Math 704 Problem Set #2 Due Mon., Feb. 9, 2004

1. Consider the extension $\mathbb{Z} \subset \mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{5}}{2}$.

(a) Use the Jacobian criterion to find which primes are ramified in this extension. (Hint: Find the minimal polynomial of α.)

(b) Verify that the prime (3) of $\mathbb{Z}$ remains prime, and the prime (11) splits into two primes $(4+\sqrt{5})$, $(4-\sqrt{5})$. In each case find the ramification index e, the degree f of the residue field extension, and the degree $d = ef$ of the local field extension.

(c) Similarly, describe the behavior of the primes (2), (5), (7), (19), and ∞ in this extension. (For ∞, just find d, since e and f are undefined. But see problem 4 below.)

(d) If parts (a)-(c) are redone for the extension $\mathbb{Z} \subset \mathbb{Z}[\sqrt{5}]$, what remains the same and what changes? Which extension is "nicer", and why?

2. (a) Describe the behavior of the prime at ∞ in the extension $\mathbb{Z} \subset \mathbb{Z}[\sqrt[3]{2}]$.

(b) Is this extension Galois? Could you have predicted this simply from your answer to (a)?

3. Consider the extension $R \subset S$, where $R = \mathbb{F}_3[x]$ and $S = R[\sqrt{F(x)}] = R[Y]/(Y^2 - F(x))$ for some $F(x) \in R$.

(a) If $F(x) = x^2 - 1$, does K_∞ (the completion of $K = \text{frac}(R)$ at the infinite prime) contain a $\sqrt{F}$? (Hint: How does PS 1 #2a(ii) apply?) Use this to determine the behavior of the infinite prime of K in the extension, and to explain the behavior at ∞ of the corresponding cover of the line. (Here, you need to work on another affine patch to make sense of the quantities e and f.)

(b) Do the same with $F(x) = x$.

(c) Do the same with $F(x) = 1 - x^2$.

4. Consider the extension $\mathbb{Z} \subset \mathbb{Z}[\sqrt{n}]$, for some $n \in \mathbb{Z}$.

(a) If $n = 11$, is there a $\sqrt{n}$ in the completion at infinity? What is the degree d of each local field extension at ∞? Given that, what would 'e' and 'f' have to be? Which part of problem 3 above does this correspond to? (Hint: See PS1 #2b.)

(b) Redo part (a) with $n = 3$. How does the difference between PS1 #2a and PS1 #2b come into play?

(c) Redo part (a) with $n = -5$. What is the corresponding part of problem 3 above, now? Given your answer, what "should" we take as the values of 'e' and 'f', for the extension at infinity?

5. Consider the ring extension $R \subset S$, where $R = \mathbb{Z}[x]$ and $S = R[Y]/(Y^2 - x)$.

(a) Find the height 1 primes of R at which this extension is ramified.

(b) For each such prime, determine which of two conditions for being unramified (condition (i) on separability, condition (ii) on uniformizers) fails.

6. (a) Is there a $\sqrt{-7}$ in the ring $\mathbb{Z}_p$ of p-adic integers, if $p = 3$? if $p = 11$? In each case, either explain why there is no $\sqrt{-7}$ in $\mathbb{Z}_p$, or prove that there is one and find its image a explictly in $\mathbb{Z}/p^2 = \mathbb{Z}_p/p^2$ (so that a is thus a $\sqrt{-7} \in \mathbb{Z}/p^2$).

(b) Prove the following strong form of Hensel's Lemma: Let $F(x) \in \mathbb{Z}_p[x]$, $x_0 \in \mathbb{Z}$, $m \geq 0$. Suppose $F(x_0) \equiv 0 \pmod{p^{2m+1}}$ but $F'(x_0) \not\equiv 0 \pmod{p^{m+1}}$. Then there is an $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ and $\alpha \equiv x_0 \pmod{p}$. (Hint: Generalize "Newton's method" to allow $m > 0$.)

(c) Deduce that there is a $\sqrt{-7}$ in $\mathbb{Z}_2$, and hence in $\mathbb{Z}/2^n$ for all n.

(d) Is there a $\sqrt{7}$ in $\mathbb{Z}/2$? in $\mathbb{Z}_2$? Explain.

7. (a) Use Hensel's Lemma to show that there is a unique formal power series $F(t) = a_1 t + a_2 t^2 + \cdots$ ($a_i \in \mathbb{R}$) such that $3F(t)^2 + F(t)e^t + \sin t = 0$. Find the first few coefficients a_i.

(b) Show that the power series $F(t)$ has a positive radius of convergence. (Hint: Use an appropriate version of the Implicit Function Theorem.)