Global Riemann-Roch formulas

Let K be a number field, $\Gamma = Gal(\bar{K}/K)$, M a finite Γ-module of exponent m; i.e. $mM = (0)$. If S is a finite set of places of K we let $\Gamma_S = Gal(K_S/K)$, where K_S is the union of all extensions of K in $\bar{K}$ that are unramified outside S. This is a much smaller group and the cohomology of such groups arises naturally in problems of arithmetic geometry. One cannot always calculate the Galois cohomology groups $H^i(\Gamma_S, M)$, but global class field theory imposes strong relations between the cohomology of M and the cohomology of $M^* = Hom(M, \mu_m)$, where μ_m is the group of m-th roots of unity in $\bar{K}$. It is natural to impose additional local conditions at the primes in S, and the cohomology groups with these conditions are called *Selmer groups* and are denoted $H^i_{\mathcal{D}}(K, M)$, the S being understood. We have already seen such groups as the cotangent spaces of deformation rings. The only interesting group is H^1. The corresponding group of cohomology of M^* is interpreted by Wiles as an error term, which he is able to eliminate by choosing appropriate local conditions. This should be compared to the use of the Riemann-Roch formula, where the error terms can also be eliminated to yield a much simpler result. In this section I derive the formula used by Wiles to control the size of Selmer groups. The result is an immediate consequence of class field theory, as interpreted by Tate and Poitou as a collection of local and global duality theorems. Complete proofs of the duality theorems are in Milne's book *Arithmetic Duality Theorems.*

In the applications it will suffice to take $m = \ell$ an *odd* prime, and we will make this hypothesis for simplicity. In this case, M and M^* are $\mathbb{F}_\ell$-vector spaces.

1. Tate's local duality.

Let M be a finite $\mathbb{F}_\ell[\Gamma]$-module, as in the above discussion. We let Γ act on $M^* = Hom(M, \mu_\ell)$ by

$$g\phi(m) = \omega_\ell(g)\phi(g^{-1}m))$$

where $\omega_\ell : \Gamma \rightarrow \mathbb{F}_\ell^\times = Aut(\mu_\ell)$ is the cyclotomic character.

Tate's local duality theorem. *Let v be a place of K, and let $\Gamma_v \subset \Gamma$ be a decomposition group at v, $I_v \subset \Gamma_v$ the inertia group.*

(a) *For all i, $H^i(\Gamma_v, M)$ is finite.*

(b) *For all integers m there are embeddings*

$$H^2(\Gamma_v, \mu_m) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

compatible with the inclusions $\mu_m \hookrightarrow \mu_n$ if $m \mid n$.

(c) *For $i = 0, 1, 2$ the cup product and (b) give rise to a perfect pairing*

$$H^i(\Gamma_v.M) \otimes H^{2-i}(\Gamma_v, M^*) \rightarrow H^2(\Gamma_v, M \otimes M^*) \rightarrow H^2(\Gamma_v, \mu_\ell) \hookrightarrow \mathbb{Q}/\mathbb{Z},$$

where the second arrow is induced from the natural contraction $M \otimes M^* \rightarrow \mu_\ell$.

(d) *Suppose v is a finite prime with residue field k_v. Then $H^i(\Gamma_v, M) = (0)$ for $i > 2$, and*

$$\dim H^1(\Gamma_v, M) = \dim H^0(\Gamma_v, M) + \dim H^2(\Gamma_v, M) + \dim M \otimes_{\mathbb{Z}} k_v.$$

In other words, the Euler characteristic $\chi_v(M) = h^0_v(M) - h^1_v(M) + h^2_v(M)$, in the obvious notation, is zero unless v divides ℓ.

(e) *If v is finite and prime to ℓ, then $H^1(\Gamma_v/I_v, M^{I_v})$ and $H^1(\Gamma_v/I_v, (M^*)^{I_v})$ are annihilators of each other under the pairing*

$$H^1(\Gamma_v, M) \otimes H^1(\Gamma_v, M^*) \to \mathbb{Q}/\mathbb{Z}.$$

If v is an archimedean prime, then Γ_v is a group of order 1 or 2 whose cohomology can (usually!) be calculated by hand.

Regarding the proofs: (b) is the usual calculation of the Brauer group. When $M = \mathbb{F}_\ell$ with trivial action then (c) is the cohomological formulation of local class field theory. One reduces to this case by restriction to the extension of K_v fixed by the subgroup of Γ_v that acts trivially on M.

2. Global Euler characteristic formulas.

In what follows, S is always a finite set of places of K containing all archimedean primes.

Global Euler characteristic formula. *Let M be a finite $\mathbb{F}_\ell[\Gamma_S]$-module, as above, and define*

$$\chi_S(M) = \dim H^0(\Gamma_S, M) - \dim H^1(\Gamma_S, M) + \dim H^2(\Gamma_S, M).$$

Assume S contains all primes of residue characteristic ℓ. Then

$$\chi_S(M) = \sum_{v \mid \infty} H^0(\Gamma_v, M) - \dim M \cdot [K : \mathbb{Q}].$$

A remark: since $H^3(\Gamma_S, M)$ does not generally vanish, the left hand side is not a true Euler characteristic. In particular, it is not additive in short exact sequences. However, the failure of additivity is exactly compensated by the first term on the right. If K is totally imaginary, $H^i(\Gamma_S, M)$ vanishes for $i > 2$ and both sides are additive, as expected. The proof is by a series of elementary reductions to the case $M = \mu_\ell$, where everything can be calculated explicitly in terms of groups of S-ideal classes and S-units.

Because the basis of our deformation theory is partially CM and partially totally real, reflecting the fact that we are deforming maps to the L-group of a unitary group, we will need a slight extension of the above formula.

Extended Euler characteristic formula. *Let K'/K be a finite Galois extension of degree prime to ℓ. Let S be a finite set of primes of K containing all primes of residue characteristic ℓ and all archimedean primes, and let K'_S be the maximal extension of K' unramified outside S. Thus K'_S is Galois over K, with Galois group Γ'_S. Let M be a finite $\mathbb{F}_\ell[\Gamma'_S]$-module, and define*

$$\chi'_S(M) = \dim H^0(\Gamma'_S, M) - \dim H^1(\Gamma'_S, M) + \dim H^2(\Gamma'_S, M).$$

Then

$$\chi'_S(M) = \sum_{v \mid \infty} H^0(\Gamma_v, M) - \dim M \cdot [K : \mathbb{Q}],$$

where the sum on the right is over archimedean places of K.

3. Poitou-Tate global duality.

The most efficient summary of the duality between the cohomology of a finite Γ_S module M and that of its dual M^* is contained in the *nine term exact sequence* of Poitou-Tate, proved as Theorem 4.10 in Milne's book. To state the theorem, we need to introduce the modified cohomology groups $H^{0,+}(\Gamma_v, M)$: $H^{0,+}(\Gamma_v, M) = 0$ if v is archimedean, and $H^{0,+}(\Gamma_v, M) = H^0(\Gamma_v, M)$ if v is finite.

Theorem (nine term exact sequence). *Let Let S be a finite set of primes of K containing all primes of residue characteristic ℓ and all archimedean primes, and write $S = S_f \coprod S_\infty$, where S_f is the subset of finite primes, S_∞ that of archimedean primes. Let M be a finite $\mathbb{F}_\ell\Gamma_S$-module. Then there is an exact sequence of finite groups*

$$\begin{array}{ccccccccc} 0 & \to & H^0(\Gamma_S, M) & \to & \oplus_{v\in S} H^{0,+}(\Gamma_v, M) & \to & H^2(\Gamma_S, M^*)^\vee & & \\ & & & & & & \downarrow & & \\ & & H^1(\Gamma_S, M^*)^\vee & \leftarrow & \oplus_{v\in S} H^1(\Gamma_v, M) & \leftarrow & H^1(\Gamma_S, M) & & \\ & & \downarrow & & & & & & \\ & & H^2(\Gamma_S, M) & \to & \oplus_{v\in S} H^2(\Gamma_v, M) & \to & H^0(\Gamma_S, M^*)^\vee & \to & 0 \end{array}$$

The analogous sequence is valid for M of any exponent m, with a slightly more complicated statement when m is divisible by 2.

4. Selmer groups.

We let S be as above. For each $v \in S$, we choose a subspace $L_v \subset H^1(\Gamma_v, M)$ with the property that, for all finite $v \notin S$, $L_v = H^1(\Gamma_v/I_v, M^{I_v})$. The collection of these L_v is denoted $\mathcal{S}$. We define the *Selmer group* $H^1_{\mathcal{S}}$ by the short exact sequence

$$0 \to H^1_{\mathcal{S}}(K, M) \to H^1(\Gamma_S, M) \to \bigoplus_{v\in S} H^1(\Gamma_v, M)/L_v. \tag{4.1}$$

"Weak Mordell-Weil theorem". $H^1(\Gamma_S, M)$ *is finite.*

This is proved by Kummer theory or by global class field theory in the usual way. It follows that the Selmer group $H^1_{\mathcal{S}}(K, M)$ is also finite.

For any $v \in S$, we define a subspace $L_v^\perp \subset H^1(\Gamma_v, M^*)$ by duality: $L_v^\perp$ is the annihilator of L_v under the Tate local duality pairing. Thus we have a Selmer group $H^1_{\mathcal{S}^*}(K, M^*)$ defined by means of the $L_v^\perp$.

Lemma. *For all finite $v \notin S$, we have*

$$\chi_{\mathcal{S},v}(M) = \dim L_v - \dim H^0(\Gamma_v, M) = 0.$$

Proof. By hypothesis, $L_v = H^1(\Gamma_v/I_v, M^{I_v})$. The Lemma thus follows from the exact sequence

$$0 \to H^0(\Gamma_v, M) \to M^{I_v} \xrightarrow{F_v - 1} M^{I_v} \to H^1(\Gamma_v/I_v, M^{I_v}) \to 0.$$

Here F_v is Frobenius at v and the isomorphism $M^{I_v}/(F_v - 1)M^{I_v} \xrightarrow{\sim} H^1(F_v^{\hat{\mathbb{Z}}}, M^{I_v})$ is periodicity of (Tate) cohomology of cyclic groups.

With this Lemma in hand, the expression on the right-hand side of the following equality makes sense. We write h^i for $\dim H^i$. Let S_f be the set of finite places in S and S_∞ the set of archimedean places of K. For $v \in S_f$ define $\chi_{\mathcal{S},v}(M)$ as above. For $v \in S_\infty$ we set $\chi_{\mathcal{S},v}(M) = \dim H^0(\Gamma_v, M^*) - \dim M[K_v; \mathbb{R}]$. This is easily seen to equal $-\dim H^0(\Gamma_v, M)$: if v is complex this is clear, whereas if v is real then $c \in \Gamma_v$ acts by -1 on μ_ℓ, whence the claim follows. Since $L_v = H^1(\Gamma_v, M) = 0$ (since ℓ is odd) the notation is consistent.

Riemann-Roch formula. *Under the above hypotheses, we have the following equality:*

$$h^1_{\mathcal{S}}(K,M) - h^1_{\mathcal{S}^*}(K,M^*) = h^0(\Gamma_K, M) - h^0(\Gamma_K, M^*) + \sum_v \chi_{\mathcal{S},v}(M)$$

By the lemma, the sum over v is actually a sum over $v \in S$.

Proof. The exact sequence (4.1), applied to M^* and $\mathcal{S}^*$, is

$$0 \to H^1_{\mathcal{S}^*}(K,M^*) \to H^1(\Gamma_S, M^*) \to \bigoplus_{v \in S_f} H^1(\Gamma_v, M^*)/L_v^\perp,$$

where we can ignore the $H^1(\Gamma_v, *)$ for $v \in S_\infty$. Dualizing this sequence, we find

$$\bigoplus_{v \in S_f} L_v \to H^1(\Gamma_S, M^*)^\vee \to H^1_{\mathcal{S}^*}(K,M^*)^\vee \to 0 \tag{4.2}$$

Now take the first six terms of the nine term exact sequence, but with the local groups $H^1(\Gamma_v, M)$ replaced by L_v :

$$\begin{array}{ccccccc} 0 & \to & H^0(\Gamma_S, M) & \to & \oplus_{v \in S_f} H^0(\Gamma_v, M) & \to & H^2(\Gamma_S, M^*)^\vee \\ & & & & & & \downarrow \\ & & H^1(K,M^*)^\vee & \leftarrow & \oplus_{v \in S_f} L_v & \leftarrow & H^1_{\mathcal{S}}(K,M) \end{array}$$

Completing this with (4.2) we obtain

$$\begin{array}{ccccccc} 0 & \to & H^0(\Gamma_S, M) & \to & \oplus_{v \in S} H^0(\Gamma_v, M) & \to & H^2(\Gamma_S, M^*)^\vee \\ & & & & & & \downarrow \\ 0 \leftarrow H^1_{\mathcal{S}^*}(K,M^*)^\vee & \leftarrow & H^1(\Gamma_S, M^*)^\vee & \leftarrow & \oplus_{v \in S_f} L_v & \leftarrow & H^1_{\mathcal{S}}(K,M) \end{array}$$

The alternating sum of dimensions of the terms in this sequence equals zero, thus

$$\begin{aligned} & h^1_{\mathcal{S}}(K,M) - h^1_{\mathcal{S}^*}(K,M^*) \\ & = h^0(\Gamma_S, M) - \sum_{v \in S_f} [\dim L_v - h^0(\Gamma_v, M)] + h^2(\Gamma_S, M^*) - h^1(\Gamma_S, M^*) \\ & = h^0(\Gamma_S, M) - h^0(\Gamma_S, M^*) + \chi_S(M^*) + \sum_{v \in S_f} \chi_{\mathcal{S},v}(M). \end{aligned}$$

Now we apply the Euler characteristic formula to calculate $\chi_S(M^*)$

$$\chi_S(M^*) = \sum_{v \mid \infty} h^0(\Gamma_v, M^*) - \dim M \cdot [K:\mathbb{Q}] = \sum_{v \in S_\infty} \chi_{\mathcal{S},v}(M).$$

Thus

$$h^1_{\mathcal{S}}(K,M) - h^1_{\mathcal{S}^*}(K,M^*) = h^0(\Gamma_S, M) - h^0(\Gamma_S, M) + \sum_{v \in S} \chi_{\mathcal{S},v}(M)$$

which concludes the proof.

5. The basic numerical coincidence.

Now we assume K is a totally real field. For each real v, let σ_v be a corresponding complex conjugation in $Gal(\overline{\mathbb{Q}}/K$. Let S_ℓ be the subset of S of all primes of K dividing ℓ. In this section we indicate how the above formula simplifies if we make certain assumptions on the local terms for $v \in S_\ell \cup S_\infty$.

5.1 Numerical hypotheses.

(1) *For all $v \in S_\ell$,*

$$\dim L_v - \dim_k H^0(\Gamma_v, M) = n(n-1)[K_v : \mathbb{Q}_\ell]/2.$$

(2) *For all $v \mid \infty$, there is a constant $c_v = \pm 1$ such that, ,*

$$\dim H^0(\Gamma_v, M) = \dim(M)^{\sigma_v = 1} = n(n-1)/2 + n\frac{1+c_v}{2}.$$

By (1),

$$\sum_{v \in S_\ell} \chi_{\mathcal{S},v}(M) = \frac{n(n-1)}{2} \sum_{v \in S_\ell} [K_v : \mathbb{Q}_\ell] = \frac{n(n-1)}{2}[K : \mathbb{Q}]. \tag{5.2}$$

By (2),
(5.3)

$$\sum_{v \in S_\infty \chi_{\mathcal{S},v}(M)} = -|S_\infty|\frac{n(n-1)}{2} - n \cdot \sum_{v \in S_\infty} \frac{1+c_v}{2} = -\frac{n(n-1)}{2}[K : \mathbb{Q}] - n \cdot \sum_{v \in S_\infty} \frac{1+c_v}{2}.$$

The contribution of S_ℓ compensates the main part of the contribution of S_∞, and the Riemann-Roch formula simplifies:
(5.4)

$$h^1_{\mathcal{S}}(K, M) - h^1_{\mathcal{S}^*}(K, M^*) = h^0(\Gamma_K, M) - h^0(\Gamma_K, M^*) + \sum_{v \in S_f \setminus S_\ell} \chi_{\mathcal{S},v}(M) - n \cdot \sum_{v \in S_\infty} \frac{1+c_v}{2}.$$

This is the form in which the Euler characteristic formula will be applied. In practice the two global terms $h^0(\Gamma_K, M)$ and $h^0(\Gamma_K, M^*)$ vanish. The basis of the Taylor-Wiles method is to choose $\mathcal{S}$ so that so that $h^1_{\mathcal{S}^*}(K, M^*) = 0$. Then the interesting dimension $h^1_{\mathcal{S}}(K, M)$ is expressed entirely in terms of local $\chi_{\mathcal{S},v}(M)$ that can be scrupulously controlled, as well as a sum $n \cdot \sum_{v \in S_\infty} \frac{1+c_v}{2}$ that will ultimately be forced to vanish. In subsequent lectures I will explain when the hypotheses 5.1 are valid.