Homework 8: EXTENDING ABSOLUTE VALUES

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

1) Suppose that $|\ |$ is an absolute value on a field K. Suppose also that L/K is a finite separable extension and that N/K is the normal closure of L/K. Choose an extension $|\ |_N$ of $|\ |$ to N. Let $\widehat{K}$ (resp. $\widehat{N}$) denote the completions of K (resp. N) with respect to $|\ |$ (resp. $|\ |_N$). Show that the map which sends $\sigma \in \mathrm{Gal}(N/K)$ to the restriction of $|\sigma\ |_N$ to L sets up a bijection between the set of double cosets

$$\mathrm{Gal}(\widehat{N}/\widehat{K})\backslash \mathrm{Gal}(N/K)/\mathrm{Gal}(N/L)$$

and the set of extensions of $|\ |$ to L. Show moreover that the completion of L with respect to the absolute value corresponding to σ is isomorphic to

$$\widehat{N}^{\mathrm{Gal}(\widehat{N}/\widehat{K})\cap\sigma\mathrm{Gal}(N/L)\sigma^{-1}}.$$

[If G is a group with subgroups H_1 and H_2 then by an (H_1, H_2)-*double coset* we mean a set of the form

$$H_1 g H_2 = \{h_1 g h_2 :\ \ h_i \in H_i\}$$

for some fixed $g \in G$. The set of all (H_1, H_2)-double cosets forms a partition of G. We denote the set of all (H_1, H_2)-double cosets by $H_1\backslash G/H_2$.]

2) Suppose that L/K is a finite Galois extension of fields and that $|\ |$ is a non-archimedean absolute value on L with finite residue field. Suppose moreover $|\ |$ is unramified over K. If $\sigma \in \mathrm{Gal}(L/K)$ show that

$$\mathrm{Frob}^{-1}_{L/K,|\sigma|} = \sigma^{-1}\mathrm{Frob}^{-1}_{L/K,|\ |}\sigma.$$

3) (a) Show that any quadratic extension $K/\mathbf{Q}$ is of the form $\mathbf{Q}(\sqrt{d})$, where $d \in \mathbf{Z}_{\neq 0,1}$ and either $d \equiv 1 \bmod 4$ is square free, or $4|d$ and $d/4$ is square free and congruent to 2 or 3 modulo 4.

(b) If $p|d$ is an odd prime show that ord_p has a unique extension to a valuation v on K and that $K_v/\mathbf{Q}_p$ is ramified of degree 2. Show moreover that $\mathcal{O}_{K_v} = \mathbf{Z}_p[\sqrt{d}]$ and that $\mathcal{D}^{-1}_{K_v/\mathbf{Q}_p} = \sqrt{d}^{-1}\mathcal{O}_{K_v}$.

(c) If $p \not| d$ is an odd prime and d has no square root in $\mathbf{F}_p$, show that ord_p has a unique extension to a valuation v on K and that $K_v/\mathbf{Q}_p$ is unramified of degree 2. Show moreover that $\mathcal{O}_{K_v} = \mathbf{Z}_2[\sqrt{d}]$.

(d) If $p \not| d$ is an odd prime and d has a square root in $\mathbf{F}_p$, show that ord_p has two extensions to K, corresponding to two embeddings $K \hookrightarrow \mathbf{Q}_p$. Show that the set of elements of K which map to $\mathbf{Z}_p$ under both these embeddings is

$$\mathbf{Z}_{(p)} \oplus \mathbf{Z}_{(p)}\sqrt{d}.$$

Given an element of K which maps to $\mathbf{Z}_p$ under one of these embeddings but not the other.

(e) Set

$$\eta_d = (d + \sqrt{d})/2.$$

What is the monic minimal polynomial $f_d(X)$ of η_d over $\mathbf{Q}$?

(f) If $d \equiv 1 \bmod 8$ show that there are two extensions of ord_2 to K, corresponding to two embeddings $K \hookrightarrow \mathbf{Q}_2$. Show that the set of elements of K which map to $\mathbf{Z}_2$ under both these embeddings is

$$\mathbf{Z}_{(2)} \oplus \mathbf{Z}_{(2)}\eta_d.$$

(g) If $d \equiv 5 \bmod 8$ show that there is a unique extension v of ord_2 to K and that $K_v/\mathbf{Q}_2$ is an unramified quadratic extension. Show also that $\mathcal{O}_{K_v} = \mathbf{Z}_2[\eta_d]$.

(h) If $2|d$ show that there is a unique extension v of ord_2 to K and that $K_v/\mathbf{Q}_2$ is a ramified quadratic extension. Show moreover that $\mathcal{O}_{K,v} = \mathbf{Z}_2[\eta_d]$ and that $\mathcal{D}^{-1}_{K_v/\mathbf{Q}_2} = (\sqrt{d})^{-1}\mathcal{O}_{K,v}$. [Hint: it might be helpful to distinguish the two possibilities for d mod 8.]

(i) Show that the set of elements of K which lie in $\mathcal{O}_{K_v}$ for all non-trivial valuations on K is $\mathbf{Z}[\eta_d]$. Show also that the set of elements of K which lie in $\mathcal{D}^{-1}_{K_v/\mathbf{Q}_v}$ for all non-trivial valuations v on K is $(\sqrt{d})^{-1}\mathbf{Z}[\eta_d]$.

(j) Let p be an odd prime. Show that $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$ is the unique quadratic extension of $\mathbf{Q}$ in which ord_p is the only non-trivial valuation which ramifies.

4) We will write ζ_n for a primitive n^{th} root of unity.

(a) Show that $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ is Galois and that there is an embedding

$$\chi : \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^\times$$

given by

$$\sigma\zeta_n = \zeta_n^{\chi(\sigma)}.$$

(b) Suppose that $p \not| n$ is a prime. If v is a valuation of $\mathbf{Q}(\zeta_n)$ extending ord_p show that $\mathbf{Q}(\zeta_n)_v/\mathbf{Q}_p$ is unramified and has degree the smallest positive integer m such that $p^m \equiv 1 \bmod n$.

Show that the primitive n^{th} roots of unity in $\mathbf{Z}_p[\zeta_n]$ remain distinct in the residue field. If $\mathrm{Frob}_p^{-1} \in \mathrm{Gal}(\mathbf{Q}(\zeta_n)_v/\mathbf{Q}_p) \subset \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$ denotes the lift of the arithmetic Frobenius element of $\mathrm{Gal}(k(\mathbf{Q}(\zeta_n)_v)/\mathbf{F}_p)$, show that

$$\chi(\mathrm{Frob}_p^{-1}) = p.$$

[The arithmetic Frobenius element of $\mathrm{Gal}(\mathbf{F}_{p^r}/\mathbf{F}_p)$ is the element that takes any $\alpha \in \mathbf{F}_{p^r}$ to α^p.] If $\mathbf{Q}(\zeta_n) \supset K$ show that there are $[K^{\langle \mathrm{Frob}_p^{-1} \rangle} : \mathbf{Q}]$ extensions of ord_p to K, where $\langle \mathrm{Frob}_p^{-1} \rangle$ denotes the subgroup of $\mathrm{Gal}(K/\mathbf{Q})$ generated by Frob_p^{-1}.

(c) Suppose that p is a prime which divides n. Let p^r denote the highest power of p dividing n. If v is an extension of ord_p to $\mathbf{Q}(\zeta_n)$ show that

$$p^{r-1}(p-1)|e_{\mathbf{Q}(\zeta_n)_v/\mathbf{Q}_p}$$

and that

$$I_{\mathbf{Q}(\zeta_n)_v/\mathbf{Q}_p} \subset \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}(\zeta_{n/p^r})).$$

Deduce that

$$\chi(I_{\mathbf{Q}(\zeta_n)_v/\mathbf{Q}_p}) = \{a \in (\mathbf{Z}/n\mathbf{Z})^\times : \ \ a \equiv 1 \bmod n/p^r\}.$$

(d) Show that

$$\chi : \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^\times.$$

Deduce that the cyclotomic polynomial

$$\Phi_n(X) = \prod_{i \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - \zeta_n^i)$$

is irreducible in $\mathbf{Q}[X]$.

(e) Suppose that p is an odd prime. Show that $\mathbf{Q}(\zeta_p)$ contains a unique quadratic extension of $\mathbf{Q}$, namely $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$. Suppose that $q \neq p$ is another odd prime. Show that the following are equivalent:

(i) $(-1)^{(p-1)/2}p$ is a square in $\mathbf{F}_q$.

(ii) There are two valuations on $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$ extending ord_q.

(iii) $\mathrm{Frob}_q^{-1} \in \mathrm{Gal}(\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})/\mathbf{Q})$ is trivial.

(iv) q is a square in $\mathbf{Z}/p\mathbf{Z}$.

[This is Gauss' famous law of quadratic reciprocity.]

5*) Suppose that $p \equiv 1 \bmod 3$ is a prime number. Choose non-trivial homomorphisms

$$\omega : \mathbf{F}_p^\times \longrightarrow \zeta_3^{(\mathbf{Z}/3\mathbf{Z})} \subset \mathbf{Q}(\zeta_{3p})^\times$$

and

$$\psi : \mathbf{F}_p \longrightarrow \zeta_p^{(\mathbf{Z}/p\mathbf{Z})} \subset \mathbf{Q}(\zeta_{3p})^\times.$$

Consider the Gauss sum

$$\tau(\omega, \psi) = \sum_{\alpha \in \mathbf{F}_p^\times} \omega(\alpha)\psi(\alpha).$$

Recall that

$$\tau(\omega, \psi)c(\tau(\omega, \psi)) = p$$

where c denotes complex conjugation (i.e. the element of $\mathrm{Gal}(\mathbf{Q}(\zeta_{3p})/\mathbf{Q})$ with $\chi(c) = -1$).

(a) Show that ord_p has two extensions to $\mathbf{Q}(\zeta_{3p})$ and these are of the form v and $v \circ c$. Also show that

$$\tau(\omega, \psi) = \sum_{\alpha \in \mathbf{F}_p^\times} \omega(\alpha)(\psi(\alpha) - 1)$$

and deduce that

$$v(\tau(\omega, \psi)) > 0$$

and

$$v(c\tau(\omega, \psi)) > 0.$$

(b) If $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_{3p})/\mathbf{Q}(\zeta_3))$ show that

$$\sigma\tau(\omega, \psi) = \omega(\chi(\sigma) \bmod p)^{-1}\tau(\omega, \psi).$$

Deduce that

$$\tau(\omega, \psi)^3 \in \mathbf{Q}(\zeta_3).$$

(c) Show that $\mathbf{Q}(\zeta_3)_v = \mathbf{Q}_p$ and $\mathbf{Q}(\zeta_3)_{v \circ c} = \mathbf{Q}_p$. Deduce that

$$v(\tau(\omega, \psi)^3) \geq 1$$

and

$$v(c\tau(\omega, \psi)^3) \geq 1.$$

(d) Show that

$$\tau(\omega, \psi)^3/p \in \mathbf{Q}(\zeta_3)$$

has valuation 1 at one valuation of $\mathbf{Q}(\zeta_3)$ extending ord_p and has valuation 0 at all other valuations of $\mathbf{Q}(\zeta_3)$.

6*) Suppose that K is a field and that S is a finite set of inequivalent, non-trivial absolute values on K. For each $|\ |_v \in S$ let K_v denote the completion of K with respect to $|\ |_v$ and suppose that L_v/K_v is a finite Galois extension. Show that we can find a finite Galois extension L/K such that for all $v \in S$ the completion of L with respect to any absolute value extending $|\ |_v$ is isomorphic to L_v over K_v. [Hint: show that we may suppose that K is infinite. For each $v \in S$ write $L_v = K_v(\alpha_v)$ and let $f_v \in K_v[X]$ denote the minimal polynomial of α_v. Let d denote the least common multiple of the degrees $[L_v : K_v]$. Show that we can find $\beta_i \in K$ so that

$$g_v(X) = \prod_{i=1}^{d/[L_v:K_v]} f_v(X + \beta_i)$$

has distinct roots. Take L to be the splitting field for a polynomial $g \in K[X]$ chosen to be sufficiently close to all the g_v.]