MATH 602 EXERCISE SET 2, FALL 2016

1. Let D be a Dedekind domain and let K be the field of fractions of D. For every non-zero maximal ideal ideal $\wp$ of D, let $D_\wp$ be the localization of D at $\wp$, let $\hat{D}_\wp = \varprojlim_n D/\wp^n$ be the $\wp$-adic completion of D, and let $\hat{K}_\wp$ be the field of fractions of $\hat{D}_\wp$.

(a) Show that $\hat{D}_\wp$ is naturally isomorphic to the completion of the discrete valuation ring $D_\wp$ for every non-zero maximal $\wp$ of D.

(b) Let I, J be two non-zero D-submodules of K. Show that the following statements are equivalent.

(b1) $I \subseteq J$

(b2) $I \cdot D_\wp \subseteq J \cdot D_\wp$ as $D_\wp$-submodules of K, for every maximal ideal $\wp$ of D.

(b3) $I \cdot \hat{D}_\wp \subseteq J \cdot \hat{D}_\wp$ as $\hat{D}_\wp$-submodules of $\hat{K}_\wp$, for every maximal ideal $\wp$ of D. Here $I \cdot \hat{D}_\wp$ is the $\hat{D}_\wp$-submodule of $\hat{K}_\wp$ generated by I; similarly for $J \cdot \hat{D}_\wp$.

2. (a) Is there a field automorphism of $\mathbb{R}$ whose restriction to $\mathbb{R} \cap \overline{\mathbb{Q}}$ is a non-trivial field automorphism of $\mathbb{R} \cap \overline{\mathbb{Q}}$? Either give a proof or a counter-example.

(b) Is there a field automorphism of $\mathbb{Q}_p$ whose restriction to $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$ is a non-trivial field automorphism of $\mathbb{Q}_p \cap \overline{\mathbb{Q}}$? Either give a proof or a counter-example. (Please examine the logic of your proof carefully. I have experience many a purported (but circular) proof for this problem.)

3. (a) Determine the ring of integers of the number field $\mathbb{Q}(\sqrt[3]{2})$.
(b) Determine the ring of integers of the number field $\mathbb{Q}[T]/(T^3 + T + 1)$.
(c) Determine the ring of integers of the number field $\mathbb{Q}(e^{\pi\sqrt{-1}/4})$.
(d) Compute the discriminants of the above number fields.
[Note: You might want also to do the same thing for all quadratic fields. This is treated in many textbooks in number theory, and also in many textbooks in algebra.]

4. Explicitely describe/determine the group ${\mathbb{Q}_p}^\times/({\mathbb{Q}_p}^\times)^2$, where p is a prime number.
[Your answer will depend on the parity of p.]

5. (This problem is a summary of a few basic properties of the conductor of an order of the ring of integers $\mathscr{O}_L$ of a number field L with respect to a subfield K.)

Let A be a Dedekind domain and let K be the fraction field of A. Let L be a finite separable extension of K and let B be the integral closure of A in L. Let $\mathscr{O}$ be an *order* in B, i.e. $\mathscr{O}$ is a subring of B which contains A and $\mathscr{O}$ contains a K-basis of L. (Consequently $B/\mathscr{O}$ is an A-module of finite length.) Let

$$\mathfrak{c}(\mathscr{O}) = \{x \in L \,|\, x \cdot B \subseteq \mathscr{O}\},$$

the conductor of the order $\mathscr{O}$, which was written as $(\mathscr{O} : B)$ in class. Let

$$\mathscr{D}^{-1}(B/A) = \{x \in L \,|\, \mathrm{Tr}_{L/K}(x \cdot B) \subset A\},$$

the inverse different of B/A. Let

$$\mathscr{D}^{-1}(\mathscr{O}/A) = \{x \in L \,|\, \mathrm{Tr}_{L/K}(x \cdot \mathscr{O}) \subset A\}.$$

(a) Show that $\mathfrak{c}(\mathscr{O})$ is the largest ideal of B which is contained in $\mathscr{O}$. (This was given in class as an exercise.)

(b) Prove that

$$\mathfrak{c}(\mathscr{O}) = \{x \in L \,|\, x \cdot \mathscr{D}^{-1}(\mathscr{O}/A) \subseteq \mathscr{D}^{-1}(B/A)\}.$$

(c) Suppose that $\alpha \in B$ is an element of B such that $L = K(\alpha)$ and let $f(T)$ be the minimal polynomial of α over K. Show that

$$\mathfrak{c}(A[\alpha]) = f'(\alpha) \cdot \mathscr{D}^{-1}(\mathscr{O}/A).$$

Note that this property implies the following.

- If $B = A[\alpha]$, then $\mathscr{D}(B/A)$ is equal to $f'(\alpha)B$.
- $\mathfrak{c}(A[\alpha]) \supset f'(\alpha)B$. In particular the localization $A[\alpha]$ at all prime ideals of B relatively prime to $f'(\alpha)$ is equal to B. Among other things this gives a lower bound of $A[\alpha]$, and reduces the computation of B to a finite number of local problems.

6. Formulate and prove a generalization of Hensel's Lemma in more than one variables.
(Your answer should specialize to the one-variable version given in class. For some reason most textbooks treatment for general Hensel's Lemma only covers the weaker/simpler case when the Jacobian determinant is a unit. You are asked to do better, i.e. the Jacobian determinant is non-zero but not necessarily a unit in the local field in question.)