4. CFF Homework, series 4, to be submitted till 1st June

All steps should be explained in detail (preferably by reference to the class assertions).

4.1. For every prime p and every $a \in \mathbb{F}_p$ determine genus of the AFF $\mathbb{F}_p(V_{w_a})$ where $w_a = y^2 - (x^3 + a) \in \mathbb{F}_p[x, y]$.

Hint: Check smoothness of w_a applying 3.12(3) if $p > 2$ and by the definition if $p = 2$. Then apply 8.3(5) and 8.4.

5 points

4.2. Let $w = y^2 + yx - x^3 + x - 1 \in \mathbb{F}_5[x, y]$. Prove that w is singular at $(1, 2) \in V_w$ and find $s \in \mathbb{F}_5(x, y)$ such that $\mathbb{F}_5(V_w) = \mathbb{F}_5(s + (w))$ (i.e. s represents a transcendental generator of the field $\mathbb{F}_5(V_w)$).

Hint: Singularity prove by the definition, use the fact that $\mathbb{F}_5(V_w) = \mathbb{F}_5(\alpha, \beta)$ for $\alpha = x + (w)$ and $\beta = y + (w)$ and then repeat the proof of the direct implication of 8.4. Do not forget that the proof suppose shifting 3.10 of singularity to $(0, 0)$.

5 points

4.3. Let $f = y^2 - x^3 + 2 \in \mathbb{F}_5[x, y]$. Show that the AFF $\mathbb{F}_5(V_f)$ is eliptic and

(a) find a generator of the corresponding cyclic group $(E(\mathbb{F}_5), \oplus, \ominus, \infty)$ $(\cong \mathbb{Z}_6)$,

(b) compute $\mathbb{F}_5$-dimension of the Riemann-Roch space $R = \mathcal{L}(\sum_{\gamma \in E(\mathbb{F}_5)} 1P_\gamma)$ and find a nonzero element contained in R.

Hint: Apply 8.4 and 3.12 to prove that $\mathbb{F}_5(V_w)$ is EFF.

(a) As in Example 8.10 determine all elements of $V_f(\mathbb{F}_5)$ and apply 8.8 to find a point $\gamma \in V_f(\mathbb{F}_5)$ satisfying $\gamma \oplus \gamma \neq \infty$ and $\gamma \oplus \gamma \neq \ominus\gamma$ which has to be an element of order 6 by Lagrange theorem. Use geometrical ideas of the proof instead explicit formulas of 8.8 (in particular: meaning of the same first coordinates of points i.e. they are opposite; the observation that $\gamma \oplus \gamma$ is the intersection of tangent at γ with the curve; the observation that if $\gamma \oplus \gamma$ is the only intersection of tangent at γ with the curve then $\gamma \oplus \gamma \oplus \gamma = \infty$.

(b) Compute degree of the divisor $A = \sum_{\gamma \in E(\mathbb{F}_5)} 1P_\gamma$ by the definition and then use 7.6(2) to determine $l(A) = \dim_{\mathbb{F}_5}(A)$. Apply positivity of A, the knowledge of elments of $\mathcal{L}(0)$ and 6.2.

10 points