2.3 Exercise Sheet 3

2.3.1 Standard Exercises

Exercise 2.3.1.

(a) Show that if R is any integral domain, then any prime element of R is irreducible.
(b) Show that if R is a UFD, then any irreducible element of R is prime as well, so that the terms "prime" and "irreducible" mean the same thing in UFDs.
(c) Show that the ring $R := \mathbb{C}[x, y, z]/(z^2 - xy)$ is an integral domain and that the class of z in R is an irreducible element that is not prime. Conclude that R is not a UFD.

Exercise 2.3.2 (Eisenstein's Irreducibility Criterion)**.**

(a) Let R be a domain and let $f \in R[t]$. Let f have degree $n \geq 1$ and write $f = a_0t^n + a_1t^{n-1} + \cdots + a_n$ for $a_0, \dots, a_n \in R$ with $a_0 \neq 0$. Show that if there is a prime ideal $P \subset R$ such that
  (i) $a_0 \notin P$,
  (ii) for each j with $1 \leq j \leq n$ we have $a_j \in P$, and
  (iii) $a_n \notin P^2$,
  then f is irreducible.
(b) Show that for each integer $r \geq 1$ and integer prime $p > 0$, the prime-power cyclotomic polynomial
$$\Phi_{p^r}(t) := \frac{t^{p^r} - 1}{t^{p^{r-1}} - 1} = \sum_{j=0}^{p-1} t^{p^{r-1}j} \in \mathbb{Z}[t]$$
is irreducible. (Hint: an $f(t) \in R[t]$ is irreducible iff for some $a \in R$, the shift $f(t + a)$ is.)
(c) Show that the polynomial $f(x, y) = x^2 + y^2 - 1 \in \mathbb{Q}[x, y]$ is irreducible.
(d) Show that if k is any field, then the polynomial $f(x, y) = y^2 - x^3 + x \in k[x, y]$ is irreducible.
(e) Given a field k, an integer $n \geq 1$, and a polynomial $p(x) \in k[x]$ of x alone, can you come up with a criterion for the irreducibility of the polynomial $f(x, y) := y^n - p(x) \in k[x, y]$?

Exercise 2.3.3. Show that if k is an algebraically closed field and $\mathfrak{p} \subset k[x, y]$ is a prime ideal, then one and exactly one of the following holds:

(a) $\mathfrak{p} = (0)$;
(b) there is an irreducible $f \in k[x, y]$ such that $\mathfrak{p} = (f)$;
(c) there are $p, q \in k$ such that $\mathfrak{p} = (x - p, y - q)$.

Compare with your knowledge of the prime ideals of $\mathbb{Z}[x]$ from Alex's course on Field Theory and Galois Theory. Can you prove an analogous result for prime ideals of $R[t]$ for any PID R?

Exercise 2.3.4. Let k be an algebraically closed field, and $C \subset \mathbb{A}^2_k$ be a curve of degree $n \geq 2$.

(a) Show that if $P \in C$ is such that $m_P(C) = n$, then C is a union of n lines through P.
(b) Conclude that if C is irreducible, then for any point $P \in C$, the multiplicity of C at P satisfies
$$1 \leq m_P(C) \leq n - 1.$$
In particular, any irreducible conic $C \subset \mathbb{A}^2_k$ is smooth.
(c) Show that if C is irreducible and if some $P \in C$ has multiplicity $m_P(C) = n - 1$, then C admits a rational parametrization.

Finally,

(d) For each $n \geq 2$ and integer j with $1 \leq j \leq n - 1$, find an irreducible curve $C \subset \mathbb{A}^2_k$ and a point $P \in C$ such that $m_P(C) = j$.

Exercise 2.3.5. (Taken from [4, Problems 3.22-23].) Let k be an algebraically closed field, $C = C_f \subset \mathbb{A}^2_k$ be a curve, and $P \in C$.

(a) Suppose that $m_P(C) \geq 2$ and that C has a unique tangent line C_ℓ at P. Show that $i_P(f, \ell) \geq m_p(C)+1$. The curve C is said to have an ordinary hypercusp of order $n := m_p(C)$ at P if equality holds; a hypercusp of order $n = 2$ is called simply a cusp.
(b) Suppose we pick coordinates so that $P = (0, 0)$ and $\ell = y$. Show that if $\operatorname{ch} k \neq 2, 3$, then P is a cusp iff $\partial^3 f/\partial x^3|_P \neq 0$. Use this to give examples.
(c) Show that if P is a cusp of C, then there is only one component of C through P.
(d) Generalize (b) and (c) to the case of hypercusps.

2.3.2 Numerical and Exploration

Exercise 2.3.6. (Adapted from [4, Problem 3.2].) Suppose $k = \mathbb{C}$. Find the multiple points, and the tangent lines at the multiple points, for each of the following curves:

(a) $y^3 - y^2 + x^3 - x^2 + 3xy^2 + 3x^2y + 2xy$,
(b) $x^3 + y^3 - 3x^2 - 3y^2 + 3xy + 1$,
(c) $(x^2 + y^2 - 3x)^2 - 4x^2(2 - x)$, and
(d) $(x^2 + y^2 - 1)^m + x^n y^n$ for $m, n \geq 1$.

Be sure to draw (or get a computer to draw) tons of pictures! Which of you answers change in positive characteristic, and what are the answers there?

Exercise 2.3.7. Let $k = \mathbb{C}$ and $P = (0, 0)$. Consider the affine plane curves C_i containing P defined by the polynomials f_i for $1 \leq i \leq 7$ below:

(i) $f_1 = x^2 - y$,
(ii) $f_2 = y^2 - x^3 + x$,
(iii) $f_3 = y^2 - x^3$,
(iv) $f_4 = y^2 - x^3 - x^2$,
(v) $f_5 = (x^2 + y^2)^3 + 3x^2y - y^3$,
(vi) $f_6 = (x^2 + y^2)^3 - 4x^2y^2$, and
(vii) $f_7 = (x^2 + y^2 - 3x)^2 - 4x^2(2 - x)$.

For each pair of integers i, j with $1 \leq i < j \leq 7$, compute the local intersection multiplicity $i_P(f_i, f_j)$ of C_i and C_j at P. What patterns do you observe? Make some conjectures.

Exercise 2.3.8. Over a field $k = \overline{k}$, how many singular points can a curve $C \subset \mathbb{A}^2_k$ of degree $n \geq 1$ have? Come up with an upper bound and a conjecture for when it is achieved.

2.3.3 PODASIPs

Prove or disprove and salvage if possible the following statements.

Exercise 2.3.9. A line is an irreducible curve.

Exercise 2.3.10. A cubic curve $C \subset \mathbb{A}^2_k$ over a field k can have at most one singular point.

Exercise 2.3.11. Given a field k, an integer $n \geq 1$, and a polynomial $p(x) \in k[x]$, the curve $C_f \subset \mathbb{A}^2_k$ defined by the vanishing of the polynomial

$$f(x, y) := y^n - p(x) \in k[x, y]$$

is smooth iff the polynomial $p(x)$ is separable, i.e. $\operatorname{disc}(p) \neq 0$.[9]

[9] See Exercise 2.2.10. When $\operatorname{ch} k \neq 2$, smooth curves of the form C_f with $n = 2$ are called hyperelliptic curves.