Homework 3: HENSEL'S LEMMA

Questions marked with an * are optional, i.e. not for credit.

1) Find $a \in \mathbf{Q}$ with $|a^2 + 6|_5 < 5^{-4}$.

2) Show that $f(X) = 5X^3 - 7X^2 + 3X + 6$ has a unique root $\alpha \in \mathbf{Z}_7$ with $|\alpha - 1|_7 < 1$. Find $a \in \mathbf{Q}$ with $|\alpha - a|_7 \leq 7^{-4}$.

3) How many roots does $f(X) = X^3 + 25X^2 + X - 9$ have in $\mathbf{Q}_p$ for $p = 2, 3, 5, 7$?

4) If α is a root of $f(X) = X^4 - 38X^2 + 225$ show that $\pm\alpha$ and $\pm 15/\alpha$ are also roots of f. Show that f is irreducible over $\mathbf{Q}$ and describe its splitting field. However show that $f(X)$ is reducible over $\mathbf{Q}_p$ for all primes p and over $\mathbf{R}$.

5) Define integers $u(n)$ by $u(0) = 0$, $u(1) = 1$ and

$$u(n) = 3u(n-1) - 7u(n-2).$$

Show that there are positive integers n for which $u(n)$ is divisible by an arbitrarily high power of 5. Find the smallest $m \in \mathbf{Z}_{>0}$ for which $625|u(m)$. [Hint: solve the recurrence relation and consider the resulting expression in $\mathbf{Z}_5$.]

6) Suppose that K is a field of characteristic p complete with respect to a discrete valuation $v : K^\times \twoheadrightarrow \mathbf{Z}$, and with residue field $\mathbf{F}_q$ (the finite field with q elements). Show that $K \supset \mathbf{F}_q$. Deduce that $K \cong \mathbf{F}_q((T))$.

7) (a) Show that any homomorphism of fields $\sigma : \mathbf{Q} \hookrightarrow \mathbf{Q}$ must be the identity.

(b) Show that $\alpha \in \mathbf{R}$ is ≥ 0 if and only if $\alpha = \beta^2$ for some $\beta \in \mathbf{R}$. If $\sigma : \mathbf{R} \hookrightarrow \mathbf{R}$ is a homomorphism of fields show that $\alpha > \beta$ implies $\sigma(\alpha) > \sigma(\beta)$. Deduce that σ must be the identity.

(c) Let p and l be prime numbers. If $\alpha \in p\mathbf{Z}_p$ show that there exists β in $\mathbf{Q}_p$ with

$$\alpha = \beta/(\beta^{2(l-1)} + 1).$$

On the other hand show that there is a constant C such that if $\beta \in \mathbf{Q}_l$ then

$$|\beta/(\beta^{2(l-1)} + 1)|_l < C.$$

Now suppose that $\sigma : \mathbf{Q}_p \hookrightarrow \mathbf{Q}_l$ is a homomorphism of fields. Show that we must have $l = p$ and that σ must be the identity.

(d) Similarly show that if p is a prime then there are no field homomorphisms $\mathbf{Q}_p \hookrightarrow \mathbf{R}$.

(d) If p is a prime show that there are no field homomorphisms $\mathbf{R} \hookrightarrow \mathbf{Q}_p$.

8) Suppose that K is complete with respect to a discrete non-archimedean absolute value $|\ |$. Let $\mathcal{O}$ denote its ring of integers and k its residue field. Let $h(X) \in \mathcal{O}[X]$ be a monic polynomial. Suppose that the image $\overline{h}(X)$ of $h(X)$ in $k[X]$ has a factorisation $\overline{h}(X) = \overline{f}(X)\overline{g}(X)$, where $\overline{f}$ and $\overline{g}$ are coprime polynomials in $k[X]$. Show that $\overline{f}(X)$ and $\overline{g}(X)$ have liftings $f(X)$ and $g(X)$ in $\mathcal{O}[X]$ with

$$h(X) = f(X)g(X).$$

[Hint: Find approximations to f and g modulo successively higher powers of the maximal ideal of $\mathcal{O}$. Recall that any element of $\overline{i}(X) \in k[X]$ can be written

$$\overline{i}(x) = \overline{a}(X)\overline{f}(X) + \overline{b}(X)\overline{g}(X)$$

for some $\overline{a}(X), \overline{b}(X) \in k[X]$. Show that if $\overline{i}$ has degree less than or equal to that of $\overline{h}$, then one may assume that $\overline{a}$ (resp. $\overline{b}$) has degree less than or equal to the degree of $\overline{g}$ (resp. $\overline{f}$).]

9) Let p denote an odd prime. If $\psi : \mathbf{F}_p \to \mathbf{C}^\times$ and $\chi : \mathbf{F}_p^\times \to \{\pm 1\}$ are non-trivial homomorphisms show that

$$\tau(\chi, \psi)^2 = \chi(-1)p.$$

Deduce that

$$\mathbf{Q}(\sqrt{\chi(-1)p}) \subset \mathbf{Q}(e^{2\pi i/p}).$$

10*) Set

$$h(X, Y, Z) = X^2YZ + XY^2Z + XYZ^2 + X^2Y^2 + Y^2Z^2 + X^2Z^2 - X^4 - Y^4 - Z^4,$$

and

$$g(X_1, X_2, ..., X_9) = h(X_1, X_2, X_3) + h(X_4, X_5, X_6) + h(X_7, X_8, X_9),$$

and

$$f(X_1, X_2, ..., X_{18}) = g(X_1, ..., X_9) + 4g(X_{10}, ..., X_{18}).$$

(a) If $x, y, z \in \mathbf{Z}_2$ do not all lie in the maximal ideal show that $|h(x, y, z) + 1|_2 \leq 1/4$.

(b) If $x_1, ..., x_9 \in Z_2$ do not all lie in the maximal ideal show that $|h(x_1, ..., x_9)|_2 \geq 1/2$.

(c) Show that $\vec{0}$ is the only zero of f in $\mathbf{Q}_2^{18}$. [A counterexample to Artin's conjecture.]