On a result of Soulé

Romyar Sharifi

Spring 2000

Let G_S denote the Galois group of the maximal extension of $\mathbf{Q}$ unramified outside the prime 2. Our aim is to prove the following theorem.

Theorem 1. *Let r be a nonzero integer. Then we have*

$$H^1(G_S, \mathbf{Q}_2(r)) \cong \begin{cases} \mathbf{Q}_2 & \text{if } r \text{ is odd} \\ 0 & \text{if } r \text{ is even} \end{cases} \tag{1}$$

and $H^2(G_S, \mathbf{Q}_2(r)) = 0$.

Soulé proved the statement of Theorem 1 for all odd primes p and r any positive integer using Chern characters in higher algebraic K-theory [2, 3]. Jannsen [1] has remarked that Theorem 1 holds in the stated case $p = 2$ (at least for the first cohomology groups), though we have not seen a proof written out anywhere. The proof we give here uses only Galois cohomology and number theory, which is made possible by the fact that 2 is a regular prime.

Fix a positive integer $n \geq 3$. Set $F = \mathbf{Q}(\zeta_{2^n})$, where ζ_{2^n} is a primitive 2^nth root of unity. Let H_S denote the Galois group of the maximal extension of F unramified outside the unique prime $1 - \zeta_{2^n}$ above 2. Set $N = \mathrm{Gal}(F/\mathbf{Q})$. Then $N \cong \Delta \oplus \Gamma$ where Δ is the group of order two generated by the image σ of complex conjugation and Γ is the cyclic group of order 2^{n-2} generated by an element τ such that $\tau(\zeta_{2^n}) = \zeta_{2^n}^{-3}$.

Lemma 2. *Let $U = U_S/U_S^{2^n}$, where U_S denotes the group of units of F unramified outside $1 - \zeta_{2^n}$. Then there is an exact sequence*

$$1 \to \mu_{2^n} \to U \to \mathbf{Z}/2^n\mathbf{Z}[\Gamma] \to 0$$

of N-modules, where Δ acts trivially on $\mathbf{Z}/2^n\mathbf{Z}[\Gamma]$.

Proof. The group U_S is generated as an N-module by $\lambda_n = 1 - \zeta_{2^n}$. Note that $\sigma(\lambda_n)/\lambda_n = -\zeta_{2^n}$. Hence the submodule $(\sigma - 1)U$ of U is isomorphic to μ_{2^n}. The quotient $U/(\sigma - 1)U$ is necessarily isomorphic to a quotient A of $\mathbf{Z}/2^n\mathbf{Z}[\Gamma]$, and we remark that $\log_{2^n} |\mathbf{Z}/2^n\mathbf{Z}[\Gamma]| = 2^{n-2}$. Dirichlet's Unit Theorem says that $\log_{2^n} |U| = 2^{n-2} + 1$. Hence $A \cong \mathbf{Z}/2^n\mathbf{Z}[\Gamma]$. ∎

Note that Lemma 2 says that

$$U \cong \mathbf{Z}/2^n\mathbf{Z}[N]/((\sigma-1)(\tau+3)). \tag{2}$$

We will generally identify U with this module when considering elements of it. We remark that $H^1(H_S, \mathbf{Z}/2^n\mathbf{Z}(r)) \cong U(r-1)$, as 2 is a regular prime. We will now compute the invariants of this group under N.

Proposition 3. *We have that*

$$H^0(N, U(r-1)) \cong \begin{cases} [\mathbf{Z}/2^n\mathbf{Z}(r)]^\Gamma \oplus \mathbf{Z}/2\mathbf{Z} & \text{if } r \text{ is even} \\ \mathbf{Z}/2^{n-1}\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} & \text{if } r \text{ is odd.} \end{cases}$$

Proof. We remark first that

$$H^0(N, \mathbf{Z}/2^n\mathbf{Z}(r)) \cong \begin{cases} [\mathbf{Z}/2^n\mathbf{Z}(r)]^\Gamma & \text{if } r \text{ is even} \\ \mathbf{Z}/2\mathbf{Z} & \text{if } r \text{ is odd.} \end{cases} \tag{3}$$

Next we remark that

$$H^0(\Gamma, \mathbf{Z}/2^n\mathbf{Z}[\Gamma](r-1)) \cong \mathbf{Z}/2^n\mathbf{Z}(r-1)$$

as Δ modules (generated by $N_r = \sum(-3)^{i(r-1)}\tau^i$) and hence

$$H^0(N, \mathbf{Z}/2^n\mathbf{Z}[\Gamma](r-1)) \cong \begin{cases} \mathbf{Z}/2\mathbf{Z} & \text{if r is even} \\ \mathbf{Z}/2^n\mathbf{Z} & \text{if r is odd.} \end{cases} \tag{4}$$

We now consider the exact sequence

$$0 \to [\mathbf{Z}/2^n\mathbf{Z}(r)]^N \to U(r-1)^N \xrightarrow{j} [\mathbf{Z}/2^n\mathbf{Z}[\Gamma](r-1)]^N \xrightarrow{d} H^1(N, \mathbf{Z}/2^n\mathbf{Z}(r)),$$

which we have from Lemma 2. We claim that j is either surjective or has cokernel of order 2, which is obvious from (4) if r is even. We consider $\mathbf{Z}/2^n\mathbf{Z}[\Gamma]$ as a subgroup of U via the isomorphism (2). When r is odd, we see that $x \in [\mathbf{Z}/2^n\mathbf{Z}[\Gamma](r-1)]^N$ implies $(\sigma+1)x \in U(r-1)^N$ and hence

$$j((\sigma+1)x) = 2x.$$

If $x \in [\mathbf{Z}/2^n\mathbf{Z}[\Gamma](r-1)]^N$ then $dx(\tau) = 0$ by definition, and $dx(\sigma) = ((-1)^{r-1}\sigma - 1)x$ inside $U(r-1)$. If r is odd then we must consider $x = N_r$, and we see easily that $dx(\sigma) = -2^{n-2}(\sigma-1)$ considered as an element of $U(r-1)$, or $dx(\sigma) = -2^{n-2}$ considered as an element of $\mathbf{Z}/2^n\mathbf{Z}(r-1)$. Furthermore, we must view the cochains in the image of d modulo coboundaries. So note that for $a \in \mathbf{Z}/2^n\mathbf{Z}(r)$ we have $\tau(a) - a = 0$ if and only if $a \equiv 0 \bmod 2^{n-2}$. In this case $\sigma(a) - a = -2a \equiv 0 \bmod 2^{n-1}$. Hence we see that when r is odd, the image of d has order 2, and we therefore conclude the same about the cokernel

of j. If r is even, then we must consider $x = 2^{n-1}N_r$, and it is easy enough to see that $dx(\sigma) = 0$, so the cokernel of j is trivial.

Let J denote the image of j. To finish the proof of the proposition, it remains to show that the sequence

$$0 \to [\mathbf{Z}/2^n\mathbf{Z}(r)]^N \to U(r-1)^N \to J \to 0$$

splits. To see this, we lift any element x of J lifts to an element $x \in \mathbf{Z}/2^n\mathbf{Z}[\Gamma] \subset U(r-1)$ in the obvious way, and then $a + x \in U(r-1)^N$ for some $a \in [\mathbf{Z}/2^n\mathbf{Z}(r)]^\Gamma$. Noting equation (3), this immediately yields the splitting when r is even. When r is odd, we must have $a \equiv 0 \bmod 2^{n-2}$ in order that a be fixed under Γ, in which case $2^{n-1}(a+x) = 0$ for $n \geq 3$, and hence we have the splitting. □

We now prove Theorem 1.

Proof of Theorem 1. Recall that r denotes a nonzero integer. We have the following sequence of low degree terms in a Hochschild-Serre spectral sequence

$$0 \to H^1(N, \mathbf{Z}/2^n\mathbf{Z}(r)) \to H^1(G_S, \mathbf{Z}/2^n\mathbf{Z}(r)) \to H^1(H_S, \mathbf{Z}/2^n\mathbf{Z}(r))^N \to H^2(N, \mathbf{Z}/2^n\mathbf{Z}(r)).$$

Furthermore, the orders of the first and last of these groups are bounded with respect to n (note N varies with n). This follows by use of the spectral sequence

$$H^s(\Delta, H^t(\Gamma, \mathbf{Z}/2^n\mathbf{Z}(r))) \Rightarrow H^{s+t}(N, \mathbf{Z}/2^n\mathbf{Z}(r)).$$

The orders of the groups $H^i(N, \mathbf{Z}/2^n\mathbf{Z}(r))$ are bounded by the product of the orders of a finite number of terms in this sequence. All of these terms are cyclic of bounded order.

Let $h_i(n) = \log_2 |H^i(G_S, \mathbf{Z}/2^n\mathbf{Z}(r))|$ and let $H^i = H^i(G_S, \mathbf{Q}_2/\mathbf{Z}_2(r))$ for $0 \leq i \leq 2$. By Proposition 3, we conclude that as n varies, $H^1(G_S, \mathbf{Z}/2^n\mathbf{Z}(r))$ is the direct sum of a cyclic group of increasingly large order with a group of bounded order when r is odd and is a group of bounded order when r is even. From this, we have immediately that

$$\lim_{n\to\infty} \frac{h_1(n)}{n} = \begin{cases} 1 & \text{if } r \text{ is odd} \\ 0 & \text{if } r \text{ is even.} \end{cases}$$

We also remark that $H^1(G_S, \mathbf{Z}/2^n\mathbf{Z}(r))$ surjects onto the 2^n-torsion of H^1 with kernel isomorphic to the finite cyclic group $H^0(G_S, \mathbf{Q}_2/\mathbf{Z}_2(r))$ for large n [4, 5]. Hence the divisible part of H^1 is isomorphic to $\mathbf{Q}_2/\mathbf{Z}_2$ if r is odd and is trivial if r is nonzero even. But the dimension of the divisible part of H^1 is exactly the dimension of $H^1(G_S, \mathbf{Q}_2(r))$ as a $\mathbf{Q}_2$-vector space [1], and therefore $H^1(G_S, \mathbf{Q}_2(r))$ is exactly as stated in the theorem.

Now consider the partial Euler-Poincaré characteristic

$$\chi(n) = h_0(n) - h_1(n) + h_2(n).$$

Via Tate-Poitou duality [6], we have also

$$\chi(n) = \log_2(|\mathbf{Z}/2^n\mathbf{Z}(r)|^{-1}|\mathbf{Z}/2^n\mathbf{Z}(r)|^\Delta) = \begin{cases} 1-n & \text{if } r \text{ is odd} \\ 0 & \text{if } r \text{ is even.} \end{cases}$$

Now let

$$A = \lim_{n\to\infty} \frac{\chi(n)}{n} = \begin{cases} -1 & \text{if } r \text{ is odd} \\ 0 & \text{if } r \text{ is even.} \end{cases}$$

As

$$\lim_{n\to\infty} \frac{h_0(n)}{n} = 0 \qquad \text{and} \qquad \lim_{n\to\infty} \frac{h_1(n)}{n} = -A,$$

we see that

$$\lim_{n\to\infty} \frac{h_2(n)}{n} = 0.$$

Since $H^2(G_S, \mathbf{Z}/2^n\mathbf{Z}(r))$ surjects onto the 2^n torsion of H^2, we conclude that the divisible part of H^2 is zero. Hence $H^2(G_S, \mathbf{Q}_2(r)) = 0$. □

References

[1] U. Jannsen, "On the structure of Galois groups as Galois modules," Number theory, Noordwijkerhout 1983, Lecture Notes in Math. 1068, Springer, 1984, 109–126.

[2] C. Soulé, "K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale," *Inventiones Mathematicae* **55** (1979), 251–295.

[3] C. Soulé, "On higher p-adic regulators," Lecture Notes in Math. **854** (1981), Springer, 372–401.

[4] P. Schneider, "Über gewisse Galoiscohomologiegruppen," *Math Z.* **168** (1979), no. 2, 181–205.

[5] R. Sharifi, "Twisted Heisenberg Representations and Local Conductors," University of Chicago Ph.D. Thesis, June 1999.

[6] J. Tate, "Duality theorems in Galois cohomology over number fields," Proceedings of the International Congress of Mathematicians (Stockholm 1962), 288–295.