1. For each of the following extensions $A \subset B$, find the set of ramified primes. At each of these primes, find the ramification index and the higher ramification groups. Also compute the discriminant and the different in two ways: using derivatives and using lattices.

a) $A = \mathbb{Z}$, $B = A[\sqrt{21}]$. (Also, what if we replace B by its integral closure?)

b) $A = \mathbb{Q}[x]$, $B = A[y]/(y^2 - x^2 + x)$.

c) $A = k[x]$, $B = A[y]/(y^2 - xy - cx)$, where $\mathrm{char}(k) = 2$ and $c \in k^\times$.

d) $A = k[x]$, $B = A[y]/(y^2 - x^2y - cx)$, where $\mathrm{char}(k) = 2$ and $c \in k^\times$.

2. Let k be a field and let $A = k[x]$.

a) Show that if k is not separably closed, then there exists a non-trivial unramified extension of A.

b) Show that if k is algebraically closed of characteristic zero, then every non-trivial cyclic extension of A must be ramified at some prime of A. [Hint: Kummer theory.]

c) Using topology, show that if $k = \mathbb{C}$ then every non-trivial extension of A must be ramified at some prime of A. [Hint: Consider covering spaces.]

d) Show that if k is algebraically closed of characteristic $p > 0$, then there exist infinitely many unramified extensions of A having degree p. Describe the behavior of each of the primes of A in such extensions.

3. (a) Let q be an odd prime power, and let $K_\infty = \mathbb{F}_q((t^{-1}))$, the infinite completion of $R = \mathbb{F}_q[t]$. Let $\mu = \{\text{roots of 1 in } R\}$. Verify the following:

(i) There is an element $s \in R$ whose norm is $N(s) = (\#\mu) + 1$, and having the following property: Every non-zero element of K_∞ can uniquely be written in the form $\alpha = \sum_{i=-\infty}^{n} a_i s^i$ for some integer n, with each $a_i \in \mu \cup \{0\}$ and $a_n \neq 0$. [Hint: There is a very simple choice for s.]

(ii) If α is as in (i), then α is a square in K_∞ iff a_n is a square in μ and n is even. [Hint: If n is even, is $s^{-n}\alpha$ a square?]

(iii) Let $S \subset K_\infty$ consist of the elements whose expressions involve only negative powers of s, together with $0 \in K_\infty$. Then S is a fundamental domain for the translation action of R on K_∞. That is, every element of K_∞ can uniquely be written as the sum of an element of S and an element of R.

(b) Now let $K_\infty = \mathbb{R}$, the infinite completion of $R = \mathbb{Z}$. What is the analog of part (a)? [Hint: There are some differences, especially in (ii).] In the analog of (a)(iii), draw S.

(c) Redo (b) for $R = \mathbb{Z}[i]$ and for $R = \mathbb{Z}[\zeta_3]$, where ζ_3 is a primitive cube root of unity. [Note: The pictures of S should be a surprise.]

4. 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 $K = \mathrm{frac}(R)$ at the infinite prime) contain a $\sqrt{F}$? (Hint: How does problem 3(a)(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 $F(x) = 1 - x^2$.

5. 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 4 above does this correspond to? (Hint: See problem 3(b).)

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

(c) Redo part (a) with $n = -5$. What is the corresponding part of problem 4 above, now? Given your answer, what "should" we take as the values of 'e' and 'f', for the extension at infinity?

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.

(e) Use part (b) to show that there is a cube root of 10 in $\mathbb{Z}_3$. [Hint: Make a clever choice of x_0.]