MATH 581G: HOMEWORK ASSIGNMENT # 4

DUE MONDAY, NOVEMBER 27

Complete any 10 of the following.

(1) (a) Let $d > 1$ be a squarefree integer, and let D be the discriminant of $K = \mathbb{Q}(\sqrt{d})$. Consider the equation

$$x^2 - Dy^2 = -4$$

If there is a integer solution to this equation, let x_1, y_1 be a minimal positive solution. If the equation has no solutions, then consider instead

$$x^2 - Dy^2 = 4$$

and let x_1, y_1 be a minimal positive solution of this equation. Show that $\epsilon := \frac{x_1+y_1\sqrt{D}}{2}$ is a fundamental unit of K (i.e. generates $\mathcal{O}_K^\times$).

(b) Determine a fundamental unit for $K = \mathbb{Q}(\sqrt{d})$ for $d = 2, 3, 5, 6, 7$, and 10 *without* just asking computer algebra software.

(2) Let $\omega = e^{2\pi i/5}$ and $\epsilon = -\omega^2(1+\omega)$.

(a) Show that ϵ is a unit in $\mathbb{Z}[\omega]$.

(b) Show that $\epsilon \in \mathbb{R}$ and that $1 < \epsilon < 2$.

(c) Show that $\mathbb{R} \cap \mathbb{Q}[\omega] = \mathbb{Q}(\sqrt{5})$.

(d) Use the above problems to prove that $\epsilon = \frac{1+\sqrt{5}}{2}$.

(e) Prove that all units in $\mathbb{Z}[\omega]$ are given by $\pm\omega^a(1+\omega)^b$ where $0 \leq 1 \leq 4$ and $b \in \mathbb{Z}$.

(3) Let K be a number field, and let L and M be two different finite extensions of K. Assume that M is Galois over K. Then the composite field LM is Galois over L and there is an injective restriction map $\mathrm{res} : \mathrm{Gal}(LM/L) \to \mathrm{Gal}(M/K)$. Let $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{u}$ and $\mathfrak{v}$ be primes of K, L, M, and LM, respectively, such that $\mathfrak{v}$ lies over $\mathfrak{q}$ and $\mathfrak{u}$, and $\mathfrak{q}$ and $\mathfrak{u}$ lie over $\mathfrak{p}$.

(a) Prove that the decomposition group $G_{\mathfrak{v}/\mathfrak{q}}$ embeds into the decomposition group $G_{\mathfrak{u}/\mathfrak{p}}$ by restricting homomorphisms, and likewise for the inertia groups of these primes.

(b) Prove that if $\mathfrak{p}$ is unramified in M, then every prime of L lying over $\mathfrak{p}$ is unramified in LM.

(c) Prove that if $\mathfrak{p}$ splits completely in M, then every prime of L lying over $\mathfrak{p}$ splits completely in LM.

(4) Prove that every finite abelian group A is the Galois group of some finite extension $L/\mathbb{Q}$.

(5) Prove that a subgroup of finite index in $\mathbb{Q}_p^\times$ is both open and closed in $\mathbb{Q}_p^\times$.

(6) Prove that the equation $5x^3 + 12y^3 + 9z^3 + 10w^3 = 0$ has solutions over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p.

(7) Prove that a p-adic number $a = \sum_{i=-m}^{\infty} a_i p^i \in \mathbb{Q}_p$ ($m \in \mathbb{Z}$ and $a_i \in \{0, \ldots, p-1\}$) is in $\mathbb{Q}$ if and only if the sequence of digits is periodic (possibly with a finite string before the first period).

(8) Prove that the field $\mathbb{Q}_p$ has no automorphisms except the identity.

(9) Let $\epsilon \in 1 + p\mathbb{Z}_p$ and let $\alpha = \sum_{i \geq 0} a_i p^i$ be a p-adic integer. Let $s_n = \sum_{i=0}^{n-1} a_i p^i$. Show that the sequence ϵ^{s_n} converges to a number $\epsilon^{\alpha} \in 1 + p\mathbb{Z}_p$. Show furthermore that this gives $1 + p\mathbb{Z}_p$ the structure of a $\mathbb{Z}_p$-module.

(10) Prove that the algebraic closure of $\mathbb{Q}_p$ has infinite degree over $\mathbb{Q}_p$.

(11) Prove the following theorem.

Theorem 0.1 (p-adic Weierstrass preparation theorem)**.** *Every nonzero power series $f(x) \in \mathbb{Z}_p[[x]]$ admits a unique representation $f(x) = p^{\mu} P(x) U(x)$ where $U(x) \in (\mathbb{Z}_p[[x]])^{\times}$ and $P(X)$ is a monic polynomial satisfying $P(X) \equiv X^n \mod p$.*

(12) Let k be a field and $K = k(t)$ the function field in one variable. Show that the valuations $v_{\mathfrak{p}}$ associated to the prime ideals $\mathfrak{p} = (p(t))$ of $k[t]$, together with the degree valuation v_{∞}, are the only valuations of K, up to equivalence. What are the residue class fields?

(13) Prove that an infinite algebraic extension of a complete field is never complete.

(14) (a) Let $X_0, X_1, \ldots$ be an infinite sequence of unknowns, p a fixed prime number and $W_n = X_0^{p^n} + pX_1^{p^{n-1}} + \ldots p^n X_n$ for $n \geq 0$. Show that there exist polynomials $S_0, S_1, \ldots$ and polynomials $P_0, P_1, \ldots$ in $\mathbb{Z}[X_0, X_1, \ldots Y_0, Y_1, \ldots]$ such that

$$W(S_0, S_1, \ldots) = W_n(X_0, X_1, \ldots) + W_n(Y_0, Y_1, \ldots),$$
$$W(P_0, P_1, \ldots) = W_n(X_0, X_1, \ldots) \cdot W_n(Y_0, Y_1, \ldots).$$

(b) Let A be a commutative ring. For infinite sequences $a = (a_0, a_1, \ldots), b = (b_0, b_1, \ldots)$ $a_i, b_i \in A$, we define

$$a + b := (S_0(a,b), S_1(a,b), \ldots), \quad a \cdot b := (P_0(a,b), P_1(a,b), \ldots).$$

Show that these operations make the set of infinite vectors $(a_0, a_1, \ldots)$ into a commutative ring with a unit. This ring is called the ring of Witt vectors of A and is denoted $W(A)$ or $\mathbb{W}(A)$.

(15) Let k be a perfect field of characteristic p. Prove that $W(k)$ is a complete discrete valuation ring of characteristic 0 with residue class k.

University of Washington, Department of Mathematics, Box 354350, Seattle, WA 98195, USA

E-mail address: bviray@math.washington.edu

URL: http://math.washington.edu/~bviray