CHAPTER VI

37. Statement of the Result Proved in Chapter VI

The purpose of this chapter is to prove the following result.

THEOREM 37.1. *There are no groups* $\mathfrak{G}$ *which satisfy conditions* (i)–(iv) *of Theorem* 27.1.

Once it is proved, Theorem 37.1 together with Theorem 27.1 will serve to complete the proof of the main theorem of this paper. In this chapter there is no reference to anything in Chapters II–V other than the statement of Theorem 27.1. The following notation is used throughout this chapter.

$\mathfrak{G}$ is a fixed group which satisfies conditions (i)–(iv) of Theorem 27.1.

$$|\mathfrak{U}| = u = \frac{p^q - 1}{p - 1}$$

$$\mathfrak{U}^* = C(\mathfrak{U}) \quad \text{and} \quad |\mathfrak{U}^*| = u^* .$$

$$\mathfrak{U}^* = \langle U_1 \rangle, \; U = U_1^{u^*/u^*} . \quad \text{Thus } \mathfrak{U} = \langle U \rangle$$

$$\mathfrak{Q}_0 = [\mathfrak{Q}, \mathfrak{P}^*] \quad \text{so that} \quad \mathfrak{Q} = \mathfrak{Q}^* \times \mathfrak{Q}_0 .$$

P and Q are fixed elements of $\mathfrak{P}^{*\sharp}$ and $\mathfrak{Q}^{*\sharp}$ respectively.

For any integer $n > 0$, $\mathscr{Z}_n$ is the ring of integers mod n. If n is a prime power then $\mathscr{F}_n$ is the field of n elements.

U acts as a linear transformation on $\mathfrak{P}$. Let $m(t)$ be the minimal polynomial of U on $\mathfrak{P}$. Then $m(t)$ is an irreducible polynomial of degree q over $\mathscr{F}_p$. Let ω be a fixed root of $m(t)$ in $\mathscr{F}_{p^q}$. Then ω is a primitive uth root of unity in $\mathscr{F}_{p^q}$ and $\omega, \omega^p, \cdots, \omega^{p^{q-1}}$ are all the characteristic roots of U on $\mathfrak{P}$.

38. The Sets $\mathscr{A}$ and $\mathscr{B}$

LEMMA 38.1. *There exists an element* $Y \in \mathfrak{Q}_0^\sharp$ *such that* $\mathfrak{P}^*$ *normalizes* $Y\mathfrak{U}^*Y^{-1}$

Proof. $\mathfrak{Q}^*$ normalizes $\mathfrak{U}^*$ and $\mathfrak{Q}^*$ is contained in a cyclic subgroup of $N(\mathfrak{U}^*)$ of order pq. Hence some element of order p in $C(\mathfrak{Q}^*)$ normalizes $\mathfrak{U}^*$. Since $C(\mathfrak{Q}^*) = \mathfrak{Q}\mathfrak{P}^*$ every subgroup of order p in $C(\mathfrak{Q}^*)$ is of the form $Y^{-1}\mathfrak{P}^*Y$ for some $Y \in \mathfrak{Q}_0$. Hence it is possible to choose $Y \in \mathfrak{Q}_0$ such that $Y^{-1}\mathfrak{P}^*Y$ normalizes $\mathfrak{U}^*$. Since $[\mathfrak{P}^*, \mathfrak{U}] \leqq \mathfrak{P}$,

$\mathfrak{P}^*$ does not normalize $\mathfrak{U}^*$, hence $Y \in \mathfrak{Q}_0^*$ and $\mathfrak{P}^*$ normalizes $Y\mathfrak{U}^*Y^{-1}$.

From now on let

$$Z_1 = YU_1Y^{-1}, \quad Z = YUY^{-1} = Z_1^{u^*/u} \tag{38.1}$$

where Y satisfies Lemma 38.1. Notice that $\mathfrak{Q}^*$ normalizes $\langle Z_1 \rangle$, since $\mathfrak{Q}^*$ normalizes $\mathfrak{U}^*$ and Y centralizes $\mathfrak{Q}^*$. Define $v, w \in \mathfrak{Z}_{u^*}$ by

$$P^{-1}Z_1P = Z_1^v, \quad Q^{-1}Z_1Q = Z_1^w \tag{38.2}$$

LEMMA 38.2. *If* $Z_0 \in \langle Z_1 \rangle$, $a \in \mathfrak{Z}_p$, $b \in \mathfrak{Z}_q$ *then* $\langle Z_0 \rangle = \langle Z_0^{v^a w^b - 1} \rangle$ *unless* $a = 0$ *and* $b = 0$.

Proof. $Z_0^{-1}P^{-a}Q^{-b}Z_0Q^bP^a = Z_0^{v^a w^b - 1}$. Hence P^aQ^b acts trivially on $\langle Z_0 \rangle / \langle Z_0^{v^a w^b - 1} \rangle$. However if $Z_0 \neq 1$ then $\mathfrak{P}^*\mathfrak{Q}^*\langle Z_0 \rangle$ is a Frobenius group with Frobenius kernel $\langle Z_0 \rangle$. Thus $\langle Z_0 \rangle = \langle Z_0^{v^a w^b - 1} \rangle$ as required.

LEMMA 38.3. *Every element of* $\mathfrak{P}\mathfrak{U}$ *has a unique representation in the form* $P^{m_1(U)}U^a$, *where* $a \in \mathfrak{Z}_u$ *and* $m_1(t)$ *is a polynomial of degree at most* $q - 1$ *over* $\mathfrak{Z}_p$.

Proof. There are up^q ordered pairs $(m_1(t), a)$ with $a \in \mathfrak{Z}_u$ and $m_1(t)$ of degree at most $q - 1$ over $\mathfrak{Z}_p$. Thus it is sufficient to show the uniqueness of $(m_1(t), a)$ in such a representation.

If $P^{m_1(U)}U^a = P^{m_1'(U)}U^{a'}$. Then reading mod $\mathfrak{P}$ yields that $a = a'$. Since $m(t)$ is irreducible we get that $m_1(t) \equiv m_1'(t) \pmod{m(t)}$. Thus $m_1(t) = m_1'(t)$ as required.

LEMMA 38.4. *Every element of* $\mathfrak{P}\mathfrak{U} - \mathfrak{U}$ *has a unique representation in the form* $U^xP^yU^z$, *where* $x, z \in \mathfrak{Z}_u$ *and* $y \in \mathfrak{Z}_p$, $y \neq 0$.

Proof. If $X \in \mathfrak{P}\mathfrak{U} - \mathfrak{U}$ and

$$X = U^xP^yU^z = U^{x_1}P^{y_1}U^{z_1}$$

then reading mod $\mathfrak{P}$ we get that $x + z \quad x_1 + z_1$. Hence

$$U^{x - x_1}P^yU^{-z+z_1} = P^{y_1}$$

Since $X \notin \mathfrak{U}$, $y \neq 0$. As $(u, p - 1) = 1$ we have that $x = x_1$, and so $y = y_1$, $z = z_1$. The representation is unique. There are $u^2(p - 1)$ ordered triples (x, y, z) with $x, z \in \mathfrak{Z}_u$ and $y \in \mathfrak{Z}_p$, $y \neq 0$. Each triple gives rise to an element of $\mathfrak{P}\mathfrak{U} - \mathfrak{U}$ and $|\mathfrak{P}\mathfrak{U} - \mathfrak{U}| = u^2(p - 1)$. The result now follows.

LEMMA 38.5. *Let* $x, z, g \in \mathfrak{Z}_p = \mathfrak{F}_p$; $y, f, h \in \mathfrak{Z}_u$. *Then*

$$P^x U^y P^z U^f P^g U^h = 1$$

if and only if

(i) $y + f + h = 0$

(ii) $x\omega^y + z + g\omega^{y+h} = 0.$

Proof. Let $R = P^x U^y P^z U^f P^g U^h$. Then

$$R = P^{x+zU^{-y}} + gU^{-y-f}U^{y+h+f}.$$

Thus by Lemma 38.3 $R = 1$ if and only if

$$y + h + f = 0, \quad x + zt^{-y} + gt^{-y-f} \equiv 0 \,(\mathrm{mod}\, m(t)).$$

The first equation allows us to rewrite the second as

$$xt^y + z + gt^{y+h} \equiv 0 \,(\mathrm{mod}\, m(t)).$$

Thus the lemma is proved.

DEFINITION 38.1. The set $\mathscr{A}$ is defined to consist of all ordered triples (a_1, a_2, a_3) such that

(i) $a_i \in \mathscr{Z}_u$, $a_i \neq 0$ for $i = 1, 2, 3$.

(ii) $a_1 + a_2 + a_3 = 0$.

(iii) $PU^{a_1}P^{-1}U^{a_2}PU^{a_3} = 1$.

DEFINITION 38.2. $\mathscr{B}$ is the set of all elements $a_1 \in \mathscr{Z}_u$ such that $(a_1, a_2, a_3) \in \mathscr{A}$ for suitable a_2, a_3.

LEMMA 38.6. $|\mathscr{A}| = |\mathscr{B}|$.

Proof. If $(a_1, a_2, a_3) \in \mathscr{A}$ then by Lemma 38.4 a_2 and a_3 are determined by a_1.

LEMMA 38.7. $(a_1, a_2, a_3) \in \mathscr{A}$ *if and only if*

(i) $a_i \in \mathscr{Z}_u$, $a_i \neq 0$ *for* $i = 1, 2, 3$

(ii) $a_1 + a_2 + a_3 = 0$

(iii) $\omega^{a_1} + \omega^{a_1+a_3} - 2 = 0$.

Proof. By Lemma 38.5,

$$PU^{a_1}P^{-1}U^{a_2}PU^{a_3} = 1$$

if and only if $a_1 + a_2 + a_3 = 0$ and $\omega^{a_1} - 2 + \omega^{a_1+a_3} = 0$. This implies the result.

LEMMA 38.8. *If* $(a_1, a_2, a_3) \in \mathscr{A}$, *then* $(-a_2, -a_1, -a_3) \in \mathscr{A}$.

Proof. If $(a_1, a_2, a_3) \in \mathscr{A}$ then by Lemma 38.7 $\omega^{-a_2} - 2 + \omega^{a_1} = 0$. As $a_1 = -a_2 - a_3$ this yields that

$$\omega^{-a_2} - 2 + \omega^{-a_2-a_3} = 0 .$$

As $-a_2 - a_1 - a_3 = 0$ the result follows from Lemma 38.7.

LEMMA 38.9. *For $0 \leqq i \leqq p-1$ let $\mathfrak{C}_i$ be the conjugate class of $\mathfrak{PU}$ which contains P^i and let $\mathfrak{K}_i$ be the sum of the elements in $\mathfrak{C}_i$ in the group ring of $\mathfrak{PU}$ over the integers. Let*

$$\mathfrak{K}_1^2 = \sum_{i=0}^{p-1} c_i \mathfrak{K}_i .$$

If $q > 3$, then $c_2 \geqq 2$.

Proof. Let $\mu_0, \mu_1, \cdots$ be all the irreducible characters of $\mathfrak{PU}/\mathfrak{P}$ and let $\chi_1, \chi_2, \cdots$ be all the other irreducible characters of $\mathfrak{PU}$. It is a well known consequence of the orthogonality relations ([4] p. 316) that

$$c_2 = \frac{up^q}{p^{3q}} \left\{ \sum_i \frac{\mu_i(P)^2 \overline{\mu_i(P^2)}}{\mu_i(1)} + \sum_j \frac{\chi_j(P)^2 \overline{\chi_j(P^2)}}{\chi_j(1)} \right\} .$$

Since $\mathfrak{U}$ is cyclic, $\mu_i(P) = \mu_i(P^2) = \mu_i(1) = 1$ for all i. By 3.16 $\chi_j(1) = u$ for all j. Thus

$$c_2 = \frac{u}{p^q} \left\{ u + \frac{1}{u} \sum_j \chi_j(P)^2 \overline{\chi_j(P^2)} \right\} . \tag{38.3}$$

By the orthogonality relations

$$\sum_j |\chi_j(P^i)|^2 \leqq |C(P^i)| \leqq p^q \quad \text{for} \quad 1 \leqq i \leqq p-1 .$$

Therefore

$$|\sum_j \chi_j(P)^2 \overline{\chi_j(P^2)}| \leqq (\max_j |\chi_j(P^2)|) \sum_j |\chi_j(P)|^2 \leqq p^{3q/2} . \tag{38.4}$$

By (38.3) and (38.4)

$$|p^q c_2 - u^2| \leqq p^{3q/2} .$$

Thus

$$p^q c_2 \geqq u^2 - p^{3q/2} . \tag{38.5}$$

Since $u = \dfrac{p^q - 1}{p - 1} > p^{q-1}$ (38.5) yields that

$$c_2 \geqq \frac{u^2}{p^q} - p^{q/2} > p^{q-2} - p^{q/2} = p^{q/2}(p^{q/2-2} - 1) .$$

As $q > 3$ and q is a prime we have $q \geqq 5$, and the lemma follows.

LEMMA 38.10. $|\mathscr{A}| = |\mathscr{B}| > 0$.

Proof. Assume first that $q = 3$. Consider the set of polynomials of the form $f_a(t) = t^3 + at^2 + (a+6)t - 1$ with $a \in \mathscr{Z}_p$. There are p of these and none of them has 0 as a root. Thus if $f_a(t)$ were reducible for every value of a there would exist $a \neq b$ such that $f_a(t)$ and $f_b(t)$ have a common root $c \in \mathscr{F}_p$. Then

$$ac^2 + (a+6)c = bc^2 + (b+6)c .$$

Since $c \neq 0$ this yields that $a(c+1) = b(c+1)$, hence $c = -1$. However $f_a(-1) = -8 \neq 0$. Thus there exists some polynomial $f_a(t)$ which is irreducible over $\mathscr{F}_p$. Let α be a root of $f_a(t)$ in $\mathscr{F}_{p^3}$. Then

$$\alpha^{p^2+p+1} = -f_a(0) = 1, \quad (1+\alpha)^{p^2+p+1} = -f_a(-1) = 8 .$$

Therefore $\alpha = \omega^{a_3}$ for some $a_3 \in \mathscr{Z}_u$, $a_3 \neq 0$, and $1 + \alpha = 2\omega^{-a_1}$ for some $a_1 \in \mathscr{Z}_u, a_1 \neq 0$. Furthermore $-\omega^{a_3} + 2\omega^{-a_1} = 1$. Thus $\omega^{a_1} + \omega^{a_1+a_3} - 2 = 0$. Since $\omega^{a_1} \neq 1$, $a_1 + a_3 \neq 0$. Hence by Lemmas 38.6 and 38.7 $|\mathscr{A}| = |\mathscr{B}| > 0$.

Assume now that $q > 3$. Then Lemma 38.9 implies the existence of $a, b \in \mathscr{Z}_u$, with $a \neq 0$ or $b \neq 0$ such that

$$U^{-a}PU^aU^{-b}PU^b = P^2 .$$

Therefore

$$PU^bP^{-2}U^{-a}PU^{a-b} = 1 . \tag{38.6}$$

Let $a_1 = b$, $a_2 = -a$, $a_3 = a - b$. Then $a_1 + a_2 + a_3 = 0$. If $b = 0$ then (38.6) becomes $P^{-1}U^{-a}PU^a = 1$; as $\mathfrak{P}\mathfrak{U}$ is a Frobenius group this implies $a = 0$ contrary to the choice of a and b. If $a = 0$ then (38.6) implies that $PU^bP^{-1}U^{-b} = 0$, hence $b = 0$. If $a - b = 0$ then (38.6) yields that $PU^aP^{-2}U^{-a}P = 1$ or U^a commutes with P^2. Thus $a = 0$, hence also $b = 0$. Therefore a_1, a_2, a_3 are all non zero and by Definition 38.1 and Lemma 38.6 $|\mathscr{A}| = |\mathscr{B}| > 0$.

The following result about finite fields is of importance for the proof of Theorem 37.1.

LEMMA 38.11. *For $x \in \mathscr{F}_{p^q}$ define $N(x) = x^{1+p+\cdots+p^{q-1}}$ and for $x \neq 2$ let $x^\sigma = \dfrac{1}{2-x}$. If $\alpha \in \mathscr{F}_{p^q} - \mathscr{F}_p$, then for some i, $N(\alpha^{\sigma^i}) \neq 1$.*

Proof. Assume that the result is false and $N(\alpha^{\sigma^i}) = 1$ for all i. We will first prove by induction that

$$\alpha^{\sigma^i} = \frac{-(i-1)\alpha + i}{-i\alpha + (i+1)} \qquad \text{for } i = 1, 2, \cdots \tag{38.7}$$

If $i = 1$ (38.7) follows from the definition of σ. Assume now that (38.7) holds for $i = k - 1$. Then

$$\begin{aligned}\alpha^{\sigma^k} &= \frac{1}{2 - \left\{\dfrac{-(k-2)\alpha + k - 1}{-(k-1)\alpha + k}\right\}} \\ &= \frac{-(k-1)\alpha + k}{-2(k-1)\alpha + 2k + (k-2)\alpha - (k-1)} \\ &= \frac{-(k-1)\alpha + k}{-k\alpha + (k+1)}.\end{aligned}$$

This establishes (38.7).

Now (38.7) implies that for $j \geqq 1$,

$$\prod_{i=1}^{j} \alpha^{\sigma^i} = \frac{\prod_{i=1}^{j}\{-(i-1)\alpha + i\}}{\prod_{i=1}^{j}\{-i\alpha + (i+1)\}} = \frac{1}{-j\alpha + (j+1)}.$$

Therefore

$$N(-j\alpha + j + 1) = \frac{1}{\prod_{i=1}^{j} N(\alpha^{\sigma^i})} = 1.$$

Thus

$$N(-a\alpha + a + 1) = 1 \qquad \text{for } a \in \mathscr{F}_p. \tag{38.8}$$

Define $f(t)$ by

$$f(t) = (t - \alpha)(t - \alpha^p) \cdots (t - \alpha^{p^{q-1}}). \tag{38.9}$$

Thus $f(t)$ has coefficients in $\mathscr{F}_p$ and (38.8) yields that

$$a^q f\left(\frac{a+1}{a}\right) = a^q N\left(\frac{a+1}{a} - \alpha\right) = N(a + 1 - a\alpha) = 1 \tag{38.10}$$

$$\text{for } a \in \mathscr{F}_p,\ a \neq 0.$$

Let $b = \dfrac{a+1}{a}$ for $a \neq 0$, then $a = \dfrac{1}{b-1}$. Hence (38.10) yields that

$$\frac{1}{(b-1)^q} f(b) = 1 \qquad \text{for } b \in \mathscr{F}_p,\ b \neq 1.$$

Therefore

$$f(b) - (b-1)^q = 0 \qquad \text{for } b \in \mathscr{F}_p,\ b \neq 1. \tag{38.11}$$

$f(t) - (t-1)^q$ is a polynomial of degree at most q. By (38.11) $f(t) - (t-1)^q$ has at least $(p-1)$ roots. As $(p-1) > q$ we must have that $f(t) = (t-1)^q$. By (38.9) α is a root of $f(t)$, hence $\alpha = 1$ contrary to the choice of α. The proof is complete.

39. The Proof of Theorem 37.1

LEMMA 39.1. *There exist functions f, g, and h such that*

(i) *f and h map $\mathscr{X}_p \times \mathscr{X}_u \times \mathscr{X}_p$ into $\mathscr{X}_u$,*

(ii) *g maps $\mathscr{X}_p \times \mathscr{X}_u \times \mathscr{X}_p$ into $\mathscr{X}_p$,*

(iii) $P^x U^y P^z U^{f(x,y,z)} P^{g(x,y,z)} U^{h(x,y,z)} = 1$.

Furthermore for $x \neq 0$, $y \neq 0$, $z \neq 0$ (iii) *determines $f(x, y, z)$, $g(x, y, z)$ and $h(x, y, z)$ uniquely and $f(x, y, z)$, $g(x, y, z)$, $h(x, y, z)$ are all non-zero.*

Proof. By Lemma 38.4 the functions exist and are uniquely defined by

$$P^x U^y P^z U^f P^g U^h = 1$$

provided that $P^x U^y P^z$ does not lie in $\mathfrak{U}$. It is easily seen that if $x \neq 0$, $y \neq 0$ and $z \neq 0$, $P^x U^y P^z$ does not lie in $\mathfrak{U}$.

Suppose that $f(x, y, z) = 0$. Then $P^x U^y P^{z+g} = U^{-h} \in \mathfrak{U}$. Then $y = -h$ and $U^y P^{z+g} U^{-y} = P^{-z} \in \mathfrak{P}^*$. Therefore either $y = 0$ or $x = 0$.

Suppose that $g(x, y, z) = 0$. Then $P^x U^y P^z = U^{-f-h}$. Thus $y = -f - h$ and $U^y P^z U^{-y} = P^{-z}$. Hence $x = 0$ or $y = 0$.

Suppose that $h(x, y, z) = 0$. Then $U^y P^z U^f P^{g+z} = 1$. Hence $y + f = 0$, then $U^y P^z U^{-y} = P^{-g-z}$. Thus $y = 0$ or $z = 0$. This completes the proof of the lemma.

Throughout the rest of this section f, g, h will denote the functions defined in Lemma 39.1. For $x \in \mathscr{X}_p$, Y as in Lemma 38.1, define

$$Y_x = Y^{-1} P^{-x} Y P^x .$$

LEMMA 39.2.

(i) $Y_x = Y^{-1} P^{-x} Y P^x = P^{-x} Y P^x Y^{-1}$

(ii) $Y P^z Y^{-1} = Y_z^{-1} P^z$

(iii) $Y P^g Y^{-1} = P^g Y_g$,

for $x, z, g \in \mathscr{X}_p$.

Proof. Since $P \in \mathfrak{P}^* \subseteq N(\mathfrak{Q}_0)$ and $\mathfrak{Q}_0$ is abelian, (i) is immediate. (iii) is a direct consequence of (i). By definition $Y_{-z} = Y^{-1} P^z Y P^{-z}$. Thus $Y_z^{-1} = P^z Y^{-1} P^{-z} Y = Y P^z Y^{-1} P^{-z}$ which implies (ii).

LEMMA 39.3. *For $x \in \mathscr{X}_p$, $P^{-x} U P^x = Y_x^{-1} U^{v^x} Y_x$.*

Proof. By (38.2) $P^xZP^{-x} = Z^{v^{-x}}$. By (38.1) $Z = YUY^{-1}$. Hence

$$Y^{-1}P^xYUY^{-1}P^{-x}Y = U^{v^{-x}}.$$

Conjugating both sides by P^x, we get that

$$Y_x^{-1}UY_x = P^{-x}U^{v^{-x}}P^x.$$

If both sides are raised to the v^xth power, the lemma follows.

LEMMA 39.4.

$$Y_xZ^vY_{-x}^{-1} = P^{-x}Z^{-h(x,y,z)}Y_{g(x,y,z)}^{-1}P^{-g(x,y,z)}Z^{-f(x,y,z)}P^{-x}.$$

Proof. Substitute (38.1) into (iii) of Lemma 39.1 to get

$$P^xY^{-1}Z^vYP^xY^{-1}Z^fYP^gY^{-1}Z^hY = 1.$$

Conjugate by $Y^{-1}P^x$ to get

$$(P^{-x}YP^xY^{-1})Z^v(YP^xY^{-1})Z^f(YP^gY^{-1})Z^hP^x = 1.$$

Now use the results of Lemma 39.2 to derive that

$$Y_xZ^vY_{-x}^{-1}P^xZ^fP^gY_gZ^hP^x = 1$$

which implies the lemma.

LEMMA 39.5. *If* $(a_1, a_2, a_3) \in \mathscr{A}$, *then*

$$Y_2Z^{a_1v}Y_3^{-1}Y_1Z^{a_2v^3}Y_2^{-1} = Y_1Z^{-a_3v^2}Y_3^{-1}.$$

Proof. In the definition of $\mathscr{A}$ conjugate (iii) by P^2. Then

$$P^{-1}U^{a_1}P^{-2}U^{a_2}PU^{a_3}P^2 = 1,$$

or

$$(P^{-1}U^{a_1}P)(P^{-3}U^{a_2}P^3) = P^{-2}U^{-a_3}P^2.$$

Hence Lemma 39.3 yields that

$$(Y_1^{-1}U^{a_1v}Y_1)(Y_3^{-1}U^{a_2v^3}Y_3) = Y_2^{-1}U^{-a_3v^2}Y_2.$$

Since $\mathfrak{Q}$ is abelian, this implies that

$$Y_2U^{a_1v}Y_3^{-1}Y_1U^{a_2v^3}Y_2^{-1} = Y_1U^{-a_3v^2}Y_3^{-1}.$$

Conjugating by Y^{-1} implies the result by (38.1) and the fact that $\mathfrak{Q}$ is abelian.

LEMMA 39.6. *For* $(a_1, a_2, a_3) \in \mathscr{A}$ *define*

$$
\begin{aligned}
g_1 &= g(2, a_1v, -3)\\
g_2 &= g(1, -a_3v^2, -3)\\
g_3 &= g(1, a_2v^3, -2)\\
k_1 &= h(2, a_1v, -3) - h(1, -a_3v^2, -3)v^{-1}\\
k_2 &= -f(2, a_1v, -3) - h(1, a_2v^3, -2)v^{-2}\\
k_3 &= -f(1, a_2v^3, -2)v^{-1} + f(1, -a_3v^2, -3)\\
k &= -g_3 - 1\,.
\end{aligned}
$$

Then

$$
Y_{g_1}Z^{k_1}PY_{g_2}^{-1} = P^{-g_1}Z^{k_2}P^2Y_{g_3}^{-1}P^kZ^{k_3}P^{g_2}\,. \tag{39.1}
$$

Proof. Use Lemmas 39.4 and 39.5 to obtain

$$
\begin{aligned}
&P^{-2}Z^{-h(2,a_1v,-3)}Y^{-1}_{g(2,a_1v,-3)}P^{-g(2,a_1v,-3)}Z^{-f(2,a_1v,-3)}P^3\,\cdot\\
&P^{-1}Z^{-h(1,a_2v^3,-2)}Y^{-1}_{g(1\,a_2v^3,-2)}P^{-g(1,a_2v^3,-2)}Z^{-f(1,a_2v^3,-2)}P^2\\
&\quad = Y_2Z^{a_1v}Y_3^{-1}Y_1Z^{a_2v^3}Y_2^{-1} = Y_1Z^{-a_3v^2}Y_3^{-1}\\
&\quad = P^{-1}Z^{-h(1,-a_3v^2,-3)}Y^{-1}_{g(1\,-a_3v^2,-3)}P^{-g(1,-a_3v^2,-3)}Z^{-f(1,-a_3v^2,-3)}P^3\,\cdot
\end{aligned}
$$

Multiply on the left by $Y_{g(2,a_1v,-3)}Z^{h(2,a_1v,-3)}P^2$ and on the right by

$$
P^{-3}Z^{f(1,-a_3v^2,-3)}P^{g(1,-a_3v^2,-3)}
$$

to get

$$
AY^{-1}_{g(1\,a_2v^3,-2)}B = Y_{g(2,a_1v,-3)}CY^{-1}_{g(1,-a_3v^2,-3)}
$$

where

$$
\begin{aligned}
A &= P^{-g(2,a_1v,-3)}Z^{-f(2,a_1v,-3)-h(1,a_2v^3,-2)v^{-2}}P^2\\
B &= P^{-g(1,a_2v^3,-2)-1}Z^{-f(1,a_2v^3,-2)v^{-1}+f(1,-a_3v^2,-3)}P^{g(1,-a_3v^2,-3)}\\
C &= Z^{h(2,a_1v,-3)-h(1,-a_3v^2,-3)v^{-1}}P\,,
\end{aligned}
$$

or equivalently

$$
A = P^{-g_1}Z^{k_2}P^2\,,\quad B = P^kZ^{k_3}P^{g_2}\,,\quad C = Z^{k_1}P\,.
$$

The lemma follows.

LEMMA 39.7. *Let* $(a_1, a_2, a_3) \in \mathscr{A}$. *Use the notation of Lemma 39.6. If* $k_1 \neq 0$, *then there exist elements* $c_1, c_3 \in \mathscr{Z}_p$ *such that*

(i) $k_3 \neq 0$

(ii) $k_2 + k_3v^{c_3} = k_1$

(iii) $Y^{-1}PYP^{-g_2} = P^{-c_1}Y^{-1}P^{-c_3}Y$.

Proof. Conjugate (39.1) by Q. Since $\mathfrak{B}^*\Omega = C(Q)$, this yields that

$$Y_{g_1}Z^{wk_1}PY_{g_2}^{-1} = P^{-g_1}Z^{wk_2}P^2Y_{g_3}^{-1}P^kZ^{wk_3}P^{g_2}.$$

Taking inverses we get

$$Y_{g_2}P^{-1}Z^{-wk_1}Y_{g_1}^{-1} = P^{-g_2}Z^{-wk_3}P^{-k}Y_{g_3}P^{-2}Z^{-wk_2}P^{g_1}.$$

Multiplying this by (39.1) on the left yields

$$Y_{g_1}Z^{(1-w)k_1}Y_{g_1}^{-1} = P^{-g_1}Z^{k_2}P^2Y_{g_3}^{-1}P^kZ^{(1-w)k_3}P^{-k}Y_{g_3}P^{-2}Z^{-wk_2}P^{g_1}.$$

Conjugating by P^{-g_1} yields

$$P^{g_1}Y_{g_1}Z^{(1-w)k_1}Y_{g_1}^{-1}P^{-g_1} = Z^{k_2}P^2Y_{g_3}^{-1}P^kZ^{(1-w)k_3}P^{-k}Y_{g_3}P^{-2}Z^{-wk_2}.$$

Use Lemma 39.2 (iii) and (38.1) to get

$$\begin{aligned}&YP^{g_1}Y^{-1}YU^{(1-w)k_1}Y^{-1}YP^{-g_1}Y^{-1}\\ &\quad = YU^{k_2}Y^{-1}P^2Y_{g_3}^{-1}P^kYU^{(1-w)k_3}Y^{-1}P^{-k}Y_{g_3}P^{-2}YU^{-wk_2}Y^{-1}.\end{aligned}$$

Conjugate this by Y to obtain

$$P^{g_1}U^{(1-w)k_1}P^{-g_1} = U^{k_2}Y^{-1}P^2Y_{g_3}^{-1}P^kYU^{(1-w)k_3}Y^{-1}P^{-k}Y_{g_3}P^{-2}YU^{-wk_2}.$$

Multiply on the left by U^{-k_2} and on the right by U^{wk_2} to obtain

$$U^{-k_2}P^{g_1}U^{(1-w)k_1}P^{-g_1}U^{wk_2} = W_1U^{k_3(1-w)}W_1^{-1},$$

(39.2)

$$W_1 = Y^{-1}P^2Y_{g_3}^{-1}P^kY.$$

Suppose that $U^{k_3(1-w)} = 1$. Then (39.2) implies that

$$P^{g_1}U^{(1-w)k_1}P^{-g_1} = U^{(1-w)k_2}.$$

By Hypothesis $k_1 \neq 0$, hence by Lemma 38.2, $U^{(1-w)k_1} \neq 1$. By Lemma 39.1 $g_1 \neq 0$. Thus the above equality cannot hold in the Frobenius group $\mathfrak{P}\mathfrak{U}$. Hence $U^{k_3(1-w)} \neq 1$. This proves statement (i) of the lemma.

Let $U_0 = W_1U^{k_3(1-w)}W_1^{-1}$. By (39.2) U_0 is a conjugate of $U^{k_3(1-w)}$ which lies in $\mathfrak{P}\mathfrak{U}$. All conjugates of $U^{k_3(1-w)}$ which lie in $\mathfrak{U}$ are of the form

$$U^{k_3(1-w)v^{c_3}w^{c'}},$$

with $c_3 \in \mathfrak{X}_p$, $c' \in \mathfrak{X}_q$. Hence

$$U_0 = W_1U^{k_3(1-w)}W_1^{-1} = W_2^{-1}U^{k_3(1-w)v^{c_3}w^{c'}}W_2 \tag{39.3}$$

for some $W_2 \in \mathfrak{P}$. Thus $W_2W_1 \in N(\mathfrak{U})$. Since $Q \in N(\mathfrak{U})$, we get that $Q^{-1}W_2W_1Q \in N(\mathfrak{U})$. By (39.2) $W_1Q = QW_1$, thus $Q^{-1}W_2W_1Q = Q^{-1}W_2QW_1$. Hence

$$W_2Q^{-1}W_2^{-1}Q = W_2W_1(Q^{-1}W_1^{-1}W_2^{-1}Q) \in N(\mathfrak{U}).$$

However $W_2Q^{-1}W_2^{-1}Q \in \mathfrak{P}$. Since $\mathfrak{P} \cap N(\mathfrak{U}) = 1$, this yields that $Q \in C(W_2)$. Hence $W_2 \in \mathfrak{P} \cap C(Q) = \mathfrak{P}^*$. Thus

$$W_2 = P^{c_2} \tag{39.4}$$

for some $c_2 \in \mathscr{Z}_p$. Now (39.2) and (39.4) show that

$$W_2W_1 \in \mathfrak{D}_0\mathfrak{P}^* \cap N(\mathfrak{U}) .$$

Since $P \in N(\langle Z \rangle)$, we have $Y^{-1}PY \in N(\mathfrak{U})$, thus $\mathfrak{D}_0\mathfrak{P}^* \cap N(\mathfrak{U}) = \langle Y^{-1}PY \rangle$. Therefore

$$W_2W_1 = Y^{-1}P^{c_0}Y \tag{39.5}$$

for some $c_0 \in \mathscr{Z}_p$. Consequently

$$(W_2W_1)^{-1}U^{k_3(1-w)v^{c_3}w^{c'}}W_2W_1 = U^{k_3(1-w)v^{c_3+c_0}w^{c'}} .$$

If this is compared with (39.3) we see that

$$c_0 + c_3 = 0, \quad c' = 0 . \tag{39.6}$$

Using (39.4) and (39.6) in (39.5) leads to

$$W_1 = P^{-c_2}Y^{-1}P^{-c_3}Y . \tag{39.7}$$

Comparing (39.2) and (39.7), we get

$$P^{-c_2}Y^{-1}P^{-c_3}Y = Y^{-1}P^{g}Y_{g_3}^{-1}P^{k}Y .$$

Conjugating by Y^{-1} gives

$$YP^{-c_2}Y^{-1}P^{-c_3} = P^{g}Y_{g_3}^{-1}P^{k} . \tag{39.8}$$

If we substitute (39.7) into (39.2) we get

$$U^{-k_2}P^{g_1}U^{(1-w)k_1}P^{-g_1}U^{k_2w} = P^{-c_2}U^{k_3(1-w)v^{c_3}}P^{c_2} .$$

Multiply on the left by $U^{-k_3v^{c_3}}P^{c_2}$ and on the right by $U^{-k_2w}P^{g_1}U^{k_1w}$ to get

$$U^{-k_3v^{c_3}}P^{c_2}U^{-k_2}P^{g_1}U^{k_1} = U^{-wk_3v^{c_3}}P^{c_2}U^{-k_2w}P^{g_1}U^{k_1w} .$$

Since the right hand side is the left hand side conjugated by Q, we see that Q centralizes the left hand side. Hence

$$U^{-k_3v^{c_3}}P^{c_2}U^{-k_2}P^{g_1}U^{k_1} = P^{c_1} \tag{39.9}$$

for some $c_1 \in \mathscr{Z}_p$. Reading (39.9) mod $\mathfrak{P}$ yields that

$$k_1 = k_2 + k_3v^{c_3}$$

which proves (ii) of the lemma. Substituting (ii) of Lemma 39.2

into (39.8) we get that

$$P^{g_2}Y_{g_3}^{-1}P^{k} = Y_{c_2}^{-1}P^{-c_2-c_3}. \tag{39.10}$$

Substituting (39.10) into (39.1) leads to

$$Y_{g_1}Z^{k_1}PY_{g_2}^{-1} = P^{-g_1}Z^{k_2}Y_{c_2}^{-1}P^{-c_2-c_3}Z^{k_3}P^{g_2}.$$

Multiply on the left by P^{g_1} and on the right by P^{-g_2}. Then using Lemma 39.2 (ii) and (iii) this becomes

$$YP^{g_1}Y^{-1}Z^{k_1}PYP^{-g_2}Y^{-1} = Z^{k_2}Y_{c_2}^{-1}P^{-c_2-c_3}Z^{k_3}.$$

Use $Z = YUY^{-1}$ to get

$$YP^{g_1}U^{k_1}Y^{-1}PYP^{-g_2}Y^{-1} = YU^{k_2}Y^{-1}Y_{c_2}^{-1}P^{-c_2-c_3}YU^{k_3}Y^{-1}.$$

Conjugate by Y and multiply on the left by U^{-k_2} to get

$$U^{-k_2}P^{g_1}U^{k_1}Y^{-1}PYP^{-g_2} = Y^{-1}Y_{c_2}^{-1}P^{-c_2-c_3}YU^{k_3}. \tag{39.11}$$

Conjugate by Q and take inverses, then

$$P^{g_2}Y^{-1}P^{-1}YU^{-k_1w}P^{-g_1}U^{k_2w} = U^{-k_3w}Y^{-1}P^{c_2+c_3}Y_{c_2}Y.$$

Multiply by (39.11) on the right to get

$$P^{g_2}Y^{-1}P^{-1}YU^{-k_1w}P^{-g_1}U^{k_2(w-1)}P^{g_1}U^{k_1}Y^{-1}PYP^{-g_2} = U^{k_3(1-w)}.$$

Conjugate by W_1^{-1} to get

$$\begin{aligned} &W_1P^{g_2}Y^{-1}P^{-1}YU^{-k_1w}P^{-g_1}U^{k_2(w-1)}P^{g_1}U^{k_1}Y^{-1}PYP^{-g_2}W_1^{-1} \\ &\quad = W_1U^{k_3(1-w)}W_1^{-1}. \end{aligned}$$

Using (39.2) and (39.3), this yields

$$\begin{aligned} &W_1P^{g_2}Y^{-1}P^{-1}Y\{U^{-k_1w}P^{-g_1}U^{k_2(w-1)}P^{g_1}U^{k_1}\}Y^{-1}PYP^{-g_2}W_1^{-1} \\ &\quad = U_0 = U^{-k_2}P^{g_1}U^{(1-w)k_1}P^{-g_1}U^{wk_2}. \end{aligned} \tag{39.12}$$

Now by the second equation in (39.12)

$$U^{-k_1w}P^{-g_1}U^{k_2w}U^{-k_2}P^{g_1}U^{k_1} = U^{-k_1w}P^{-g_1}U^{k_2w}U_0U^{-k_2w}P^{g_1}U^{k_1w}.$$

Thus the first equation in (39.12) implies that

$$U^{-k_2w}P^{g_1}U^{k_1w}Y^{-1}PYP^{-g_2}W_1^{-1} \in C(U_0).$$

By (39.3) and (39.4), $C(U_0) = P^{-c_2}\mathfrak{U}^*P^{c_2}$. Hence

$$U^{-k_2w}P^{g_1}U^{k_1w}Y^{-1}PYP^{-g_2}W_1^{-1} = P^{-c_2}U_2P^{c_2} \tag{39.13}$$

for some $U_2 \in \mathfrak{U}^*$. We wish to show that $U_2 \in \mathfrak{U}$. To do this conjugate (39.13) by Q to get

$$U^{-k_2w^2}P^{g_1}U^{k_1w^2}Y^{-1}PYP^{-g_2}W_1^{-1} = P^{-c_2}U_2^{w}P^{c_2} \tag{39.14}$$

by (39.7). Multiply (39.13) by the inverse of (39.14) on the right to get

$$U^{-k_2w}P^{g_1}U^{k_1w}U^{-k_1w^2}P^{-g_1}U^{k_2w^2} = P^{-c_2}U_2^{1-w}P^{c_2}\,. \tag{39.15}$$

By Lemma 38.2 U_2 and U_2^{1-w} have the same order. Since the left hand side of (39.15) is in $\mathfrak{B}\mathfrak{U}$, this implies that the order of U_2 divides u, thus $U_2 \in \mathfrak{U}$.

Multiply (39.13) on the left by $U_2^{-1}P^{c_2}$ and on the right by $W_1P^{g_2}Y^{-1}P^{-1}Y$ to get

$$U_2^{-1}P^{c_2}U^{-k_2w}P^{g_1}U^{k_1w} = P^{c_2}W_1P^{g_2}Y^{-1}P^{-1}Y\,. \tag{39.16}$$

By (39.7) the right hand side is in $C(Q)$, while the left hand side is in $\mathfrak{B}\mathfrak{U}$. Since $C(Q) \cap \mathfrak{B}\mathfrak{U} = \mathfrak{B}^*$, this yields that

$$U_2^{-1}P^{c_2}U^{-k_2w}P^{g_1}U^{k_1w} = P^{c''} \tag{39.17}$$

for some $c'' \in \mathscr{Z}_p$. Conjugate by Q^{-1} to get

$$U_2^{-w^{-1}}P^{c_2}U^{-k_2}P^{g_1}U^{k_1} = P^{c''}\,.$$

Comparing this with (39.9) yields that

$$U_2^{w^{-1}}P^{c''} = U^{k_3v^{c_3}}P^{c_1}\,,$$

so that

$$U_2^{w^{-1}} = U^{k_3v^{c_3}}\,, \quad c_1 = c''\,.$$

Using (39.16) and (39.17) this yields

$$P^{c_1} = P^{c_2}W_1P^{g_2}Y^{-1}P^{-1}Y$$

or

$$P^{c_1-c_2}Y^{-1}PYP^{-g_2} = W_1\,.$$

Hence by (39.7)

$$P^{c_1-c_2}Y^{-1}PYP^{-g_2} = P^{-c_2}Y^{-1}P^{-c_3}Y\,.$$

This immediately implies (iii) of the lemma and thus completes the proof.

LEMMA 39.8. *Let* $(a_1, a_2, a_3) \in \mathscr{A}$, *and let* k_1 *have the same meaning as in Lemma* 39.6. *Then* $k_1 = 0$.

Proof. Suppose that $k_1 \neq 0$, so that Lemma 39.7 may be applied. Let

$$h_1 = h(2, a_1v, -3)$$
$$h_2 = h(1, a_2v^3, -2)$$
$$h_3 = h(1, -a_3v^2, -3)\,.$$

By Lemma 38.5 (i)

$$f(2, a_1v, -3) = -a_1v - h_1$$
$$f(1, a_2v^3, -2) = -a_2v^3 - h_2$$
$$f(1, -a_3v^2, -3) = a_3v^2 - h_3\,.$$

Hence in the notation of Lemma 39.6

$$k_1 = h_1 - h_3v^{-1}$$
$$k_2 = a_1v + h_1 - h_2v^{-2}$$
$$k_3 = a_2v^3 + h_2v^{-1} + a_3v^2 - h_3\,.$$

Since $a_1 + a_2 + a_3 = 0$, this yields that

$$k_3 = -a_1v^2 + h_2v^{-1} - h_3$$
$$k_1 - k_2 = -a_1v + h_2v^{-2} - h_3v^{-1}\,.$$

Thus

$$(k_1 - k_2)v = k_3$$

or

$$k_2 + k_3v^{-1} = k_1\,.$$

By Lemma 39.7 (ii) this implies that $k_3(v^{c_3} - v^{-1}) = 0$. If $c_3 \neq -1$, then by Lemma 38.2, $(v^{c_3} - v^{-1})$ has an inverse in $\mathscr{R}_u$. Thus $k_3 = 0$ contrary to Lemma 39.7 (i). Therefore $c_3 = -1$. Now Lemma 39.7 (iii) becomes

$$Y^{-1}PYP^{-g_2} = P^{-c_1}Y^{-1}PY\,. \tag{39.18}$$

Reading (39.18) mod $\mathfrak{Q}$ implies that $g_2 = c_1$. Thus (39.18) yields that $Y^{-1}PY$ and P^{-g_2} commute. Since $g_2 \neq 0$ by Lemma 39.1, this implies that

$$P^{-1}Y^{-1}PY \in \mathfrak{Q}_0 \cap C(P) = \{1\}\,.$$

Thus $Y \in \mathfrak{Q}_0 \cap C(P) = \{1\}$ which is not the case. Therefore $k_1 = 0$ as required.

LEMMA 39.9 *Let* $(a_1, a_2, a_3) \in \mathscr{A}$, *let* k_2 *and* k_3 *have the same meaning as in Lemma* 39.6. *Then* $k_2 = k_3 = 0$.

Proof. Since $k_1 = 0$ by Lemma 39.8, (39.1) becomes

$$Y_{g_1}PY_{g_2}^{-1} = P^{-g_1}Z^{k_2}P^2Y_{g_3}^{-1}P^kZ^{k_3}P^{g_2}. \tag{39.19}$$

Conjugating by Q and using (38.2) we get that

$$Y_{g_1}PY_{g_2}^{-1} = P^{-g_1}Z^{wk_2}P^2Y_{g_3}^{-1}P^kZ^{wk_3}P^{g_2}. \tag{39.20}$$

Now (39.19) and (39.20) imply that

$$Z^{k_2}P^2Y_{g_3}^{-1}P^kZ^{k_3} = Z^{wk_2}P^2Y_{g_3}^{-1}P^kZ^{wk_3}.$$

Therefore

$$P^2Y_{g_3}^{-1}P^kZ^{k_3(1-w)}P^{-k}Y_{g_3}P^{-2} = Z^{k_2(w-1)}. \tag{39.21}$$

Suppose that $k_3 \neq 0$. Then by Lemma 38.2 $k_3(1-w) \neq 0$. As $\langle Z\rangle$ is a T.I. set in $\mathfrak{G}$, (39.21) now implies that $P^2Y_{g_3}^{-1}P^k \in N(\langle Z\rangle)$. As $P \in N(\langle Z\rangle)$ this implies that

$$Y^{-1}P^{-g_3}YP^{g_3} = Y_{g_3} \in N(\langle Z\rangle) \cap \mathfrak{Q}_0 = \langle 1\rangle.$$

Therefore P^{g_3} commutes with Y. Hence $g_3 = 0$. This is contrary to Lemma 39.1. Thus $k_3 = 0$.

Now (39.21) implies that $k_2(w-1) = 0$. Therefore by Lemma 38.2 $k_2 = 0$.

LEMMA 39.10. *Let* $(a_1, a_2, a_3) \in \mathscr{A}$ *and* g_3 *have the same meaning as in Lemma* 39.6. *Then* $g_3 = 1$.

Proof. In view of Lemmas 39.8 and 39.9 equation (39.1) becomes

$$Y_{g_1}PY_{g_2}^{-1} = P^{-g_1}P^2Y_{g_3}^{-1}P^kP^{g_2}. \tag{39.22}$$

Reading (39.22) mod $\mathfrak{Q}_0$ implies that

$$1 = -g_1 + 2 + k + g_2$$

or using the definition of k

$$-1 - g_3 = k = -1 + g_1 - g_2. \tag{39.23}$$

Hence $g_3 = g_2 - g_1$ and (39.22) becomes

$$Y_{g_1}PY_{g_2}^{-1} = P^{2-g_1}Y_{g_2-g_1}^{-1}P^{g_1-1}. \tag{39.24}$$

P acts as a linear transformation on $\mathfrak{Q}_0$. It is convenient to use the exponential notation. Thus $Y^P = P^{-1}YP$, so that $Y_x = Y^{-1+P^x}$. (39.24) can be rewritten as

$$P^{-1}Y_{g_1}PY_{g_2}^{-1} = P^{-(g_1-1)}Y_{g_2-g_1}^{-1}P^{g_1-1}.$$

In exponential notation this becomes

$$Y^{(-1+P^{g_1})P+(1-P^{g_2})} = Y^{(1-P^{g_2-g_1})P^{g_1-1}}. \tag{39.25}$$

Define

$$\begin{aligned} A &= (-1+P^{g_1})P + (1-P^{g_2}) - (1-P^{g_2-g_1})P^{g_1-1} \\ &= (1-P) + P^{g_1-1}(P^2-1) - P^{g_2-1}(P-1). \end{aligned} \tag{39.26}$$

Since $\mathfrak{P}^*\mathfrak{Q}_0$ is a Frobenius group with Frobenius kernel $\mathfrak{Q}_0$, $1-P$ is an invertible linear transformation on $\mathfrak{Q}_0$. By (39.25) A annihilates Y. Hence also $A(1-P)^{-1}$ annihilates Y. By (39.26)

$$\begin{aligned} A(1-P)^{-1} &= 1 - P^{g_1-1}(P+1) + P^{g_2-1} \\ &= 1 - P^{g_1} + 1 - P^{g_1-1} - 1 + P^{g_2-1}. \end{aligned}$$

Therefore

$$Y_{g_2-1}Y_{g_1-1}^{-1}Y_{g_1}^{-1} = Y^{(-1+P^{g_2-1})-(-1+P^{g_1-1})-(-1+P^{g_1})} = 1.$$

Thus

$$Y_{g_2-1} = Y_{g_1}Y_{g_1-1}. \tag{39.27}$$

By Lemma 39.3

$$Y_{g_2-1}^{-1}U^{v^{g_2-1}}Y_{g_2-1} = P^{-(g_2-1)}UP^{(g_2-1)}.$$

By (39.27) this yields that

$$Y_{g_1-1}^{-1}Y_{g_1}^{-1}U^{v^{g_2-1}}Y_{g_1}Y_{g_1-1} = P^{-(g_2-1)}UP^{(g_2-1)}. \tag{39.28}$$

Lemma 39.2 also implies that

$$Y_{g_1}^{-1}U^{v^{g_1}}Y_{g_1} = P^{-g_1}UP^{g_1}.$$

Raising this to the $v^{g_2-g_1-1}$th power we get that

$$Y_{g_1}^{-1}U^{v^{g_2-1}}Y_{g_1} = P^{-g_1}U^{v^{g_2-g_1-1}}P^{g_1}. \tag{39.29}$$

Now (39.28) and (39.29) yield that

$$Y_{g_1-1}^{-1}P^{-g_1}U^{v^{g_2-g_1-1}}P^{g_1}Y_{g_1-1} = P^{-(g_2-1)}UP^{(g_2-1)}. \tag{39.30}$$

Another application of Lemma 39.3 gives

$$Y_{g_1-1}^{-1}U^{v^{g_1-1}}Y_{g_1-1} = P^{-(g_1-1)}UP^{(g_1-1)}. \tag{39.31}$$

Thus (39.30) and (39.31) imply that

$$\begin{aligned} &Y_{g_1-1}^{-1}[P^{-g_1}U^{v^{g_2-g_1-1}}P^{g_1},\ U^{v^{g_1-1}}]Y_{g_1-1} \\ &\quad = [P^{-(g_2-1)}UP^{(g_2-1)},\ P^{-(g_1-1)}UP^{(g_1-1)}]. \end{aligned} \tag{39.32}$$

Since $g_1 \neq 0$, $P^{-g_1}U^{v^{g_2-g_1-1}}P^{g_1} \notin \mathfrak{U}$. Therefore

$$[P^{-g_1}U^{v^{g_2-g_1-1}}P^{g_1},\ U^{v^{g_1-1}}] \in \mathfrak{P}^{\sharp}\ .$$

As $\mathfrak{P}$ is a T.I. set in $\mathfrak{G}$ (39.32) now implies that

$$Y_{g_1-1} \in N(\mathfrak{P}) \cap \mathfrak{Q}_0 = 1\ .$$

Therefore P^{g_1-1} commutes with Y and so $g_1 = 1$. Now (39.27) yields that $Y_{g_2-1} = Y_1$, or

$$Y^{-1}P^{-(g_2-1)}YP^{(g_2-1)} = Y^{-1}P^{-1}YP\ .$$

Consequently $P^{-(g_2-2)}YP^{(g_2-2)} = Y$. Hence $g_2 = 2$. Now (39.23) implies that $g_3 = 1$ as required.

LEMMA 39.11. *Let $\mathscr{B}$ have the same meaning as in Definition* 38.2. *If $a \in \mathscr{B}$ then $-a \in \mathscr{B}$.*

Proof. Let $a = a_1 \in \mathscr{B}$ and suppose that $(a_1, a_2, a_3) \in \mathscr{A}$. By Lemma 38.8 $(-a_2, -a_1, -a_3) \in \mathscr{A}$. Let $(-a_2, -a_1, -a_3)$ play the role of (a_1, a_2, a_3). By Lemma 39.10 $g_3 = g(1, -a_1v^3, -2) = 1$. Thus Lemmas 38.5 and 39.1 imply that

$$-a_1v^3 + f(1, -a_1v^3, -2) + h(1, -a_1v^3, -2) = 0 \tag{39.33}$$

$$\omega^{-a_1v^3} - 2 + \omega^{-a_1v^3+h(1,-a_1v^3,-2)} = 0\ . \tag{39.34}$$

Let $b_1 = -a_1v^3$, $b_2 = f(1, -a_1v^3, -2)$ and $b_3 = h(1, -a_1v^3, -2)$. By Lemma 39.1 $b_i \neq 0$ for $i = 1, 2, 3$. By (39.33) $b_1 + b_2 + b_3 = 0$. Now it follows from (39.34) and Lemma 38.7 that $(b_1, b_2, b_3) \in \mathscr{A}$. Thus $-av^3 = -a_1v^3 = b_1 \in \mathscr{B}$.

Since a was an arbitrary element of $\mathscr{B}$ we get that for any integer n, $a(-v^3)^n \in \mathscr{B}$. Thus in particular, $a(-v^3)^p \in \mathscr{B}$. Hence by (38.2), $-a = -av^{3p} \in \mathscr{B}$ as was to be shown.

It is now very easy to complete the proof of Theorem 37.1.

Define the set $\mathscr{C}$ by

$$\mathscr{C} = \{\omega^a \mid a \in \mathscr{B}\}\ .$$

Since $|\mathscr{B}| = |\mathscr{C}|$, Lemma 38.10 yields that $\mathscr{C}$ is not empty. The definition of $\mathscr{B}$ and Lemma 38.7 yield that $1 \notin \mathscr{C}$ and $\alpha \in \mathscr{C}$ if and only if $2 - \alpha \in \mathscr{C}$. Lemma 39.11 implies that $\alpha \in \mathscr{C}$ if and only if $\alpha^{-1} \in \mathscr{C}$. Therefore if $\alpha \in \mathscr{C}$ then $\dfrac{1}{2-\alpha} \in \mathscr{C}$. Since $u = 1 + p + \cdots + p^{q-1}$, we have $N(\alpha) = \alpha^{1+p+\cdots+p^{q-1}} = 1$ for $\alpha \in \mathscr{C}$. Thus if σ has the same meaning as in Lemma 38.11 then there exists $\alpha \in \mathscr{F}_{p^q} - \mathscr{F}_p$ such that $N(\alpha^{\sigma^i}) = 1$ for all values of i. This contradicts Lemma 38.11, and completes the proof of the main theorem of this paper.