CHAPTER IX

Theorems of Tate and Nakayama

§1. p-Groups

Let p be a prime number. Recall that a finite group G is called a *p-group* if its order Card(G) is a power of p.

Lemma 1. *Suppose* G *is a p-group acting on a finite set* E, *and let* E^G *be the subset of elements fixed by* G. *Then*

$$\mathrm{Card}(E^G) \equiv \mathrm{Card}(E) \quad \text{mod. } p.$$

Indeed, $E - E^G$ is the disjoint union of orbits Gx not reduced to a single point, each having cardinality equal to the index of its stabilizer in G, which is divisible by p.

Lemma 2. *If a p-group acts on a p-group of order* >1, *then the fixed points form a subgroup of order* >1.

Indeed, the number of fixed points is divisible by p (lemma 1).

Theorem 1. *The center of a p-group of order* >1 *has order* >1.

Apply the preceding lemma, letting the group act on itself by inner automorphisms. □

Corollary. *A group* G *of order* p^n *admits a composition series*

$$\{1\} = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$$

with all the G_i *normal in* G (and the G_i/G_{i+1} cyclic of order p).

This follows from theorem 1, by induction on n.

Theorem 2. *Every linear representation* $\neq 0$ *of a p-group over a field of characteristic p contains the unit representation.*

Let E be the representation space. Let x be a non-zero element of E, H the subgroup of E generated by the $s.x$, $s \in G$; H is a finite dimensional vector space over the prime field $\mathbf{F}_p$. Applying lemma 2 to H gives the existence of $y \in H$, $y \neq 0$, such that $s.y = y$ for all $s \in G$. □

Corollary. *Let* G *be a p-group, and let k be a field of characteristic p. The kernel* I_G *of the augmentation homomorphism* $k[G] \to k$ *is the radical of* $k[G]$, *which is a nilpotent ideal.*

Indeed, the radical $\mathfrak{r}$ of kG is the intersection of the kernels of the irreducible representations of $k[G]$ (or of G—it is the same), and theorem 2 shows that the unit representation is the only irreducible representation of G over k; hence $\mathfrak{r} = I_G$. As $k[G]$ is a finite dimensional k-algebra, it is well-known that its radical is nilpotent (cf. Bourbaki, *Alg.*, Chap. VIII, §6, th. 3).

§2. Sylow Subgroups

Theorem 3 (Sylow). *Let* G *be a group of order* $n = p^m q$, *with p prime and* $(p, q) = 1$. *Then there exist subgroups of* G *having order* p^m (called Sylow p-subgroups); *they are all conjugate to one another, and every p-group contained in* G *is contained in one of them.*

Proof (after G. A. Miller and H. Wielandt). Let E be the family of all subsets X of G having p^m elements. The group G operates on E by translations, and

$$\mathrm{Card}(E) = \binom{n}{p^m}.$$

Lemma 3. *If* $n = p^m q$, *with* $(p, q) = 1$, *then*

$$\binom{n}{p^m} \equiv q \quad \text{mod. } p.$$

Indeed, let X and Y be indeterminates over a field of characteristic p. Then

$$(X+Y)^n = (X+Y)^{p^m q} = (X^{p^m} + Y^{p^m})^q = X^{p^m q} + qX^{p^m(q-1)}Y^{p^m} + \cdots + Y^{p^m q},$$

and comparing this with the binomial expansion of $(X+Y)^n$ gives the congruence. □