HOMEWORK 8 FOR 18.725, FALL 2015
DUE THURSDAY, NOVEMBER 12 BY 1PM.

(1) (a) Prove that if $X = \text{Spec}(A)$ is affine and locally factorial, then $\text{Pic}(X)$ is trivial iff $A$ is a UFD.

(b) Let $X \subset \mathbb{P}^n$ be a projective variety. Suppose that the homogeneous coordinate ring of $X$ is a UFD. Show that $\text{Pic}(X) \cong \mathbb{Z}$.

(2) (a) Let $X \subset \mathbb{P}^2$ be the plane curve given by $zy^2 = x^3 - x^2z$. Prove that $\text{Pic}^0(X) \cong k^*$. 

[Hint: Recall the map $\mathbb{P}^1 \to X$ sending two points (say, 0, $\infty$) to $x_0 = (0:0:1)$ and inducing an isomorphism $\mathbb{P}^1 \setminus \{0, \infty\} \to X \setminus x_0$. Pull-back of a degree zero line bundle to $\mathbb{P}^1$ is trivial, while its fibers at 0 and $\infty$ are identified. The ratio of that identification with the one coming from the trivialization of the line bundle is an element in $k^*$.]

(b) Let $X \subset \mathbb{P}^2$ be the plane curve given by $zy^2 = x^3$. Prove that $\text{Pic}^0(X) \cong (k,+)$.

[Hint: Recall the bijective map $\mathbb{P}^1 \to X$ sending, say, 0 to $x_0 = (0:0:1)$ and inducing an isomorphism $\mathbb{P}^1 \setminus 0 \to X \setminus x_0$. Pull-back of a degree zero line bundle to $\mathbb{P}^1$ is a sheaf $L$, s.t. on the one hand $L \cong \mathcal{O}$, while on the other hand we have an isomorphism $L \otimes (\mathcal{O}_{\mathbb{P}^1}/(\mathcal{O}_{\mathbb{P}^1}(-2(0)))) \cong \mathcal{O}_{\mathbb{P}^1}/(\mathcal{O}_{\mathbb{P}^1}(-2(0)))$. Compare the last isomorphism with one coming from the trivialization of $L$ to get an element in $k^*$.]

(c) In both cases (a,b) describe the kernel of the map $\text{Div}_C(X) \to \text{Div}_W(X)$.

(3) Let $X = (k^n \setminus \{0\})/\{\pm 1\} (n > 1)$. Compute $\text{Pic}(X)$.

[Hint: the answer is $\mathbb{Z}/2\mathbb{Z}$. Divisors in $X$ are in bijection with divisors in $\mathbb{A}^n$ invariant under the map $x \mapsto -x$. Such a divisor $D$ is the divisor of a function $f$ which is either even or odd; the corresponding divisor on $X$ is principal iff $f$ is even.]

(4) Show that the number of singular points of an irreducible plane curve of degree $n$ can not exceed $\frac{(n-1)(n-2)}{2} + 1$. 

[Hint: Use linear algebra to find a degree $n$ curve passing through $\frac{(n-1)(n-2)}{2} + 1$ singular points and as many nonsingular points as possible, then apply Bezout Theorem. Make sure to use that $X$ is irreducible; otherwise the statement fails already for $n = 2$.]

(5) (Optional problem)

(a) Let $A$ be an associative algebra. For $a \in A$ define $ad(a) \in \text{End}(A)$ by $ad(a) : x \mapsto ax - xa$. Show that if $A$ is an algebra over $\mathbb{F}_p$ then $ad(a)^p = ad(a^p)$.

(b) Let $\partial$ be a derivation of an associative $\mathbb{F}_p$-algebra $C$. Show that $\partial^p$ is also a derivation of $C$.

[Hint: Apply part (a) to $A = \text{End}_{\mathbb{F}_p}(C)$, $a = \partial$ and $x$ the operator of left multiplication by an element in $C$.]
Thus for an affine algebraic variety $X = \text{Spec}(C)$ over a field of characteristic $p > 0$ and a vector field $\xi \in \text{Vect}(X)$ we get another vector field $\xi^{[p]}$ on $X$, $\xi^{[p]} \cdot f = \xi \cdot \cdots \cdot \xi \cdot f$, where $\xi$ appears $p$ times in the right hand side; $\xi^{[p]}$ is called the restricted power of $\xi$. The definition clearly extends to nonaffine varieties.

(c) Recall that an irreducible normal curve $X$ is an elliptic curve if the sheaf of Kahler differentials on $X$ is trivial\(^1\) (isomorphic to $O$). Thus an elliptic curve carries a unique (up to scaling) nonzero vector field $\xi$. The elliptic curve is called \textit{supersingular} if $\xi^{[p]} = 0$; otherwise it is called \textit{ordinary}.

Let $f$ be a cubic polynomial with no multiple root. Check that the projective closure of the curve $y^2 = f(x)$ is a supersingular elliptic curve iff $x^{p-1}$ enters $f(x)^{(p-1)/2}$ with zero coefficient ($p \neq 2$).

---

\(^1\)Oftentimes by an elliptic curve one understands a curve with this property together with a fixed point $x_0 \in X$.

\(^2\)There are several other equivalent forms of the definition. For example, an elliptic curve $X$ over $F_q$ is supersingular iff $|X(F_{q^n})|$ is prime to $p$ for all $n$. 