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 $[\mathfrak{P}^*, \mathfrak{U}] \leqq \mathfrak{P}$,