Homework 12 - Number Theory

Exercise 1. (Hilbert symbols, continued.) Denote by

$$(-,-)_p\colon \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \mu_2$$

the Hilbert symbol for square classes of p-adic numbers.

a) For $a \in \mathbb{Z}_p$, let

$$N_a = \{z \in \mathbb{Q}_p^\times | z = x^2 - ay^2 \text{ for some } x, y \in \mathbb{Z}_p\}.$$

Show there is an equality $N_a = \mathbb{Q}_p^\times$ if and only if $a \in (\mathbb{Q}_p^\times)^2$.

b) The Hilbert symbol $(-,-)_p$ is a symmetric nondegenerate bilinear form.

If v is a discrete valuation on a field F, the associated *tame symbol* is the map

$$\tau_v\colon F^\times \times F^\times \to k_v^\times$$

defined by

$$(a, b) \mapsto (-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)} + \mathfrak{m}_v.$$

(This defines an element of $k_v^\times$ because $v(\pm a^{v(b)} b^{-v(a)}) = 0$.)

c) Suppose p is an odd prime and $a, b \in \mathbb{Q}_p^\times$. Identify $\{\pm\bar{1}\}$ in the residue field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ with $\mu_2 = \mathbb{Z}^\times$. Verify the formula

$$(a, b)_p = \tau_p(a, b)^{\frac{p-1}{2}}$$

where $\tau_p(-,-)$ is the tame symbol associated to the p-adic valuation on $\mathbb{Q}_p$.

If $a \in \mathbb{Q}_2^\times$ there is a unique expression $a = 2^i(-1)^j 5^k r$ where $i \in \mathbb{Z}$, $j, k \in \{0, 1\}$ and $r \in 1 + 8\mathbb{Z}_2 = (\mathbb{Z}_2^\times)^2$. Likewise, if $b \in \mathbb{Q}_2^\times$, write $a = 2^I(-1)^J 5^K s$.

d) Verify the formula

$$(a, b)_2 = (-1)^{iK + jJ + kI}.$$

e) Compute the Hilbert symbols of $\mathbb{R}$ and $\mathbb{C}$.

Exercise 2. (Group (co)homology.)

a) (Shapiro's lemma.) Let H be a subgroup of G. For any H-module N, there is a canonical isomorphism

$$H^r(G, \mathrm{Ind}_H^G N) \cong H^r(H, N)$$

for all $r \geq 0$. Conclude that if M is an induced G-module, then $H^r(G, M) = 0$ for $r > 0$.

b) (Cup-products.) For classes $m \in H^r(G, M)$ and $n \in H^r(G, N)$ represented by cocycles ϕ and ρ, respectively, the cup-product $m \cup n$ is represented by the cocycle

$$(g_1, \ldots, g_{r+s}) \mapsto \phi(g_1, \ldots, g_r) g_1 \cdots g_r \rho(g_{r+1}, \ldots, g_{r+s}).$$

Show that the cup-product is well-defined and verify the formulas

$$(k \cup m) \cup n = k \cup (m \cup n), \quad m \cup n = (-1)^{rs} n \cup m.$$

c) If there is an exact sequence of G-modules

$$0 \to M' \to M \to M'' \to 0$$

and two of the Herbrand quotients $h(M)$, $h(M')$, $h(M'')$ are defined, then is is the third, and

$$h(M) = h(M')h(M'').$$

d) Read Chapter II of J. Milne's notes on class field theory:

$$http://www.jmilne.org/math/CourseNotes/CFT.pdf$$

Exercise 3. Let $m > 0$ be a square-free integer and $K = \mathbb{Q}(\sqrt{m})$.

a) Show there is an isomorphism

$$\mathcal{O}_K^\times \cong \mathbb{Z}/2 \times \mathbb{Z}.$$

Conclude that the equation $x^2 - my^2 = 1$ has infinitely many integer solutions when $m \equiv 2, 3 \bmod 4$, while the equation $x^2 - my^2 = 4$ has infinitely many integer solutions when $m \equiv 1 \bmod 4$.

b) If $m \equiv 2, 3 \bmod 4$, let b be the smallest positive integer such that one of $mb^2 \pm 1$ is a square a^2 for $a > 0$. Show that $a + b\sqrt{m}$ is a fundamental unit of K. Determine the fundamental unit of K when $m = 2$ and $m = 3$.

c) Devise an algorithm computing the fundamental unit of K when $m \equiv 1 \bmod 4$. Determine the fundamental unit for $\mathbb{Q}(\sqrt{5})$.