Exercises due Dec. 16: Norm residue symbol and mth power reciprocity law, or: The duality between class field theory and Kummer theory.

Let m be a fixed integer ≥ 1. Let K be a field containing the mth roots of unity and write $\mu_m = \mu_m(K)$ for the cyclic group they form.

A. THE NORM RESIDUE SYMBOL. Assume K is a local field. Note then that our hypothesis implies that $(K^*)^m$ is of finite index in K^*, because it implies that $\mathrm{char}(K)$ does not divide m . Assuming the basic theorems of local class field theory we can define a map $K^* \times K^* \to \mu_m$ by putting

$$(a,b) = (a,b)_{K,m} = \beta^{\sigma_a - 1} = \beta^{\sigma_a}/\beta$$

where β is an mth root of b in a fixed K^{ab}, and $\sigma_a = (a, K^{\mathrm{ab}}/K)$. Thus, $K(b^{1/m})$ is the class field over K with norm group the set of a in K^* such that $(a,b) = 1$.

Exercise 1. Show that (a,b) induces a non-degenerate pairing $K^*/(K^*)^m \times K^*/(K^*)^m \to \mu_m$ such that $(a,-a) = 1, \qquad (a,b)(b,a) = 1, \qquad$ and for $\quad a \neq 1, \quad (a,1-a) = 1.$

B. THE mTH POWER RESIDUE SYMBOL. Now assume our local field K is nonarchimedean. Let $k = O/P$ be its residue field and put $|k| = q = p^\nu$. Assume also that p does not divide m, i.e., $m \notin P$, and note that this implies that elements of μ_m are in different residue classes, so that reduction mod P gives an isomorphism $\mu_m(K) \xrightarrow{\sim} \mu_m(k)$. In particular, m divides $|k^*| = q-1$, and since k^* is cyclic, $\mu_m(k) = (k^*)^{\frac{q-1}{m}}$.

The mth power residue symbol is the homomorphism $O^* \to \mu_m$ denoted by $a \mapsto (\frac{a}{P})$ and defined by

$$(\frac{a}{P}) \in \mu_m \qquad \text{and} \qquad (\frac{a}{P}) \equiv a^{\frac{q-1}{m}} \mod P$$

Exercise 2. Show that if $b \in O^*$ and $m \notin P$, then $(a,b) = (\frac{b}{P})^{v_K(a)}$. More generally, show that for arbitrary $a, b \in K^*$, we have $(a,b) = (\frac{\{a,b\}}{P})$, where $\{a,b\} := (-1)^{v(a)v(b)} \frac{b^{v(a)}}{a^{v(b)}}$, where $v = v_K$. (Suggestion: Write $a = \pi^r u$ and $b = \pi^s v$, where π is a uniformiser and $u, v \in O^*$.)

C. THE GLOBAL mTH POWER RECIPROCITY LAW. Now assume K is a global field containing the mth roots of unity. Let S be a finite set of places of K containing the archimedian places and the places dividing m. For a field element $\alpha \in K^*$, Let $(\alpha)_S$ denote the divisor $\prod_{P \notin S} P^{v_P(\alpha)}$. For a divisor $D = \prod_{P \notin S} P^{\nu_P}$ with support disjoint from S and the support of $(\alpha)_S$, define $(\frac{\alpha}{D}) = \prod_{P \notin S} (\frac{a}{P})^{\nu_P}$, where $(\frac{\alpha}{P})$ is the mth power residue symbol in K_P, the completion of K at the place of P.

Exercise 3. Suppose $\alpha, \beta \in K^*$ and the supports of $(\alpha)_S$ and $(\beta)_S$ are disjoint, that is, $v_P(\alpha)v_P(\beta) = 0$ for all $P \notin S$. Show that Artin's reciprocity law implies

$$(\frac{\alpha}{(\beta)_S})(\frac{\beta}{(\alpha)_S})^{-1} = \prod_{v \in S} (\alpha,\beta)_{K_v,m},$$

and check that this is Gauss's law for $K = \mathbb{Q}, m = 2, S = \{\infty, 2\}$.

D. THE CASE $m = 4$. Let $K = \mathbb{Q}(i)$ and $A = \mathbb{Z}[i]$, the ring of "Gaussian" integers, a well-known P.I.D. Let $\lambda = 1 - i$. Then $(2) = (\lambda)^2$ and λ is a Gaussian prime. Let $K_\lambda = \mathbb{Q}_2(i)$ be the completion of K for the λ-adic valuation v_λ and let A_λ denote the valuation ring in K_λ. Its maximal ideal is λA_λ and its residue field is $\mathbb{F}_2$. For $j \geq 1$ put $U_j = 1 + \lambda^j A_\lambda$. Note that $U_1 = A_\lambda^*$, and U_j/U_{j+1} is a group of order 2 for each $j \geq 1$.

For $a \in U_1$, put $m(a) = v_\lambda(a-1)$, so $a \in U_{m(a)}$ but $a \notin U_{m(a)+1}$. Put $\eta_j = 1 - \lambda^j$. Check that

$$m(i) = 1, \quad m(i^2) = 2, \quad m(\eta_3) = 3, \quad m(\eta_4) = 4, \quad m(\eta_3^2) = 5, \quad m(\eta_4^2) = 6,$$

and for $j \geq 7, m(\eta_{j-4}^4) = j$. Conclude from this data that $U_1^4 = U_7$, and U_1/U_1^4 is a free $\mathbb{Z}/4\mathbb{Z}$-module of rank three, with basis the classes of $i,\ \eta_3 = 3 + 2i,\ \eta_4 = 5$, and every element $a \in K_\lambda^*$ can be written uniquely as $a = \lambda^\nu i^j a^*$ with $\nu \in \mathbb{Z}, j \in \{0,1,2,3\}, a^* \in U_3$.

Let $(a,b) = (a,b)_{K_\lambda,4}$ be the $m = 4$ norm residue symbol in K_λ and let $\left(\frac{\alpha}{(\pi)}\right)$ be the 4th power residue symbol at an odd Gaussian prime π. To determine (x,y) explicitly for all x, y it suffices to compute $(\lambda,\lambda), (\lambda,i), (\lambda,a^*), (i,i), (i,a^*)$, and (a^*,b^*) for a^* and b^* in U_3, because of the rules in Exercise 1. Those rules also give simple proofs that the three symbols involving only i and λ are 1. (One could also use Exercise 3 to show that those three are 1.)

Exercise 4. Show that $(i,a) = i^{\frac{\mathrm{N}\,a-1}{4}}$ for all $a \in U_1$, where $\mathrm{N} = \mathrm{N}_{K_\lambda/\mathbb{Q}_2}$. (Check that $\mathrm{N}\,U_1 = 1 + 4\mathbb{Z}_2$, so the right side makes sense, that the right side is multiplicative in a, and that, by Exercise 3, the formula does hold when $a = \pi$ is an odd Gaussian prime. Why does this suffice?)

Exercise 5. The formulas $(i,a) = i^{-\frac{1}{4}\,\mathrm{Tr}(\log a)}$ and $(\lambda,a) = i^{\frac{1}{8}\,\mathrm{Tr}(\lambda \log a)}$ hold for $a \in U_1$, where $\mathrm{Tr} = \mathrm{Tr}_{K_\lambda/\mathbb{Q}_2}$ and $\log \alpha = \sum_{j=1}^{\infty} \frac{(-1)^{j-1}}{j}(\alpha - 1)^j$. Explain why, in order to prove this, it suffices to check the formulas for the two cases $a = \eta_3$ and $a = \eta_4$. (You are not required to check them, though that's easy with a computer once one works out the left sides with Exercise 3 to get $(i,\eta_3) = -i,\ (i,\eta_4) = -1,\ (\lambda,\eta_3) = 1,\ (\lambda,\eta_4) = -i$.) (One can also prove the first formula, assuming Exercise 4, using $\mathrm{Tr} \circ \log = \log \circ \mathrm{N}$.)

Exercise 6 (Quartic reciprocity). For relatively prime Gauss integers $\alpha, \beta \equiv 1 \mod \lambda^3$, show $\left(\frac{\alpha}{(\beta)}\right)\left(\frac{\beta}{(\alpha)}\right)^{-1} = 1$ if either α or β is $\equiv 1 \mod 4$, and $= -1$ if neither α nor β is $\equiv 1 \mod 4$. Since every Gauss integer α is of the form $\lambda^\nu i^j \alpha^*$ with a (unique) $\alpha^* \equiv 1 \mod \lambda^3$, this "reciprocity" and the "supplementary" rules for $\left(\frac{i}{(\alpha)}\right) = (i,\alpha)$ and $\left(\frac{\lambda}{(\alpha)}\right) = (\lambda,\alpha)$ tell the whole story.

Exercise 7. Give an element $b \in K_\lambda$ such that the extension $K(b^{\frac{1}{4}})/K$ is unramified of degree 4. (It might help, if necessary, to reread the last sentence before Exercise 1.)