PACIFIC JOURNAL OF MATHEMATICS
Vol. 181, No. 3, 1997

A GENERALIZATION OF A RESULT OF SINNOTT

H. Kisilevsky

To the memory of Olga Taussky-Todd,
a friend, a collegue and an inspiration

1. Sinnott's Theorem.

Let p be a prime number and suppose that Γ is a pro-p-group isomorphic to $\mathbb{Z}_p$, the additive group of p-adic integers. For each integer n, let $\Gamma_n = p^n\Gamma$ and $G_n = \Gamma/\Gamma_n$.

Let A be a discrete Γ-module and define

$$A_n = A^{\Gamma_n} = \{a \in A \mid \gamma(a) = a \quad \text{for all} \quad \gamma \in \Gamma_n\}.$$

Then $A = \cup A_n$.

Proposition 1. *If A_n is finite for all n, then*

$$|A_{n+1}| \equiv |A_n| \pmod{p^{n+1}}.$$

Proof. A_{n+1} is a finite G_{n+1}-module so that

$$A_{n+1} = B \cup C$$

where B is the set of those elements in A_{n+1} not fixed by any non-trivial element of G_{n+1}, and $C = A_{n+1} \setminus B$. Since G_{n+1} is a cyclic group it follows that every element of C is fixed by the the subgroup of order p in G_{n+1}, and so $C \subseteq A^{\Gamma_n} = A_n$. The opposite inclusion is clear so $C = A_n$. Counting we have,

$$|A_{n+1}| = |B| + |A_n|.$$

Since B is a union of orbits each of which contains p^{n+1} elements it follows that

$$|A_{n+1}| \equiv |A_n| \pmod{p^{n+1}}.$$

$\square$

Corollary 1. *If A_n is finite for all n, then $\lim_{n\to\infty} |A_n|$ exists p-adically.*

Proof. It follows from Proposition 1 that for all $m \geq n$

$$|A_m| \equiv |A_n| \pmod{p^{n+1}}.$$

Hence the sequence $\{|A_n|\}_{n=1,2,\ldots}$ is a p-adic Cauchy sequence and therefore has a p-adic limit. □

Let k_∞/k be a $\mathbb{Z}_p$-extension of number fields (resp. function fields over finite fields) and denote by C_n the ideal class group (resp. the group of divisor classes of degree zero) of the n^{th}-layer k_n of k_∞/k. For any set S of prime numbers, finite or infinite, let $C_n(S)$ be the largest subgroup of C_n whose order is divisible only by primes in S. Let

$$C(S) = \varinjlim C_n(S)$$

be the direct limit with respect to the natural maps induced by extension of ideals.

We obtain the following generalization of a result of Sinnott (proved in the case of a cyclotomic $\mathbb{Z}_p$-extension of a CM ground field and for the "minus" class number).

Corollary 2 (Sinnott [**S**]). *Let k_∞/k be a $\mathbb{Z}_p$-extension of the global field k. For any set of prime numbers S, if $p \notin S$, then $\lim_{n\to\infty} |C_n(S)|$ exists p-adically.*

Proof. Since $p \notin S$ it follows that for $n \leq m$, the natural map $C_n(S) \longrightarrow C_m(S)$ is an injection. Then $C(S) = \cup C_n(S)$ and

$$C_n(S) = C(S)^{\Gamma_n}.$$

The result then follows from Proposition 1. □

Remark. It is a consequence of Iwasawa theory that $\lim_{n\to\infty} |C_n(S)|$ exists p-adically for *any* set S of primes.

Corollary 3 (Washington [**W**]). *Let k_∞/k be a $\mathbb{Z}_p$-extension of global fields and let l be a prime $l \neq p$. Take $S = \{l\}$ so that $C_n(S)$ is the l-primary part of the class group of k_n. If $|C_n(S)| = l^{a_n}$, then either $\{a_n\}$ is eventually constant or else there is a constant c, independent of n such that $a_n \geq cp^n$ for infinitely many n.*

Proof. It follows from Proposition 1 that

$$l^{a_{n+1}} \equiv l^{a_n} \pmod{p^{n+1}}$$

and therefore $a_{n+1} - a_n$ is divisible by the order of $l \pmod{p^{n+1}}$. For large n this order is cp^n for some constant c (depending only on l) hence either $\{a_n\}$ is eventually constant or else $a_n \geq cp^n$ for infinitely many n. □

2. Function fields.

Let k_∞/k be the constant $\mathbb{Z}_p$-extension of the function field k, and let h_n be the number of divisor classes of degree zero (the class number) of the n^{th} layer k_n. Denote by h'_n the "prime-to-p" part of h_n so that $h'_n = h_n/p^{e_n} = h_n(S)$ where S is the set of all primes other than p, and e_n is the largest power of p in h_n. Then h_n is given by

$$h_n = \prod_{i=1}^{2g}(1-\alpha_i^{p^n}) = p^{e_n}h'_n$$

where

$$\zeta_k(s) = Z_k(t) = \frac{\prod(1-\alpha_i t)}{(1-t)(1-qt)}$$

is the ζ-function of k, $q = p^f$ is the order of the finite field of k, and $t = q^{-s}$. The numbers α_i are algebraic integers with $\alpha_i\overline{\alpha}_i = q$.

Let $K = \mathbb{Q}(\alpha_1, \dots, \alpha_{2g})$ be the field generated over the rational field $\mathbb{Q}$ by the reciprocal roots of $Z_k(t)$, and fix $\mathcal{P}$ a prime ideal of K dividing p. We compute the $\mathcal{P}$-adic limit $\lim_{n\to\infty} h'_n$ in a completion $K_\mathcal{P}$ of K. Note that if α_i is not a $\mathcal{P}$-unit then

$$\lim_{n\to\infty}(1-\alpha_i^{p^n}) = 1,$$

and hence

$$\lim_{n\to\infty} h'_n = \lim_{n\to\infty} h_n/p^{e_n} = \lim_{n\to\infty} p^{-e_n}\prod{}^{\circ}(1-\alpha_i^{p^n})$$

where the product is taken over those i such that α_i is a $\mathcal{P}$-unit. Observe also that if α is a 1-unit, (i.e., if α is congruent to 1 mod $\mathcal{P}$), then we can define u_n by the equation

$$\alpha^{p^n} = 1 + p^n u_n.$$

Taking p-adic logarithms we find,

$$p^n \log_p \alpha = p^n u_n - p^{2n}u_n^2/2 + \cdots$$

so

$$u_n \equiv \log_p \alpha \pmod{p^n}.$$

Now

$$p^{-e_n}\prod{}^{\circ}(1-\alpha_i^{p^n}) = p^{-e_n}\prod{}'(1-\alpha_i^{p^n})\cdot\prod{}''(1-\alpha_i^{p^n})$$

where the product $\prod'$ is taken over those i such that α_i is a 1-unit, and $\prod''$ is taken over those i such that α_i is a $\mathcal{P}$-unit but not a 1-unit. Let $\nu_i \in \mathbb{Q}$

be the p-adic valuation of $\log \alpha_i$. Let λ be the number of i such that α_i is a 1-unit. Since h'_n is prime to p, it follows that

$$e_n = \lambda n + \sum_{i=1}^{\lambda} \nu_i,$$

for all sufficiently large n, and that

$$\lim_{n\to\infty} p^{-e_n} {\prod}'(1-\alpha_i^{p^n}) = (-1)^{\lambda} \frac{\prod' \log_p \alpha_i}{p^{\sum \nu_i}}.$$

Since $\lim_{n\to\infty} h'_n$ and $\lim_{n\to\infty} p^{-e_n} \prod'(1-\alpha_i^{p^n})$ exist p-adically, it follows that

$$\lim_{n\to\infty} {\prod}''(1-\alpha_i^{p^n})$$

exists.

For any unit $\beta \in K_{\mathcal{P}}$

$$\beta = \omega(\beta) \cdot \langle \beta \rangle$$

where $\omega(\beta)$ is a root of unity of order dividing $p^r - 1$ with $p^r = N_{K/\mathbb{Q}}(\mathcal{P})$ and $\langle \beta \rangle$ a 1-unit. It is then clear that

$$\omega(\beta) = \lim_{n\to\infty} \beta^{p^{rn}}.$$

Since the limit $\lim_{n\to\infty} \prod''(1-\alpha_i^{p^n})$ exists, it can be computed by letting n run through multiples of r, and we obtain the following:

Proposition 2. *For the constant $\mathbb{Z}_p$-extension of function fields we have*

$$\lim_{n\to\infty} h'_n = (-1)^{\lambda} \cdot \frac{\prod' \log_p \alpha_i}{p^{\sum \nu_i}} \cdot {\prod}''(1-\omega(\alpha_i)).$$

Corollary 4. *For the constant $\mathbb{Z}_p$-extension of function fields and for any integer j,*

$${\prod}''(1-\omega(\alpha_i)) = {\prod}''(1-\omega^j(\alpha_i)).$$

This can be proved directly using the fact that $Z_k(t)$ is a rational function in $\mathbb{Q}(t)$.

References

[S] W. Sinnott, *Talk given at Iwasawa Conference*, MSRI, 1985.

[W] L.C. Washington, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math., **49**(**1**) (1978), 87-97.

This work was supported in part by grants from NSERC and FCAR.

Concordia University
1455 de Maisonneuve Blvd. West
Montréal, Quebec, H3G 1M8, CANADA
E-mail address: kisilev@cicma.concordia.ca