5.1. Ramification

Kummer’s theorem is a special case of Fermat’s last theorem, first described here in the remarks at the end of Section 3.1. To investigate Kummer’s theorem, we need a characterization of units in cyclotomic fields. To eliminate certain candidates, we need the idea of ramification.

We consider here the problem of ramification in a general setting. Let $K$ be an algebraic number field, and let $p$ be a prime ideal in $K$. By Theorem 3.25(iv), $p$ divides exactly one ideal $(p)$ where $p$ is a rational prime. It is therefore natural to factorize all ideals of the form $(p)$, where $p$ runs through all rational primes, into products of prime ideals. Suppose that $(p) = p_1 \ldots p_r$. Then we say that $(p)$ is unramified in $K$ if $p_1, \ldots, p_r$ are distinct; otherwise $(p)$ is ramified in $K$.

A result of Dedekind says that $(p)$ is unramified in $K$ if and only if $p \nmid \Delta$, where $\Delta$ is the discriminant of $K$. We prove this part of the result here.

**Theorem 5.1.** Suppose that $K$ is an algebraic number field with discriminant $\Delta$. Suppose further that the rational prime $p$ satisfies $p \nmid \Delta$. Then $(p)$ is unramified in $K$; in other words, $(p)$ is not divisible by the square of a prime ideal in $K$.

Let $\alpha \in \mathcal{O}$, the ring of integers in an algebraic number field $K$. By the trace of $\alpha$, we mean the number $S(\alpha) = \alpha^{(1)} + \ldots + \alpha^{(n)}$, where $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are the $K$-conjugates of $\alpha$. Clearly $S(\alpha)$ is a rational integer, since $-S(\alpha)$ is the second coefficient of the field polynomial for $\alpha$. On the other hand, $S(\alpha \alpha) = \alpha S(\alpha)$ for any rational integer $\alpha$.

**Proof of Theorem 5.1.** Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{O}$. For every $i = 1, \ldots, n$, let $\omega_i^{(1)}, \ldots, \omega_i^{(n)}$ denote the $K$-conjugates of $\omega_i$. Then

$$\Delta = \begin{vmatrix} \omega_1^{(1)} & \ldots & \omega_n^{(1)} \\ \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}^2 = \begin{vmatrix} \omega_1^{(1)} & \ldots & \omega_1^{(n)} \\ \vdots & \ddots & \vdots \\ \omega_n^{(1)} & \ldots & \omega_n^{(n)} \end{vmatrix} = \left( \sum_{k=1}^{n} \omega_i^{(k)} \omega_j^{(k)} \right) = |(S(\omega_i \omega_j))|.$$

Suppose on the contrary that $(p)$ is ramified. Then $(p)$ has a square factor $p^2$, where $p$ is a prime ideal in $K$. Let $(p) = p^2q$, and let $\alpha \in \mathcal{O}$ such that $\alpha \in pq$ and $\alpha \notin p^2q$, so that $pq | \langle \alpha \rangle$ and $p^2q | \langle \alpha \rangle$. Then $\alpha \neq 0$, $p \nmid \alpha$ and $p \nmid \alpha^2$ in $K$.

Let $\beta \in \mathcal{O}$. We next show that $p \mid S(\alpha \beta)$ in $\mathbb{Q}$. Since $p \geq 2$, we have $\alpha^2 \mid \alpha^p \beta^p$, so that $p \mid \alpha^p \beta^p$, and so $(\alpha \beta)^p/p \in \mathcal{O}$. By the two comments before this proof, we have $S((\alpha \beta)^p) = pS((\alpha \beta)^p/p)$, and so $S((\alpha \beta)^p) \in (p)$. Now let $\beta^{(1)}, \ldots, \beta^{(n)}$ denote the $K$-conjugates of $\beta$. Then

$$(S(\alpha \beta))^p = (\alpha^{(1)} \beta^{(1)})^p + \ldots + (\alpha^{(n)} \beta^{(n)})^p = (\alpha^{(1)} \beta^{(1)})^p + \ldots + (\alpha^{(n)} \beta^{(n)})^p + p\gamma = S((\alpha \beta)^p) + p\gamma,$$
where $\gamma \in \mathcal{O}$. It follows that $(S(\alpha\beta))^{p} \in \langle p \rangle$ for any $\beta \in \mathcal{O}$. Since $S(\alpha\beta) \in \mathbb{Z}$, we must have $p \mid S(\alpha\beta)$ in $\mathbb{Q}$.

Let $\alpha = b_{1}\omega_{1} + \ldots + b_{n}\omega_{n}$, where $b_{1}, \ldots, b_{n} \in \mathbb{Z}$. Since $p \nmid \alpha$ in $K$, we have $p \nmid b_{k}$ for some $k = 1, \ldots, n$. On the other hand, for every $i = 1, \ldots, n$, the prime $p$ divides

$$S(\alpha\omega_{i}) = S \left( \sum_{j=1}^{n} b_{j}\omega_{j} \right) = \sum_{j=1}^{n} b_{j}S(\omega_{j}\omega_{i})$$

in $\mathbb{Q}$. Consider now the $n \times n$ matrix $(S(\omega_{j}\omega_{i}))$. For every $i, j = 1, \ldots, n$, let $A_{ij}$ denote the cofactor of the entry $S(\omega_{j}\omega_{i})$ in the matrix. Then for every $k = 1, \ldots, n$, the prime $p$ divides

$$\sum_{i=1}^{n} A_{ik} \sum_{j=1}^{n} b_{j}S(\omega_{j}\omega_{i}) = \sum_{j=1}^{n} b_{j} \sum_{i=1}^{n} A_{ik}S(\omega_{j}\omega_{i}) = b_{k}\Delta$$

in $\mathbb{Q}$. Since $p \nmid b_{k}$ for some $k = 1, \ldots, n$, we must have $p \mid \Delta$, a contradiction. \hfill \Box

### 5.2. Units in Cyclotomic Fields

We only use the following special case of Theorem 5.1.

**Theorem 5.3.** Suppose that $p$ is an odd prime, $\zeta = e^{2\pi i/p}$ be a primitive $p$-th root of unity, and consider the cyclotomic field $K = \mathbb{Q}(\zeta)$. If a rational prime $q$ is different from $p$, then $q$ is unramified in $K$.

For the remainder of this chapter, $p$ denotes a fixed odd prime, $\zeta = e^{2\pi i/p}$, $K = \mathbb{Q}(\zeta)$, $\lambda = 1 - \zeta$ and $l = \langle \lambda \rangle$. In this section, we establish a sequence of results leading to the characterization of units in $K$.

**Theorem 5.4.** Suppose that $p$ is an odd prime, $\zeta = e^{2\pi i/p}$, $K = \mathbb{Q}(\zeta)$, $\lambda = 1 - \zeta$ and $l = \langle \lambda \rangle$. Then

(i) $\varphi^{-1} = \langle p \rangle$; and

(ii) $N(l) = p$.

**Proof.** (i) We first of all show that for every $j = 1, \ldots, p - 1$, the numbers $1 - \zeta$ and $1 - \zeta^{j}$ are associates. To see this, note that $1 - \zeta^{j} = (1 - \zeta)(1 + \zeta + \ldots + \zeta^{j-1})$, so clearly $(1 - \zeta) \mid (1 - \zeta^{j})$. On the other hand, there exists an integer $t$, satisfying $1 \leq t \leq p - 1$, such that $jt \equiv 1 \bmod p$. Then $1 - \zeta = 1 - \zeta^{jt}$, and it follows easily that $(1 - \zeta^{j}) \mid (1 - \zeta)$.

It now follows from (2.16) that

$$N(\langle p \rangle) = \prod_{j=1}^{p-1} (1 - \zeta^{j}) = \prod_{j=1}^{p-1} (1 - \zeta) = p^{\varphi^{-1}}.$$

(ii) follows immediately on taking norms, noting that $N(\langle p \rangle) = p^{\varphi^{-1}}$. \hfill \Box

Next, we use Theorem 5.2 to establish the following result.

**Theorem 5.5.** Suppose that $p$ is an odd prime, $\zeta = e^{2\pi i/p}$, $K = \mathbb{Q}(\zeta)$, $\lambda = 1 - \zeta$ and $l = \langle \lambda \rangle$. Then

(i) $i \not\in K$; and

(ii) for any odd prime $q \neq p$, we have $e^{2\pi i/q} \not\in K$.

**Proof.** (i) Suppose on the contrary that $i \in K$. Since $i$ is a unit, we have $\langle 1 + i \rangle = \langle 1 - i \rangle$, and so $\langle 2 \rangle = \langle 1 + i \rangle\langle 1 - i \rangle = (1 + i)^{2}$, contradicting Theorem 5.2.

(ii) Suppose on the contrary that $e^{2\pi i/q} \in K$. Then by a similar argument as in the proof of Theorem 5.3(i), we can show that $\langle q \rangle = \langle 1 - e^{2\pi i/q} \rangle^{q-1}$, contradicting Theorem 5.2. \hfill \Box

**Theorem 5.6.** Suppose that $p$ is an odd prime and $\zeta = e^{2\pi i/p}$. Then the only roots of unity in $K = \mathbb{Q}(\zeta)$ are $\pm \zeta^{s}$, where $1 \leq s \leq p$.

**Proof.** Suppose that a root of unity $\alpha = e^{2\pi i/m} \in K$. We may assume, without loss of generality, that $m > 0$ and $(m, u) = 1$. The theorem asserts that there exist $s, k \in \mathbb{Z}$ such that

$$\frac{2\pi i}{m} = \frac{2\pi i}{p} + k\pi i, \quad \text{or} \quad \frac{2\pi u}{m} = 2s + kp.$$

If $m \mid 2pu$, then such $s$ and $k$ exist, since $2s$ runs through a complete set of residues modulo $p$ as $s$ runs through $1, \ldots, p$. In view of the assumption $(m, u) = 1$, it suffices to show that $m \mid 2p$. If $m \nmid 2p,$
then one of the following must be true: (i) $4 \mid m$; (ii) $q \mid m$, where $q \neq p$ is an odd prime; (iii) $p^2 \mid m$.

Also, since $(m, a) = 1$, there exists $r$ such that $ur \equiv 1 \mod m$, so that $\alpha^r = e^{2\pi iur/m} = e^{2\pi i/m} \in K$.

Our proof will be complete if we can show that none of (i)–(iii) holds.

(i) If $4 \mid m$, then $i = e^{2\pi i/4} \in K$, contradicting Theorem 5.4(i).

(ii) If $q \neq p$ is an odd prime such that $q \mid m$, then $e^{2\pi i/q} \in K$, contradicting Theorem 5.4(ii).

(iii) If $p^2 \mid m$, then $\tau = e^{2\pi i/p^2} \in K$. Clearly $\tau$ is a root of the polynomial $t^p - 1$ but not of the polynomial $t^p - 1$, and is therefore a root of the polynomial

$$f(t) = \frac{t^p - 1}{t^p - 1} = t^p(p-1) + t^p(p-2) + \ldots + 1.$$ 

Applying Eisenstein’s criterion to $f(t + 1)$, one can show that $f(t)$ is irreducible. Hence $\tau$ is of degree $p(p-1) > p-1$ over $\mathbb{Q}$. Since $[K : \mathbb{Q}] = p-1$, we must have $\tau \notin K$. \hfill \Box

**Theorem 5.6.** Suppose that $p$ is an odd prime, $\zeta = e^{2\pi i/p}$ and $l = (\lambda)$, where $\lambda = 1 - \zeta$. Then for every $\alpha \in \mathbb{Z}[\zeta]$, there exists $a \in \mathbb{Z}$ such that $\alpha^p \equiv a \mod p$.

**Proof.** By Theorem 5.3(ii), we have $N(t) = p$, so that there are exactly $p$ incongruent residue classes modulo $t$. We first show that $0, 1, \ldots, p-1$ form a complete set of residues modulo $t$. Suppose, on the contrary, that $0 \leq a < b \leq p-1$ and $b-a \in l$. By Theorem 3.25(ii), we have $p \in l$. Since $(b-a,p) = 1$, we must therefore have $1 \in l$, a contradiction since $l$ is prime.

It now follows that there exists $b \in \mathbb{Z}$ such that $\alpha \equiv b \mod l$. Clearly

$$\alpha^p - b^p = \prod_{j=0}^{p-1} (\alpha - \zeta^j b).$$

Since $\zeta \equiv 1 \mod l$, each of the factors $\alpha - \zeta^j b \equiv a - b \equiv 0 \mod l$. It follows that $\alpha^p - b^p \equiv 0 \mod p$. \hfill \Box

**Theorem 5.7.** Suppose that $p(t) \in \mathbb{Z}[t]$ is monic, and that all its roots in $\mathbb{C}$ have absolute value 1. Then these roots are roots of unity.

**Proof.** Let $w_1, \ldots, w_k$ be the roots. For every $\ell \in \mathbb{N}$, let

$$p_\ell(t) = (t-w_1^\ell) \cdots (t-w_k^\ell).$$

Then it is not difficult to show, using arguments on symmetric polynomials, that $p_\ell(t) \in \mathbb{Z}[t]$. Suppose that

$$p_\ell(t) = t^k + a_{k-1}t^{k-1} + \ldots + a_0.$$ 

Then by estimating the size of the elementary symmetric polynomials in $w_1, \ldots, w_k$ and noting that $|w_1| = \ldots = |w_k| = 1$, we have

$$|a_j| \leq \binom{k}{j}$$

for every $j = 0, 1, \ldots, k-1$. Clearly there are only finitely many polynomials of the form (5.1) in $\mathbb{Z}[t]$ with coefficients satisfying (5.2). Hence there exist $\ell, m \in \mathbb{N}$ satisfying $\ell < m$ such that $p_\ell(t) = p_m(t)$ and the roots agree pairwise, so that $w_1^\ell = w_1^m$, ..., $w_k^\ell = w_k^m$. Then $w_i^{m-\ell} = 1$ for every $i = 1, \ldots, k$. \hfill \Box

**Theorem 5.8 (Kummer’s lemma).** Suppose that $p$ is an odd prime, $\zeta = e^{2\pi i/p}$, $K = \mathbb{Q}(\zeta)$, $\lambda = 1 - \zeta$ and $l = (\lambda)$. Then every unit in $\mathbb{Z}[\zeta]$ is of the form $\zeta^\eta g$, where $g \in \mathbb{N}$ and $r \in \mathbb{R}$.

**Proof.** Suppose that $\varepsilon \in \mathbb{Z}[\zeta]$ is a unit. Since $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\zeta]$, there exists $r(t) \in \mathbb{Z}[t]$ such that $\varepsilon = r(\zeta)$. The $K$-conjugates of $\varepsilon$ are given by $\varepsilon^{(s)} = r(\zeta^s)$, where $s = 1, \ldots, p-1$. Now $N(\varepsilon) = \varepsilon^{(1)} \cdots \varepsilon^{(p-1)} = \pm 1$, so each $\varepsilon^{(s)}$ is a unit. Furthermore,

$$\varepsilon^{(p-s)} = r(\zeta^{p-s}) = r(\zeta^{-s}) = r(\zeta^s) = \overline{\varepsilon^{(s)}},$$

and so $\varepsilon^{(s)} \varepsilon^{(p-s)} = |\varepsilon^{(s)}|^2 > 0$. Hence $N(\varepsilon) = 1$. 

5.2. Units in Cyclotomic Fields 45
The numbers $\varepsilon(s)/\varepsilon(p-s)$, where $s = 1, \ldots, p-1$, are units of absolute value 1. The usual symmetric polynomial argument gives

$$
\prod_{s=1}^{p-1} \left( \frac{t - \varepsilon(s)}{\varepsilon(p-s)} \right) \in \mathbb{Z}[t].
$$

It follows from Theorem 5.7 that each $\varepsilon(s)/\varepsilon(p-s)$ is a root of unity. In particular, $\varepsilon/\varepsilon(p-1)$ is a root of unity and so, by Theorem 5.5, there exists $n \in \mathbb{N}$ such that $\varepsilon/\varepsilon(p-1) = \pm \zeta^n = \pm \zeta^{u+p}$. Since $p$ is odd, it follows that

$$
\varepsilon/\varepsilon(p-1) = \pm \zeta^g
$$

for some $g \in \mathbb{N}$.

We now investigate the sign on the right hand side of (5.3). Since 0, 1, \ldots, $p-1$ form a complete set of residues modulo 1, we have

$$
\zeta^{-g} \varepsilon \equiv v \mod 1
$$

for some $v \in \mathbb{Z}$. Taking complex conjugates in (5.4), we have

$$
\zeta^g \varepsilon^{(p-1)} \equiv v \mod (\bar{\lambda}).
$$

Clearly $\bar{\lambda} = 1 - \zeta^{p-1}$ is an associate of $\lambda$, so that $(\bar{\lambda}) = 1$. Eliminating $v$, we have

$$
\varepsilon/\varepsilon^{(p-1)} \equiv \zeta^{2g} \mod 1.
$$

Suppose that $\varepsilon/\varepsilon^{(p-1)} = -\zeta^{2g}$. Then 1 $\mid (2\zeta^{2g})$. Taking norms, we have $N(1) \mid 2^{p-1}$, contradicting Theorem 5.3(ii). Hence $\varepsilon/\varepsilon^{(p-1)} = \zeta^{2g}$, so that

$$
\zeta^{-g} \varepsilon = \zeta^g \varepsilon^{(p-1)}.
$$

The two sides of (5.5) are complex conjugates of each other, and are therefore real. It follows that $\zeta^{-g} \varepsilon = r \in \mathbb{R}$.  

\section*{5.3. A Special Case of Fermat’s Last Theorem}

Let $p$ be an odd prime, $\zeta = e^{2\pi i/p}$, and consider the cyclotomic field $K = \mathbb{Q}(\zeta)$. Let $h$ be the class number of $K$. If $p \nmid h$, then we say that $p$ is regular; otherwise $p$ is irregular.

Kummer’s result states that if an odd prime $p$ is regular, then the Fermat equation $x^p + y^p = z^p$ has no non-trivial solution in rational integers $x$, $y$ and $z$. Here we prove the following weaker version of Kummer’s theorem.

\textbf{Theorem 5.9.} Suppose that $p$ is a regular odd prime. Then the Fermat equation $x^p + y^p = z^p$ has no solutions in integers satisfying $p \nmid xyz$.

\textbf{Proof.} Note, first of all that, in view of the substitution $z \mapsto -z$, we can work on the equation

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

which has greater symmetry. Assume, on the contrary, that there exists a solution $(x, y, z)$ of (5.6) in integers $x$, $y$ and $z$ prime to $p$. We may assume further that $x$, $y$ and $z$ are pairwise coprime. Factorizing (5.6) in $\mathbb{Q}(\zeta)$, we have

$$
\prod_{j=1}^{p-1} (x + \zeta^j y) = -z^p,
$$

and so

$$
\prod_{j=1}^{p-1} (x + \zeta^j y) = (z)^p.
$$

We now claim that the factors on the left hand side of (5.7) are pairwise coprime. To see this, suppose on the contrary that a prime ideal $\mathfrak{p}$ divides $(x + \zeta^k y)$ and $(x + \zeta^\ell y)$, where $0 \leq k < \ell \leq p-1$. Then $x + \zeta^k y \in \mathfrak{p}$ and $x + \zeta^\ell y \in \mathfrak{p}$, so that their difference

$$
y \zeta^k (1 - \zeta^{\ell-k}) \in \mathfrak{p}.
$$
Since $1 - \zeta^{\ell-k}$ is an associate of $1 - \zeta = \lambda$ and $\zeta^k$ is a unit, we must have $y\lambda \in p$, so that $p \mid \langle y \rangle \langle \lambda \rangle$. Since $p$ is a prime ideal, we must therefore have $p \mid \langle y \rangle$ or $p \mid \langle \lambda \rangle$, and so $y \in p$ or $p \mid l$. On the other hand, it follows immediately from (5.7) that

$$z \in p.$$  

Suppose first of all that $y \in p$. Since $y$ and $z$ are coprime, it follows that $1 \in p$, a contradiction. Hence $p \mid l$. Since $l$ is prime, we must have $p = l$. It then follows from (5.9) that $z \in l$, so that

$$p = N(l) \mid N(\langle z \rangle) = z^{p-1},$$  

and so $p \mid z$, a contradiction.

Since the factors on the left hand side of (5.7) are pairwise coprime, it follows from the unique factorization theorem that each factor on the left hand side of (5.7) is the $p$-th power of an ideal. In particular, there exists an ideal $a$ such that

$$\langle x + \zeta y \rangle = a^p.$$  

Hence $a^p$ is principal. Recall that $p$ is regular, so that $p \not\mid h$, where $h$ is the class number of $\mathbb{Q}(\zeta)$. It then follows from Theorem 4.9(ii) that $a$ is principal, so that $a = \langle \delta \rangle$ for some $\delta \in \mathbb{Z}[\zeta]$. Then

$$x + \zeta y = \epsilon\delta^p,$$

where $\epsilon$ is a unit in $\mathbb{Q}(\zeta)$. Combining this with Theorem 5.8, we conclude that

$$x + \zeta y = r\zeta^2\delta^p$$

for some $g \in \mathbb{N}$ and $r \in \mathbb{R}$. On the other hand, it follows from Theorem 5.6 that there exists $a \in \mathbb{Z}$ such that

$$\delta^p \equiv a \mod p.$$  

Combining (5.10) and (5.11), we have $x + \zeta y \equiv r\zeta^g \mod p$, and so it follows from Theorem 5.3(i) that

$$x + \zeta y \equiv r\zeta^g \mod (p).$$

Multiplying both sides by the unit $\zeta^{-g}$ in $\mathbb{Q}(\zeta)$, we obtain

$$\zeta^{-g}(x + \zeta y) \equiv ra \mod (p).$$

Taking complex conjugates, we have

$$\zeta^g(x + \zeta^{-1}y) \equiv ra \mod (p).$$

Combining these and eliminating $ra$, we have

$$x\zeta^{-g} + y\zeta^{1-g} - x\zeta^g - y\zeta^{g-1} \equiv 0 \mod (p).$$

We next show that $g \not\equiv 0 \mod p$ and $g \not\equiv 1 \mod p$. Suppose on the contrary that $g \equiv 0 \mod p$. Then $\zeta^g = 1$, and (5.12) becomes

$$y(\zeta^{-1} - 1) \equiv 0 \mod (p),$$

so that $y(1 + \zeta)(1 - \zeta) \equiv 0 \mod (p)$. Noting that $1 + \zeta = (1 - \zeta^2)/(1 - \zeta)$ is a unit, and recalling Theorem 5.3(i), that $\langle \lambda \rangle^{p-1} \equiv p^{-1} \equiv \langle p \rangle$, we conclude that

$$y\lambda \equiv 0 \mod (\lambda)^{p-1}.$$  

But then $p - 1 \geq 2$, so it follows that $\langle \lambda \rangle \mid \langle y \rangle$. Taking norms, we deduce that $p \mid y$, a contradiction. Likewise, suppose on the contrary that $g \equiv 1 \mod p$. Then $\zeta^{1-g} = 1$, and (5.12) becomes

$$x(\zeta^{-1} - \zeta) \equiv 0 \mod (p).$$

A similar argument leads to a contradiction.

The congruence (5.12) can be rewritten in the form

$$\alpha p = x\zeta^{-g} + y\zeta^{1-g} - x\zeta^g - y\zeta^{g-1},$$

where $\alpha \in \mathbb{Z}[\zeta]$. Since $g \not\equiv 0 \mod p$ and $g \not\equiv 1 \mod p$, none of the four exponents of $\zeta$ on the right hand side is divisible by $p$. Next, note that

$$\alpha = \frac{x}{p}\zeta^{-g} + \frac{y}{p}\zeta^{1-g} - \frac{x}{p}\zeta^g - \frac{y}{p}\zeta^{g-1},$$

If no two of these four exponents are congruent modulo $p$, then $p \mid x$ and $p \mid y$, for $\alpha \in \mathbb{Z}[\zeta]$ and its representation in terms of the $\mathbb{Z}$-basis $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ is unique, with coefficients in $\mathbb{Z}$. Since $p \not\mid x$ and $p \not\mid y$ by our hypothesis, two of these four exponents must be congruent modulo $p$. Since
$g \not\equiv 0 \mod p$ and $g \not\equiv 1 \mod p$, the only possibility for two of these four exponents to be congruent modulo $p$ is to have $2g \equiv 1 \mod p$.

Noting that $\zeta^p = 1$, and with $2g \equiv 1 \mod p$, we can now rewrite (5.13) as

$$\alpha p\zeta^g = x + y\zeta - x\zeta^{2g} - y\zeta^{2g-1} = x + y\zeta - x\zeta - y = (x - y)(1 - \zeta) = (x - y)\lambda.$$  

Taking norms, we obtain $N(\alpha)p^{p-1} = (x - y)^{p-1}p$, so that $p \mid (x - y)$, and so

$$x \equiv y \mod p.$$  

The symmetry of the equation (5.6) now gives

$$y \equiv z \mod p.$$  

It follows that

$$0 \equiv x^p + y^p + z^p \equiv 3x^p \mod p.$$  

Since $p \nmid x$, we must have $p = 3$.

To complete our proof, it remains to consider the case $p = 3$. Since $3 \nmid x$ by hypothesis, and $\{-1, 0, 1\}$ is a complete set of residues modulo 3, we must have $x \equiv \pm 1 \mod 3$, so that $x^3 \equiv \pm 1 \mod 9$.  

Since $3 \nmid y$ and $3 \nmid z$ by hypothesis, we have

$$0 = x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \mod 9,$$

clearly impossible.  $\Box$