1. Material covered

(Quick sketch)

These notes are not meant as course notes and are not carefully written. They serve mainly as a summary and/or reminder for what we have done in class.

On September 27, we did/saw the following statements (some stated as facts without proof). Examples are left out here. As in Silverman's "The arithmetic of elliptic curves", of which we are following parts of chapters I and II, phrased for curves, we take our field k to be perfect, though it was mentioned that this can be avoided by working with the set of all discrete valuation rings inside the function field $k(C)$ instead of the set $C(\overline{k})$ of all points over $\overline{k}$.

- Definition of projective curve over k (points in $\mathbb{P}^2(\overline{k})$ satisfying $F(x,y,z) = 0$ for some homogeneous polynomial $F \in k[x,y,z]$ that is irreducible over $\overline{k}$).
- Definition of a function in the function field of an affine curve being *regular* at a point.
- Local ring at a point on an affine curve consists of functions that are regular at that point.
- An open subset $U \subset C$ is a subset that is the complement of finitely many points.
- If C is a smooth affine curve, then
$$A[C] = \bigcap_{\mathfrak{m}} A[C]_{\mathfrak{m}},$$
where the intersection runs over all maximal ideals $\mathfrak{m}$ of $A[C]$.
- From a similar definition where we only intersect the local rings for all but finitely many maximal ideals, we concluded that the function field of a projective curve can be defined as the function field of an affine part, which does not depend on the affine part we choose.
- Local ring of a point on a projective curve is the local ring of that point on some affine part of the curve. Again, this does not depend on the affine part that was chosen.
- Definition of morphism from a curve to a projective curve.
- Every map from a smooth curve C to a projective curve D that is a morphism outside a finite number of points of C, can be extended to a morphism $C \to D$, so can be defined on the whole curve C.
- Two smooth projective curves C and D are isomorphic if and only if their function fields are isomorphic as fields.
- We defined divisors and the free abelian group $\mathrm{Div}_{\overline{k}}(C)$ and the subgroup
$$\mathrm{Div}_k(C) = (\mathrm{Div}_{\overline{k}}(C))^G = \{D \in \mathrm{Div}_{\overline{k}}(C) \ : \ \sigma(D) = D \text{ for all } \sigma \in G\}$$
with $G = \mathrm{Gal}(\overline{k}/k)$. [This is where, if you want to do things over a field that is not perfect, you should let $\mathrm{Div}_k(C)$ be the free abelian group on all discrete valuation rings of the function field $k(C)$.]
- Defined principal divisor $(f) = \sum_P v_P(f) \cdot (P)$ for $f \in k(C)^*$.
- Defined the degree of a divisor $\sum_P n_P(P)$ as $\sum_P n_P$. This also gives a degree on divisor classes, because the degree of a principal divisor is 0.
- Set $\mathrm{Pic}_k(C) = \mathrm{Div}_k(C)/\mathrm{Princ}(C)$ where $\mathrm{Princ}(C)$ is the subgroup of all principal divisors (f) with $f \in k(C)$.
- Set $\mathrm{Pic}^0_k(C) = \{[D] \in \mathrm{Pic}_k(C) : \deg[D] = 0\}$.
- Divisor $D = \sum_P n_(P)$ is effective ($D \geq 0$) if and only if $n_P \geq 0$ for all P.
- Definition of vector space $L(D) = \{0\} \cup \{f \in k(C)^* : (f) + D \geq 0\}$.
- Set $l(D) = \dim_k L(D)$.
- If $\deg D < 0$, then $L(D) = 0$ and $l(D) = 0$.
- Riemann-Roch: Let C be a smooth projective curve over k. Then there exists an integer $g \geq 0$ such that for every $D \in \mathrm{Div}_k(C)$ with $\deg D \geq 2g-1$ we have $l(D) = \deg D + 1 - g$. This number is called the genus of C.
- The genus of $\mathbb{P}^1$ is 0.
- The genus of a smooth projective curve of degree d in $\mathbb{P}^2$ equals $\frac{1}{2}(d-1)(d-2)$.
- An elliptic curve over k is a curve over k of genus 1, together with a point $\mathcal{O}$.

For the remainder, let C be an elliptic curve, and $\mathcal{O}$ its special point.

- The is a bijection $C(k) \to \mathrm{Pic}^0_k(C)$ given by $P \mapsto [(P)-(\mathcal{O})]$. This gives a group structure on $C(k)$, namely $P+Q=R$ if and only if $[(P)-(\mathcal{O})]+[(Q)-(\mathcal{O})]=[(R)-(\mathcal{O})]$, so if and only if $(P)+(Q)-(R)-(\mathcal{O})$ is a principal divisor. (proof is repeated and extended in the last exercise below)
- There are constants a_1, a_2, a_3, a_4, a_6 such that C is isomorphic to the (smooth) projective curve given by
$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$
(proof is finished in an exercise)
- [This was actually not said in class, but you have seen it before] If the characteristic of k is not 2 or 3, then we can complete the square (in terms of Y) and obtain a new Weierstrass equation where te coefficients of XYZ and YZ^2 are 0. Completing the cubic (in terms of X), then also gets rid of the coefficient of X^2Z. Therefore, there are then coefficients a and b such that C is isomorphic to to the smooth projective curve that has affine equation
$$y^2 = x^3 + ax + b.$$
- A smooth cubic projective curve C with a point $\mathcal{O}$ is an elliptic curve. The group law is given as follows. Take two points P and Q. Let l be the line through P and Q and let S be the third intersection point of l with C. Let m be the line through S and $\mathcal{O}$. Let R be the third intersection point of m with C. Then $R = P + Q$. (proof is repeated/finished in the last exercise below)

2. Homework

You may use all facts that were mentioned during the lecture, in particular everything that is written above (unless you're asked to finish a proof, of course). For the homework, choose **four** exercises from

- Cassels, §7: 1,2 (at most one of these)
- Cassels, §8: 3,4,5,6,7
- Silverman–Tate: 1.18, 1.19, 1.20
- Silverman: 2.4, 2.5 (at least one of these).
- The exercises below (at least one of these).

(1) Let C be a smooth, projective curve of genus 1 over a field k, and let $\mathcal{O}$ be a point in $C(k)$. In class we have seen that there are functions $x, y \in k(C)$ with $x \in L(2(\mathcal{O})) \setminus L((\mathcal{O}))$ and $y \in L(3(\mathcal{O})) \setminus L(2(\mathcal{O}))$.
   (a) Show (as in class) that, after replacing x and y by a multiple if necessary, there are constants a_1, a_2, a_3, a_4, a_6 such that the functions x and y satisfy
   $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$
   (b) Let D be the projective curve given by
   $$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$
   Show that there is a morphism $\varphi\colon C \to D$ that sends $P \in C \setminus \{\mathcal{O}\}$ to $(x(P) : y(P) : 1)$ and $\mathcal{O}$ to $(0 : 1 : 0)$.
   (c) Use Riemann-Roch to show that φ is injective and deduce that φ is an isomorphism. [This is the part we left as an exercise.]

(2) (a) Let C be the projective curve over $\mathbb{Q}$ given by $U^3 + V^3 = dW^3$ and let $\mathcal{O}$ be the point $[1 : -1 : 0]$. Show that
   $$x = \frac{W}{U+V} \qquad \text{and} \qquad y = \frac{U-V}{U+V}$$
   are elements of the function field and that they satisfy $x \in L(2(\mathcal{O}))$ and $y \in L(3(\mathcal{O}))$. What is the linear relation between $1, x, y, x^2, x^3, xy, y^2$?
   (b) In each of the examples (i), (ii), and (iii) of Cassels' §8, express the functions x_W, y_W that give the Weierstrass coordinates in terms of the original variables. Show that indeed we have $x_W \in L(2(\mathcal{O}))$ and $y_W \in L(3(\mathcal{O}))$.

(3) (a) First do exercise 2.6 from Silverman.
   (b) Now show that if C is a smooth projective curve of degree 3 and $\mathcal{O}$ a distinguished point, then the group law is indeed given as claimed in class: the sum of two points P and Q is obtained by taking the third intersection point S of the curve C and the line through P and Q, and then taking the third intersection point $(P + Q)$ of the curve C and the line through S and $\mathcal{O}$.
   (c) Show that if C is a smooth projective curve of degree 3 and $\mathcal{O}$ a distinguished point, then there is a point T such that for any three collinear points P, Q, R on C we have $P + Q + R = T$.

(4) Let k be an algebraically closed field of characteristic not 2 and C the affine curve given by $x^2 + y^2 = 1$. Let P and Q be the points $(-1, 0)$ and $(1, 0)$, respectively, and set $U = C(k) \setminus \{P, Q\}$. Show that we have
   $$k[x, y, y^{-1}]/(x^2 + y^2 - 1) = \bigcap_{P \in U} \mathcal{O}_P.$$