Algebraic Number Theory
MATH 512

Solutions to Assignment 6

1. (a) $L = \mathbb{Q}(\sqrt{-1})$, and $\sqrt{-1}$ is a root of unity of order prime to 7. Therefore $L/\mathbb{Q}_7$ is unramified. For example, if ζ is a primitive 48th root of unity, then $\sqrt{-1}$ is a power of ζ, but $\mathbb{Q}_7(\zeta)/\mathbb{Q}_7$ is unramified (of degree 2). In fact, $L = \mathbb{Q}(\zeta)$. Since $L/\mathbb{Q}_7$ is an unramified quadratic extension, the residue extension is quadratic.

(b) Since a is not square mod 7, the class of γ mod $\mathfrak{p}_L$ lies in $\mathfrak{k}_L \setminus \mathbb{F}_7$ and therefore generates $\mathfrak{k}_L$ over $\mathbb{F}_7$. Hence we may take $f(x) = x^2 - a$ in the proof of Lemma 75. Now, $f(\gamma) = 0 \in \mathfrak{p}_L^2$, therefore $f(\gamma + 7) \in \mathfrak{p}_L \setminus \mathfrak{p}_L^2$ since 7 is a uniformizer of L. The aforementioned proof then shows that $\mathcal{O}_L = \mathbb{Z}_7[\gamma + 7] = \mathbb{Z}_7[\gamma]$.

2. (a) $L/\mathbb{Q}_p$ is totally ramified, so $G_0 = G$ by the remark following the proof of Proposition 74.

(b)

$$\begin{aligned} v(\sigma_a(\zeta) - \zeta) &= v(\zeta^a - \zeta) \\ &= v(\zeta^{a-1} - 1). \end{aligned}$$

However, $\zeta^{a-1} - 1$ is a primitive p^{r-m_a}th root of unity by definition of m_a, and is therefore a uniformizer of $\mathbb{Q}_p(\zeta_{p^{r-m_a}})$. Since $L/\mathbb{Q}_p(\zeta_{p^{r-m_a}})$ is totally ramified of degree p^{m_a}, we thus have $v(\zeta^{a-1} - 1) = p^{m_a}$.

(c) By Lemma 75, $\mathcal{O}_L = \mathbb{Z}_p[\zeta]$, and so

$$\begin{aligned} \sigma_a \in G_n &\Leftrightarrow v(\sigma_a(\zeta) - \zeta) \geq n + 1 \\ &\Leftrightarrow p^{m_a} \geq n + 1 \\ &\Leftrightarrow m_a \geq k. \end{aligned}$$

(d) $m_a \geq k$ if and only if $a \equiv 1 \bmod p^k$. Now use part (c).

3. (a) If $a \cdot_g \beta = 0$, then

$$\begin{aligned} 0 &= \mathbf{1}_{f,g}(a \cdot_g \beta) \\ &= \mathbf{1}_{f,g} \circ [a]_g(\beta) \\ &= [a]_f \circ \mathbf{1}_{f,g}(\beta) \\ &= a \cdot_f \mathbf{1}_{f,g}(\beta). \end{aligned}$$

(b) Define maps

$$\begin{aligned} \varphi : \mathfrak{p}_{K_s} &\to \mathfrak{p}_{K_s} \\ \beta &\mapsto \mathbf{1}_{f,g}(\beta) \end{aligned}$$

and

$$\begin{array}{rcl} \psi : \mathfrak{p}_{K_{\mathrm{s}}} & \to & \mathfrak{p}_{K_{\mathrm{s}}} \\ \beta & \mapsto & \mathbf{1}_{g,f}(\beta). \end{array}$$

We first claim that $\mathbf{1}_{g,f} \circ \mathbf{1}_{f,g}(x) = x$. Indeed, certainly $\mathbf{1}_{g,f} \circ \mathbf{1}_{f,g}(x) \equiv x \bmod \deg 2$, and further for any $a \in \mathcal{O}_K$,

$$\begin{array}{rcl} \mathbf{1}_{g,f} \circ \mathbf{1}_{f,g} \circ [a]_g & = & \mathbf{1}_{g,f} \circ [a]_f \circ \mathbf{1}_{f,g} \\ & = & [a]_g \circ \mathbf{1}_{g,f} \circ \mathbf{1}_{f,g}. \end{array}$$

Hence, by the uniqueness statement given at the beginning of the exercise, $\mathbf{1}_{g,f} \circ \mathbf{1}_{f,g}(x) = x$. Similarly, $\mathbf{1}_{f,g} \circ \mathbf{1}_{g,f}(x) = x$. Thus φ and ψ are mutually inverse bijections.

Now, by part (a), if $\alpha \in \mathfrak{p}_{K_{\mathrm{s}}}$ has $a \cdot_g \alpha = 0$, then $a \cdot_f \varphi(\alpha) = a \cdot_f \mathbf{1}_{f,g}(\alpha) = 0$, so φ maps $\{\alpha \in \mathfrak{p}_{K_{\mathrm{s}}} \mid a \cdot_g \alpha = 0\}$ into $\{\alpha \in \mathfrak{p}_{K_{\mathrm{s}}} \mid a \cdot_f \alpha = 0\}$. Reversing the roles of f and g in part (a), we see that ψ maps $\{\alpha \in \mathfrak{p}_{K_{\mathrm{s}}} \mid a \cdot_f \alpha = 0\}$ into $\{\alpha \in \mathfrak{p}_{K_{\mathrm{s}}} \mid a \cdot_g \alpha = 0\}$, and we are done.

4. (a) $f(x) \equiv \pi x \bmod \deg 2$ and f commutes with itself, therefore by the uniqueness statement in Theorem 78, $[\pi]_f = f$.

(b) Let $g_\beta(x) = f(x) - \beta$. Suppose $\alpha \in \bar{K}$ is a root of $g_\beta(x)$, i.e. $g_\beta(\alpha) = 0$. Since $g_\beta(x)$ has coefficients with absolute value at most 1 (extending the absolute value on K to $\bar{K}$), α also has absolute value at most 1 by the argument used for question **3** of Assignment 4. As $g_\beta(x) - x^q$ has coefficients of absolute value less than 1, α must then also have absolute value less than 1. If we suppose that α is in fact a *double* root of $g_\beta(x)$, i.e. $g'_\beta(\alpha) = 0$, then $\pi = -q\alpha^{q-1}$. This forces $q \neq 0$ in K, but in that case

$$\begin{array}{rcl} |\pi| & = & |q\alpha^{q-1}| \\ & = & |q| \cdot |\alpha|^{q-1} \\ & < & |q| \\ & \leq & |\pi|, \end{array}$$

a contradiction. Therefore $g_\beta(x)$ is separable, so that all of its roots, which are necessarily distinct, lie in K_{s}, or in fact $\mathfrak{p}_{K_{\mathrm{s}}}$ by the above argument. Since $g_\beta(x)$ has degree q, there are therefore q distinct solutions $\alpha \in \mathfrak{p}_{K_{\mathrm{s}}}$ to the equation $g_\beta(\alpha) = 0$, or in other words, to $\pi \cdot_f \alpha = \beta$ since $[\pi]_f = f$ by part (a).

(c) By question **3**, we may assume that $g = f$ with f as in parts (a) and (b). We prove the statement by induction on n. For $n = 1$, this is part (b) with $\beta = 0$. Now assume that the statement holds for some $n \geq 1$. For $\alpha \in \mathfrak{p}_{K_{\mathrm{s}}}$, $\pi^{n+1} \cdot_f \alpha = 0$ if and only if $\pi^n \cdot_f (\pi \cdot_f \alpha) = 0$, if and only if $\pi \cdot_f \alpha$ is one of the q^n elements $\beta \in \mathfrak{p}_{K_{\mathrm{s}}}$ with $\pi^n \cdot_f \beta = 0$. For each of these q^n elements β, there are q elements $\alpha \in \mathfrak{p}_{K_{\mathrm{s}}}$ with $\pi \cdot_f \alpha = \beta$, by part (b). Thus there are q^{n+1} elements $\alpha \in \mathfrak{p}_{K_{\mathrm{s}}}$ with $\pi \cdot_f \alpha = 0$.