curve given by $y^2 = x^3 + ax + b$, with $a, b \in \mathbf{Z}$. The point of this section is to show that if a point on $C(\mathbf{Q})$, has finite order, then we must have $x, y \in \mathbf{Z}$.

$$C : y^2 = x^3 + ax + b$$

$$C_N : y^2 = x^3 + p^{4N}ax + p^{6N}b$$

$C_N^s(k)$ means non singular (i.e., smooth) points on $C_N(k)$.



Putting this together we have the following filtration:

$$\mathcal{C}(\mathbf{Q}_p) \xleftarrow{\text{inclusion}} \mathcal{C}^0(\mathbf{Q}_p) \xleftarrow{\text{inclusion}} \mathcal{C}^1(\mathbf{Q}_p) \xleftarrow{\text{inclusion}} \mathcal{C}^2(\mathbf{Q}_p) \xleftarrow{\text{inclusion}} \dots \xleftarrow{\text{inclusion}} \mathcal{C}^N(\mathbf{Q}_p) \xleftarrow{\text{inclusion}} \mathcal{C}^{N+1}(\mathbf{Q}_p) \xleftarrow{\text{inclusion}} \dots$$

$\xrightarrow{\text{quotient}} \cong \mathcal{C}^s(\mathbf{F}_p) \quad \xrightarrow{\text{quotient}} \cong \mathcal{C}_1^s(\mathbf{F}_p) \quad \xrightarrow{\text{quotient}} \cong \mathcal{C}_N^s(\mathbf{F}_p)$

Since the group law on the nonsingular points of $y^2 = x^3$ over a field k is isomorphic to $k, +$, we have

$$\mathcal{C}^N(\mathbf{Q}_p) / \mathcal{C}^{N+1}(\mathbf{Q}_p) \cong \mathcal{C}_N^s(\mathbf{F}_p) \cong (\mathbf{F}_p, +) \cong \mathbf{Z}/p\mathbf{Z}.$$

So if a point has finite order prime to p , then it cannot be in $\mathcal{C}^1(\mathbf{Q}_p)$, and so must have the form (x, y) with $x, y \in \mathbf{Z}_p$.

The next thing is to show that the fact that the coordinates are p -adic integers is also true if a point has any finite order, not just orders coprime to p .