# INTRO TO ALGEBRAIC GEOMETRY, PROBLEM SET 8

Due Thursday November 11 at my office (2-271) by noon. You're strongly encouraged to collaborate (although write up solutions separately), and you're also strongly encouraged to ask me questions (if you're stuck, or if the question is vaguely worded, or if you want to try out an argument).

1. Prove that the valuations of $\overline{k}(t)$ described in class (corresponding to the points of $\mathbb{P}^1$) are all the non-trivial valuations of $\overline{k}(t)$ over $\overline{k}$.
2. (a) Let $\mathfrak{m}$ and $\mathfrak{n}$ be two ideals of $R$ such that there is an integer $i$ such that $\mathfrak{m}^i \subset \mathfrak{n}$ and $\mathfrak{n}^i \subset \mathfrak{m}$. Show that the completion of $R$ with respect to $\mathfrak{m}$ is isomorphic to the completion of $R$ with respect to $\mathfrak{n}$.

   Explanation of the word *completion*: Given a ring $R$ and an ideal $\mathfrak{m}$, put a topology ("the $\mathfrak{m}$-adic topology") on the ring $R$ by declaring subsets of the form $a + \mathfrak{m}^n$ ($a \in R$, $n \in \mathbb{Z}^+$) to be open. (In other words, translates of powers of $\mathfrak{m}$ form a base of the topology.) Then elements of $\hat{R}$ correspond to Cauchy sequences modulo equivalence. (This is analogous to defining $\mathbb{R}$ as the completion of $\mathbb{Q}$ with respect to the classical topology.) Seen in this way, completion depends only on the topology, not on the choice of $\mathfrak{m}$. One way of doing this problem — probably not the way you should choose — is to justify the argument above, and then show that $\mathfrak{m}$ and $\mathfrak{n}$ define the same topology on $R$.

   (b) Prove that the completion of a discrete valuation ring $(R, \mathfrak{m})$ is also a discrete valuation ring (called a *complete* discrete valuation ring). (Recall that a topological space is complete if all Cauchy sequences have limits; this motivates the terminology.)

   (c) Let $\mathfrak{m}$ be a maximal ideal in a ring $R$, so $\mathfrak{m}R_{\mathfrak{m}}$ is the maximal ideal of the local ring $R_{\mathfrak{m}}$. If $\hat{R}$ is the completion of $R$ with respect to $\mathfrak{m}$, and $\hat{R_{\mathfrak{m}}}$ is the completion of $R_{\mathfrak{m}}$ with respect to $\mathfrak{m}R_{\mathfrak{m}}$, prove that $\hat{R} \cong \hat{R_{\mathfrak{m}}}$.

   In the vague and imprecise language of "smaller and smaller neighborhoods", the construction of $R_{\mathfrak{m}}$ from $\mathfrak{m}$ is analogous to looking at a "small" neighborhood of the point corresponding to $\mathfrak{m}$, and taking completion corresponds to looking at a "smaller" ("formal") neighborhood of the point. Intuitively, this exercise tells you that you can look immediately at the smaller neighborhood, or you can get there in two jumps (via the small neighborhood), and you'll see the same thing.
3. *Hensel's Lemma.* Suppose $(R, \mathfrak{m})$ is a complete local ring. Let $f(X) \in R[X]$. (For example, $R$ could be $\mathbb{Z}_p$, and the coefficients of $f$ could be integers.) Let $x \in R$, $n \in \mathbb{Z}^{>0}$ such that $f(x) \equiv 0 \pmod{\mathfrak{m}^n}$ and $v(f'(x)) = 0$ (i.e. $f'(x)$ is invertible in $R$). Prove that there exists $y$ in $R$ *(should that be $\hat{R}$?)* such that $f(y) = 0$ and $y \equiv x \pmod{\mathfrak{m}^n}$. Hence for example you can solve $x^2 = -1$ in the 5-adics, or $y^n = 1 + t$ in $\overline{k}[[t]]$ in characteristic not dividing $n$. (This is an

*Date*: November 4, 1999.

analogue of Newton's method in calculus — do you see how? This result can be made much stronger.)

4. *Hensel's Lemma (another version).* Suppose $(R, \mathfrak{m})$ is a complete discrete valuation ring. If $e \in R$, denote its image in the field $R/\mathfrak{m}$ by $\overline{e}$. If $f \in R[T]$ is a monic polynomial (with coefficients in $R$) such that $\overline{f}$ factors as $\overline{f} = g_0 h_0$ with $g_0$ and $h_0$ monic and coprime (coprime means the ideal $(g, h)$ is $R/\mathfrak{m}[T]$), then $f$ itself factors as $f = gh$ with $g$ and $h$ monic and such that $\overline{g} = g_0$ and $\overline{h} = h_0$. In general, any local ring $(R, \mathfrak{m})$ for which the conclusion of (this version of) Hensel's lemma holds is said to be *Henselian*.
5. *Classification of plane curve singularities of multiplicity 2.* Suppose $f(x, y) \in \overline{k}[[x, y]]$, where $\operatorname{char} \overline{k} \neq 2$, and the multiplicity of $f$ is 2 (i.e. $f$ has a non-zero degree 2 term, but no degree 0 or degree 1 term). Suppose $f(x, y)$ cuts out a reduced curve, i.e. $\overline{k}[[x, y]]/(f)$ has no nilpotent elements. Prove that there is a change of variables (invertible!) such that $f(u, v)$ is some (invertible) constant times $v^2 - u^{n+1}$ $(n \geq 1)$. Such a singularity is called an $A_n$ curve singularity. When $n = 1$, this is called a *node*; when $n = 2$, it is a *cusp*; when $n = 3$, it is a *tacnode*. *(This was harder than I intended.)*
6. **Harthshorne Ex. I.6.2** *An elliptic curve.* Let $Y$ be the curve $y^2 = x^3 - x$ in $\mathbb{A}^2$, and assume that the characteristic of $\overline{k}$ is not 2. In this exercise, you will explicitly see that $Y$ is not rational (i.e. birational to $\mathbb{P}^1$), or equivalently that $k(Y)$ is not a pure transcendental extension of $\overline{k}$. You will use the fact that if $Q$ is a nonsingular rational (separated) curve not isomorphic to $\mathbb{P}^1$, then $Q$ is isomorphic to an open subset of $\mathbb{A}^1$; we will prove this in the next week or two.
   (a) Show that $Y$ is nonsingular, and deduce that $A = A(Y) \cong \overline{k}[x, y]/(y^2 - x^3 + x)$ is an integrally closed domain.
   (b) Let $\overline{k}[x]$ be the subring of $k(Y)$ generated by the image of $x$ in $A$. Show that $\overline{k}[x]$ is a polynomial ring, and that $A$ is the integral closure of $\overline{k}[x]$ in $k(Y)$.
   (c) Show that there is an automorphism (which can be thought of as a Galois group) $\sigma : A \to A$ which sends $y$ to $-y$ and leaves $x$ fixed. For any $a \in A$, define the *norm* of $a$ to be $N(a) = a\sigma(a)$. Show that $N(a) \in \overline{k}[x]$, $N(1) = 1$, and $N(ab) = N(a)N(b)$ for any $a, b \in A$.
   (d) Using the norm, show that the units in $A$ are precisely the nonzero elements of $\overline{k}$. Show that $x$ and $y$ are irreducible elements of $A$. Show that $A$ is *not* a unique factorization domain.
   (e) Prove that $Y$ is not a rational curve.