Trends in Mathematics - New Series
Information Center for Mathematical Sciences
Volume 11, Number 2, 2009, pages 9-13

ASARC Workshop
Daecheon & Muju 2009

ON THE IDEAL CLASS GROUPS FOR CYCLOTOMIC FIELDS

SEY YOON KIM

Abstract. Let p be an odd prime number, and put $K := \mathbb{Q}(e^{2\pi i/p})$. We shall review the basic structure of the Sylow p-subgroup of the ideal class group for the number field $\mathbb{Q}(e^{2\pi i/p})$ regarded as a $\mathbb{F}_p[\mathrm{Gal}(K/\mathbb{Q})]$-module, and recall Vandiver's conjecture. Then we shall consider a problem which naturally arises from studying the conjecture.

1. Introduction

Let $p > 3$ be a prime number, and $\zeta := e^{2\pi i/p}$. We put $K := \mathbb{Q}(\zeta)$. Then K is a galois extension of $\mathbb{Q}$ such that $G := \mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$. We set $G =: \{\sigma_a : a \in \mathbb{Z} - p\,\mathbb{Z}\}$, where $\zeta^{\sigma_a} = \zeta^a$.

For any $a \in \mathbb{Z}$, we set $\overline{a} := a + p\,\mathbb{Z}$. Then for each $t = 1, \ldots, p-1$, we put

$$e_t := -\sum_{a=1}^{p-1} \overline{a}^{\,p-1-t}\, \sigma_a \in \mathbb{F}_p[G].$$

For any $s, t \in \{1, \ldots, p-1\}$, it is easy to see that the following hold:

i) $\sum_{t=1}^{p-1} e_t = 1$;

ii) $e_t^2 = e_t$;

iii) $e_s e_t = 0$ if $s \neq t$;

iv) $\sigma_a e_t = \overline{a}^{\,t} e_t$.

Further, for any $\mathbb{F}_p[G]$-module M and each $t = 1, \ldots, p-1$, we put $M_t := e_t \cdot M$, which is again an $\mathbb{F}_p[G]$-module. Then there is a natural isomorphism

$$M \xrightarrow{\sim} \bigoplus_{t=1}^{p-1} M_t\,.$$

as $\mathbb{F}_p[G]$-modules.

Let $\mathcal{A}$ be the Sylow p-subgroup of the ideal class group for $\mathbb{Z}[\zeta]$. Then $\mathcal{A}$ is naturally a $\mathbb{F}_p[G]$-module. It is not difficult to see that both $\mathcal{A}_1$ and $\mathcal{A}_{p-1}$ are trivial.

2. The Bernoulli Numbers

To state basic theorems on the structure of $\mathcal{A}$, we need to consider the Bernoulli numbers.

The Bernoulli numbers are the rational numbers $B_0, B_1, B_2, \ldots$ that satisfy

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n, \quad |x| < \pi.$$

Alternatively, the Bernoulli numbers are defined inductively as follows: $B_0 = 1$ and

$$1 + 2B_1 = 0, \tag{1}$$

$$1 + 3B_1 + 3B_2 = 0, \tag{2}$$

$$1 + 4B_1 + 6B_2 + 4B_3 = 0, \tag{3}$$

and in general,

$$(m+1)B_m = -\sum_{k=0}^{m-1} \binom{m+1}{k} B_k.$$

For instances,

$$B_1 = -\frac{1}{2}, \;\; B_2 = \frac{1}{6}, \;\; B_3 = 0, \;\; B_4 = -\frac{1}{30}, \;\; B_5 = 0, \;\; B_6 = \frac{1}{42}.$$

As can be expected from the examples, we have:

Theorem 1. *For any $k \geq 1$, one has that $B_{2k+1} = 0$ and that $(-1)^{k+1} B_{2k} > 0$.* □

The Bernoulli numbers were originally defined to have the following result:

Theorem 2 (Bernoulli)**.** *For any $m \geq 1$ and $n \geq 2$, one has*

$$1^m + 2^m + \cdots + (n-1)^m = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}.$$

□

Also we have the following properties:

Theorem 3. *For any $k \geq 1$, the denominator of $|B_{2k}|$ is the product of the prime numbers in the set $\{q : 2k \equiv 0 \pmod{q-1}\}$.* □

Theorem 4 (Euler). *For any $k \geq 1$,*

$$2\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k+1} \frac{(2\pi)^{2k}}{(2k)!} B_{2k}\,.$$

□

3. The Basic Structure of $\mathcal{A}$

The following two theorems provide a satisfactory answer to the most basic question concerning the odd parts of $\mathcal{A}$:

Theorem 5 (Herbrand). *For any $t \in \{1, \ldots, \frac{p-3}{2}\}$, if $\mathcal{A}_{2t+1} = 0$, then p divides the numerator of $|B_{2t}|$.* □

Theorem 6 (Ribet). *For any $t \in \{1, \ldots, \frac{p-3}{2}\}$, if p divides the numerator of $|B_{2t}|$, then $\mathcal{A}_{2t+1} = 0$.* □

Now for the even parts, there is no known general answer. However we have:

Theorem 7. *For any $t \in \{1, \ldots, \frac{p-1}{2}\}$, if $\mathcal{A}_{2t+1} = 0$, then $\mathcal{A}_{2t} = 0$.* □

Further, the following conjecture has been given:

Conjecture 1 (Vandiver). *For any $t \in \{1, \ldots, \frac{p-1}{2}\}$, one has $\mathcal{A}_{2t} = 0$.*

4. Vandiver's Conjecture and K-groups of $\mathbb{Z}$

There is rather unexpected relation of Vandiver's conjecture to the algebraic K-groups of $\mathbb{Z}$.

Let R be a ring, not necessarily commutative. Then for each $n \geq 1$, Quillen's algebraic K-group of R is defined to be

$$K_n(R) := \pi_n(B(GL(R))^+),$$

where one has that $GL(R)$ is the direct limit of $\{GL_n(R) : n \in \mathbb{N}\}$, where the connecting maps are naturally defined, and that $B(GL(R))$ is the classifying space of the group $B(GL(R))$, and lastly that $B(GL(R))^+$ is the topological space given as the result of applying Quillen's $+$-construction on $B(GL(R))$. In general, given a topological space X, the chief property of X^+ is that $\pi(X^+)$ is isomorphic to the abelianisation of $\pi(X)$.

Algebraic K-groups are very difficult to compute in general. However,

Theorem 8 (Quillen). *Let q be a prime power. Then for any $m \in \mathbb{N}$,*

$$K_{2m}(\mathbb{F}_q) = 0\,, \quad K_{2m+1}(\mathbb{F}_q) \cong \mathbb{Z}/(q^m - 1)\mathbb{Z}\,.$$

□

The algebraic K-groups have many nice properties. For example,

Theorem 9. *For any ring R and $n \geq 1$, one has $K_n(R) \cong K_n(R[X])$.* □

Combining the two results, we obtain:

Theorem 10. *Let q be a prime power. Then for any $m \geq 1$,*

$$K_{2m}(\mathbb{F}_q[X]) = 0\,, \quad K_{2m+1}(\mathbb{F}_q[X]) \cong \mathbb{Z}/(q^m - 1)\mathbb{Z}\,.$$

□

Then the similarities between $\mathbb{Z}$ and rings of the form $\mathbb{F}_q[X]$ suggest that there might be a partial periodicity for the K-groups of $\mathbb{Z}$. In relation to this conjecture, one has:

Theorem 11 (Kurihara[1])**.** *The following is equivalent:*

i) $K_{4m}(\mathbb{Z}) = 0$ for any $m \geq 1$;

ii) Vandiver's conjecture is true for all odd prime l. □

After a tremendous amount work, it has been established that $K_4(\mathbb{Z}) = 0$[2].

5. Problems Related to Vandiver's Conjecture

The following result provides a means to study Vandiver's conjecture in a concrete setting:

Theorem 12. [3, §8.3] *For any $t \in \{1, \ldots, \frac{p-3}{2}\}$, the following is equivalent:*

$$\mathcal{A}_{2t}(\mathbb{Z}) = 0 \quad \Longleftrightarrow \quad \prod_{a=1}^{p-1}(1-\zeta^a)^{a^{p-1-2t}} \notin K^{\times p}. \tag{4}$$

□

We remark that it is trivial that $\prod_{a=1}^{p-1}(1-\zeta^a)^{a^{p-1-(2t+1)}} \in K^{\times p}$ for any given $t \in \{1, \ldots, \frac{p-3}{2}\}$.

More generally, given $c \in \mathbb{Q}^\times$ and $m \in \{2, \ldots, p-2\}$, one may ask whether $\prod_{a=1}^{p-1}(1-c\,\zeta^a)^{a^{p-1-m}} \in K^{\times p}$. We have proved:

Proposition 1. *Let $c \in \mathbb{Z}_{(p)}^\times$ be given such that $c \notin 1 + p\mathbb{Z}_{(p)}$. Then*

$$\prod_{a=1}^{p-1}(1-c\,\zeta^a)^{a^{p-1-m}} \notin K^{\times p}$$

for any $m \in \{2, \ldots, p-2\}$. □

Although this result does not have any direct implication on Vandiver's conjecture, the methods used in the proof can be to a certain extent applied to studying those elements of K given in (4).

References

[1] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbb{Z}$, *Compositio Math.*, **81** (1992), 223-236.

[2] J. Rognes, $K_4(\mathbb{Z})$ is the trivial group, *Topology*, **39** (2000), 267-281.

[3] L. C. Washington, *Introduction to Cyclotomic Fields*, Second Edition, Springer-Verlag, New York 1997.