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*

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

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 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 $r = I_G$. 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*

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

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. □

Back to the proof of Sylow's theorem: lemma 3 shows that $\mathrm{Card}(E) \not\equiv 0 \bmod p$. Hence there exists an $X \in E$ such that the orbit $G.X$ of X in E satisfies $\mathrm{Card}(G.X) \not\equiv 0 \bmod p$. If H is the stabilizer of X (subgroup of all $s \in G$ such that $s.X = X$), then $G.X$ is equipotent to G/H, whence $(G:H) \not\equiv 0 \bmod p$, so that p^m divides the order of H. On the other hand, if $x \in X$, then $H \subset X.x^{-1}$, so

$$\mathrm{Card}(H) \leq \mathrm{Card}(X) = p^m.$$

Therefore $\mathrm{Card}(H) = p^m$ and H is a Sylow p-subgroup of G.

Now let H' be a p-group contained in G, and consider the action of H' on the homogeneous space G/H, where H is a Sylow p-subgroup of G. Since $\mathrm{Card}(G/H) = q \not\equiv 0 \bmod p$, lemma 1 applied to G/H guarantees that the set of fixed points of H' is non-empty; this means that H' is contained in a conjugate of H. If in addition $\mathrm{Card}(H') = p^m$, H' must be equal to a conjugate of H. □

The following "functorial" properties of the Sylow subgroups are immediate consequences of th. 3:

a) If G' is any subgroup of G, then each Sylow p-subgroup of G' is the intersection with G' of a Sylow p-subgroup of G.
b) If G' is any quotient group of G, then the Sylow p-subgroups of G' are the images of the Sylow p-subgroups of G.

Sylow subgroups occur in cohomology via the next theorem.

Theorem 4. *Let G be a finite group, p a prime number, and G_p a Sylow p-subgroup of G. Then for every G-module A and every $n \in \mathbf{Z}$, the restriction homomorphism*

$$\mathrm{Res}: \hat{H}^n(G, A) \to \hat{H}^n(G_p, A)$$

is injective on the p-primary component of $\hat{H}^n(G, A)$.

Given x in the kernel of Res. If $q = \mathrm{Card}(G/G_p)$, then

$$q.x = \mathrm{Cor} \circ \mathrm{Res}(x) = 0 \quad \text{(Chap. VIII, prop. 4).}$$

But if x belongs to the p-primary component of $\hat{H}^n(G, A)$, there is an integer r such that $p^r.x = 0$. As $(q, p^r) = 1$, it follows that $x = 0$. □

Corollary. *Let G be a finite group, A a G-module, n an integer. Suppose that for every prime number p, $\hat{H}^n(G_p, A) = 0$, where G_p is a Sylow p-subgroup of G. Then $\hat{H}^n(G, A) = 0$.*

Indeed, all the primary components of $\hat{H}^n(G, A)$ are zero.

Remark. A characterisation of the *image* of $\mathrm{Res}: \hat{H}^n(G, A) \to \hat{H}^n(G_p, A)$ is given in Cartan-Eilenberg ([13], Chap. XII, th. 10.1).

EXERCISES

1. With the notation from the proof of th. 3, let d be the number of Sylow p-subgroups of G. Show that the number of translates of these subgroups is dq; by comparing with the number of elements of E, deduce that $d \equiv 1 \bmod p$.
2. Let G be a subgroup of a finite group $\tilde{G}$, and let $\tilde{P}$ be a p-Sylow subgroup of $\tilde{G}$.
   a) Show that there is a conjugate of $\tilde{P}$ whose intersection with G is a p-Sylow subgroup of G. (Hint: make G act on $\tilde{G}/\tilde{P}$ and note that one of the orbits has order prime to p.)
   b) Deduce from a) another proof of the existence of a p-subgroup of G (take for $\tilde{G}$ a group for which the existence of p-Sylow subgroups can be checked directly, for instance $GL_n(\mathbf{Z}/p\mathbf{Z})$.)

§3. Induced Modules; Cohomologically Trivial Modules

Let G be a finite group and A a G-module. A is called *cohomologically trivial* if, for every subgroup H of G and every $n \in \mathbf{Z}$, $\hat{H}^n(H, A) = 0$.

EXAMPLES. Every *induced* module is cohomologically trivial: indeed, such a module is also induced for every subgroup H of G, and we saw in Chap. VIII, §1 that the cohomology vanishes. The same holds for *relatively projective* modules, since they are direct factors of induced modules.

Starting with an induced module A, other examples can be constructed by the following process:

Let $\mathscr{C}$ be the category of abelian groups, $T: \mathscr{C} \times \mathscr{C} \to \mathscr{C}$ an additive bifunctor that we take to be bicovariant (to fix ideas). If A and B are G-modules, define a G-module structure on $T(A, B)$ as follows: each $s \in G$ defines an element $s_A \in \mathrm{Hom}(A, A)$ and an element $s_B \in \mathrm{Hom}(B, B)$, hence an element $T(s_A, s_B) \in \mathrm{Hom}(T(A, B), T(A, B))$: this is the automorphism of $T(A, B)$ associated to s.

Proposition 1. *If A is induced* (resp. *relatively projective*), *then $T(A, B)$ is induced* (resp. *relatively projective*), *hence cohomologically trivial.*

We may assume that A is induced (passing to a direct factor otherwise); then A is the direct sum of the $s.A'$ for some subgroup A'. The group $T(A, B)$ is then the direct sum of the $T(s.A', B)$; however, $T(s.A', B) = T(s.A', s.B) = s.T(A', B)$, so $T(A, B)$ is induced. □

Corollary. *Suppose one of the G-modules A, B is relatively projective. Then the G-modules below are relatively projective (hence cohomologically trivial):*

$$A \otimes B, \quad \mathrm{Hom}(A, B), \quad \mathrm{Tor}(A, B), \quad \mathrm{Ext}(A, B).$$

[Of course, the functors $\otimes$, Hom, ..., are relative to the ring $\mathbf{Z}$ of integers.]

§4. Cohomology of a p-Group

Lemma 4. *Let* G *be a p-group and* A *a* G*-module such that* $pA = 0$. *Then the three following conditions are equivalent*:

i) $A = 0$.
ii) $H^0(G, A) = 0$.
iii) $H_0(G, A) = 0$.

The implications i) $\Rightarrow$ ii) and i) $\Rightarrow$ iii) are trivial. The implication ii) $\Rightarrow$ i) has been proved in theorem 2. Let us show that iii) $\Rightarrow$ i). Let $A' = \mathrm{Hom}(A, \mathbf{F}_p)$ be the dual of A as an $\mathbf{F}_p$-vector space. It is easily seen that $H^0(G, A')$ is dual to $H_0(G, A)$. Hence $H^0(G, A') = 0$, whence $A' = 0$ and $A = 0$.

[Another proof that iii) $\Rightarrow$ i): Let $\mathfrak{r}$ be the augmentation ideal of $\mathbf{F}_p[G]$. The vanishing of $H_0(G, A)$ means that $A = \mathfrak{r}A$. But $\mathfrak{r}$ is nilpotent (cor. to th. 2). Hence $A = 0$.]

Lemma 5. *With the hypotheses of lemma* 4, *suppose that* $H_1(G, A) = 0$. *Then* A *is a free module over the algebra* $\Lambda = \mathbf{F}_p[G]$.

Let $\mathfrak{r}$ be the augmentation ideal of Λ. Then $A/\mathfrak{r}A = H_0(G, A)$, and this is a vector space over $\mathbf{F}_p$. Let h_λ be a basis of this vector space, and lift it to a family $a_\lambda \in A$. Since the h_λ generate $A/\mathfrak{r}A$, the a_λ generate A (apply lemma 4 to the quotient of A by the sub-Λ-module generated by the a_λ). Thus we have defined a surjective G-homomorphism of a free Λ-module L onto A; by construction, this homomorphism induces an isomorphism of $L/\mathfrak{r}L$ onto $A/\mathfrak{r}A$. Let R be the kernel of this homomorphism. Then there is an exact sequence

$$H_1(G, A) \to H_0(G, R) \to H_0(G, L) \to H_0(G, A).$$

As $H_1(G, A) = 0$ and $H_0(G, L) \to H_0(G, A)$ is bijective, it follows that $H_0(G, R) = 0$, whence $R = 0$ (lemma 4). □

Remark. The two lemmas above are special cases of general theorems on "non-commutative local rings"—cf. Bourbaki, *Alg. comm.*, Chap. II, §3.

Theorem 5. *Let* G *be a p-group and* A *a* G*-module annihilated by* p. *The following conditions are equivalent*:

i) *There exists an integer* q *such that* $\hat{H}^q(G, A) = 0$,
ii) A *is cohomologically trivial,*
iii) A *is an induced* G*-module,*
iv) A *is a free* $\mathbf{F}_p[G]$*-module.*

Obviously it suffices to prove i) $\Rightarrow$ iv). The shifting procedure already used several times enables us to construct a G-module B, annihilated by p,

such that $\hat{H}^n(G, A) = \hat{H}^{n-q-2}(G, B)$ for all n. If $\hat{H}^q(G, A) = 0$, then $H_1(G, B) = 0$, hence, by lemma 5, B is Λ-free. Its cohomology groups are then zero; in particular,

$$H_1(G, A) = \hat{H}^{-2}(G, A) = \hat{H}^{-q-4}(G, B) = 0,$$

and lemma 5 concludes the proof. □

Theorem 6. *Let* G *be a p-group and let* A *be a* G*-module without p-torsion. The following conditions are equivalent*:

i) $\hat{H}^q(G, A) = 0$ *for two consecutive values of* q,
ii) A *is cohomologically trivial,*
iii) *the* $\mathbf{F}_p[G]$*-module* A/pA *is free.*

Since A has no p-torsion, there is an exact sequence

$$0 \to A \xrightarrow{p} A \to A/pA \to 0.$$

Passing to the cohomology gives the exact sequence

$$\hat{H}^q(G, A) \xrightarrow{p} \hat{H}^q(G, A) \to \hat{H}^q(G, A/pA) \to \hat{H}^{q+1}(G, A) \xrightarrow{p} \hat{H}^{q+1}(G, A).$$

If $\hat{H}^q(G, A) = \hat{H}^{q+1}(G, A) = 0$, this sequence shows that $\hat{H}^q(G, A/pA) = 0$, and A/pA is free by th. 5. Thus i) $\Rightarrow$ iii). If iii) holds, the same exact sequence shows that multiplication by p is bijective on all the $\hat{H}^q(G, A)$; as this endomorphism is nilpotent, $\hat{H}^q(G, A) = 0$. The same reasoning applies to every subgroup H of G, for A/pA is $\mathbf{F}_p[H]$-free. Therefore iii) $\Rightarrow$ ii). Finally, the implication ii) $\Rightarrow$ i) is trivial. □

Corollary. *Let* A *be a* $\mathbf{Z}$*-free* G*-module satisfying the equivalent conditions of theorem* 6. *Then for every torsion-free* G*-module* B, *the* G*-module* $N = \mathrm{Hom}_{\mathbf{Z}}(A, B)$ *is cohomologically trivial.*

The module N is torsion-free. We will check that N/pN is cohomologically trivial; this will imply the result we seek, in view of the preceding theorems. The exact sequence

$$0 \to B \xrightarrow{p} B \to B/pB \to 0$$

gives the exact sequence

$$0 \to N \xrightarrow{p} N \to \mathrm{Hom}(A, B/pB) \to 0$$

whence an isomorphism $N/pN = \mathrm{Hom}(A/pA, B/pB)$. Now A/pA is free over $\mathbf{F}_p[G]$, hence induced, so the corollary to prop. 1 insures that N/pN is cohomologically trivial. □

Remark. This corollary is in fact only a lemma for th. 7 below; once that theorem is proved, we will know that A is projective, hence N is relatively projective.

§5. Cohomology of a Finite Group

Theorem 7. *Let* G *be a finite group,* A *a* **Z***-free* G*-module, and* G_p *a Sylow p-subgroup of* G*, for each p. The following conditions are equivalent*:

i) *For every prime number p, the* G_p*-module* A *satisfies the equivalent conditions of theorem* 6,
ii) A *is* **Z**[G]*-projective.*

We must show that i) implies ii). Write A as a quotient of a free **Z**[G]-module L:

$$0 \to N \to L \to A \to 0.$$

The **Z**-module A being free yields the exact sequence

$$(*) \qquad 0 \to \mathrm{Hom}_{\mathbf{Z}}(A, N) \to \mathrm{Hom}_{\mathbf{Z}}(A, L) \to \mathrm{Hom}_{\mathbf{Z}}(A, A) \to 0.$$

By the corollary to theorem 6, i) implies that the G_p-module $\mathrm{Hom}_{\mathbf{Z}}(A, N)$ has cohomology zero in all dimensions, therefore that $H^1(G, \mathrm{Hom}_{\mathbf{Z}}(A, N)) = 0$ by the corollary to th. 4.

The exact cohomology sequence (*) then shows that

$$\mathrm{Hom}_G(A, L) \to \mathrm{Hom}_G(A, A)$$

is surjective; in particular, the identity map of A extends to a G-homomorphism of A into L, so that A is a direct factor of L as G-module, i.e., projective. □

Remark. Let P, P′ be projective modules of finite type over **Z**[G]; call them *equivalent* if there exist free modules L, L′ of finite type such that $P \oplus L$ is isomorphic to $P' \oplus L'$. Let P(G) be the set of equivalence classes of projective **Z**[G]-modules of finite type (for this equivalence relation). The law of composition $(P, P') \to P \oplus P'$ makes P(G) into an abelian group, called the *group of classes of projective* G*-modules.* When G is cyclic of prime order *p*, it has been shown by Rim [51] that P(G) is isomorphic to the group of ideal classes of the field of *p*th roots of unity; in particular, $P(G) \neq 0$, which shows the existence of projective G-modules that are not free. Swan [62] has made a deeper study of P(G), showing in particular that it is a *finite* group.

Lemma 6. *Let* $0 \to X_1 \to X_2 \to \cdots \to X_n \to 0$ *be an exact sequence of* G*-modules. If all but one of the* X_i *are cohomologically trivial, then that one also is.*

Put $N_i = \mathrm{Ker}(X_i \to X_{i+1})$, $N_0 = N_{n+1} = 0$. Then there are $n+1$ exact sequences

$$(E_i) \qquad 0 \to N_i \to X_i \to N_{i+1} \to 0, \qquad 0 \leq i \leq n.$$

If X_i is cohomologically trivial for $i \neq q$, then the sequences $E_0, \ldots, E_{q-1}$ show that $N_1, \ldots, N_q$ are cohomologically trivial, and $E_{q+1}, \ldots, E_n$ show that $N_{q+1}, \ldots, N_n$ are too. Conclude by using sequence E_q. □

Theorem 8. *Let* A *be any* G*-module. The following are equivalent*:

i) *For every prime p,* $\hat{H}^q(G_p, A) = 0$ *for two consecutive values of q* (that may depend on *p*),
ii) A *is cohomologically trivial,*
iii) *There exists an exact sequence* $0 \to P_k \to P_{k-1} \to \cdots \to P_0 \to A \to 0$, *where the* P_i *are projective* **Z**[G]*-modules,*
iv) *There exists an exact sequence* $0 \to P_1 \to P_0 \to A \to 0$, *where the* P_i *are* **Z**[G]*-projective.*

(In the terminology of Cartan-Eilenberg, condition iii) means that the *projection dimension* of A is finite, and condition iv) that it is ≤ 1.)

We have iv) ⇒ iii) trivially, iii) ⇒ ii) by lemma 6, and ii) ⇒ i) trivially. Let us show i) ⇒ iv): Let $0 \to R \to L \to A \to 0$ be an exact sequence of G-modules, with L free over **Z**[G]: *a fortiori*, L is **Z**-free, hence also R. On the other hand, R satisfies hypothesis i) of th. 7, so is **Z**[G]-projective. □

Theorem 9. *Let* A, B *be* G*-modules, with* A *cohomologically trivial. In order that* $A \otimes B$ (resp. Hom(A, B), resp. Hom(B, A)) *be cohomologically trivial, it is necessary and sufficient that* Tor(A, B) (resp. Ext(A, B), resp. Ext(B, A)) *be.*

(Once more, the functors ⊗, Tor, etc. are taken over the ring **Z**.)

By th. 8, iv), A has a resolution by projective modules

$$0 \to P_1 \to P_0 \to A \to 0.$$

Hence there is an exact sequence

$$0 \to \mathrm{Tor}(A, B) \to P_1 \otimes B \to P_0 \otimes B \to A \otimes B \to 0.$$

The corollary to prop. 1 shows that $P_1 \otimes B$ and $P_0 \otimes B$ are cohomologically trivial; applying lemma 6, we see that $A \otimes B$ is cohomologically trivial if and only if Tor(A, B) is. Same proof for Hom(A, B) and Ext(A, B). For Hom(B, A), use the six term exact sequence

$$0 \to \mathrm{Hom}(B, P_1) \to \mathrm{Hom}(B, P_0) \to \mathrm{Hom}(B, A) \to \mathrm{Ext}(B, P_1) \to \mathrm{Ext}(B, P_0) \to \mathrm{Ext}(B, A) \to 0.$$

The corollary to prop. 1 shows that the four modules

$$\mathrm{Hom}(B, P_1), \quad \mathrm{Hom}(B, P_0), \quad \mathrm{Ext}(B, P_1), \quad \mathrm{Ext}(B, P_0)$$

are cohomologically trivial; conclude, as before, by applying lemma 6. □

Corollary. *If* A *is cohomologically trivial, and if* A *or* B *is torsion-free, then* $A \otimes B$ *is cohomologically trivial.*

Indeed, Tor(A, B) is zero.