Algebraic Number Theory
MATH 512

Solutions to Assignment 5

1. We introduce some convenient notation: Let $b_n = \prod_{k=1}^{n}(1+a_n) \neq 0$, and $c_n = b_{n+1} - b_n$. Note that in fact, $c_n = a_{n+1}b_n$.

Assume first that $a_n \to 0$. Choose $N \geq 1$ such that for $k > N$, $|a_k| < 1$. Then for $k > N$, $|1 + a_k| = 1$ and so for $n \geq N$ we have $|b_n| = |b_N|$. Now let $\epsilon > 0$ and choose $N' \geq N$ such that for $n \geq N'$, $|a_n| < \epsilon |b_N|^{-1}$. Then for $n \geq N'$,

$$|c_n| = |a_{n+1}| \cdot |b_n| = |a_{n+1}| \cdot |b_N| < \epsilon.$$

Thus $c_n \to 0$, and so $\{b_n\}_n$ converges by Lemma 61. Since $|b_n| = |b_N|$ for $n \geq N$, the limit b of the b_n also satisfies $|b| = |b_N| \neq 0$, and so $b \neq 0$.

Conversely, suppose the sequence $\{b_n\}_n$ converges to some $b \neq 0$. Then firstly $c_n \to 0$ (since $c_n = b_{n+1} - b_n$), and secondly there is $N \geq 1$ such that $|b_n| \geq \delta$ for $n \geq N$, where $\delta = \frac{1}{2}|b| > 0$. Then

$$|a_{n+1}| = |c_n|/|b_n| \leq |c_n|/\delta,$$

and $|c_n|/\delta \to 0$. Therefore $|a_n| \to 0$.

2. Let $K = \mathbb{Q}_p(\alpha)$ and $L = \mathbb{Q}_p(\beta)$. Since a, b are not square mod p, K and L are both quadratic over $\mathbb{Q}_p$. Write $\mathrm{Gal}(K/\mathbb{Q}_p) = \langle \sigma \rangle$. Then $|\sigma(\alpha) - \alpha| = |-2\alpha| = 1$. On the other hand, if $M = KL$, then in $\mathcal{O}_M/\mathfrak{p}_M$,

$$\begin{aligned} \overline{\alpha}^2 &= \overline{a} \\ &= \overline{b} \\ &= \overline{\beta}^2, \end{aligned}$$

so $\overline{\alpha} = (-1)^r \overline{\beta}$ with $r \in \{0, 1\}$. Therefore $|(-1)^r\beta - \alpha| < 1 = |\sigma(\alpha) - \alpha|$. By Krasner's Lemma, $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p((-1)^r\beta) = \mathbb{Q}_p(\beta)$.

3. (a) Let $f(x) = x^3 - x + 1$. We show that $f(x)$ has exactly one root in $\mathbb{Q}_7$, and that this root is a simple root. Firstly, any root in $\mathbb{Q}_7$ must necessarily lie in $\mathbb{Z}_7$ – this involves the same proof as question **3** in Assignment 4. Further, if $\alpha \in \mathbb{Z}_7$ is a root and $\alpha \equiv a \bmod 7\mathbb{Z}_7$ with $a \in \{0, 1, \ldots, 6\}$, then $f(a) \equiv 0 \bmod 7$. One checks that the only possibility is $a = 2$. Since $f'(2) = 11$, a unit in $\mathbb{Z}_7$, Hensel's Lemma tells us that $f(x)$ has root α in $\mathbb{Z}_7$ congruent to 2 mod $7\mathbb{Z}_7$. In fact, α must be a simple root since $f'(\alpha) \neq 0$.

Therefore, if $g(x) \in \mathbb{Z}_7[x]$ is the unique polynomial with $f(x) = (x - \alpha)g(x)$, then $g(x)$ is quadratic and irreducible over $\mathbb{Q}_7$. Thus $L/\mathbb{Q}_7$ is quadratic.

(b) One finds easily that $g(x) = x^2 + \alpha x - 1/\alpha \in \mathbb{Z}_7[x]$, and completing the square we see that $L = \mathbb{Q}_7(\sqrt{\frac{1}{4}\alpha^2 + \alpha^{-1}})$. Using $\alpha^3 = \alpha - 1$, one finds the more convenient description that $L = \mathbb{Q}_7(\gamma)$ where γ is a square root of $\beta = \alpha^2 + 3\alpha$.

In $\mathbb{Z}_7/7\mathbb{Z}_7$, $\overline{\beta} = \overline{\alpha}^2 + 3\overline{\alpha} = \overline{3}$, therefore in $\mathcal{O}_L/\mathfrak{p}_L$, $\overline{\gamma}^2 = \overline{\beta} = \overline{3}$. Now, let δ be a square root of 3 and let $M = \mathbb{Q}_7(\gamma, \delta)$. Then in $\mathcal{O}_M/\mathfrak{p}_M$, $\overline{\gamma}^2 = \overline{3} = \overline{\delta}^2$, so $\overline{\gamma} = (-1)^r\overline{\delta}$ for some $r \in \{0, 1\}$. If $|\cdot|$ is the absolute value on $\mathbb{Q}_7$ extended to M, the above says $|(-1)^r\delta - \gamma| < 1$. However, writing $\mathrm{Gal}(L/\mathbb{Q}_7) = \langle\sigma\rangle$, we see that $|\sigma(\gamma) - \gamma| = |-2\gamma| = 1$, since 2γ is a unit in L. Hence $|(-1)^r\delta - \gamma| < |\sigma(\gamma) - \gamma|$, so Krasner's Lemma tells us that $\gamma \in \mathbb{Q}_7(\delta)$, or in other words, $L = \mathbb{Q}_7(\delta) = \mathbb{Q}_7(\sqrt{3})$.

Now, adding 7 repeatedly by using question **2**, and factoring out squares whenever possible, we see that

$$\mathbb{Q}_7(\sqrt{3}) = \mathbb{Q}_7(\sqrt{10}) = \mathbb{Q}_7(\sqrt{17}) = \mathbb{Q}_7(\sqrt{6}) = \mathbb{Q}_7(\sqrt{13}) = \mathbb{Q}(\sqrt{5}).$$

Since 3, 5 and 6 represent all three non-squares mod 7, we are done (again, by question **2**).

4. (a) The map $U_K^n \to \mathfrak{k}_K$ is surjective. It is a group homomorphism since $a + b + ab\pi^n \equiv a + b \bmod \mathfrak{p}_K$. Further, $1 + a\pi^n$ is in the kernel if and only if $a \in \mathfrak{p}_K$, if and only if $1 + a\pi^n \in U_K^{n+1}$. Therefore $U_K^n/U_K^{n+1} \simeq \mathfrak{k}_K$. Since K is a local field, $\mathfrak{k}_K$ is finite. Further, the additive group of the field $\mathfrak{k}_K$ is a p-group because $\mathfrak{k}_K$ has characteristic p.

(b) We proceed by induction on n. The case $n = 1$ is trivial. Now assume that U_K^1/U_K^n is a finite p-group for some $n \geq 1$. Then the isomorphism

$$\frac{U_K^1/U_K^{n+1}}{U_K^n/U_K^{n+1}} \simeq U_K^1/U_K^n$$

together with part (a) completes the induction.

(c) Define a map $U_K^1 \to \varprojlim_n U_K^1/U_K^n$ by sending a principal unit u to the element of $\varprojlim_n U_K^1/U_K^n$ that has $u \bmod U_K^n$ in the nth component. This map is a group homomorphism. If u is in the kernel of this map, then it is in U_K^n for all n, which is to say that $\nu(u - 1) \geq n$ for all n, where ν is the normalized valuation on K. Therefore $u - 1 = 0$, i.e. $u = 1$. Thus the map is injective.

Now suppose we are given principal units u_n, $n = 1, 2, 3, \ldots$, such that $u_m/u_n \in U_K^m$ whenever $m \leq n$ (i.e. $(u_n \bmod U_K^n)_n \in \varprojlim_n U_K^1/U_K^n$). Then for such m, n we have $u_m - u_n \in \mathfrak{p}^m$, i.e. $\nu(u_m - u_n) \geq m$, i.e. the sequence $\{u_n\}$ is Cauchy and so has a limit $u \in K$. The sequence $\{u_n - 1\}$ converges to $u - 1$, and if $u \neq 1$ then for large enough n, $\nu(u - 1) = \nu(u_n - 1) \geq 1$. Thus $u \in U_K^1$. Further, u maps to $(u_n \bmod U_K^n)_n$. Indeed, given $n \geq 1$, choose $m \geq n$ such that $u - u_m \in \mathfrak{p}_K^n$. Then $u \equiv u_m \equiv u_n \bmod \mathfrak{p}_K^n$.

5. (a) A sufficient condition is $n > 2\nu(m)$ where ν is the normalized valuation on K. Indeed, suppose $n > 2\nu(m)$. Take $a \in U_K^n$ and let $f(x) = x^m - a \in \mathcal{O}_K[x]$. Then $|f(1)| < |f'(1)^2|$ if and only if $|1-a| < |m^2|$, if and only if $\nu(1-a) > 2\nu(m)$. However, $\nu(1 - a) \geq n \geq 2\nu(m)$, so indeed, $|f(1)| < |f'(1)^2|$. Thus, by Hensel's Lemma, there is $\alpha \in \mathcal{O}_K$ such that $f(\alpha) = 0$, i.e. $\alpha^m = a$, i.e. $a \in (U_K)^m$.

(b) Consider the natural map $U_K \to U_K/(U_K)^m$. Choosing $n > 2\nu(m)$, we see from part (a) that U_K^n is in the kernel of this map, so that U_K/U_K^n surjects onto $U_K/(U_K)^m$. It is therefore enough to show that U_K/U_K^n is finite. We know that $U_K/U_K^1 \simeq \mathfrak{k}_K$ is finite, so we are reduced to showing that U_K^1/U_K^n is finite. However, we saw that this is the case in question **4**.

(c) Let K be a characteristic 0 local field, and let $m \geq 1$. Fix an algebraic closure $\bar{K}$ of K and let $L = K(\zeta_m)$ where ζ_m is a primitive mth root of unity in $\bar{K}$. Since $L^\times = \langle \pi \rangle \times U_L$ where π is a uniformizer of L, $L^\times/(L^\times)^m \cong \mathbb{Z}/m\mathbb{Z} \times U_L/(U_L)^m$, which is finite by part (b). Therefore, by Kummer theory, L admits only finitely many abelian extensions of exponent m in $\bar{K}$. Let M be the maximal such extension of L. In other words, M is the compositum of the finitely many exponent m abelian extensions of L in $\bar{K}$. If F/K is abelian of exponent m, then FL/L is also abelian of exponent m, so that $FL \subseteq M$. In particular, $K \subseteq F \subseteq M$. Since M/K is a finite separable extension, there are therefore only finitely many possibilities for F.