GLOBAL CLASS FIELD THEORY

1) Suppose $n \in \mathbb{Z}_{>0}$, K is a number field containing a primitive n^{th} root of 1 and that S is a finite set of places of K containing all infinite places and all places dividing n and such that S generates the class group of $\mathcal{O}_K$. Let $a \in K^\times$ and suppose that $K(a^{1/n})/K$ is unramified outside S. Show that $a \in \mathcal{O}_K[1/S]^\times (K^\times)^n$. [Hint: Show that $a = ub$ with $u \in \mathcal{O}_K[1/S]^\times$ and $b \in K^\times$ having numerator and denominator coprime to S. Then show that $b = vc^n$ with $v \in \mathcal{O}_K[1/S]^\times$ and $c \in K^\times$.]

2) Show that 16 is an 8^{th}-power in $\mathbb{Q}_v$ for all places $v \neq 2$ of $\mathbb{Q}$. [Hint: Show that $\mathbb{Q}(\sqrt{-1}, \sqrt{2})/\mathbb{Q}$ is unramified at all odd primes, and deduce that for all odd primes p, one of $1 + \sqrt{-1}$, $\sqrt{2}$ or $\sqrt{-2}$ lies in $\mathbb{Q}_p$.]

3) Let $G \supset H$ be finite groups and suppose that $G = \coprod_{r \in R} Hr$. Let $\mathfrak{a}_G$ denote the kernel of the homomorphism $\mathbb{Z}[G] \to \mathbb{Z}$, which sends $g \mapsto 1$ for all $g \in G$. If $g \in G$ and $r \in R$ write $Hrg = Hs(r, g)$, where $s(r, g) \in R$.

(a) Recall that by the transfer $\mathrm{tr} : G/[G, G] \to H/[H, H]$ we mean the dual of the corestriction map $H^1(H, \mathbb{Q}/\mathbb{Z}) \to H^1(G, \mathbb{Q}/\mathbb{Z})$.

(b) Show that their is an isomorphism of abelian groups $G/[G, G] \xrightarrow{\sim} \mathfrak{a}_G/\mathfrak{a}_G^2$ sending $g \mapsto g - 1$. Show moreover that the transfer map $\mathrm{tr} : G/[G, G] \to H/[H, H]$ corresponds to the composite

$$\mathfrak{a}_G/\mathfrak{a}_G^2 \xrightarrow{\mathrm{tr}_R} \mathfrak{a}_G/\mathfrak{a}_H\mathfrak{a}_G \xrightarrow{\theta_R} \mathfrak{a}_H/\mathfrak{a}_H^2,$$

where tr_R is induced by multiplication on the left by $\sum_{r \in R} r$ and where θ_R sends $hr - 1$ (with $h \in H$ and $r \in R$) to $h - 1$. [Remember to check that tr_R and θ_R are well defined.]

(c) Show that R is a $\mathbb{Z}$-basis of $\mathbb{Z}[G]/\mathfrak{a}_H\mathbb{Z}[G]$. If $\mu \in \mathbb{Z}[G]/\mathfrak{a}_H\mathbb{Z}[G]$ and $\mu\mathfrak{a}_G \subset \mathfrak{a}_H\mathbb{Z}[G]$ show that $\mu = \nu \sum_{r \in R} r$, for some $\nu \in \mathbb{Z}$.

(d) Show that $\mathbb{Z}[G]/\mathfrak{a}_{[G,G]}\mathbb{Z}[G]$ is abelian.

(e) Now suppose that $H = [G, G]$. Let $g_1, ..., g_t$ generate G. Then we get an induced map $\mathbb{Z}^t \twoheadrightarrow G/[G, G]$. Let $\vec{m}(1), ..., \vec{m}(t)$ be a basis of the kernel. Show that $\det(\vec{m}(i)_j) = [G : [G, G]]$.

Show also that we can find $\mu(i) \in \mathbb{Z}[G]^t$ with $\mu(i) \equiv \vec{m}(i) \bmod \mathfrak{a}_G^t$ and

$$\sum_j \mu(i)_j(g_j - 1) = 0$$

for $i = 1, ..., t$. Set $\mu = \det(\mu(i)_j) \in \mathbb{Z}[G]/\mathfrak{a}_{[G,G]}\mathbb{Z}[G]$. Show that $\mu \equiv [G : [G, G]] \bmod \mathfrak{a}_G$, that $\mu(g_i - 1) \in \mathfrak{a}_{[G,G]}\mathfrak{a}_G$ and that $\mu\mathfrak{a}_G \subset \mathfrak{a}_{[G,G]}\mathfrak{a}_G$.

Show that $\mu = \sum_{r \in R} r$. Conclude that $\mathrm{tr}_R = 0$ and hence that

$$\mathrm{tr} : G/[G, G] \to [G, G]/[[G, G], [G, G]]$$

is zero.

4) Let K be a number field and S a finite set of places of K. Suppose that for $v \in S$ we have a finite order continuous character $\chi_v : \mathrm{Gal}\,(\overline{K}_v/K_v) \to \mathbb{C}^\times$. Show that there is a finite order continuous character $\chi : \mathrm{Gal}\,(\overline{K}/K) \to \mathbb{C}^\times$ with $\chi|_{\mathrm{Gal}\,(\overline{K}_v/K_v)} = \chi_v$ for all $v \in S$. [Hint: We may assume that S contains all infinite places of K. Let χ_S denote the character $\prod_{v \in S} \chi_v \circ r_{K_v}$ of $K_S^\times$ and let n denote the order of its image. Choose an open subgroup U of $\prod_{v \notin S} \mathcal{O}_{K,v}^\times$ such that $U \cap \mathcal{O}_K[1/S]^\times \subset (\mathcal{O}_K[1/S]^\times)^n$. Choose a character χ^S of $\prod_{v \notin S} \mathcal{O}_{K,v}^\times$ such that $\chi^S|_{\mathcal{O}_K[1/S]^\times} = \chi_S|_{\mathcal{O}_K[1/S]^\times}^{-1}$. Consider the character

$$\chi_S \chi^S : (K_S^\times \prod_{v \notin S} \mathcal{O}_{K,v}^\times)/(\mathcal{O}_K[1/S]^\times (K_\infty^\times)^0) \longrightarrow \mathbb{C}^\times.]$$

5) Let K denote a number field. By an *ordered invertible $\mathcal{O}_K$-module* we mean a pair $(M, \{C_x\})$, where M is a torsion free $\mathcal{O}_K$-module with $M \otimes_{\mathcal{O}_K} K \cong K$, and where, for each real place x of K, C_x is a connected component of $M \otimes_{\mathcal{O}_K} K_x - \{0\}$. We will denote by $\mathrm{Cl}^+(K)$ (the *strict class group* of K) the set of isomorphism classes of ordered invertible $\mathcal{O}_K$-modules. Define

$$(M, \{C_x\}) \otimes (N\{D_x\}) = (M \otimes_{\mathcal{O}_K} N, \{C_x D_x\}),$$

where $C_x D_x$ denotes the set of $a \otimes b$ with $a \in C_x$ and $b \in D_x$. Show that $\otimes$ induces a product on $\mathrm{Cl}^+(K)$, which makes $\mathrm{Cl}^+(K)$ an abelian group isomorphic to

$$\mathbb{A}_K^\times/(K^\times (K_\infty^\times)^0 \prod_{v \not| \infty} \mathcal{O}_{K,v}^\times).$$

Also show that if H^+/K is the maximal abelian extension unramified at all finite places, then $\mathrm{Gal}\,(H^+/K) \cong \mathrm{Cl}^+(K)$.

6) Let I denote a non-zero ideal of $\mathcal{O}_K$. Denote by $K^{\equiv 1\,(I)}$ the subset of $K^\times$ consisting of elements of the form α/β where $\alpha, \beta \in \mathcal{O}_K$ and $\alpha - \beta \in I$ and $(\alpha) + I = (\beta) + I = \mathcal{O}_K$. Show that $K^{\equiv 1\,(I)}$ is a subgroup of $K^\times$. Let $\mathcal{I}^I$ denote the group of fractional ideals J of K with $v(J)v(I) = 0$ for all finite places v of K. Show that if $\alpha \in K^{\equiv 1\,(I)}$ then $\alpha\mathcal{O}_K \in \mathcal{I}^I$. Denote by $\mathrm{Cl}_I(K)$ (the *ray class group of K of conductor I*) the quotient of $\mathcal{I}^I$ by the subgroup of elements of the form $\alpha\mathcal{O}_K$ with $\alpha \in K^{\equiv 1\,(I)}$. Also let $U(I)$ denote the subgroup of $\prod_{v \not| \infty} \mathcal{O}_{K,v}^\times$ consisting of elements congruent to 1 modulo $I \prod_{v \not| \infty} \mathcal{O}_{K,v}$. Show that

$$\mathrm{Cl}_I(K) \cong \mathbb{A}_K^\times/(K^\times K_\infty^\times U(I)).$$

We say that a finite abelian extension L/K has conductor dividing I if for each finite place v of K and each place w of L above v the local Artin map

$$K_v^\times \twoheadrightarrow \mathrm{Gal}\,(L_w/K_v)$$

vanishes on the subgroup of $\mathcal{O}_{K,v}^\times$ consisting of elements congruent to 1 modulo $I\mathcal{O}_{K,v}$. Let H_I/K denote the maximal abelian extension of conductor I in which all infinite places split completely (the *ray class field of conductor* I). Show that H_I is well defined and that $\mathrm{Gal}\,(H_I/K)$ is isomorphic to $\mathrm{Cl}_I(K)$.

7) (a) Suppose that L/K is a finite cyclic extension of number fields. Show that $a \in K$ is a from L if and only if for each place w of L it is a norm for $L_w/K_{w|_K}$. [Hint: Consider the map $H^2(\mathrm{Gal}\,(L/K), L^\times) \to H^2(\mathrm{Gal}\,(L/K), \mathbb{A}_L^\times)$.]

(b) Let $L = \mathbb{Q}[\sqrt{13}, \sqrt{17}]$. Show that 2 is not a norm for $L/\mathbb{Q}$. Show however that it is a norm for $L_w/\mathbb{Q}_{w|_\mathbb{Q}}$ for each place w of L.

8) By a *quadratic form* in n-variables over a field K we shall mean a homogeneous polynomial of degree 2 in n-variables over K. Two quadratic forms are called *equivalent* if one can be changed into the other by an invertible linear change of variables. A quadratic form is said to *represent* $a \in K$ if it takes the value a at some *non-zero* point of K^n.

(a) Show that any quadratic form is equivalent to a diagonal quadratic form $a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2$. [Hint: Complete the square.]

(b) If two quadratic forms are equivalent, show that they represent the same elements of K.

(c) If $q(X_1, ..., X_n)$ is a quadratic form show that $q(X_1, ..., X_n)$ represents $a \in K^\times$ if and only if $q(X_1, ..., X_n) - aX_{n+1}^2$ represents zero.

(d) If $a, b \in K^\times$ show that $X_1^2 - aX_2^2 - bX_3^2$ represents zero if and only if $b \in \mathbf{N}_{K(\sqrt{a})/K}K(\sqrt{a})^\times$. [Hint: Consider separately the cases $a \in (K^\times)^2$ and $b \in (K^\times)^2$.]

(e) Suppose that $a, b, c \in K^\times$ and $X_1^2 - aX_2^2 - cX_3^2 + bcX_4^2$ represents zero at $(x_1, x_2, x_3, x_4) \in K^4$. If neither a nor b is a square in K, show that

$$c = \mathbf{N}_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})}((x_1 + x_2\sqrt{a})/(x_3 + x_4\sqrt{b})) \in \mathbf{N}_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})}K(\sqrt{a}, \sqrt{b})^\times.$$

If a or b is a square in K show that $X_1^2 - aX_2^2 - cX_3^2 + bcX_4^2$ represents zero and $c \in \mathbf{N}_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})}K(\sqrt{a}, \sqrt{b})^\times$.

(f) Conversely if $a, b, c \in K^\times$ and $c \in \mathbf{N}_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})}K(\sqrt{a}, \sqrt{b})^\times$, show that $X_1^2 - aX_2^2 - cX_3^2 + bcX_4^2$ represents zero. [Hint: Suppose first that $[K(\sqrt{a}, \sqrt{b}) : K] = 4$ and that $c = \mathbf{N}_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})}(x + y\sqrt{a} + z\sqrt{b} + w\sqrt{ab})$ with $x \neq 0$. Show that

$$c = \mathbf{N}_{K(\sqrt{a},\sqrt{b})/K(\sqrt{ab})}(x + y\sqrt{b})(x^2 - bz^2)/(x(x + z\sqrt{b})).$$

Deduce that $X_1^2 - aX_2^2 - cX_3^2 + bcX_4^2$ represents zero. Treat the other cases similarly.]

Now suppose that K is a number field and that $q(X_1, ..., X_n)$ is a quadratic form over K. In the rest of this question we will show that q represents zero over K if and only if it represents zero over K_v for every place v of K. We will argue by induction on n.

(g) Treat the case $n = 1$.

(h) Treat the case $n = 2$.

(i) Treat the case $n = 3$. Also show that in this case q represents zero in K_v for almost all v.

(j) Treat the case $n = 4$.

(k) Assume that $n \geq 5$ and that q represents zero in K_v for all places v of K. We will show (by induction) that q represents zero in K.

Reduce to the case $q(X_1, ..., X_n) = aX_1^2 + bX_2^2 - r(X_3, ..., X_n)$ with $a, b \in K^\times$. Show that there is a finite set S of places such that r represents zero in K_v for all $v \notin S$. For $v \in S$ show that there exist $x_1(v), x_2(v) \in K_v$ such that r represents $ax_1(v)^2 + bx_2(v)^2$ over K_v. Show that we may choose $x_1, x_2 \in K^\times$ such that

$$(ax_1^2 + bx_2^2)/(ax_1(v)^2 + bx_2(v)^2) \in (K_v^\times)^2$$

for all $v \in S$. Then show that

$$(ax_1^2 + bx_2^2)Y^2 - r(X_3, ..., X_n)$$

represents zero in K, and deduce that q does also.

9) Let K be a number field containing a primitive n^{th} root of unity. If v is a finite place of K recall (from last semester's examination) the pairing

$$\begin{array}{rcl} (\ ,\ )_v : K_v^\times \times K_v^\times & \longrightarrow & \mu_n(K) \\ (a, b) & \longmapsto & (da)(r_{K_v}(b)). \end{array}$$

where d denotes the boundary map

$$d : K_v^\times/(K_v^\times)^n \longrightarrow H^1(\mathrm{Gal}\,(\overline{K}_v/K_v), \mu_n(K_v)) = \mathrm{Hom}\,(\mathrm{Gal}\,(\overline{K}_v/K_v), \mu_n(K)).$$

Let S denote the set of finite places of K dividing n. If $a \in K^\times$ write $S(a)$ for the union of S with the set of places for which a has nontrivial valuation. Define a pairing

$$\begin{array}{rcl} (-) : K^\times \times (\mathbb{A}_K^{S\cup\infty})^\times & \longrightarrow & \mu_n(K) \\ (a, \beta) & \longmapsto & (da)(r_K(\beta))^{-1}. \end{array}$$

(a) If $\beta_v = 1$ for all $v \in S(a)$ show that $\left(\frac{a}{\beta}\right)$ depends only on $\beta\mathcal{O}_K$. We write $\left(\frac{a}{\beta\mathcal{O}_K}\right)$, the *power residue symbol.*

(b) If $K/\mathbb{Q}$ is Galois and $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q})$ show that

$$\sigma\left(\frac{a}{\beta}\right) = \left(\frac{\sigma a}{\sigma\beta}\right).$$

(c) Suppose that I is a nonzero (integral) ideal of $\mathcal{O}_K$ coprime to n. Suppose that $a, a' \in \mathcal{O}_K$ are coprime to nI and satisfy $a - a' \in I$. Show that

$$\left(\frac{a}{I}\right) = \left(\frac{a'}{I}\right).$$

[Hint: Suppose first that I is a prime ideal. Show that

$$\left(\frac{a}{I}\right) \equiv a^{(\#\mathcal{O}_K/I-1)/n} \bmod I.]$$

(d) If I is a nonzero prime ideal of $\mathcal{O}_K$ coprime to n and if $\zeta \in \mu_n(K)$, show that

$$\left(\frac{\zeta}{I}\right) = \zeta^{(\#\mathcal{O}_K/I-1)/n}.$$

[Hint: Use a similar method to part (c).]

(e) If $a, b \in K^\times$ and $S(a) \cap S(b) = S$ show that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} \prod_{v \in S} (b, a)_v = \prod_v (b, a)_v = 1.$$

[Hint: First reduce to the case $a, b \in \mathcal{O}_K$.] Deduce that

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in S} (a, b)_v.$$

[The *power residue law*.]

(f) In the case $K = \mathbb{Q}$ and $n = 2$ deduce the law of quadratic reciprocity. [Hint: Let p and q be distinct odd primes. If $p \equiv 1 \bmod 4$ show that $\mathbb{Q}_2(\sqrt{p})$ is unramified over $\mathbb{Q}_2$ and deduce that $(p, q)_2 = 1$. If $q \equiv 1 \bmod 4$, also show that $(p, q)_2 = 1$. If $p \equiv q \equiv -1 \bmod 4$, show that $\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2$ is ramified and that

$$r_{\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2} : \mathbb{Z}_2^\times \twoheadrightarrow \mathrm{Gal}\,(\mathbb{Q}_2(\sqrt{p})/\mathbb{Q}_2)$$

is non-trivial at q.]

10)[H.Lenstra and P.Stevenhagen's proof of Wieferich's criterion and Sophie Germain's theorem.] Suppose that p is an odd prime and that x, y, z are coprime rational integers with

$$x^p + y^p + z^p = 0$$

and $p \not| xyz$. Let ζ_p denote a primitive p^{th} root of unity.

(a) Show that

$$x + y\zeta_p \equiv (x + y)\zeta_p^{y/(x+y)} \bmod (\zeta_p - 1)^2.$$

Deduce that

$$(x + y\zeta_p)\zeta_p^{y/z}$$

is a p^{th}-power in $\mathbb{Z}_p[\zeta_p]^\times$.

(b) Show that if a prime $\wp$ divides two of the ideals $(x + y\zeta_p^i)$ for $i = 0, ..., p-1$ then $\wp | p$ and $\wp | z$. Deduce that $(x + y\zeta_p)$ is the p^{th} power of some ideal of $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$.

(c) Using the last question show that if a is a rational integer coprime to p and z then

$$\left(\frac{(x + y\zeta_p)\zeta_p^{y/z}}{a}\right) = 1.$$

(d) Suppose that $q|y$ is a prime. Show that $\left(\frac{x}{q}\right) \in \mathbb{Q}$, and hence that

$$1 = \left(\frac{x}{q}\right) = \left(\frac{\zeta_p}{q}\right)^{-y/z}.$$

(e) Show that $\left(\frac{\zeta_p}{q}\right) = \zeta_p^{(q^{p-1}-1)/p}$. Deduce that

$$q^{p-1} \equiv 1 \bmod p^2.$$

(f) Now suppose that $q = 2p + 1$ is prime. Show that $q \not| y$. On the other hand, considering $x^p + y^p + z^p = 0 \bmod q$, show that $q | xyz$.

(g) If p is an odd prime and $X^p + Y^p + Z^p = 0$ has a solution in integers x, y, z with $p \not| xyz$, show that $2^{p-1} \equiv 1 \bmod p^2$ (Wieferich's criterion, 1909) and that $2p+1$ is not prime (Sophie Germain's theorem, 1823).