

This is easily seen by applying say  $B$  to an arbitrary vector  $x$ , and using the definition of  $T_u$ . In each case, for some  $x$  the left-hand side cannot equal the right-hand side.

For any vector  $x \in F^{(n)}$  we have

$$Bx - x \in (u, v),$$

where  $(u, v)$  is the plane generated by  $u, v$ . It follows that  $BH \subset H$ , so

$$BH = H \quad \text{and} \quad Bx - x \in H.$$

We now distinguish two cases to conclude the proof. First assume that  $B$  commutes with all transvections with respect to  $H$ . Let  $w \in H$ . Then from the definitions, we find for any vector  $x$ :

$$BT_w x = Bx + \lambda(x)Bw$$

$$T_w Bx = Bx + \lambda(Bx)w = Bx + \lambda(x)w.$$

Since we are in the case  $BT_w = T_w B$ , it follows that  $Bw = w$ . Therefore  $B$  leaves every vector of  $H$  fixed. Since we have seen that  $Bx - x \in H$  for all  $x$ , it follows that  $B$  is a transvection and is in  $G$ , thus proving the theorem in this case.

Second, suppose there is a transvection  $T_w$  with  $w \in H$  such that  $B$  does not commute with  $T_w$ . Let

$$C = BT_w B^{-1} T_w^{-1}.$$

Then  $C \neq I$  and  $C \in G$ . Furthermore  $C$  is a product of  $T_w^{-1}$  and  $BT_w B^{-1}$  whose hyperplanes are  $H$  and  $BH$ , which is also  $H$  by what we have already proved. Therefore  $C$  is a transvection, since it is a product of transvections with the same hyperplane. And  $C \in G$ . This concludes the proof in the second case, and also concludes the proof of Theorem 9.6.

We now return to the main theorem, that  $PSL_n(F)$  is simple. Let  $\bar{G}$  be a normal subgroup of  $PSL_n(F)$ , and let  $G$  be its inverse image in  $SL_n(F)$ . Then  $G$  is  $SL_n$ -invariant, and if  $\bar{G} \neq 1$ , then  $G$  is not equal to the center of  $SL_n(F)$ . Therefore  $G$  contains  $SL_n(F)$  by Theorem 9.6, and therefore  $\bar{G} = PSL_n(F)$ , thus proving that  $PSL_n(F)$  is simple.

**Example.** By Exercise 41 of Chapter I, or whatever other means, one sees that  $PSL_2(\mathbf{F}_5) \approx A_5$  (where  $\mathbf{F}_5$  is the finite field with 5 elements). While you are in the mood, show also that

$$PGL_2(\mathbf{F}_3) \approx S_4 \quad \text{but} \quad SL_2(\mathbf{F}_3) \neq S_4; \quad PSL_2(\mathbf{F}_3) \approx A_4.$$

---

**EXERCISES**

1. Interpret the rank of a matrix  $A$  in terms of the dimensions of the image and kernel of the linear map  $L_A$ .
2. (a) Let  $A$  be an invertible matrix in a commutative ring  $R$ . Show that  $(A)^{-1} = {}^t(A^{-1})$ .  
 (b) Let  $f$  be a non-singular bilinear form on the module  $E$  over  $R$ . Let  $A$  be an  $R$ -automorphism of  $E$ . Show that  $({}^t A)^{-1} = {}^t(A^{-1})$ . Prove the same thing in the hermitian case, i.e.  $(A^*)^{-1} = (A^{-1})^*$ .
3. Let  $V$ ,  $W$  be finite dimensional vector spaces over a field  $k$ . Suppose given non-degenerate bilinear forms on  $V$  and  $W$  respectively, denoted both by  $\langle \cdot, \cdot \rangle$ . Let  $L: V \rightarrow W$  be a surjective linear map and let  ${}^t L$  be its transpose; that is,  $\langle Lv, w \rangle = \langle v, {}^t Lw \rangle$  for  $v \in V$  and  $w \in W$ .  
 (a) Show that  ${}^t L$  is injective.  
 (b) Assume in addition that if  $v \in V$ ,  $v \neq 0$  then  $\langle v, v \rangle \neq 0$ . Show that

$$V = \text{Ker } L \oplus \text{Im } {}^t L,$$

and that the two summands are orthogonal. (Cf. Exercise 33 for an example.)

4. Let  $A_1, \dots, A_r$  be row vectors of dimension  $n$ , over a field  $k$ . Let  $X = (x_1, \dots, x_n)$ . Let  $b_1, \dots, b_r \in k$ . By a system of linear equations in  $k$  one means a system of type

$$A_1 \cdot X = b_1, \dots, A_r \cdot X = b_r.$$

If  $b_1 = \dots = b_r = 0$ , one says the system is homogeneous. We call  $n$  the number of variables, and  $r$  the number of equations. A solution  $X$  of the homogeneous system is called **trivial** if  $x_i = 0$ ,  $i = 1, \dots, n$ .

- (a) Show that a homogeneous system of  $r$  linear equations in  $n$  unknowns with  $n > r$  always has a non-trivial solution.  
 (b) Let  $L$  be a system of homogeneous linear equations over a field  $k$ . Let  $k$  be a subfield of  $k'$ . If  $L$  has a non-trivial solution in  $k'$ , show that it has a non-trivial solution in  $k$ .
5. Let  $M$  be an  $n \times n$  matrix over a field  $k$ . Assume that  $\text{tr}(MX) = 0$  for all  $n \times n$  matrices  $X$  in  $k$ . Show that  $M = O$ .
6. Let  $S$  be a set of  $n \times n$  matrices over a field  $k$ . Show that there exists a column vector  $X \neq 0$  of dimension  $n$  in  $k$ , such that  $MX = X$  for all  $M \in S$  if and only if there exists such a vector in some extension field  $k'$  of  $k$ .
7. Let  $\mathbf{H}$  be the division ring over the reals generated by elements  $i, j, k$  such that  $i^2 = j^2 = k^2 = -1$ , and

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Then  $\mathbf{H}$  has an automorphism of order 2, given by

$$a_0 + a_1i + a_2j + a_3k \mapsto a_0 - a_1i - a_2j - a_3k.$$

Denote this automorphism by  $\alpha \mapsto \bar{\alpha}$ . What is  $\alpha\bar{\alpha}$ ? Show that the theory of hermitian

forms can be carried out over  $\mathbf{H}$ , which is called the division ring of **quaternions** (or by abuse of language, the non-commutative field of quaternions).

8. Let  $N$  be a strictly upper triangular  $n \times n$  matrix, that is  $N = (a_{ij})$  and  $a_{ij} = 0$  if  $i \geq j$ . Show that  $N^n = 0$ .
9. Let  $E$  be a vector space over  $k$ , of dimension  $n$ . Let  $T: E \rightarrow E$  be a linear map such that  $T$  is nilpotent, that is  $T^m = 0$  for some positive integer  $m$ . Show that there exists a basis of  $E$  over  $k$  such that the matrix of  $T$  with respect to this basis is strictly upper triangular.
10. If  $N$  is a nilpotent  $n \times n$  matrix, show that  $I + N$  is invertible.
11. Let  $R$  be the set of all upper triangular  $n \times n$  matrices  $(a_{ij})$  with  $a_{ij}$  in some field  $k$ , so  $a_{ij} = 0$  if  $i > j$ . Let  $J$  be the set of all strictly upper triangular matrices. Show that  $J$  is a two-sided ideal in  $R$ . How would you describe the factor ring  $R/J$ ?
12. Let  $G$  be the group of upper triangular matrices with non-zero diagonal elements. Let  $H$  be the subgroup consisting of those matrices whose diagonal element is 1. (Actually prove that  $H$  is a subgroup). How would you describe the factor group  $G/H$ ?
13. Let  $R$  be the ring of  $n \times n$  matrices over a field  $k$ . Let  $L$  be the subset of matrices which are 0 except on the first column.
  - (a) Show that  $L$  is a left ideal.
  - (b) Show that  $L$  is a minimal left ideal; that is, if  $L' \subset L$  is a left ideal and  $L' \neq 0$ , then  $L' = L$ . (For more on this situation, see Chapter VII, §5.)
14. Let  $F$  be any field. Let  $D$  be the subgroup of diagonal matrices in  $GL_n(F)$ . Let  $N$  be the normalizer of  $D$  in  $GL_n(F)$ . Show that  $N/D$  is isomorphic to the symmetric group on  $n$  elements.
15. Let  $F$  be a finite field with  $q$  elements. Show that the order of  $GL_n(F)$  is

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1).$$

[*Hint:* Let  $x_1, \dots, x_n$  be a basis of  $F^n$ . Any element of  $GL_n(F)$  is uniquely determined by its effect on this basis, and thus the order of  $GL_n(F)$  is equal to the number of all possible bases. If  $A \in GL_n(F)$ , let  $Ax_i = y_i$ . For  $y_1$  we can select any of the  $q^n - 1$  non-zero vectors in  $F^n$ . Suppose inductively that we have already chosen  $y_1, \dots, y_r$  with  $r < n$ . These vectors span a subspace of dimension  $r$  which contains  $q^r$  elements. For  $y_{r+1}$  we can select any of the  $q^n - q^r$  elements outside of this subspace. The formula drops out.]

16. Again let  $F$  be a finite field with  $q$  elements. Show that the order of  $SL_n(F)$  is

$$q^{n(n-1)/2} \prod_{i=2}^n (q^i - 1);$$

and that the order of  $PSL_n(F)$  is

$$\frac{1}{d} q^{n(n-1)/2} \prod_{i=2}^{n-1} (q^i - 1),$$

where  $d$  is the greatest common divisor of  $n$  and  $q - 1$ .

17. Let  $F$  be a finite field with  $q$  elements. Show that the group of all upper triangular matrices with 1 on the diagonal is a Sylow subgroup of  $GL_n(F)$  and of  $SL_n(F)$ .
18. The reduction map  $\mathbf{Z} \rightarrow \mathbf{Z}/N\mathbf{Z}$ , where  $N$  is a positive integer defines a homomorphism

$$SL_2(\mathbf{Z}) \rightarrow SL_2(\mathbf{Z}/N\mathbf{Z}).$$

Show that this homomorphism is surjective. [Hint: Use elementary divisors, i.e. the structure of submodules of rank 2 over the principal ring  $\mathbf{Z}$ .]

19. Show that the order of  $SL_2(\mathbf{Z}/N\mathbf{Z})$  is equal to

$$N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

where the product is taken over all primes dividing  $N$ .

20. Show that one has an exact sequence

$$1 \rightarrow SL_2(\mathbf{Z}/N\mathbf{Z}) \rightarrow GL_2(\mathbf{Z}/N\mathbf{Z}) \xrightarrow{\det} (\mathbf{Z}/N\mathbf{Z})^* \rightarrow 1.$$

In fact, show that

$$GL_2(\mathbf{Z}/N\mathbf{Z}) = SL_2(\mathbf{Z}/N\mathbf{Z})G_N,$$

where  $G_N$  is the group of matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \quad \text{with} \quad d \in (\mathbf{Z}/N\mathbf{Z})^*.$$

21. Show that  $SL_2(\mathbf{Z})$  is generated by the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

22. Let  $p$  be a prime  $\geq 5$ . Let  $G$  be a subgroup of  $SL_2(\mathbf{Z}/p^n\mathbf{Z})$  with  $n \geq 1$ . Assume that the image of  $G$  in  $SL_2(\mathbf{Z}/p\mathbf{Z})$  under the natural homomorphism is all of  $SL_2(\mathbf{Z}/p\mathbf{Z})$ . Prove that  $G = SL_2(\mathbf{Z}/p^n\mathbf{Z})$ .

*Note.* Exercise 22 is a generalization by Serre of a result of Shimura; see Serre's *Abelian  $\ell$ -adic Representations and elliptic curves*, Benjamin, 1968, IV, §3, Lemma 3. See also my exposition in *Elliptic Functions*, Springer Verlag, reprinted from Addison-Wesley, 1973, Chapter 17, §4.

23. Let  $k$  be a field in which every quadratic polynomial has a root. Let  $B$  be the Borel subgroup of  $GL_2(k)$ . Show that  $G$  is the union of all the conjugates of  $B$ . (This cannot happen for finite groups!)
24. Let  $A, B$  be square matrices of the same size over a field  $k$ . Assume that  $B$  is non-singular. If  $t$  is a variable, show that  $\det(A + tB)$  is a polynomial in  $t$ , whose leading coefficient is  $\det(B)$ , and whose constant term is  $\det(A)$ .
25. Let  $a_{11}, \dots, a_{1n}$  be elements from a principal ideal ring, and assume that they generate the unit ideal. Suppose  $n > 1$ . Show that there exists a matrix  $(a_{ij})$  with this given first row, and whose determinant is equal to 1.

26. Let  $A$  be a commutative ring, and  $I = (x_1, \dots, x_r)$  an ideal. Let  $c_{ij} \in A$  and let

$$y_i = \sum_{j=1}^r c_{ij} x_j.$$

Let  $I' = (y_1, \dots, y_r)$ . Let  $D = \det(c_{ij})$ . Show that  $DI \subset I'$ .

27. Let  $L$  be a free module over  $\mathbb{Z}$  with basis  $e_1, \dots, e_n$ . Let  $M$  be a free submodule of the same rank, with basis  $u_1, \dots, u_n$ . Let  $u_i = \sum c_{ij} e_j$ . Show that the index  $(L : M)$  is given by the determinant:

$$(L : M) = |\det(c_{ij})|.$$

28. (**The Dedekind determinant**). Let  $G$  be a finite commutative group and let  $F$  be the vector space of functions of  $G$  into  $\mathbb{C}$ . Show that the characters of  $G$  (homomorphisms of  $G$  into the roots of unity) form a basis for this space. If  $f : G \rightarrow \mathbb{C}$  is a function, show that for  $a, b \in G$ ,

$$\det(f(ab^{-1})) = \prod_x \sum_{a \in G} \chi(a) f(a),$$

where the product is taken over all characters. [Hint: Use both the characters and the characteristic functions of elements of  $G$  as bases for  $F$ , and consider the linear map

$$T = \sum f(a) T_a,$$

where  $T_a$  is translation by  $a$ .] Also show that

$$\det(f(ab^{-1})) = \left( \sum_{a \in G} f(a) \right) \det(f(ab^{-1}) - f(b^{-1})),$$

where the determinant on the left is taken for all  $a, b \in G$ , and the determinant on the right is taken only for  $a, b \neq 1$ .

29. Let  $\mathfrak{g}$  be a module over the commutative ring  $R$ . A bilinear map  $\mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$ , written  $(x, y) \mapsto [x, y]$ , is said to make  $\mathfrak{g}$  a **Lie algebra** if it is anti-symmetric, i.e.  $[x, y] = -[y, x]$ , and if the map  $D_x : \mathfrak{g} \rightarrow \mathfrak{g}$  defined by  $D_x(y) = [x, y]$  is a derivation of  $\mathfrak{g}$  into itself, that is

$$D([y, z]) = [Dy, z] + [y, Dz] \quad \text{and} \quad D(cy) = cD(y)$$

for all  $x, y, z \in \mathfrak{g}$  and  $c \in R$ .

- (a) Let  $A$  be an associative algebra over  $R$ . For  $x, y \in A$ , define  $[x, y] = xy - yx$ . Show that this makes  $A$  into a Lie algebra. Example: the algebra of  $R$ -endomorphisms of a module  $M$ , especially the algebra of matrices  $\text{Mat}_n(R)$ .
- (b) Let  $M$  be a module over  $R$ . For two derivations  $D_1, D_2$  of  $M$ , define  $[D_1, D_2] = D_1 D_2 - D_2 D_1$ . Show that the set of derivations of  $M$  is a Lie subalgebra of  $\text{End}_R(M)$ .
- (c) Show that the map  $x \mapsto \bar{D}_x$  is a Lie homomorphism of  $\mathfrak{g}$  into the Lie algebra of derivations of  $\mathfrak{g}$  into itself.
30. Given a set of polynomials  $\{P_v(X_{ij})\}$  in the polynomial ring  $R[X_{ij}]$  ( $1 \leq i, j \leq n$ ), a zero of this set in  $R$  is a matrix  $x = (x_{ij})$  such that  $x_{ij} \in R$  and  $P_v(x_{ij}) = 0$  for all  $v$ . We use vector notation, and write  $(X) = (X_{ij})$ . We let  $G(R)$  denote the set of zeros

of our set of polynomials  $\{P_v\}$ . Thus  $G(R) \subset M_n(R)$ , and if  $R'$  is any commutative associative  $R$ -algebra we have  $G(R') \subset M_n(R')$ . We say that the set  $\{P_v\}$  defines an **algebraic group over  $R$**  if  $G(R')$  is a subgroup of the group  $GL_n(R')$  for all  $R'$  (where  $GL_n(R')$  is the multiplicative group of invertible matrices in  $R'$ ).

As an example, the group of matrices satisfying the equation  $XX = I_n$  is an algebraic group.

Let  $R'$  be the  $R$ -algebra which is free, with a basis  $\{1, t\}$  such that  $t^2 = 0$ . Thus  $R' = R[t]$ . Let  $\mathfrak{g}$  be the set of matrices  $x \in M_n(R)$  such that  $I_n + tx \in G(R[t])$ . Show that  $\mathfrak{g}$  is a Lie algebra. [Hint: Note that

$$P_v(I_n + tX) = P_v(I_n) + \text{grad } P_v(I_n)tX.$$

Use the algebra  $R[t, u]$  where  $t^2 = u^2 = 0$  to show that if  $I_n + tx \in G(R[t])$  and  $I_n + uy \in G(R[u])$  then  $[x, y] \in \mathfrak{g}$ .]

(I have taken the above from the first four pages of [Se 65]. For more information on Lie algebras and Lie Groups, see [Bo 82] and [Ja 79].

[Bo 82] N. BOURBAKI, *Lie Algebras and Lie Groups*, Masson, 1982

[Ja 79] N. JACOBSON, *Lie Algebras*, Dover, 1979 (reprinted from Interscience, 1962)

[Se 65] J. P. SERRE, *Lie Algebras and Lie Groups*, Benjamin, 1965. Reprinted Springer Lecture Notes 1500. Springer/Verlag 1992

### Non-commutative cocycles

Let  $K$  be a finite Galois extension of a field  $k$ . Let  $\Gamma = GL_n(K)$ , and  $G = \text{Gal}(K/k)$ . Then  $G$  operates on  $\Gamma$ . By a **cocycle** of  $G$  in  $\Gamma$  we mean a family of elements  $\{A(\sigma)\}$  satisfying the relation

$$A(\sigma)\sigma A(\tau) = A(\sigma\tau).$$

We say that the cocycle **splits** if there exists  $B \in \Gamma$  such that

$$A(\sigma) = B^{-1}\sigma B \quad \text{for all } \sigma \in G.$$

In this non-commutative case, cocycles do not form a group, but one could define an equivalence relation to define cohomology classes. For our purposes here, we care only whether a cocycle splits or not. When every cocycle splits, we also say that  $H^1(G, \Gamma) = 0$  (or 1).

31. Prove that  $H^1(G, GL_n(K)) = 1$ . [Hint: Let  $\{e_1, \dots, e_N\}$  be a basis of  $\text{Mat}_n(k)$  over  $k$ , say the matrices with 1 in some component and 0 elsewhere. Let

$$x = \sum_{i=1}^N x_i e_i$$

with variables  $x_i$ . There exists a polynomial  $P(X)$  such that  $x$  is invertible if and only if  $P(x_1, \dots, x_N) \neq 0$ . Instead of  $P(x_1, \dots, x_N)$  we also write  $P(x)$ . Let  $\{A(\sigma)\}$  be a cocycle. Let  $\{t_\sigma\}$  be algebraically independent variables over  $k$ . Then

$$P\left(\sum_{\gamma \in G} t_\gamma A(\gamma)\right) \neq 0$$

because the polynomial does not vanish when one  $t_\gamma$  is replaced by 1 and the others are replaced by 0. By the algebraic independence of automorphisms from Galois theory, there exists an element  $y \in K$  such that if we put

$$B = \sum_\gamma (\gamma y) A(\gamma)$$

then  $P(B) \neq 0$ , so  $B$  is invertible. It is then immediately verified that  $A(\sigma) = B\sigma B^{-1}$ . But when  $k$  is finite, cf. my *Algebraic Groups over Finite Fields*, Am. J. Vol 78 No. 3, 1956.]

32. **Invariant bases.** (A. Speiser, *Zahlentheoretische Sätze aus der Gruppentheorie*, *Math. Z.* 5 (1919) pp. 1–6. See also Kolchin-Lang, *Proc. AMS* Vol. 11 No. 1, 1960). Let  $K$  be a finite Galois extension of  $k$ ,  $G = \text{Gal}(K/k)$  as in the preceding exercise. Let  $V$  be a finite-dimensional vector space over  $K$ , and suppose  $G$  operates on  $V$  in such a way that  $\sigma(av) = \sigma(a)\sigma(v)$  for  $a \in K$  and  $v \in V$ . Prove that there exists a basis  $\{w_1, \dots, w_n\}$  such that  $\sigma w_i = w_i$  for all  $i = 1, \dots, n$  and all  $\sigma \in G$  (an invariant basis). *Hint:* Let  $\{v_1, \dots, v_n\}$  be any basis, and let

$$\sigma \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = A(\sigma) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

where  $A(\sigma)$  is a matrix in  $GL_n(K)$ . Solve for  $B$  in the equation  $(\sigma B)A(\sigma) = B$ , and let

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = B \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

The next exercises on harmonic polynomials have their source in Whittaker, *Math. Ann.* 1902; see also Whittaker and Watson, *Modern Analysis*, Chapter XIII.

33. **Harmonic polynomials.** Let  $\text{Pol}(n, d)$  denote the vector space of homogeneous polynomials of degree  $d$  in  $n$  variables  $X_1, \dots, X_n$  over a field  $k$  of characteristic 0. For an  $n$ -tuple of integers  $(\nu_1, \dots, \nu_n)$  with  $\nu_i \geq 0$  we denote by  $M_{(\nu)}$  as usual the monomial

$$M_{(\nu)}(X) = X_1^{\nu_1} \cdots X_n^{\nu_n}.$$

Prove:

- The number of monomials of degree  $d$  is  $\binom{n-1+d}{n-1}$ , so this number is the dimension of  $\text{Pol}(n, d)$ .
- Let  $(D) = (D_1, \dots, D_n)$  where  $D_i$  is the partial derivative with respect to the  $i$ -th variable. Then we can define  $P(D)$  as usual. For  $P, Q \in \text{Pol}(n, d)$ , define

$$\langle P, Q \rangle = P(D)Q(0).$$

Prove that this defines a symmetric non-degenerate scalar product on  $\text{Pol}(n, d)$ . If  $k$  is not real, it may happen that  $P \neq 0$  but  $\langle P, P \rangle = 0$ . However, if the ground field is real, then  $\langle P, P \rangle > 0$  for  $P \neq 0$ . Show also that the monomials of degree  $d$  form an orthogonal basis. What is  $\langle M_{(\nu)}, M_{(\nu)} \rangle$ ?

- The map  $P \mapsto P(D)$  is an isomorphism of  $\text{Pol}(n, d)$  onto its dual.

- (d) Let  $\Delta = D_1^2 + \cdots + D_n^2$ . Note that  $\Delta: \text{Pol}(n, d) \rightarrow \text{Pol}(n, d-2)$  is a linear map. Prove that  $\Delta$  is surjective.
- (e) Define  $\text{Har}(n, d) = \text{Ker}\Delta$  = vector space of **harmonic homogeneous polynomials** of degree  $d$ . Prove that

$$\dim \text{Har}(n, d) = (n+d-3)!(n+2d-2)/(n-2)!d!.$$

In particular, if  $n = 3$ , then  $\dim \text{Har}(3, d) = 2d+1$ .

- (f) Let  $r^2 = X_1^2 + \cdots + X_n^2$ . Let  $S$  denote multiplication by  $r^2$ . Show that

$$\langle \Delta P, Q \rangle = \langle P, SQ \rangle \text{ for } P \in \text{Pol}(n, d) \text{ and } Q \in \text{Pol}(n, d-2),$$

so  $\Delta = S$ . More generally, for  $R \in \text{Pol}(n, m)$  and  $Q \in \text{Pol}(n, d-m)$  we have

$$\langle R(D)P, Q \rangle = \langle P, RQ \rangle.$$

- (g) Show that  $[\Delta, S] = 4d + 2n$  on  $\text{Pol}(n, d)$ . Here  $[\Delta, S] = \Delta \circ S - S \circ \Delta$ . Actually,  $[\Delta, S] = 4E + 2n$ , where  $E$  is the Euler operator  $E = \sum X_i D_i$ , which is, however, the degree operator on homogeneous polynomials.
- (h) Prove that  $\text{Pol}(n, d) = \text{Har}(n, d) \oplus r^2 \text{Pol}(n, d-2)$  and that the two summands are orthogonal. This is a classical theorem used in the theory of the Laplace operator.
- (i) Let  $(c_1, \dots, c_n) \in k^n$  be such that  $\sum c_i^2 = 0$ . Let

$$H_c^d(X) = (c_1 X_1 + \cdots + c_n X_n)^d.$$

Show that  $H_c^d$  is harmonic, i.e. lies in  $\text{Har}(n, d)$ .

- (j) For any  $Q \in \text{Pol}(n, d)$ , and a positive integer  $m$ , show that

$$Q(D)H_c^m(X) = m(m-1) \cdots (m-d+1)Q(c)H_c^{m-d}(X).$$

34. (Continuation of Exercise 33). Prove:

**Theorem.** Let  $k$  be algebraically closed of characteristic 0. Let  $n \geq 3$ . Then  $\text{Har}(n, d)$  as a vector space over  $k$  is generated by all polynomials  $H_c^d$  with  $(c) \in k^n$  such that  $\sum c_i^2 = 0$ .

[Hint: Let  $Q \in \text{Har}(n, d)$  be orthogonal to all polynomials  $H_c^d$  with  $(c) \in k^n$ . By Exercise 33(h), it suffices to prove that  $r^2|Q$ . But if  $\sum c_i^2 = 0$ , then by Exercise 33(j) we conclude that  $Q(c) = 0$ . By the Hilbert Nullstellensatz, it follows that there exists a polynomial  $F(X)$  such that

$$Q(X)^s = r^2(X)F(X) \text{ for some positive integer } s.$$

But  $n \geq 3$  implies that  $r^2(X)$  is irreducible, so  $r^2(X)$  divides  $Q(X)$ .]

35. (Continuation of Exercise 34). Prove that the representation of  $O(n) = U_n(\mathbf{R})$  on  $\text{Har}(n, d)$  is irreducible.

Readers will find a proof in the following:

S. HELGASON, *Topics in Harmonic Analysis on Homogeneous Spaces*, Birkhäuser, 1981 (see especially §3, Theorem 3.1(ii))

N. VILENKO, *Special Functions and the Theory of Group Representations*, AMS Translations of mathematical monographs Vol. 22, 1968 (Russian original, 1965), Chapter IX, §2.

R. HOWE and E. C. TAN, *Non-Abelian Harmonic Analysis*, Universitext, Springer Verlag, New York, 1992.

The Howe-Tan proof runs as follows. We now use the hermitian product

$$\langle P, Q \rangle = \int_{\mathbf{S}^{n-1}} P(x) \overline{Q(x)} d\sigma(x),$$

where  $\sigma$  is the rotation invariant measure on the  $(n-1)$ -sphere  $\mathbf{S}^{n-1}$ . Let  $e_1, \dots, e_n$  be the unit vectors in  $\mathbf{R}^n$ . We can identify  $O(n-1)$  as the subgroup of  $O(n)$  leaving  $e_n$  fixed. Observe that  $O(n)$  operates on  $\text{Har}(n, d)$ , say on the right by composition  $P \mapsto P \circ A$ ,  $A \in O(n)$ , and this operation commutes with  $\Delta$ . Let

$$\lambda: \text{Har}(n, d) \rightarrow \mathbf{C}$$

be the functional such that  $\lambda(P) = P(e_n)$ . Then  $\lambda$  is  $O(n-1)$ -invariant, and since the hermitian product is non-degenerate, there exists a harmonic polynomial  $Q_n$  such that

$$\lambda(P) = \langle P, Q_n \rangle \quad \text{for all } P \in \text{Har}(n, d).$$

Let  $M \subset \text{Har}(n, d)$  be an  $O(n)$ -submodule. Then the restriction  $\lambda_M$  of  $\lambda$  to  $M$  is nontrivial because  $O(n)$  acts transitively on  $\mathbf{S}^{n-1}$ . Let  $Q_n^M$  be the orthogonal projection of  $Q_n$  on  $M$ . Then  $Q_n^M$  is  $O(n-1)$ -invariant, and so is a linear combination

$$Q_n^M(x) = \sum_{j+2k=d} c_j x_n^j r_{n-1}^{2k}.$$

Furthermore  $Q_n^M$  is harmonic. From this you can show that  $Q_n^M$  is uniquely determined, by showing the existence of recursive relations among the coefficients  $c_j$ . Thus the submodule  $M$  is uniquely determined, and must be all of  $\text{Har}(n, d)$ .

### Irreducibility of $\mathfrak{sl}_n(F)$ .

36. Let  $F$  be a field of characteristic 0. Let  $\mathfrak{g} = \mathfrak{sl}_n(F)$  be the vector space of matrices with trace 0, with its Lie algebra structure  $[X, Y] = XY - YX$ . Let  $E_{ij}$  be the matrix having  $(i, j)$ -component 1 and all other components 0. Let  $G = SL_n(F)$ . Let  $A$  be the multiplicative group of diagonal matrices over  $F$ .

- (a) Let  $H_i = E_{ii} - E_{i+1, i+1}$  for  $i = 1, \dots, n-1$ . Show that the elements  $E_{ij}$  ( $i \neq j$ ),  $H_1, \dots, H_{n-1}$  form a basis of  $\mathfrak{g}$  over  $F$ .
- (b) For  $g \in G$  let  $\mathbf{c}(g)$  be the conjugation action on  $\mathfrak{g}$ , that is  $\mathbf{c}(g)X = gXg^{-1}$ . Show that each  $E_{ij}$  is an eigenvector for this action restricted to the group  $A$ .
- (c) Show that the conjugation representation of  $G$  on  $\mathfrak{g}$  is irreducible, that is, if  $V \neq 0$  is a subspace of  $\mathfrak{g}$  which is  $\mathbf{c}(G)$ -stable, then  $V = \mathfrak{g}$ . Hint: Look up the sketch of the proof in [Jol 01], Chapter VII, Theorem 1.5, and put in all the details. Note that for  $i \neq j$  the matrix  $E_{ij}$  is nilpotent, so for variable  $t$ , the exponential series  $\exp(tE_{ij})$  is actually a polynomial. The derivative with respect to  $t$  can be taken in the formal power series  $F[[t]]$ , not using limits. If  $X$  is a matrix, and  $x(t) = \exp(tX)$ , show that

$$\left. \frac{d}{dt} x(t) Y x(t)^{-1} \right|_{t=0} = XY - YX = [X, Y].$$

---

# CHAPTER XIV

---

## Representation of One Endomorphism

We deal here with one endomorphism of a module, actually a free module, and especially a finite dimensional vector space over a field  $k$ . We obtain the Jordan canonical form for a representing matrix, which has a particularly simple shape when  $k$  is algebraically closed. This leads to a discussion of eigenvalues and the characteristic polynomial. The main theorem can be viewed as giving an example for the general structure theorem of modules over a principal ring. In the present case, the principal ring is the polynomial ring  $k[X]$  in one variable.

---

### §1. REPRESENTATIONS

Let  $k$  be a commutative ring and  $E$  a module over  $k$ . As usual, we denote by  $\text{End}_k(E)$  the ring of  $k$ -endomorphisms of  $E$ , i.e. the ring of  $k$ -linear maps of  $E$  into itself.

Let  $R$  be a  $k$ -algebra (given by a ring-homomorphism  $k \rightarrow R$  which allows us to consider  $R$  as a  $k$ -module). By a **representation** of  $R$  in  $E$  one means a  $k$ -algebra homomorphism  $R \rightarrow \text{End}_k(E)$ , that is a ring-homomorphism

$$\rho : R \rightarrow \text{End}_k(E)$$

which makes the following diagram commutative:

$$\begin{array}{ccc} R & \longrightarrow & \text{End}_k(E) \\ & \swarrow & \nearrow \\ & k & \end{array}$$

[As usual, we view  $\text{End}_k(E)$  as a  $k$ -algebra; if  $I$  denotes the identity map of  $E$ , we have the homomorphism of  $k$  into  $\text{End}_k(E)$  given by  $a \mapsto aI$ . We shall also use  $I$  to denote the unit matrix if bases have been chosen. The context will always make our meaning clear.]

We shall meet several examples of representations in the sequel, with various types of rings (both commutative and non-commutative). In this chapter, the rings will be commutative.

We observe that  $E$  may be viewed as an  $\text{End}_k(E)$  module. Hence  $E$  may be viewed as an  $R$ -module, defining the operation of  $R$  on  $E$  by letting

$$(x, v) \mapsto \rho(x)v$$

for  $x \in R$  and  $v \in E$ . We usually write  $xv$  instead of  $\rho(x)v$ .

A subgroup  $F$  of  $E$  such that  $RF \subset F$  will be said to be an **invariant** submodule of  $E$ . (It is both  $R$ -invariant and  $k$ -invariant.) We also say that it is invariant under the representation.

We say that the representation is **irreducible**, or **simple**, if  $E \neq 0$ , and if the only invariant submodules are  $0$  and  $E$  itself.

The purpose of representation theories is to determine the structure of all representations of various interesting rings, and to classify their irreducible representations. In most cases, we take  $k$  to be a field, which may or may not be algebraically closed. The difficulties in proving theorems about representations may therefore lie in the complication of the ring  $R$ , or the complication of the field  $k$ , or the complication of the module  $E$ , or all three.

A representation  $\rho$  as above is said to be **completely reducible** or **semi-simple** if  $E$  is an  $R$ -direct sum of  $R$ -submodules  $E_i$ ,

$$E = E_1 \oplus \cdots \oplus E_m$$

such that each  $E_i$  is irreducible. We also say that  $E$  is completely reducible. It is not true that all representations are completely reducible, and in fact those considered in this chapter will not be in general. Certain types of completely reducible representations will be studied later.

There is a special type of representation which will occur very frequently. Let  $v \in E$  and assume that  $E = Rv$ . We shall also write  $E = (v)$ . We then say that  $E$  is **principal** (over  $R$ ), and that the representation is **principal**. If that is the case, the set of elements  $x \in R$  such that  $xv = 0$  is a left ideal  $\mathfrak{a}$  of  $R$  (obvious). The map of  $R$  onto  $E$  given by

$$x \mapsto xv$$

induces an isomorphism of  $R$ -modules,

$$R/\mathfrak{a} \rightarrow E$$

(viewing  $R$  as a left module over itself, and  $R/\mathfrak{a}$  as the factor module). In this map, the unit element 1 of  $R$  corresponds to the generator  $v$  of  $E$ .

As a matter of notation, if  $v_1, \dots, v_n \in E$ , we let  $(v_1, \dots, v_n)$  denote the submodule of  $E$  generated by  $v_1, \dots, v_n$ .

Assume that  $E$  has a decomposition into a direct sum of  $R$ -submodules

$$E = E_1 \oplus \dots \oplus E_s.$$

Assume that each  $E_i$  is free and of dimension  $\geq 1$  over  $k$ . Let  $\mathfrak{G}_1, \dots, \mathfrak{G}_s$  be bases for  $E_1, \dots, E_s$  respectively over  $k$ . Then  $\{\mathfrak{G}_1, \dots, \mathfrak{G}_s\}$  is a basis for  $E$ . Let  $\varphi \in R$ , and let  $\varphi_i$  be the endomorphism induced by  $\varphi$  on  $E_i$ . Let  $M_i$  be the matrix of  $\varphi_i$  with respect to the basis  $\mathfrak{G}_i$ . Then the matrix  $M$  of  $\varphi$  with respect to  $\{\mathfrak{G}_1, \dots, \mathfrak{G}_s\}$  looks like

$$\begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & \ddots & 0 \\ 0 & \cdots & 0 & M_s \end{pmatrix}.$$

A matrix of this type is said to be decomposed into **blocks**,  $M_1, \dots, M_s$ . When we have such a decomposition, the study of  $\varphi$  or its matrix is completely reduced (so to speak) to the study of the blocks.

It does not always happen that we have such a reduction, but frequently something almost as good happens. Let  $E'$  be a submodule of  $E$ , invariant under  $R$ . Assume that there exists a basis of  $E'$  over  $k$ , say  $\{v_1, \dots, v_m\}$ , and that this basis can be completed to a basis of  $E$ ,

$$\{v_1, \dots, v_m, v_{m+1}, \dots, v_n\}.$$

This is always the case if  $k$  is a field.

Let  $\varphi \in R$ . Then the matrix of  $\varphi$  with respect to this basis has the form

$$\begin{pmatrix} M' & * \\ 0 & M'' \end{pmatrix}.$$

Indeed, since  $E'$  is mapped into itself by  $\varphi$ , it is clear that we get  $M'$  in the upper left, and a zero matrix below it. Furthermore, for each  $j = m + 1, \dots, n$  we can write

$$\varphi v = c_{j1}v_1 + \dots + c_{jm}v_m + c_{j,m+1}v_{m+1} + \dots + c_{jn}v_n.$$

The transpose of the matrix  $(c_{ji})$  then becomes the matrix

$$\begin{pmatrix} * \\ M'' \end{pmatrix}$$

occurring on the right in the matrix representing  $\varphi$ .

Furthermore, consider an exact sequence

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0.$$

Let  $\bar{v}_{m+1}, \dots, \bar{v}_n$  be the images of  $v_{m+1}, \dots, v_n$  under the canonical map  $E \rightarrow E''$ . We can define a linear map

$$\varphi'': E'' \rightarrow E''$$

in a natural way so that  $(\bar{v}) = \varphi''(\bar{v})$  for all  $v \in E$ . Then it is clear that the matrix of  $\varphi''$  with respect to the basis  $\{\bar{v}_1, \dots, \bar{v}_n\}$  is  $M''$ .

## §2. DECOMPOSITION OVER ONE ENDOMORPHISM

Let  $k$  be a field and  $E$  a finite-dimensional vector space over  $k$ ,  $E \neq 0$ . Let  $A \in \text{End}_k(E)$  be a linear map of  $E$  into itself. Let  $t$  be transcendental over  $k$ . We shall define a representation of the polynomial ring  $k[t]$  in  $E$ . Namely, we have a homomorphism

$$k[t] \rightarrow k[A] \subset \text{End}_k(E)$$

which is obtained by substituting  $A$  for  $t$  in polynomials. The ring  $k[A]$  is the subring of  $\text{End}_k(E)$  generated by  $A$ , and is commutative because powers of  $A$  commute with each other. Thus if  $f(t)$  is a polynomial and  $v \in E$ , then

$$f(t)v = f(A)v.$$

The kernel of the homomorphism  $f(t) \mapsto f(A)$  is a principal ideal of  $k[t]$ , which is  $\neq 0$  because  $k[A]$  is finite dimensional over  $k$ . It is generated by a unique polynomial of degree  $> 0$ , having leading coefficient 1. This polynomial will be called the **minimal polynomial** of  $A$  over  $k$ , and will be denoted by  $q_A(t)$ . It is of course not necessarily irreducible.

Assume that there exists an element  $v \in E$  such that  $E = k[t]v = k[A]v$ . This means that  $E$  is generated over  $k$  by the elements

$$v, Av, A^2v, \dots$$

We called such a module **principal**, and if  $R = k[t]$  we may write  $E = Rv = (v)$ . If  $q_A(t) = t^d + a_{d-1}t^{d-1} + \dots + a_0$  then the elements

$$v, Av, \dots, A^{d-1}v$$

constitute a basis for  $E$  over  $k$ . This is proved in the same way as the analogous statement for finite field extensions. First we note that they are linearly independent, because any relation of linear dependence over  $k$  would yield a poly-

nomial  $g(t)$  of degree less than  $\deg q_A$  and such that  $g(A) = 0$ . Second, they generate  $E$  because any polynomial  $f(t)$  can be written  $f(t) = g(t)q_A(t) + r(t)$  with  $\deg r < \deg q_A$ . Hence  $f(A) = r(A)$ .

With respect to this basis, it is clear that the matrix of  $A$  is of the following type:

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{d-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}.$$

If  $E = (v)$  is principal, then  $E$  is isomorphic to  $k[t]/(q_A(t))$  under the map  $f(t) \mapsto f(A)v$ . The polynomial  $q_A$  is uniquely determined by  $A$ , and does not depend on the choice of generator  $v$  for  $E$ . This is essentially obvious, because if  $f_1, f_2$  are two polynomials with leading coefficient 1, then  $k[t]/(f_1(t))$  is isomorphic to  $k[t]/(f_2(t))$  if and only if  $f_1 = f_2$ . (Decompose each polynomial into prime powers and apply the structure theorem for modules over principal rings.)

If  $E$  is principal then we shall call the polynomial  $q_A$  above the **polynomial invariant of  $E$** , with respect to  $A$ , or simply its **invariant**.

**Theorem 2.1.** *Let  $E$  be a non-zero finite-dimensional space over the field  $k$ , and let  $A \in \text{End}_k(E)$ . Then  $E$  admits a direct sum decomposition*

$$E = E_1 \oplus \cdots \oplus E_r,$$

where each  $E_i$  is a principal  $k[A]$ -submodule, with invariant  $q_i \neq 0$  such that

$$q_1 | q_2 | \cdots | q_r.$$

The sequence  $(q_1, \dots, q_r)$  is uniquely determined by  $E$  and  $A$ , and  $q_r$  is the minimal polynomial of  $A$ .

*Proof.* The first statement is simply a rephrasing in the present language for the structure theorem for modules over principal rings. Furthermore, it is clear that  $q_r(A) = 0$  since  $q_i | q_r$  for each  $i$ . No polynomial of lower degree than  $q_r$  can annihilate  $E$ , because in particular, such a polynomial does not annihilate  $E_r$ . Thus  $q_r$  is the minimal polynomial.

We shall call  $(q_1, \dots, q_r)$  the **invariants** of the pair  $(E, A)$ . Let  $E = k^{(n)}$ , and let  $A$  be an  $n \times n$  matrix, which we view as a linear map of  $E$  into itself. The invariants  $(q_1, \dots, q_r)$  will be called the **invariants of  $A$  (over  $k$ )**.

**Corollary 2.2.** *Let  $k'$  be an extension field of  $k$  and let  $A$  be an  $n \times n$  matrix in  $k$ . The invariants of  $A$  over  $k$  are the same as its invariants over  $k'$ .*

*Proof.* Let  $\{v_1, \dots, v_n\}$  be a basis of  $k^{(n)}$  over  $k$ . Then we may view it also as a basis of  $k'^{(n)}$  over  $k'$ . (The unit vectors are in the  $k$ -space generated by  $v_1, \dots, v_n$ ; hence  $v_1, \dots, v_n$  generate the  $n$ -dimensional space  $k'^{(n)}$  over  $k'$ .) Let  $E = k^{(n)}$ . Let  $L_A$  be the linear map of  $E$  determined by  $A$ . Let  $L'_A$  be the linear map of  $k'^{(n)}$  determined by  $A$ . The matrix of  $L_A$  with respect to our given basis is the same as the matrix of  $L'_A$ . We can select the basis corresponding to the decomposition

$$E = E_1 \oplus \cdots \oplus E_r$$

determined by the invariants  $q_1, \dots, q_r$ . It follows that the invariants don't change when we lift the basis to one of  $k'^{(n)}$ .

**Corollary 2.3.** *Let  $A, B$  be  $n \times n$  matrices over a field  $k$  and let  $k'$  be an extension field of  $k$ . Assume that there is an invertible matrix  $C'$  in  $k'$  such that  $B = C'AC'^{-1}$ . Then there is an invertible matrix  $C$  in  $k$  such that  $B = CAC^{-1}$ .*

*Proof.* Exercise.

The structure theorem for modules over principal rings gives us two kinds of decompositions. One is according to the invariants of the preceding theorem. The other is according to prime powers.

Let  $E \neq 0$  be a finite dimensional space over the field  $k$ , and let  $A : E \rightarrow E$  be in  $\text{End}_k(E)$ . Let  $q = q_A$  be its minimal polynomial. Then  $q$  has a factorization,

$$q = p_1^{e_1} \cdots p_s^{e_s} \quad (e_i \geq 1)$$

into prime powers (distinct). Hence  $E$  is a direct sum of submodules

$$E = E(p_1) \oplus \cdots \oplus E(p_s),$$

such that each  $E(p_i)$  is annihilated by  $p_i^{e_i}$ . Furthermore, each such submodule can be expressed as a direct sum of submodules isomorphic to  $k[t]/(p^e)$  for some irreducible polynomial  $p$  and some integer  $e \geq 1$ .

**Theorem 2.4.** *Let  $q_A(t) = (t - \alpha)^e$  for some  $\alpha \in k$ ,  $e \geq 1$ . Assume that  $E$  is isomorphic to  $k[t]/(q)$ . Then  $E$  has a basis over  $k$  such that the matrix of  $A$  relative to this basis is of type*

$$\begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 1 & \alpha & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & \alpha \end{pmatrix}.$$

*Proof.* Since  $E$  is isomorphic to  $k[t]/(q)$ , there exists an element  $v \in E$  such that  $k[t]v = E$ . This element corresponds to the unit element of  $k[t]$  in the isomorphism

$$k[t]/(q) \rightarrow E.$$

We contend that the elements

$$v, (t - \alpha)v, \dots, (t - \alpha)^{e-1}v,$$

or equivalently,

$$v, (A - \alpha)v, \dots, (A - \alpha)^{e-1}v,$$

form a basis for  $E$  over  $k$ . They are linearly independent over  $k$  because any relation of linear dependence would yield a relation of linear dependence between

$$v, Av, \dots, A^{e-1}v,$$

and hence would yield a polynomial  $g(t)$  of degree less than  $\deg q$  such that  $g(A) = 0$ . Since  $\dim E = e$ , it follows that our elements form a basis for  $E$  over  $k$ . But  $(A - \alpha)^e = 0$ . It is then clear from the definitions that the matrix of  $A$  with respect to this basis has the shape stated in our theorem.

**Corollary 2.5.** *Let  $k$  be algebraically closed, and let  $E$  be a finite-dimensional non-zero vector space over  $k$ . Let  $A \in \text{End}_k(E)$ . Then there exists a basis of  $E$  over  $k$  such that the matrix of  $A$  with respect to this basis consists of blocks, and each block is of the type described in the theorem.*

A matrix having the form described in the preceding corollary is said to be in **Jordan canonical form**.

**Remark 1.** A matrix (or an endomorphism)  $N$  is said to be **nilpotent** if there exists an integer  $d > 0$  such that  $N^d = 0$ . We see that in the decomposition of Theorem 2.4 or Corollary 2.5, the matrix  $M$  is written in the form

$$M = B + N$$

where  $N$  is nilpotent. In fact,  $N$  is a triangular matrix (i.e. it has zero coefficients on and above the diagonal), and  $B$  is a diagonal matrix, whose diagonal elements are the roots of the minimal polynomial. Such a decomposition can always be achieved whenever the field  $k$  is such that all the roots of the minimal polynomial lie in  $k$ . We observe also that the only case when the matrix  $N$  is 0 is when all the roots of the minimal polynomial have multiplicity 1. In this case, if  $n = \dim E$ , then the matrix  $M$  is a diagonal matrix, with  $n$  distinct elements on the diagonal.

**Remark 2.** The main theorem of this section can also be viewed as falling under the general pattern of decomposing a module into a direct sum as far as possible, and also giving normalized bases for vector spaces with respect to various structures, so that one can tell in a simple way the effect of an endomorphism. More formally, consider the category of pairs  $(E, A)$ , consisting of a finite dimensional vector space  $E$  over a field  $k$ , and an endomorphism  $A: E \rightarrow E$ . By a morphism of such pairs

$$f: (E, A) \rightarrow (E', A')$$

we mean a  $k$ -homomorphism  $f: E \rightarrow E'$  such that the following diagram is commutative:

$$\begin{array}{ccc} E & \xrightarrow{f} & E' \\ A \downarrow & & \downarrow A' \\ E & \xrightarrow{f} & E' \end{array}$$

It is then immediate that such pairs form a category, so we have the notion of isomorphism. One can reformulate Theorem 2.1 by stating:

**Theorem 2.6.** *Two pairs  $(E, A)$  and  $(F, B)$  are isomorphic if and only if they have the same invariants.*

You can prove this as Exercise 19. The Jordan basis gives a normalized form for the matrix associated with such a pair and an appropriate basis.

In the next chapter, we shall find conditions under which a normalized matrix is actually diagonal, for hermitian, symmetric, and unitary operators over the complex numbers.

As an example and application of Theorem 2.6, we prove:

**Corollary 2.7.** *Let  $k$  be a field and let  $K$  be a finite separable extension of degree  $n$ . Let  $V$  be a finite dimensional vector space of dimension  $n$  over  $k$ , and let  $\rho, \rho': K \rightarrow \text{End}_k(V)$  be two representations of  $K$  on  $V$ ; that is, embeddings of  $K$  in  $\text{End}_k(V)$ . Then  $\rho, \rho'$  are conjugate; that is, there exists  $B \in \text{Aut}_k(V)$  such that*

$$\rho'(\xi) = B\rho(\xi)B^{-1} \text{ for all } \xi \in K.$$

*Proof.* By the primitive element theorem of field theory, there exists an element  $\alpha \in K$  such that  $K = k[\alpha]$ . Let  $p(t)$  be the irreducible polynomial of  $\alpha$  over  $k$ . Then  $(V, \rho(\alpha))$  and  $(V, \rho'(\alpha))$  have the same invariant, namely  $p(t)$ . Hence these pairs are isomorphic by Theorem 2.6, which means that there exists  $B \in \text{Aut}_k(V)$  such that

$$\rho'(\alpha) = B\rho(\alpha)B^{-1}.$$

But all elements of  $K$  are linear combinations of powers of  $\alpha$  with coefficients in  $k$ , so it follows immediately that  $\rho'(\xi) = B\rho(\xi)B^{-1}$  for all  $\xi \in K$ , as desired.

To get a representation of  $K$  as in corollary 2.7, one may of course select a basis of  $K$ , and represent multiplication of elements of  $K$  on  $K$  by matrices with respect to this basis. In some sense, Corollary 2.7 tells us that this is the only way to get such representations. We shall return to this point of view when considering Cartan subgroups of  $GL_n$  in Chapter XVIII, §12.

---

### §3. THE CHARACTERISTIC POLYNOMIAL

Let  $k$  be a commutative ring and  $E$  a free module of dimension  $n$  over  $k$ . We consider the polynomial ring  $k[t]$ , and a linear map  $A : E \rightarrow E$ . We have a homomorphism

$$k[t] \rightarrow k[A]$$

as before, mapping a polynomial  $f(t)$  on  $f(A)$ , and  $E$  becomes a module over the ring  $R = k[t]$ . Let  $M$  be any  $n \times n$  matrix in  $k$  (for instance the matrix of  $A$  relative to a basis of  $E$ ). We define the **characteristic polynomial**  $P_M(t)$  to be the determinant

$$\det(tI_n - M)$$

where  $I_n$  is the unit  $n \times n$  matrix. It is an element of  $k[t]$ . Furthermore, if  $N$  is an invertible matrix in  $R$ , then

$$\det(tI_n - N^{-1}MN) = \det(N^{-1}(tI_n - M)N) = \det(tI_n - M).$$

Hence the characteristic polynomial of  $N^{-1}MN$  is the same as that of  $M$ . We may therefore define the characteristic polynomial of  $A$ , and denote by  $P_A$ , the characteristic polynomial of any matrix  $M$  associated with  $A$  with respect to some basis. (If  $E = 0$ , we **define the characteristic polynomial to be 1**.)

If  $\varphi : k \rightarrow k'$  is a homomorphism of commutative rings, and  $M$  is an  $n \times n$  matrix in  $k$ , then it is clear that

$$P_{\varphi M}(t) = \varphi P_M(t)$$

where  $\varphi P_M$  is obtained from  $P_M$  by applying  $\varphi$  to the coefficients of  $P_M$ .

**Theorem 3.1.** (Cayley-Hamilton). *We have  $P_A(A) = 0$ .*

*Proof.* Let  $\{v_1, \dots, v_n\}$  be a basis of  $E$  over  $k$ . Then

$$tv_j = \sum_{i=1}^n a_{ij}v_i$$

where  $(a_{ij}) = M$  is the matrix of  $A$  with respect to the basis. Let  $\tilde{B}(t)$  be the matrix with coefficients in  $k[t]$ , defined in Chapter XIII, such that

$$\tilde{B}(t)B(t) = P_A(t)I_n.$$

Then

$$\tilde{B}(t)B(t) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} P_A(t)v_1 \\ \vdots \\ P_A(t)v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

because

$$B(t) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Hence  $P_A(t)E = 0$ , and therefore  $P_A(A)E = 0$ . This means that  $P_A(A) = 0$ , as was to be shown.

Assume now that  $k$  is a field. Let  $E$  be a finite-dimensional vector space over  $k$ , and let  $A \in \text{End}_k(E)$ . By an **eigenvector**  $w$  of  $A$  in  $E$  one means an element  $w \in E$ , such that there exists an element  $\lambda \in k$  for which  $Aw = \lambda w$ . If  $w \neq 0$ , then  $\lambda$  is determined uniquely, and is called an **eigenvalue** of  $A$ . Of course, distinct eigenvectors may have the same eigenvalue.

**Theorem 3.2.** *The eigenvalues of  $A$  are precisely the roots of the characteristic polynomial of  $A$ .*

*Proof.* Let  $\lambda$  be an eigenvalue. Then  $A - \lambda I$  is not invertible in  $\text{End}_k(E)$ , and hence  $\det(A - \lambda I) = 0$ . Hence  $\lambda$  is a root of  $P_A$ . The arguments are reversible, so we also get the converse.

For simplicity of notation, we often write  $A - \lambda$  instead of  $A - \lambda I$ .

**Theorem 3.3.** *Let  $w_1, \dots, w_m$  be non-zero eigenvectors of  $A$ , having distinct eigenvalues. Then they are linearly independent.*

*Proof.* Suppose that we have

$$a_1 w_1 + \dots + a_m w_m = 0$$

with  $a_i \in k$ , and let this be a shortest relation with not all  $a_i = 0$  (assuming such exists). Then  $a_i \neq 0$  for all  $i$ . Let  $\lambda_1, \dots, \lambda_m$  be the eigenvalues of our vectors. Apply  $A - \lambda_1$  to the above relation. We get

$$a_2(\lambda_2 - \lambda_1)w_2 + \dots + a_m(\lambda_m - \lambda_1)w_m = 0,$$

which shortens our relation, contradiction.

**Corollary 3.4.** *If  $A$  has  $n$  distinct eigenvalues  $\lambda_1, \dots, \lambda_n$  belonging to eigenvectors  $v_1, \dots, v_n$ , and  $\dim E = n$ , then  $\{v_1, \dots, v_n\}$  is a basis for  $E$ . The matrix*

of  $A$  with respect to this basis is the diagonal matrix:

$$\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}.$$

**Warning.** It is not always true that there exists a basis of  $E$  consisting of eigenvectors!

**Remark.** Let  $k$  be a subfield of  $k'$ . If  $M$  is a matrix in  $k$ , we can define its characteristic polynomial with respect to  $k$ , and also with respect to  $k'$ . It is clear that the characteristic polynomials thus obtained are equal. If  $E$  is a vector space over  $k$ , we shall see later how to extend it to a vector space over  $k'$ . A linear map  $A$  extends to a linear map of the extended space, and the characteristic polynomial of the linear map does not change either. Actually, if we select a basis for  $E$  over  $k$ , then  $E \approx k^{(n)}$ , and  $k^{(n)} \subset k'^{(n)}$  in a natural way. Thus selecting a basis allows us to extend the vector space, but this seems to depend on the choice of basis. We shall give an invariant definition later.

Let  $E = E_1 \oplus \cdots \oplus E_r$  be an expression of  $E$  as a direct sum of vector spaces over  $k$ . Let  $A \in \text{End}_k(E)$ , and assume that  $AE_i \subset E_i$  for all  $i = 1, \dots, r$ . Then  $A$  induces a linear map on  $E_i$ . We can select a basis for  $E$  consisting of bases for  $E_1, \dots, E_r$ , and then the matrix for  $A$  consists of blocks. Hence we see that

$$P_A(t) = \prod_{i=1}^r P_{A_i}(t).$$

Thus the characteristic polynomial is multiplicative on direct sums.

Our condition above that  $AE_i \subset E_i$  can also be formulated by saying that  $E$  is expressed as a  $k[A]$ -direct sum of  $k[A]$ -submodules, or also a  $k[t]$ -direct sum of  $k[t]$ -submodules. We shall apply this to the decomposition of  $E$  given in Theorem 2.1.

**Theorem 3.5.** *Let  $E$  be a finite-dimensional vector space over a field  $k$ , let  $A \in \text{End}_k(E)$ , and let  $q_1, \dots, q_r$  be the invariants of  $(E, A)$ . Then*

$$P_A(t) = q_1(t) \cdots q_r(t).$$

*Proof.* We assume that  $E = k^{(n)}$  and that  $A$  is represented by a matrix  $M$ . We have seen that the invariants do not change when we extend  $k$  to a larger field, and neither does the characteristic polynomial. Hence we may assume that  $k$  is algebraically closed. In view of Theorem 2.1 we may assume that  $M$  has a

single invariant  $q$ . Write

$$q(t) = (t - \alpha_1)^{e_1} \cdots (t - \alpha_s)^{e_s}$$

with distinct  $\alpha_1, \dots, \alpha_s$ . We view  $M$  as a linear map, and split out vector space further into a direct sum of submodules (over  $k[t]$ ) having invariants

$$(t - \alpha_1)^{e_1}, \dots, (t - \alpha_s)^{e_s}$$

respectively (this is the prime power decomposition). For each one of these submodules, we can select a basis so that the matrix of the induced linear map has the shape described in Theorem 2.4. From this it is immediately clear that the characteristic polynomial of the map having invariant  $(t - \alpha)^e$  is precisely  $(t - \alpha)^e$ , and our theorem is proved.

**Corollary 3.6.** *The minimal polynomial of  $A$  and its characteristic polynomial have the same irreducible factors.*

*Proof.* Because  $q_r$  is the minimal polynomial, by Theorem 2.1.

We shall generalize our remark concerning the multiplicativity of the characteristic polynomial over direct sums.

**Theorem 3.7.** *Let  $k$  be a commutative ring, and in the following diagram,*

$$\begin{array}{ccccccc} 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' \longrightarrow 0 \\ & & \downarrow A' & & \downarrow A & & \downarrow A'' \\ 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' \longrightarrow 0 \end{array}$$

*let the rows be exact sequences of free modules over  $k$ , of finite dimension, and let the vertical maps be  $k$ -linear maps making the diagram commutative. Then*

$$P_A(t) = P_{A'}(t)P_{A''}(t).$$

*Proof.* We may assume that  $E'$  is a submodule of  $E$ . We select a basis  $\{v_1, \dots, v_m\}$  for  $E'$ . Let  $\{\bar{v}_{m+1}, \dots, \bar{v}_n\}$  be a basis for  $E''$ , and let  $v_{m+1}, \dots, v_n$  be elements of  $E$  mapping on  $\bar{v}_{m+1}, \dots, \bar{v}_n$  respectively. Then

$$\{v_1, \dots, v_m, v_{m+1}, \dots, v_n\}$$

is a basis for  $E$  (same proof as Theorem 5.2 of Chapter III), and we are in the situation discussed in §1. The matrix for  $A$  has the shape

$$\begin{pmatrix} M' & * \\ 0 & M'' \end{pmatrix}$$

where  $M'$  is the matrix for  $A'$  and  $M''$  is the matrix for  $A''$ . Taking the characteristic polynomial with respect to this matrix obviously yields our multiplicative property.

**Theorem 3.8.** *Let  $k$  be a commutative ring, and  $E$  a free module of dimension  $n$  over  $k$ . Let  $A \in \text{End}_k(E)$ . Let*

$$P_A(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0.$$

*Then*

$$\text{tr}(A) = -c_{n-1} \quad \text{and} \quad \det(A) = (-1)^n c_0.$$

*Proof.* For the determinant, we observe that  $P_A(0) = c_0$ . Substituting  $t = 0$  in the definition of the characteristic polynomial by the determinant shows that  $c_0 = (-1)^n \det(A)$ .

For the trace, let  $M$  be the matrix representing  $A$  with respect to some basis,  $M = (a_{ij})$ . We consider the determinant  $\det(tI_n - a_{ij})$ . In its expansion as a sum over permutations, it will contain a diagonal term

$$(t - a_{11}) \cdots (t - a_{nn}),$$

which will give a contribution to the coefficient of  $t^{n-1}$  equal to

$$-(a_{11} + \cdots + a_{nn}).$$

No other term in this expansion will give a contribution to the coefficient of  $t^{n-1}$ , because the power of  $t$  occurring in another term will be at most  $t^{n-2}$ . This proves our assertion concerning the trace.

**Corollary 3.9.** *Let the notation be as in Theorem 3.7. Then*

$$\text{tr}(A) = \text{tr}(A') + \text{tr}(A'') \quad \text{and} \quad \det(A) = \det(A') \det(A'').$$

*Proof.* Clear.

We shall now interpret our results in the Euler-Grothendieck group.

Let  $k$  be a commutative ring. We consider the category whose objects are pairs  $(E, A)$ , where  $E$  is a  $k$ -module, and  $A \in \text{End}_k(E)$ . We define a morphism

$$(E', A') \rightarrow (E, A)$$

to be a  $k$ -linear map  $E' \xrightarrow{f} E$  making the following diagram commutative:

$$\begin{array}{ccc} E' & \xrightarrow{f} & E \\ A' \downarrow & & \downarrow A \\ E' & \xrightarrow{f} & E \end{array}$$

Then we can define the kernel of such a morphism to be again a pair. Indeed, let  $E'_0$  be the kernel of  $f: E' \rightarrow E$ . Then  $A'$  maps  $E'_0$  into itself because

$$fA'E'_0 = AfE'_0 = 0.$$

We let  $A'_0$  be the restriction of  $A'$  on  $E'_0$ . The pair  $(E'_0, A'_0)$  is defined to be the kernel of our morphism.

We shall denote by  $f$  again the morphism of the pair  $(E', A') \rightarrow (E, A)$ . We can speak of an exact sequence

$$(E', A') \rightarrow (E, A) \rightarrow (E'', A''),$$

meaning that the induced sequence

$$E' \rightarrow E \rightarrow E''$$

is exact. We also write 0 instead of  $(0, 0)$ , according to our universal convention to use the symbol 0 for all things which behave like a zero element.

We observe that our pairs now behave formally like modules, and they in fact form an abelian category.

Assume that  $k$  is a field. Let  $\mathfrak{Q}$  consist of all pairs  $(E, A)$  where  $E$  is finite dimensional over  $k$ .

*Then Theorem 3.7 asserts that the characteristic polynomial is an Euler-Poincaré map defined for each object in our category  $\mathfrak{Q}$ , with values into the multiplicative monoid of polynomials with leading coefficient 1.*

Since the values of the map are in a monoid, this generalizes slightly the notion of Chapter III, §8, when we took the values in a group. Of course when  $k$  is a field, which is the most frequent application, we can view the values of our map to be in the multiplicative group of non-zero rational functions, so our previous situation applies.

A similar remark holds now for the trace and the determinant. *If  $k$  is a field, the trace is an Euler map into the additive group of the field, and the determinant is an Euler map into the multiplicative group of the field.* We note also that all these maps (like all Euler maps) are defined on the isomorphism classes of pairs, and are defined on the Euler-Grothendieck group.

**Theorem 3.10.** *Let  $k$  be a commutative ring,  $M$  an  $n \times n$  matrix in  $k$ , and  $f$  a polynomial in  $k[t]$ . Assume that  $P_M(t)$  has a factorization,*

$$P_M(t) = \prod_{i=1}^n (t - \alpha_i)$$

*into linear factors over  $k$ . Then the characteristic polynomial of  $f(M)$  is given by*

$$P_{f(M)}(t) = \prod_{i=1}^n (t - f(\alpha_i)),$$

and

$$\text{tr}(f(M)) = \sum_{i=1}^n f(\alpha_i), \quad \det(f(M)) = \prod_{i=1}^n f(\alpha_i).$$

*Proof.* Assume first that  $k$  is a field. Then using the canonical decomposition in terms of matrices given in Theorem 2.4, we find that our assertion is immediately obvious. When  $k$  is a ring, we use a substitution argument. It is however necessary to know that if  $X = (x_{ij})$  is a matrix with algebraically independent coefficients over  $\mathbf{Z}$ , then  $P_X(t)$  has  $n$  distinct roots  $y_1, \dots, y_n$  [in an algebraic closure of  $\mathbf{Q}(X)$ ] and that we have a homomorphism

$$\mathbf{Z}[x_{ij}, y_1, \dots, y_n] \rightarrow k$$

mapping  $X$  on  $M$  and  $y_1, \dots, y_n$  on  $\alpha_1, \dots, \alpha_n$ . This is obvious to the reader who read the chapter on integral ring extensions, and the reader who has not can forget about this part of the theorem.

## EXERCISES

1. Let  $T$  be an upper triangular square matrix over a commutative ring (i.e. all the elements below and on the diagonal are 0). Show that  $T$  is nilpotent.
2. Carry out explicitly the proof that the determinant of a matrix

$$\begin{pmatrix} M_1 & & * & * \\ 0 & M_2 & & \\ 0 & 0 & \ddots & * \\ \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & \cdots & 0 & M_s \end{pmatrix}$$

where each  $M_i$  is a square matrix, is equal to the product of the determinants of the matrices  $M_1, \dots, M_s$ .

3. Let  $k$  be a commutative ring, and let  $M, M'$  be square  $n \times n$  matrices in  $k$ . Show that the characteristic polynomials of  $MM'$  and  $M'M$  are equal.
4. Show that the eigenvalues of the matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

in the complex numbers are  $\pm 1, \pm i$ .

5. Let  $M, M'$  be square matrices over a field  $k$ . Let  $q, q'$  be their respective minimal polynomials. Show that the minimal polynomial of

$$\begin{pmatrix} M & 0 \\ 0 & M' \end{pmatrix}$$

is the least common multiple of  $q, q'$ .

6. Let  $A$  be a nilpotent endomorphism of a finite dimensional vector space  $E$  over the field  $k$ . Show that  $\text{tr}(A) = 0$ .
7. Let  $R$  be a principal entire ring. Let  $E$  be a free module over  $R$ , and let  $E^\vee = \text{Hom}_R(E, R)$  be its dual module. Then  $E^\vee$  is free of dimension  $n$ . Let  $F$  be a submodule of  $E$ . Show that  $E^\vee/F^\perp$  can be viewed as a submodule of  $F^\vee$ , and that its invariants are the same as the invariants of  $F$  in  $E$ .
8. Let  $E$  be a finite-dimensional vector space over a field  $k$ . Let  $A \in \text{Aut}_k(E)$ . Show that the following conditions are equivalent:
- $A = I + N$ , with  $N$  nilpotent.
  - There exists a basis of  $E$  such that the matrix of  $A$  with respect to this basis has all its diagonal elements equal to 1 and all elements above the diagonal equal to 0.
  - All roots of the characteristic polynomial of  $A$  (in the algebraic closure of  $k$ ) are equal to 1.
9. Let  $k$  be a field of characteristic 0, and let  $M$  be an  $n \times n$  matrix in  $k$ . Show that  $M$  is nilpotent if and only if  $\text{tr}(M^v) = 0$  for  $1 \leq v \leq n$ .
10. Generalize Theorem 3.10 to rational functions (instead of polynomials), assuming that  $k$  is a field.
11. Let  $E$  be a finite-dimensional space over the field  $k$ . Let  $\alpha \in k$ . Let  $E_\alpha$  be the subspace of  $E$  generated by all eigenvectors of a given endomorphism  $A$  of  $E$ , having  $\alpha$  as an eigenvalue. Show that every non-zero element of  $E_\alpha$  is an eigenvector of  $A$  having  $\alpha$  as an eigenvalue.
12. Let  $E$  be finite dimensional over the field  $k$ . Let  $A \in \text{End}_k(E)$ . Let  $v$  be an eigenvector for  $A$ . Let  $B \in \text{End}_k(E)$  be such that  $AB = BA$ . Show that  $Bv$  is also an eigenvector for  $A$  (if  $Bv \neq 0$ ), with the same eigenvalue.

### Diagonalizable endomorphisms

Let  $E$  be a finite-dimensional vector space over a field  $k$ , and let  $S \in \text{End}_k(E)$ . We say that  $S$  is **diagonalizable** if there exists a basis of  $E$  consisting of eigenvectors of  $S$ . The matrix of  $S$  with respect to this basis is then a diagonal matrix.

13. (a) If  $S$  is diagonalizable, then its minimal polynomial over  $k$  is of type

$$q(t) = \prod_{i=1}^m (t - \lambda_i),$$

where  $\lambda_1, \dots, \lambda_m$  are distinct elements of  $k$ .

- (b) Conversely, if the minimal polynomial of  $S$  is of the preceding type, then  $S$  is diagonalizable. [Hint: The space can be decomposed as a direct sum of the subspaces  $E_{\lambda_i}$  annihilated by  $S - \lambda_i$ .]

- (c) If  $S$  is diagonalizable, and if  $F$  is a subspace of  $E$  such that  $SF \subset F$ , show that  $S$  is diagonalizable as an endomorphism of  $F$ , i.e. that  $F$  has a basis consisting of eigenvectors of  $S$ .
- (d) Let  $S, T$  be endomorphisms of  $E$ , and assume that  $S, T$  commute. Assume that both  $S, T$  are diagonalizable. Show that they are simultaneously diagonalizable, i.e. there exists a basis of  $E$  consisting of eigenvectors for both  $S$  and  $T$ . [Hint: If  $\lambda$  is an eigenvalue of  $S$ , and  $E_\lambda$  is the subspace of  $E$  consisting of all vectors  $v$  such that  $Sv = \lambda v$ , then  $TE_\lambda \subset E_\lambda$ .]
14. Let  $E$  be a finite-dimensional vector space over an algebraically closed field  $k$ . Let  $A \in \text{End}_k(E)$ . Show that  $A$  can be written in a unique way as a sum

$$A = S + N$$

where  $S$  is diagonalizable,  $N$  is nilpotent, and  $SN = NS$ . Show that  $S, N$  can be expressed as polynomials in  $A$ . [Hint: Let  $P_A(t) = \prod (t - \lambda_i)^{m_i}$  be the factorization of  $P_A(t)$  with distinct  $\lambda_i$ . Let  $E_i$  be the kernel of  $(A - \lambda_i)^{m_i}$ . Then  $E$  is the direct sum of the  $E_i$ . Define  $S$  on  $E$  so that on  $E_i$ ,  $Sv = \lambda_i v$  for all  $v \in E_i$ . Let  $N = A - S$ . Show that  $S, N$  satisfy our requirements. To get  $S$  as a polynomial in  $A$ , let  $g$  be a polynomial such that  $g(t) \equiv \lambda_i \pmod{(t - \lambda_i)^{m_i}}$  for all  $i$ , and  $g(t) \equiv 0 \pmod{t}$ . Then  $S = g(A)$  and  $N = A - g(A)$ .]

15. After you have read the section on the tensor product of vector spaces, you can easily do the following exercise. Let  $E, F$  be finite-dimensional vector spaces over an algebraically closed field  $k$ , and let  $A : E \rightarrow E$  and  $B : F \rightarrow F$  be  $k$ -endomorphisms of  $E, F$ , respectively. Let

$$P_A(t) = \prod (t - \alpha_i)^{n_i} \quad \text{and} \quad P_B(t) = \prod (t - \beta_j)^{m_j}$$

be the factorizations of their respectively characteristic polynomials, into distinct linear factors. Then

$$P_{A \otimes B}(t) = \prod_{i, j} (t - \alpha_i \beta_j)^{n_i m_j}.$$

[Hint: Decompose  $E$  into the direct sum of subspaces  $E_i$ , where  $E_i$  is the subspace of  $E$  annihilated by some power of  $A - \alpha_i$ . Do the same for  $F$ , getting a decomposition into a direct sum of subspaces  $F_j$ . Then show that some power of  $A \otimes B - \alpha_i \beta_j$  annihilates  $E_i \otimes F_j$ . Use the fact that  $E \otimes F$  is the direct sum of the subspaces  $E_i \otimes F_j$ , and that  $\dim_k(E_i \otimes F_j) = n_i m_j$ .]

16. Let  $\Gamma$  be a free abelian group of dimension  $n \geq 1$ . Let  $\Gamma'$  be a subgroup of dimension  $n$  also. Let  $\{v_1, \dots, v_n\}$  be a basis of  $\Gamma$ , and let  $\{w_1, \dots, w_n\}$  be a basis of  $\Gamma'$ . Write

$$w_i = \sum a_{ij} v_j.$$

Show that the index  $(\Gamma : \Gamma')$  is equal to the absolute value of the determinant of the matrix  $(a_{ij})$ .

17. Prove the normal basis theorem for finite extensions of a finite field.
18. Let  $A = (a_{ij})$  be a square  $n \times n$  matrix over a commutative ring  $k$ . Let  $A_{ij}$  be the matrix obtained by deleting the  $i$ -th row and  $j$ -th column from  $A$ . Let  $b_{ij} = (-1)^{i+j} \det(A_{ji})$ , and let  $B$  be the matrix  $(b_{ij})$ . Show that  $\det(B) = \det(A)^{n-1}$ , by reducing the problem to the case when  $A$  is a matrix with variable coefficients over the integers. Use this same method to give an alternative proof of the Cayley-Hamilton theorem, that  $P_A(A) = 0$ .

19. Let  $(E, A)$  and  $(E', A')$  be pairs consisting of a finite-dimensional vector space over a field  $k$ , and a  $k$ -endomorphism. Show that these pairs are isomorphic if and only if their invariants are equal.
20. (a) How many non-conjugate elements of  $GL_2(\mathbb{C})$  are there with characteristic polynomial  $t^3(t+1)^2(t-1)$ ?
- (b) How many with characteristic polynomial  $t^3 - 1001t$ ?
21. Let  $V$  be a finite dimensional vector space over  $\mathbb{Q}$  and let  $A: V \rightarrow V$  be a  $\mathbb{Q}$ -linear map such that  $A^5 = \text{Id}$ . Assume that if  $v \in V$  is such that  $Av = v$ , then  $v = 0$ . Prove that  $\dim V$  is divisible by 4.
22. Let  $V$  be a finite dimensional vector space over  $\mathbb{R}$ , and let  $A: V \rightarrow V$  be an  $\mathbb{R}$ -linear map such that  $A^2 = -\text{Id}$ . Show that  $\dim V$  is even, and that  $V$  is a direct sum of 2-dimensional  $A$ -invariant subspaces.
23. Let  $E$  be a finite-dimensional vector space over an algebraically closed field  $k$ . Let  $A, B$  be  $k$ -endomorphisms of  $E$  which commute, i.e.  $AB = BA$ . Show that  $A$  and  $B$  have a common eigenvector. [Hint: Consider a subspace consisting of all vectors having a fixed element of  $k$  as eigenvalue.]
24. Let  $V$  be a finite dimensional vector space over a field  $k$ . Let  $A$  be an endomorphism of  $V$ . Let  $\text{Tr}(A^m)$  be the trace of  $A^m$  as an endomorphism of  $V$ . Show that the following power series in the variable  $t$  are equal:

$$\exp\left(\sum_{m=1}^{\infty} -\text{Tr}(A^m) \frac{t^m}{m}\right) = \det(I - tA) \quad \text{or} \quad -\frac{d}{dt} \log \det(I - tA) = \sum_{m=1}^{\infty} \text{Tr}(A^m) t^m.$$

Compare with Exercise 23 of Chapter XVIII.

25. Let  $V, W$  be finite dimensional vector spaces over  $k$ , of dimension  $n$ . Let  $(v, w) \mapsto \langle v, w \rangle$  be a non-singular bilinear form on  $V \times W$ . Let  $c \in k$ , and let  $A: V \rightarrow V$  and  $V: W \rightarrow W$  be endomorphisms such that

$$\langle Av, Bw \rangle = c \langle v, w \rangle \text{ for all } v \in V \text{ and } w \in W.$$

Show that

$$\det(A)\det(tI - B) = (-1)^n \det(cI - tA)$$

and

$$\det(A)\det(B) = c^n.$$

For an application of Exercises 24 and 25 to a context of topology or algebraic geometry, see Hartshorne's *Algebraic Geometry*, Appendix C, §4.

26. Let  $G = SL_n(\mathbb{C})$  and let  $K$  be the complex unitary group. Let  $A$  be the group of diagonal matrices with positive real components on the diagonal.

- (a) Show that if  $g \in \text{Nor}_G(A)$  (normalizer of  $A$  in  $G$ ), then  $\mathbf{c}(g)$  (conjugation by  $g$ ) permutes the diagonal components of  $A$ , thus giving rise to a homomorphism  $\text{Nor}_G(A) \rightarrow W$  to the group  $W$  of permutations of the diagonal coordinates.

By definition, the kernel of the above homomorphism is the centralizer  $\text{Cen}_G(A)$ .

- (b) Show that actually all permutations of the coordinates can be achieved by elements of  $K$ , so we get an isomorphism

$$W \approx \text{Nor}_G(A)/\text{Cen}_G(A) \approx \text{Nor}_K(A)/\text{Cen}_K(A).$$

In fact, the  $K$  on the right can be taken to be the real unitary group, because permutation matrices can be taken to have real components (0 or  $\pm 1$ ).

---

# CHAPTER XV

---

## Structure of Bilinear Forms

There are three major types of bilinear forms: hermitian (or symmetric), unitary, and alternating (skew-symmetric). In this chapter, we give structure theorems giving normalized expressions for these forms with respect to suitable bases. The chapter also follows the standard pattern of decomposing an object into a direct sum of simple objects, insofar as possible.

---

### §1. PRELIMINARIES, ORTHOGONAL SUMS

The purpose of this chapter is to go somewhat deeper into the structure theory for our three types of forms. To do this we shall assume most of the time that our ground ring is a field, and in fact a field of characteristic  $\neq 2$  in the symmetric case.

We recall our three definitions. Let  $E$  be a module over a commutative ring  $R$ . Let  $g : E \times E \rightarrow R$  be a map. If  $g$  is bilinear, we call  $g$  a **symmetric** form if  $g(x, y) = g(y, x)$  for all  $x, y \in E$ . We call  $g$  **alternating** if  $g(x, x) = 0$ , and hence  $g(x, y) = -g(y, x)$  for all  $x, y \in E$ . If  $R$  has an automorphism of order 2, written  $a \mapsto \bar{a}$ , we say that  $g$  is a **hermitian** form if it is linear in its first variable, antilinear in its second, and

$$g(x, y) = \overline{g(y, x)}.$$

We shall write  $g(x, y) = \langle x, y \rangle$  if the reference to  $g$  is clear. We also occasionally write  $g(x, y) = x \cdot y$  or  $g(x, x) = x^2$ . We sometimes call  $g$  a **scalar product**.

If  $v_1, \dots, v_m \in E$ , we denote by  $(v_1, \dots, v_m)$  the submodule of  $E$  generated by  $v_1, \dots, v_m$ .

Let  $g$  be symmetric, alternating, or hermitian. Then it is clear that the left kernel of  $g$  is equal to its right kernel, and it will simply be called the **kernel** of  $g$ .

In any one of these cases, we say that  $g$  is **non-degenerate** if its kernel is 0. Assume that  $E$  is finite dimensional over the field  $k$ . The form is non-degenerate if and only if it is non-singular, i.e., induces an isomorphism of  $E$  with its dual space (anti-dual in the case of hermitian forms).

Except for the few remarks on the anti-linearity made in the previous chapter, we don't use the results of the duality in that chapter. We need only the duality over fields, given in Chapter III. Furthermore, we don't essentially meet matrices again, except for the remarks on the pfaffian in §10.

We introduce one more notation. In the study of forms on vector spaces, we shall frequently decompose the vector space into direct sums of orthogonal subspaces. If  $E$  is a vector space with a form  $g$  as above, and  $F, F'$  are subspaces, we shall write

$$E = F \perp F'$$

to mean that  $E$  is the direct sum of  $F$  and  $F'$ , and that  $F$  is orthogonal (or perpendicular) to  $F'$ , in other words,  $x \perp y$  (or  $\langle x, y \rangle = 0$ ) for all  $x \in F$  and  $y \in F'$ . We then say that  $E$  is the **orthogonal sum** of  $F$  and  $F'$ . There will be no confusion with the use of the symbol  $\perp$  when we write  $F \perp F'$  to mean simply that  $F$  is perpendicular to  $F'$ . The context always makes our meaning clear.

*Most of this chapter is devoted to giving certain orthogonal decompositions of a vector space with one of our three types of forms, so that each factor in the sum is an easily recognizable type.*

In the symmetric and hermitian case, we shall be especially concerned with direct sum decompositions into factors which are 1-dimensional. Thus if  $\langle \cdot, \cdot \rangle$  is symmetric or hermitian, we shall say that  $\{v_1, \dots, v_n\}$  is an **orthogonal basis** (with respect to the form) if  $\langle v_i, v_j \rangle = 0$  whenever  $i \neq j$ . We see that an orthogonal basis gives such a decomposition. If the form is nondegenerate, and if  $\{v_1, \dots, v_n\}$  is an orthogonal basis, then we see at once that  $\langle v_i, v_i \rangle \neq 0$  for all  $i$ .

**Proposition 1.1.** *Let  $E$  be a vector space over the field  $k$ , and let  $g$  be a form of one of the three above types. Suppose that  $E$  is expressed as an orthogonal sum,*

$$E = E_1 \perp \dots \perp E_m.$$

*Then  $g$  is non-degenerate on  $E$  if and only if it is non-degenerate on each  $E_i$ . If  $E_i^0$  is the kernel of the restriction of  $g$  to  $E_i$ , then the kernel of  $g$  in  $E$  is the orthogonal sum*

$$E^0 = E_1^0 \perp \dots \perp E_m^0.$$

*Proof.* Elements  $v, w$  of  $E$  can be written uniquely

$$v = \sum_{i=1}^m v_i, \quad w = \sum_{i=1}^m w_i$$

with  $v_i, w_i \in E_i$ . Then

$$v \cdot w = \sum_{i=1}^m v_i \cdot w_i,$$

and  $v \cdot w = 0$  if  $v_i \cdot w_i = 0$  for each  $i = 1, \dots, m$ . From this our assertion is obvious.

Observe that if  $E_1, \dots, E_m$  are vector spaces over  $k$ , and  $g_1, \dots, g_m$  are forms on these spaces respectively, then we can define a form  $g = g_1 \oplus \dots \oplus g_m$  on the direct sum  $E = E_1 \oplus \dots \oplus E_m$ ; namely if  $v, w$  are written as above, then we let

$$g(v, w) = \sum_{i=1}^m g_i(v_i, w_i).$$

It is then clear that, in fact, we have  $E = E_1 \perp \dots \perp E_m$ . We could also write  $g = g_1 \perp \dots \perp g_m$ .

**Proposition 1.2.** *Let  $E$  be a finite-dimensional space over the field  $k$ , and let  $g$  be a form of the preceding type on  $E$ . Assume that  $g$  is non-degenerate. Let  $F$  be a subspace of  $E$ . The form is non-degenerate on  $F$  if and only if  $F + F^\perp = E$ , and also if and only if it is non-degenerate on  $F^\perp$ .*

*Proof.* We have (as a trivial consequence of Chapter III, §5)

$$\dim F + \dim F^\perp = \dim E = \dim(F + F^\perp) + \dim(F \cap F^\perp).$$

Hence  $F + F^\perp = E$  if and only if  $\dim(F \cap F^\perp) = 0$ . Our first assertion follows at once. Since  $F, F^\perp$  enter symmetrically in the dimension condition, our second assertion also follows.

Instead of saying that a form is non-degenerate on  $E$ , we shall sometimes say, by abuse of language, that  $E$  is non-degenerate.

Let  $E$  be a finite-dimensional space over the field  $k$ , and let  $g$  be a form of the preceding type. Let  $E_0$  be the kernel of the form. Then we get an induced form of the same type

$$g_0 : E/E_0 \times E/E_0 \rightarrow k,$$

because  $g(x, y)$  depends only on the coset of  $x$  and the coset of  $y$  modulo  $E_0$ . Furthermore,  $g_0$  is non-degenerate since its kernel on both sides is 0.

Let  $E, E'$  be finite-dimensional vector spaces, with forms  $g, g'$  as above, respectively. A linear map  $\sigma : E \rightarrow E'$  is said to be **metric** if

$$g'(\sigma x, \sigma y) = g(x, y)$$

or in the dot notation,  $\sigma x \cdot \sigma y = x \cdot y$  for all  $x, y \in E$ . If  $\sigma$  is a linear isomorphism, and is metric, then we say that  $\sigma$  is an **isometry**.

Let  $E, E_0$  be as above. Then we have an induced form on the factor space  $E/E_0$ . If  $W$  is a complementary subspace of  $E_0$ , in other words,  $E = E_0 \oplus W$ , and if we let  $\sigma : E \rightarrow E/E_0$  be the canonical map, then  $\sigma$  is metric, and induces an isometry of  $W$  on  $E/E_0$ . This assertion is obvious, and shows that if

$$E = E_0 \oplus W'$$

is another direct sum decomposition of  $E$ , then  $W'$  is isometric to  $W$ . We know that  $W \approx E/E_0$  is nondegenerate. Hence our form determines a unique non-degenerate form, up to isometry, on complementary subspaces of the kernel.

## §2. QUADRATIC MAPS

Let  $R$  be a commutative ring and let  $E, F$  be  $R$ -modules. We suppress the prefix  $R$ - as usual. We recall that a bilinear map  $f : E \times E \rightarrow F$  is said to be symmetric if  $f(x, y) = f(y, x)$  for all  $x, y \in E$ .

We say that  $F$  is **without 2-torsion** if for all  $y \in F$  such that  $2y = 0$  we have  $y = 0$ . (This holds if 2 is invertible in  $R$ .)

Let  $f : E \rightarrow F$  be a mapping. We shall say that  $f$  is **quadratic** (i.e.  $R$ -quadratic) if there exists a symmetric bilinear map  $g : E \times E \rightarrow F$  and a linear map  $h : E \rightarrow F$  such that for all  $x \in E$  we have

$$f(x) = g(x, x) + h(x).$$

**Proposition 2.1.** *Assume that  $F$  is without 2-torsion. Let  $f : E \rightarrow F$  be quadratic, expressed as above in terms of a symmetric bilinear map and a linear map. Then  $g, h$  are uniquely determined by  $f$ . For all  $x, y \in E$  we have*

$$2g(x, y) = f(x + y) - f(x) - f(y).$$

*Proof.* If we compute  $f(x + y) - f(x) - f(y)$ , then we obtain  $2g(x, y)$ . If  $g_1$  is symmetric bilinear,  $h_1$  is linear, and  $f(x) = g_1(x, x) + h_1(x)$ , then  $2g(x, y) = 2g_1(x, y)$ . Since  $F$  is assumed to be without 2-torsion, it follows that  $g(x, y) = g_1(x, y)$  for all  $x, y \in E$ , and thus that  $g$  is uniquely determined. But then  $h$  is determined by the relation

$$h(x) = f(x) - g(x, x).$$

We call  $g, h$  the bilinear and linear maps **associated** with  $f$ .

If  $f : E \rightarrow F$  is a map, we define

$$\Delta f : E \times E \rightarrow F$$

by

$$\Delta f(x, y) = f(x + y) - f(x) - f(y).$$

We say that  $f$  is **homogeneous quadratic** if it is quadratic, and if its associated linear map is 0. We shall say that  $F$  is **uniquely divisible** by 2 if for each  $z \in F$  there exists a unique  $u \in F$  such that  $2u = z$ . (Again this holds if 2 is invertible in  $R$ .)

**Proposition 2.2.** *Let  $f: E \rightarrow F$  be a map such that  $\Delta f$  is bilinear. Assume that  $F$  is uniquely divisible by 2. Then the map  $x \mapsto f(x) - \frac{1}{2}\Delta f(x, x)$  is  $\mathbf{Z}$ -linear. If  $f$  satisfies the condition  $f(2x) = 4f(x)$ , then  $f$  is homogeneous quadratic.*

*Proof.* Obvious.

By a **quadratic form** on  $E$ , one means a homogeneous quadratic map  $f: E \rightarrow R$ , with values in  $R$ .

In what follows, we are principally concerned with symmetric bilinear forms. The quadratic forms play a secondary role.

### §3. SYMMETRIC FORMS, ORTHOGONAL BASES

*Let  $k$  be a field of characteristic  $\neq 2$ .*

Let  $E$  be a vector space over  $k$ , with the symmetric form  $g$ . We say that  $g$  is a **null form** or that  $E$  is a **null space** if  $\langle x, y \rangle = 0$  for all  $x, y \in E$ . Since we assumed that the characteristic of  $k$  is  $\neq 2$ , the condition  $x^2 = 0$  for all  $x \in E$  implies that  $g$  is a null form. Indeed,

$$4x \cdot y = (x + y)^2 - (x - y)^2.$$

**Theorem 3.1.** *Let  $E$  be  $\neq 0$  and finite dimensional over  $k$ . Let  $g$  be a symmetric form on  $E$ . Then there exists an orthogonal basis.*

*Proof.* We assume first that  $g$  is non-degenerate, and prove our assertion by induction in that case. If the dimension  $n$  is 1, then our assertion is obvious.

Assume  $n > 1$ . Let  $v_1 \in E$  be such that  $v_1^2 \neq 0$  (such an element exists since  $g$  is assumed non-degenerate). Let  $F = (v_1)$  be the subspace generated by  $v_1$ . Then  $F$  is non-degenerate, and by Proposition 1.2, we have

$$E = F + F^\perp.$$

Furthermore,  $\dim F^\perp = n - 1$ . Let  $\{v_2, \dots, v_n\}$  be an orthogonal basis of  $F^\perp$ .

Then  $\{v_1, \dots, v_n\}$  are pairwise orthogonal. Furthermore, they are linearly independent, for if

$$a_1 v_1 + \dots + a_n v_n = 0$$

with  $a_i \in k$  then we take the scalar product with  $v_i$  to get  $a_i v_i^2 = 0$  whence  $a_i = 0$  for all  $i$ .

**Remark.** We have shown in fact that if  $g$  is non-degenerate, and  $v \in E$  is such that  $v^2 \neq 0$  then we can complete  $v$  to an orthogonal basis of  $E$ .

Suppose that the form  $g$  is degenerate. Let  $E_0$  be its kernel. We can write  $E$  as a direct sum

$$E = E_0 \oplus W$$

for some subspace  $W$ . The restriction of  $g$  to  $W$  is non-degenerate; otherwise there would be an element of  $W$  which is in the kernel of  $E$ , and  $\neq 0$ . Hence if  $\{v_1, \dots, v_r\}$  is a basis of  $E_0$ , and  $\{w_1, \dots, w_{n-r}\}$  is an orthogonal basis of  $W$ , then

$$\{v_1, \dots, v_r, w_1, \dots, w_{n-r}\}$$

is an orthogonal basis of  $E$ , as was to be shown.

**Corollary 3.2.** Let  $\{v_1, \dots, v_n\}$  be an orthogonal basis of  $E$ . Assume that  $v_i^2 \neq 0$  for  $i \leq r$  and  $v_i^2 = 0$  for  $i > r$ . Then the kernel of  $E$  is equal to  $\{v_{r+1}, \dots, v_n\}$ .

*Proof.* Obvious.

If  $\{v_1, \dots, v_n\}$  is an orthogonal basis of  $E$  and if we write

$$X = x_1 v_1 + \dots + x_n v_n$$

with  $x_i \in k$ , then

$$X^2 = a_1 x_1^2 + \dots + a_n x_n^2$$

where  $a_i = \langle v_i, v_i \rangle$ . In this representation of the form, we say that it is **diagonalized**. With respect to an orthogonal basis, we see at once that the associated matrix of the form is a diagonal matrix, namely

$$\begin{pmatrix} a_1 & & & & & \\ & a_2 & & & & \\ & & \ddots & & & \\ & & & a_r & & \\ 0 & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

**Example.** Note that Exercise 33 of Chapter XIII gave an interesting example of an orthogonal decomposition involving harmonic polynomials.

## §4. SYMMETRIC FORMS OVER ORDERED FIELDS

**Theorem 4.1.** (Sylvester) *Let  $k$  be an ordered field and let  $E$  be a finite dimensional vector space over  $k$ , with a non-degenerate symmetric form  $g$ . There exists an integer  $r \geq 0$  such that, if  $\{v_1, \dots, v_n\}$  is an orthogonal basis of  $E$ , then precisely  $r$  among the  $n$  elements  $v_1^2, \dots, v_n^2$  are  $> 0$ , and  $n - r$  among these elements are  $< 0$ .*

*Proof.* Let  $a_i = v_i^2$ , for  $i = 1, \dots, n$ . After renumbering the basis elements, say  $a_1, \dots, a_r > 0$  and  $a_i < 0$  for  $i > r$ . Let  $\{w_1, \dots, w_n\}$  be any orthogonal basis, and let  $b_i = w_i^2$ . Say  $b_1, \dots, b_s > 0$  and  $b_j < 0$  for  $j > s$ . We shall prove that  $r = s$ . Indeed, it will suffice to prove that

$$v_1, \dots, v_r, w_{s+1}, \dots, w_n$$

are linearly independent, for then we get  $r + n - s \leq n$ , whence  $r \leq s$ , and  $r = s$  by symmetry. Suppose that

$$x_1 v_1 + \dots + x_r v_r + y_{s+1} w_{s+1} + \dots + y_n w_n = 0.$$

Then

$$x_1 v_1 + \dots + x_r v_r = -y_{s+1} w_{s+1} - \dots - y_n w_n.$$

Squaring both sides yields

$$a_1 x_1^2 + \dots + a_r x_r^2 = b_{s+1} y_{s+1}^2 + \dots + b_n y_n^2.$$

The left-hand side is  $\geq 0$ , and the right-hand side is  $\leq 0$ . Hence both sides are equal to 0, and it follows that  $x_i = y_j = 0$ , in other words that our vectors are linearly independent.

**Corollary 4.2.** *Assume that every positive element of  $k$  is a square. Then there exists an orthogonal basis  $\{v_1, \dots, v_n\}$  of  $E$  such that  $v_i^2 = 1$  for  $i \leq r$  and  $v_i^2 = -1$  for  $i > r$ , and  $r$  is uniquely determined.*

*Proof.* We divide each vector in an orthogonal basis by the square root of the absolute value of its square.

A basis having the property of the corollary is called **orthonormal**. If  $X$  is an element of  $E$  having coordinates  $(x_1, \dots, x_n)$  with respect to this basis, then

$$X^2 = x_1^2 + \dots + x_r^2 - x_{r+1}^2 - \dots - x_n^2.$$

We say that a symmetric form  $g$  is **positive definite** if  $X^2 > 0$  for all  $X \in E, X \neq 0$ . This is the case if and only if  $r = n$  in Theorem 4.1. We say that  $g$  is **negative definite** if  $X^2 < 0$  for all  $X \in E, X \neq 0$ .

**Corollary 4.3.** *The vector space  $E$  admits an orthogonal decomposition  $E = E^+ \perp E^-$  such that  $g$  is positive definite on  $E^+$  and negative definite on  $E^-$ . The dimension of  $E^+$  (or  $E^-$ ) is the same in all such decompositions.*

Let us now assume that the form  $g$  is positive definite and that every positive element of  $k$  is a square.

We define the **norm** of an element  $v \in E$  by

$$|v| = \sqrt{v \cdot v}.$$

Then we have  $|v| > 0$  if  $v \neq 0$ . We also have the **Schwarz inequality**

$$|v \cdot w| \leq |v| |w|$$

for all  $v, w \in E$ . This is proved in the usual way, expanding

$$0 \leq (av \pm bw)^2 = (av \pm bw) \cdot (av \pm bw)$$

by bilinearity, and letting  $b = |v|$  and  $a = |w|$ . One then gets

$$\mp 2ab v \cdot w \leq 2|v|^2 |w|^2.$$

If  $|v|$  or  $|w| = 0$  our inequality is trivial. If neither is 0 we divide by  $|v| |w|$  to get what we want.

From the Schwarz inequality, we deduce the triangle inequality

$$|v + w| \leq |v| + |w|.$$

We leave it to the reader as a routine exercise.

When we have a positive definite form, there is a canonical way of getting an orthonormal basis, starting with an arbitrary basis  $\{v_1, \dots, v_n\}$  and proceeding inductively. Let

$$v'_1 = \frac{1}{|v_1|} v_1.$$

Then  $v_1$  has norm 1. Let

$$w_2 = v_2 - (v_2 \cdot v'_1)v'_1,$$

and then

$$v'_2 = \frac{1}{|w_2|} w_2.$$

Inductively, we let

$$w_r = v_r - (v_r \cdot v'_1)v'_1 - \cdots - (v_r \cdot v'_{r-1})v'_{r-1}$$

and then

$$v'_r = \frac{1}{|w_r|} w_r.$$

The  $\{v'_1, \dots, v'_n\}$  is an orthonormal basis. The inductive process just described is known as the **Gram-Schmidt orthogonalization**.

## §5. HERMITIAN FORMS

Let  $k_0$  be an ordered field (a subfield of the reals, if you wish) and let  $k = k_0(i)$ , where  $i = \sqrt{-1}$ . Then  $k$  has an automorphism of order 2, whose fixed field is  $k_0$ .

Let  $E$  be a finite-dimensional vector space over  $k$ . We shall deal with a hermitian form on  $E$ , i.e. a map

$$E \times E \rightarrow k$$

written

$$(x, y) \mapsto \langle x, y \rangle$$

which is  $k$ -linear in its first variable,  $k$ -anti-linear in its second variable, and such that

$$\langle x, y \rangle = \overline{\langle y, x \rangle}$$

for all  $x, y \in E$ .

We observe that  $\langle x, x \rangle \in k_0$  for all  $x \in E$ . This is essentially the reason why the proofs of statements concerning symmetric forms hold essentially without change in the hermitian case. We shall now make the list of the properties which apply to this case.

**Theorem 5.1.** *There exists an orthogonal basis. If the form is non-degenerate, there exists an integer  $r$  having the following property. If  $\{v_1, \dots, v_n\}$  is an orthogonal basis, then precisely  $r$  among the  $n$  elements*

$$\langle v_1, v_1 \rangle, \dots, \langle v_n, v_n \rangle$$

*are  $> 0$  and  $n - r$  among these elements are  $< 0$ .*

An orthogonal basis  $\{v_1, \dots, v_n\}$  such that  $\langle v_i, v_i \rangle = 1$  or  $-1$  is called an **orthonormal** basis.

**Corollary 5.2.** *Assume that the form is non-degenerate, and that every positive element of  $k_0$  is a square. Then there exists an orthonormal basis.*

We say that the hermitian form is **positive definite** if  $\langle x, x \rangle > 0$  for all  $x \in E$ . We say that it is **negative definite** if  $\langle x, x \rangle < 0$  for all  $x \in E, x \neq 0$ .

**Corollary 5.3.** *Assume that the form is non-degenerate. Then  $E$  admits an orthogonal decomposition  $E = E^+ \perp E^-$  such that the form is positive definite on  $E^+$  and negative definite on  $E^-$ . The dimension of  $E^+$  (or  $E^-$ ) is the same in all such decompositions.*

The proofs of Theorem 5.1 and its corollaries are identical with those of the analogous results for symmetric forms, and will be left to the reader.

We have the **polarization identity**, for any  $k$ -linear map  $A : E \rightarrow E$ , namely

$$\langle A(x + y), (x + y) \rangle - \langle A(x - y), (x - y) \rangle = 2[\langle Ax, y \rangle + \langle Ay, x \rangle].$$

If  $\langle Ax, x \rangle = 0$  for all  $x$ , we replace  $x$  by  $ix$  and get

$$\langle Ax, y \rangle + \langle Ay, x \rangle = 0,$$

$$i\langle Ax, y \rangle - i\langle Ay, x \rangle = 0.$$

From this we conclude:

*If  $\langle Ax, x \rangle = 0$ , for all  $x$ , then  $A = 0$ .*

This is the only statement which has no analogue in the case of symmetric forms. The presence of  $i$  in one of the above linear equations is essential to the conclusion. In practice, one uses the statement in the complex case, and one meets an analogous situation in the real case when  $A$  is symmetric. Then the statement for symmetric maps is obvious.

*Assume that the hermitian form is positive definite, and that every positive element of  $k_0$  is a square.*

We have the **Schwarz inequality**, namely

$$|\langle x, y \rangle|^2 \leq \langle x, x \rangle \langle y, y \rangle$$

whose proof comes again by expanding

$$0 \leq \langle \alpha x + \beta y, \alpha x + \beta y \rangle$$

and setting  $\alpha = \langle y, y \rangle$  and  $\beta = -\langle x, y \rangle$ .

We define the norm of  $|x|$  to be

$$|x| = \sqrt{\langle x, x \rangle}.$$

Then we get at once the triangle inequality

$$|x + y| \leq |x| + |y|,$$

and for  $\alpha \in k$ ,

$$|\alpha x| = |\alpha| |x|.$$

Just as in the symmetric case, given a basis, one can find an orthonormal basis by the inductive procedure of subtracting successive projections. We leave this to the reader.

## §6. THE SPECTRAL THEOREM (HERMITIAN CASE)

Throughout this section, we let  $E$  be a finite dimensional space over  $\mathbf{C}$ , of dimension  $\geq 1$ , and we endow  $E$  with a positive definite hermitian form.

Let  $A : E \rightarrow E$  be a linear map (i.e.  $\mathbf{C}$ -linear map) of  $E$  into itself. For fixed  $y \in E$ , the map  $x \mapsto \langle Ax, y \rangle$  is a linear functional, and hence there exists a unique element  $y^* \in E$  such that

$$\langle Ax, y \rangle = \langle x, y^* \rangle$$

for all  $x \in E$ . We define the map  $A^* : E \rightarrow E$  by  $A^*y = y^*$ . It is immediately clear that  $A^*$  is linear, and we shall call  $A^*$  the **adjoint** of  $A$  with respect to our hermitian form.

The following formulas are trivially verified, for any linear maps  $A, B$  of  $E$  into itself:

$$(A + B)^* = A^* + B^*, \quad A^{**} = A,$$

$$(\alpha A)^* = \bar{\alpha} A^*, \quad (AB)^* = B^*A^*.$$

A linear map  $A$  is called **self-adjoint** (or **hermitian**) if  $A^* = A$ .

**Proposition 6.1.** *A is hermitian if and only if  $\langle Ax, x \rangle$  is real for all  $x \in E$ .*

*Proof.* Let  $A$  be hermitian. Then

$$\overline{\langle Ax, x \rangle} = \overline{\langle x, Ax \rangle} = \langle Ax, x \rangle,$$

whence  $\langle Ax, x \rangle$  is real. Conversely, assume  $\langle Ax, x \rangle$  is real for all  $x$ . Then

$$\langle Ax, x \rangle = \overline{\langle Ax, x \rangle} = \langle x, Ax \rangle = \langle A^*x, x \rangle,$$

and consequently  $\langle (A - A^*)x, x \rangle = 0$  for all  $x$ . Hence  $A = A^*$  by polarization.

Let  $A : E \rightarrow E$  be a linear map. An element  $\xi \in E$  is called an **eigenvector** of  $A$  if there exists  $\lambda \in \mathbf{C}$  such that  $A\xi = \lambda\xi$ . If  $\xi \neq 0$ , then we say that  $\lambda$  is an **eigenvalue** of  $A$ , belonging to  $\xi$ .

**Proposition 6.2.** *Let  $A$  be hermitian. Then all eigenvalues belonging to nonzero eigenvectors of  $A$  are real. If  $\xi, \xi'$  are eigenvectors  $\neq 0$  having eigenvalues  $\lambda, \lambda'$  respectively, and if  $\lambda \neq \lambda'$ , then  $\xi \perp \xi'$ .*

*Proof.* Let  $\lambda$  be an eigenvalue, belonging to the eigenvector  $\xi \neq 0$ . Then  $\langle A\xi, \xi \rangle = \langle \xi, A\xi \rangle$ , and these two numbers are equal respectively to  $\lambda\langle \xi, \xi \rangle$  and  $\bar{\lambda}\langle \xi, \xi \rangle$ . Since  $\xi \neq 0$ , it follows that  $\lambda = \bar{\lambda}$ , i.e. that  $\lambda$  is real. Secondly, assume that  $\xi, \xi'$  and  $\lambda, \lambda'$  are as described above. Then

$$\langle A\xi, \xi' \rangle = \lambda\langle \xi, \xi' \rangle = \langle \xi, A\xi' \rangle = \lambda'\langle \xi, \xi' \rangle,$$

from which it follows that  $\langle \xi, \xi' \rangle = 0$ .

**Lemma 6.3.** *Let  $A : E \rightarrow E$  be a linear map, and  $\dim E \geq 1$ . Then there exists at least one non-zero eigenvector of  $A$ .*

*Proof.* We consider  $\mathbf{C}[A]$ , i.e. the ring generated by  $A$  over  $\mathbf{C}$ . As a vector space over  $\mathbf{C}$ , it is contained in the ring of endomorphisms of  $E$ , which is finite dimensional, the dimension being the same as for the ring of all  $n \times n$  matrices if  $n = \dim E$ . Hence there exists a non-zero polynomial  $P$  with coefficients in  $\mathbf{C}$  such that  $P(A) = 0$ . We can factor  $P$  into a product of linear factors,

$$P(X) = (X - \lambda_1) \cdots (X - \lambda_m)$$

with  $\lambda_j \in \mathbf{C}$ . Then  $(A - \lambda_1 I) \cdots (A - \lambda_m I) = 0$ . Hence not all factors  $A - \lambda_j I$  can be isomorphisms, and there exists  $\lambda \in \mathbf{C}$  such that  $A - \lambda I$  is not an isomorphism. Hence it has an element  $\xi \neq 0$  in its kernel, and we get  $A\xi - \lambda\xi = 0$ . This shows that  $\xi$  is a non-zero eigenvector, as desired.

**Theorem 6.4. (Spectral Theorem, Hermitian Case).** *Let  $E$  be a non-zero finite dimensional vector space over the complex numbers, with a positive definite hermitian form. Let  $A : E \rightarrow E$  be a hermitian linear map. Then  $E$  has an orthogonal basis consisting of eigenvectors of  $A$ .*

*Proof.* Let  $\xi_1$  be a non-zero eigenvector, with eigenvalue  $\lambda_1$ , and let  $E_1$  be the subspace generated by  $\xi_1$ . Then  $A$  maps  $E_1^\perp$  into itself, because

$$\langle AE_1^\perp, \xi_1 \rangle = \langle E_1^\perp, A\xi_1 \rangle = \langle E_1^\perp, \lambda_1 \xi_1 \rangle = \lambda_1 \langle E_1^\perp, \xi_1 \rangle = 0,$$

whence  $AE_1^\perp$  is perpendicular to  $\xi_1$ .

Since  $\xi_1 \neq 0$  we have  $\langle \xi_1, \xi_1 \rangle > 0$  and hence, since our hermitian form is non-degenerate (being positive definite), we have

$$E = E_1 \oplus E_1^\perp.$$

The restriction of our form to  $E_1^\perp$  is positive definite (if  $\dim E > 1$ ). From Proposition 6.1, we see at once that the restriction of  $A$  to  $E_1^\perp$  is hermitian. Hence we can complete the proof by induction.

**Corollary 6.5.** *Hypotheses being as in the theorem, there exists an orthonormal basis consisting of eigenvectors of  $A$ .*

*Proof.* Divide each vector in an orthogonal basis by its norm.

**Corollary 6.6.** *Let  $E$  be a non-zero finite dimensional vector space over the complex numbers, with a positive definite hermitian form  $f$ . Let  $g$  be another hermitian form on  $E$ . Then there exists a basis of  $E$  which is orthogonal for both  $f$  and  $g$ .*

*Proof.* We write  $f(x, y) = \langle x, y \rangle$ . Since  $f$  is non-singular, being positive definite, there exists a unique hermitian linear map  $A$  such that  $f(x, y) = \langle Ax, y \rangle$  for all  $x, y \in E$ . We apply the theorem to  $A$ , and find a basis as in the theorem, say  $\{v_1, \dots, v_n\}$ . Let  $\lambda_i$  be the eigenvalue such that  $Av_i = \lambda_i v_i$ . Then

$$g(v_i, v_j) = \langle Av_i, v_j \rangle = \lambda_i \langle v_i, v_j \rangle,$$

and therefore our basis is also orthogonal for  $g$ , as was to be shown.

We recall that a linear map  $U : E \rightarrow E$  is **unitary** if and only if  $U^* = U^{-1}$ . This condition is equivalent to the property that  $\langle Ux, Uy \rangle = \langle x, y \rangle$  for all elements  $x, y \in E$ . In other words,  $U$  is an automorphism of the form  $f$ .

**Theorem 6.7. (Spectral Theorem, Unitary Case).** *Let  $E$  be a non-zero finite dimensional vector space over the complex numbers, with a positive definite hermitian form. Let  $U : E \rightarrow E$  be a unitary linear map. Then  $E$  has an orthogonal basis consisting of eigenvectors of  $U$ .*

*Proof.* Let  $\xi_1 \neq 0$  be an eigenvector of  $U$ . It is immediately verified that the subspace of  $E$  orthogonal to  $\xi_1$  is mapped into itself by  $U$ , using the relation  $U^* = U^{-1}$ , because if  $\eta$  is perpendicular to  $\xi_1$ , then

$$\langle U\eta, \xi_1 \rangle = \langle \eta, U^*\xi_1 \rangle = \langle \eta, U^{-1}\xi_1 \rangle = \langle \eta, \lambda^{-1}\xi_1 \rangle = 0.$$

Thus we can finish the proof by induction as before.

**Remark.** If  $\lambda$  is an eigenvalue of the unitary map  $U$ , then  $\lambda$  has necessarily absolute value 1 (because  $U$  preserves length), whence  $\lambda$  can be written in the form  $e^{i\theta}$  with  $\theta$  real, and we may view  $U$  as a rotation.

Let  $A : E \rightarrow E$  be an invertible linear map. Just as one writes a non-zero complex number  $z = re^{i\theta}$  with  $r > 0$ , there exists a decomposition of  $A$  as a product called its polar decomposition. Let  $P : E \rightarrow E$  be linear. We say that  $P$  is **semipositive** if  $P$  is hermitian and we have  $\langle Px, x \rangle \geq 0$  for all  $x \in E$ . If we have  $\langle Px, x \rangle > 0$  for all  $x \neq 0$  in  $E$  then we say that  $P$  is **positive definite**. For

example, if we let  $P = A^*A$  then we see that  $P$  is positive definite, because

$$\langle A^*Ax, x \rangle = \langle Ax, Ax \rangle > 0 \text{ if } x \neq 0.$$

**Proposition 6.8.** *Let  $P$  be semipositive. Then  $P$  has a unique semipositive square root  $B : E \rightarrow E$ , i.e. a semipositive linear map such that  $B^2 = P$ .*

*Proof.* For simplicity, we assume that  $P$  is positive definite. By the spectral theorem, there exists a basis of  $E$  consisting of eigenvectors. The eigenvalues must be  $> 0$  (immediate from the condition of positivity). The linear map defined by sending each eigenvector to its multiple by the square root of the corresponding eigenvalue satisfies the required conditions. As for uniqueness, since  $B$  commutes with  $P$  because  $B^2 = P$ , it follows that if  $\{v_1, \dots, v_n\}$  is a basis consisting of eigenvectors for  $P$ , then each  $v_i$  is also an eigenvector for  $B$ . (Cf. Chapter XIV, Exercises 12 and 13(d).) Since a positive number has a unique positive square root, it follows that  $B$  is uniquely determined as the unique linear map whose effect on  $v_i$  is multiplication by the square root of the corresponding eigenvalue for  $P$ .

**Theorem 6.9.** *Let  $A : E \rightarrow E$  be an invertible linear map. Then  $A$  can be written in a unique way as a product  $A = UP$ , where  $U$  is unitary and  $P$  is positive definite.*

*Proof.* Let  $P = (A^*A)^{1/2}$ , and let  $U = AP^{-1}$ . Using the definitions, it is immediately verified that  $U$  is unitary, so we get the existence of the decomposition. As for uniqueness, suppose  $A = U_1P_1$ . Let

$$U_2 = PP_1^{-1} = U^{-1}U_1.$$

Then  $U_2$  is unitary, so  $U_2^*U_2 = I$ . From the fact that  $P^* = P$  and  $P_1^* = P_1$ , we conclude that  $P^2 = P_1^2$ . Since  $P, P_1$  are Hermitian positive definite, it follows as in Proposition 6.8 that  $P = P_1$ , thus proving the theorem.

**Remark.** The arguments used to prove Theorem 6.9 apply in the case of Hilbert space in analysis. Cf. my *Real Analysis*. However, for the uniqueness, since there may not be “eigenvalues”, one has to use another technique from analysis, described in that book.

As a matter of terminology, the expression  $A = UP$  in Theorem 6.9 is called the **polar decomposition** of  $A$ . Of course, it does matter in what order we write the decomposition. There is also a unique decomposition  $A = P_1U_1$  with  $P_1$  positive definite and  $U_1$  unitary (apply Theorem 6.9 to  $A^{-1}$ , and then take inverses).

---

## §7. THE SPECTRAL THEOREM (SYMMETRIC CASE)

Let  $E$  be a finite dimensional vector space over the real numbers, and let  $g$  be a symmetric positive definite form on  $E$ . If  $A : E \rightarrow E$  is a linear map, then we know

that its transpose, relative to  $g$ , is defined by the condition

$$\langle Ax, y \rangle = \langle x, {}^t A y \rangle$$

for all  $x, y \in E$ . We say that  $A$  is **symmetric** if  $A = {}^t A$ . As before, an element  $\xi \in E$  is called an eigenvector of  $A$  if there exists  $\lambda \in R$  such that  $A\xi = \lambda\xi$ , and  $\lambda$  is called an eigenvalue if  $\xi \neq 0$ .

**Theorem 7.1. (Spectral Theorem, Symmetric Case).** *Let  $E \neq 0$ . Let  $A : E \rightarrow E$  be a symmetric linear map. Then  $E$  has an orthogonal basis consisting of eigenvectors of  $A$ .*

*Proof.* If we select an orthogonal basis for the positive definite form, then the matrix of  $A$  with respect to this basis is a real symmetric matrix, and we are reduced to considering the case when  $E = \mathbf{R}^n$ . Let  $M$  be the matrix representing  $A$ . We may view  $M$  as operating on  $\mathbf{C}^n$ , and then  $M$  represents a hermitian linear map. Let  $z \neq 0$  be a complex eigenvector for  $M$ , and write

$$z = x + iy,$$

with  $x, y \in \mathbf{R}^n$ . By Proposition 6.2, we know that an eigenvalue  $\lambda$  for  $M$ , belonging to  $z$ , is real, and we have  $Mz = \lambda z$ . Hence  $Mx = \lambda x$  and  $My = \lambda y$ . But we must have  $x \neq 0$  or  $y \neq 0$ . Thus we have found a nonzero eigenvector for  $M$ , namely,  $A$ , in  $E$ . We can now proceed as before. The orthogonal complement of this eigenvector in  $E$  has dimension  $(n - 1)$ , and is mapped into itself by  $A$ . We can therefore finish the proof by induction.

**Remarks.** The spectral theorems are valid over a real closed field; our proofs don't need any change. Furthermore, the proofs are reasonably close to those which would be given in analysis for Hilbert spaces, and compact operators. The existence of eigenvalues and eigenvectors must however be proved differently, for instance using the Gelfand-Mazur theorem which we have actually proved in Chapter XII, or using a variational principle (i.e. finding a maximum or minimum for the quadratic function depending on the operator).

**Corollary 7.2.** *Hypotheses being as in the theorem, there exists an orthonormal basis consisting of eigenvectors of  $A$ .*

*Proof.* Divide each vector in an orthogonal basis by its norm.

**Corollary 7.3.** *Let  $E$  be a non-zero finite dimensional vector space over the reals, with a positive definite symmetric form  $f$ . Let  $g$  be another symmetric form on  $E$ . Then there exists a basis of  $E$  which is orthogonal for both  $f$  and  $g$ .*

*Proof.* We write  $f(x, y) = \langle x, y \rangle$ . Since  $f$  is non-singular, being positive definite, there exists a unique symmetric linear map  $A$  such that

$$g(x, y) = \langle Ax, y \rangle$$

for all  $x, y \in E$ . We apply the theorem to  $A$ , and find a basis as in the theorem. It is clearly an orthogonal basis for  $g$  (cf. the same proof in the hermitian case).

The analogues of Proposition 6.8 and the polar decomposition also hold in the present case, with the same proofs. See Exercise 9.

## §8. ALTERNATING FORMS

Let  $E$  be a vector space over the field  $k$ , on which we now make no restriction. We let  $f$  be an alternating form on  $E$ , i.e. a bilinear map  $f: E \times E \rightarrow k$  such that  $f(x, x) = x^2 = 0$  for all  $x \in E$ . Then

$$x \cdot y = -y \cdot x$$

for all  $x, y \in E$ , as one sees by substituting  $(x + y)$  for  $x$  in  $x^2 = 0$ .

We define a **hyperbolic plane** (for the alternating form) to be a 2-dimensional space which is non-degenerate. We get automatically an element  $w$  such that  $w^2 = 0$ ,  $w \neq 0$ . If  $P$  is a hyperbolic plane, and  $w \in P$ ,  $w \neq 0$ , then there exists an element  $y \neq 0$  in  $P$  such that  $w \cdot y \neq 0$ . After dividing  $y$  by some constant, we may assume that  $w \cdot y = 1$ . Then  $y \cdot w = -1$ . Hence the matrix of the form with respect to the basis  $\{w, y\}$  is

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The pair  $w, y$  is called a **hyperbolic pair** as before. Given a 2-dimensional vector space over  $k$  with a bilinear form, and a pair of elements  $\{w, y\}$  satisfying the relations

$$w^2 = y^2 = 0, \quad y \cdot w = -1, \quad w \cdot y = 1,$$

then we see that the form is alternating, and that  $(w, y)$  is a hyperbolic plane for the form.

Given an alternating form  $f$  on  $E$ , we say that  $E$  (or  $f$ ) is **hyperbolic** if  $E$  is an orthogonal sum of hyperbolic planes. We say that  $E$  (or  $f$ ) is **null** if  $x \cdot y = 0$  for all  $x, y \in E$ .

**Theorem 8.1.** *Let  $f$  be an alternating form on the finite dimensional vector space  $E$  over  $k$ . Then  $E$  is an orthogonal sum of its kernel and a hyperbolic subspace. If  $E$  is non-degenerate, then  $E$  is a hyperbolic space, and its dimension is even.*

*Proof.* A complementary subspace to the kernel is non-degenerate, and hence we may assume that  $E$  is non-degenerate. Let  $w \in E$ ,  $w \neq 0$ . There exists  $y \in E$  such that  $w \cdot y \neq 0$  and  $y \neq 0$ . Then  $(w, y)$  is non-degenerate, hence is a hyperbolic plane  $P$ . We have  $E = P \oplus P^\perp$  and  $P^\perp$  is non-degenerate. We

complete the proof by induction.

**Corollary 8.2.** *All alternating non-degenerate forms of a given dimension over a field  $k$  are isometric.*

We see from Theorem 8.1 that there exists a basis of  $E$  such that relative to this basis, the matrix of the alternating form is

$$\begin{pmatrix} 0 & 1 & & & & & & \\ -1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & -1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & 0 & 1 & \\ & & & & & -1 & 0 & \\ & & & & & & & 0 \\ & & & & & & & \\ & & & & & & & 0 \end{pmatrix}.$$

For convenience of writing, we reorder the basis elements of our orthogonal sum of hyperbolic planes in such a way that the matrix of the form is

$$\begin{pmatrix} 0 & I_r & 0 \\ -I_r & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where  $I_r$  is the unit  $r \times r$  matrix. The matrix

$$\begin{pmatrix} 0 & I_r \\ -I_r & 0 \end{pmatrix}$$

is called the **standard alternating** matrix.

**Corollary 8.3.** *Let  $E$  be a finite dimensional vector space over  $k$ , with a non-degenerate symmetric form denoted by  $\langle \cdot, \cdot \rangle$ . Let  $\Omega$  be a non-degenerate alternating form on  $E$ . Then there exists a direct sum decomposition  $E = E_1 \oplus E_2$  and a symmetric automorphism  $A$  of  $E$  (with respect to  $\langle \cdot, \cdot \rangle$ ) having the following property. If  $x, y \in E$  are written*

$$x = (x_1, x_2) \quad \text{with} \quad x_1 \in E_1 \quad \text{and} \quad x_2 \in E_2,$$

$$y = (y_1, y_2) \quad \text{with} \quad y_1 \in E_1 \quad \text{and} \quad y_2 \in E_2,$$

then

$$\Omega(x, y) = \langle Ax_1, y_2 \rangle - \langle Ax_2, y_1 \rangle.$$

*Proof.* Take a basis of  $E$  such that the matrix of  $\Omega$  with respect to this basis is the standard alternating matrix. Let  $f$  be the symmetric non-degenerate form on  $E$  given by the dot product with respect to this basis. Then we obtain a direct sum decomposition of  $E$  into subspaces  $E_1, E_2$  (corresponding to the first  $n$ , resp. the last  $n$  coordinates), such that

$$\Omega(x, y) = f(x_1, y_2) - f(x_2, y_1).$$

Since  $\langle \cdot, \cdot \rangle$  is assumed non-degenerate, we can find an automorphism  $A$  having the desired effect, and  $A$  is symmetric because  $f$  is symmetric.

## §9. THE PFAFFIAN

An alternating matrix is a matrix  $G$  such that  $'G = -G$  and the diagonal elements are equal to 0. As we saw in Chapter XIII, §6, it is the matrix of an alternating form. We let  $G$  be an  $n \times n$  matrix, and assume  $n$  is even. (For odd  $n$ , cf. exercises.)

We start over a field of characteristic 0. By Corollary 8.2, there exists a non-singular matrix  $C$  such that  $'CGC$  is the matrix

$$\begin{pmatrix} 0 & I_r & 0 \\ -I_r & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

and hence

$$\det(C)^2 \det(G) = 1 \quad \text{or} \quad 0$$

according as the kernel of the alternating form is trivial or non-trivial. Thus in any case, we see that  $\det(G)$  is a square in the field.

Now we move over to the integers  $\mathbf{Z}$ . Let  $t_{ij}$  ( $1 \leq i < j \leq n$ ) be  $n(n-1)/2$  algebraically independent elements over  $\mathbf{Q}$ , let  $t_{ii} = 0$  for  $i = 1, \dots, n$ , and let  $t_{ij} = -t_{ji}$  for  $i > j$ . Then the matrix  $T = (t_{ij})$  is alternating, and hence  $\det(T)$  is a square in the field  $\mathbf{Q}(t)$  obtained from  $\mathbf{Q}$  by adjoining all the variables  $t_{ij}$ . However,  $\det(T)$  is a polynomial in  $\mathbf{Z}[t]$ , and since we have unique factorization in  $\mathbf{Z}[t]$ , it follows that  $\det(T)$  is the square of a polynomial in  $\mathbf{Z}[t]$ . We can write

$$\det(T) = P(t)^2.$$

The polynomial  $P$  is uniquely determined up to a factor of  $\pm 1$ . If we substitute

values for the  $t_{ij}$  so that the matrix  $T$  specializes to

$$\begin{pmatrix} 0 & I_{n/2} \\ -I_{n/2} & 0 \end{pmatrix},$$

then we see that there exists a unique polynomial  $P$  with integer coefficients taking the value 1 for this specialized set of values of  $(t)$ . We call  $P$  the **generic Pfaffian** of size  $n$ , and write it  $\text{Pf}$ .

Let  $R$  be a commutative ring. We have a homomorphism

$$\mathbf{Z}[t] \rightarrow R[t]$$

induced by the unique homomorphism of  $\mathbf{Z}$  into  $R$ . The image of the generic Pfaffian of size  $n$  in  $R[t]$  is a polynomial with coefficients in  $R$ , which we still denote by  $\text{Pf}$ . If  $G$  is an alternating matrix with coefficients in  $R$ , then we write  $\text{Pf}(G)$  for the value of  $\text{Pf}(t)$  when we substitute  $g_{ij}$  for  $t_{ij}$  in  $\text{Pf}$ . Since the determinant commutes with homomorphisms, we have:

**Theorem 9.1.** *Let  $R$  be a commutative ring. Let  $(g_{ij}) = G$  be an alternating matrix with  $g_{ij} \in R$ . Then*

$$\det(G) = (\text{Pf}(G))^2.$$

Furthermore, if  $C$  is an  $n \times n$  matrix in  $R$ , then

$$\text{Pf}(CG'C) = \det(C) \text{Pf}(G).$$

*Proof.* The first statement has been proved above. The second statement will follow if we can prove it over  $\mathbf{Z}$ . Let  $u_{ij}$  ( $i, j = 1, \dots, n$ ) be algebraically independent over  $\mathbf{Q}$ , and such that  $u_{ij}, t_{ij}$  are algebraically independent over  $\mathbf{Q}$ . Let  $U$  be the matrix  $(u_{ij})$ . Then

$$\text{Pf}(UT'U) = \pm \det(U) \text{Pf}(T),$$

as follows immediately from taking the square of both sides. Substitute values for  $U$  and  $T$  such that  $U$  becomes the unit matrix and  $T$  becomes the standard alternating matrix. We conclude that we must have a + sign on the right-hand side. Our assertion now follows as usual for any substitution of  $U$  to a matrix in  $R$ , and any substitution of  $T$  to an alternating matrix in  $R$ , as was to be shown.

---

## §10. WITT'S THEOREM

We go back to symmetric forms and we let  $k$  be a field of characteristic  $\neq 2$ .

Let  $E$  be a vector space over  $k$ , with a symmetric form. We say that  $E$  is a **hyperbolic plane** if the form is non-degenerate, if  $E$  has dimension 2, and if there exists an element  $w \neq 0$  in  $E$  such that  $w^2 = 0$ . We say that  $E$  is a **hyperbolic space** if it is an orthogonal sum of hyperbolic planes. We also say that the form on  $E$  is hyperbolic.

Suppose that  $E$  is a hyperbolic plane, with an element  $w \neq 0$  such that  $w^2 = 0$ . Let  $u \in E$  be such that  $E = (w, u)$ . Then  $u \cdot w \neq 0$ ; otherwise  $w$  would be a non-zero element in the kernel. Let  $b \in k$  be such that  $w \cdot bu = bw \cdot u = 1$ .

Then select  $a \in k$  such that

$$(aw + bu)^2 = 2abw \cdot u + b^2u^2 = 0.$$

(This can be done since we deal with a linear equation in  $a$ .) Put  $v = aw + bu$ . Then we have found a basis for  $E$ , namely  $E = (w, v)$  such that

$$w^2 = v^2 = 0 \quad \text{and} \quad w \cdot v = 1.$$

Relative to this basis, the matrix of our form is therefore

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We observe that, conversely, a space  $E$  having a basis  $\{w, v\}$  satisfying  $w^2 = v^2 = 0$  and  $w \cdot v = 1$  is non-degenerate, and thus is a hyperbolic plane. A basis  $\{w, v\}$  satisfying these relations will be called a **hyperbolic pair**.

An orthogonal sum of non-degenerate spaces is non-degenerate and hence a hyperbolic space is non-degenerate. We note that a hyperbolic space always has even dimension.

**Lemma 10.1.** *Let  $E$  be a finite dimensional vector space over  $k$ , with a non-degenerate symmetric form  $g$ . Let  $F$  be a subspace,  $F_0$  the kernel of  $F$ , and suppose we have an orthogonal decomposition*

$$F = F_0 \perp U.$$

*Let  $\{w_1, \dots, w_s\}$  be a basis of  $F_0$ . Then there exist elements  $v_1, \dots, v_s$  in  $E$  perpendicular to  $U$ , such that each pair  $\{w_i, v_i\}$  is a hyperbolic pair generating a hyperbolic plane  $P_i$ , and such that we have an orthogonal decomposition*

$$U \perp P_1 \perp \dots \perp P_s.$$

*Proof.* Let

$$U_1 = (w_2, \dots, w_s) \oplus U.$$

Then  $U_1$  is contained in  $F_0 \oplus U$  properly, and consequently  $(F_0 \oplus U)^\perp$  is

contained in  $U_1^\perp$  properly. Hence there exists an element  $u_1 \in U_1^\perp$  but

$$u_1 \notin (F_0 \oplus U)^\perp.$$

We have  $w_1 \cdot u_1 \neq 0$ , and hence  $(w_1, u_1)$  is a hyperbolic plane  $P_1$ . We have seen previously that we can find  $v_1 \in P_1$  such that  $\{w_1, v_1\}$  is a hyperbolic pair. Furthermore, we obtain an orthogonal sum decomposition

$$F_1 = (w_2, \dots, w_s) \perp P_1 \perp U.$$

Then it is clear that  $(w_2, \dots, w_s)$  is the kernel of  $F_1$ , and we can complete the proof by induction.

**Theorem 10.2** *Let  $E$  be a finite dimensional vector space over  $k$ , and let  $g$  be a non-degenerate symmetric form on  $E$ . Let  $F, F'$  be subspaces of  $E$ , and let  $\sigma: F \rightarrow F'$  be an isometry. Then  $\sigma$  can be extended to an isometry of  $E$  onto itself.*

*Proof.* We shall first reduce the proof to the case when  $F$  is non-degenerate.

We can write  $F = F_0 \perp U$  as in the lemma of the preceding section, and then  $\sigma F = F' = \sigma F_0 \perp \sigma U$ . Furthermore,  $\sigma F_0 = F'_0$  is the kernel of  $F'$ . Now we can enlarge both  $F$  and  $F'$  as in the lemma to orthogonal sums

$$U \perp P_1 \perp \dots \perp P_s \quad \text{and} \quad \sigma U \perp P'_1 \perp \dots \perp P'_s$$

corresponding to a choice of basis in  $F_0$  and its corresponding image in  $F'_0$ . Thus we can extend  $\sigma$  to an isometry of these extended spaces, which are non-degenerate. This gives us the desired reduction.

We assume that  $F, F'$  are non-degenerate, and proceed stepwise.

Suppose first that  $F' = F$ , i.e. that  $\sigma$  is an isometry of  $F$  onto itself. We can extend  $\sigma$  to  $E$  simply by leaving every element of  $F^\perp$  fixed.

Next, assume that  $\dim F = \dim F' = 1$  and that  $F \neq F'$ . Say  $F = (v)$  and  $F' = (v')$ . Then  $v^2 = v'^2$ . Furthermore,  $(v, v')$  has dimension 2.

If  $(v, v')$  is non-degenerate, it has an isometry extending  $\sigma$ , which maps  $v$  on  $v'$  and  $v'$  on  $v$ . We can apply the preceding step to conclude the proof.

If  $(v, v')$  is degenerate, its kernel has dimension 1. Let  $w$  be a basis for this kernel. There exist  $a, b \in k$  such that  $v' = av + bw$ . Then  $v'^2 = a^2v^2$  and hence  $a = \pm 1$ . Replacing  $v'$  by  $-v'$  if necessary, we may assume  $a = 1$ . Replacing  $w$  by  $bw$ , we may assume  $v' = v + w$ . Let  $z = v + v'$ . We apply Lemma 10.1 to the space

$$(w, z) = (w) \perp (z).$$

We can find an element  $y \in E$  such that

$$y \cdot z = 0, \quad y^2 = 0, \quad \text{and} \quad w \cdot y = 1.$$

The space  $(z, w, y) = (z) \perp (w, y)$  is non-degenerate, being an orthogonal sum of  $(z)$  and the hyperbolic plane  $(w, y)$ . It has an isometry such that

$$z \leftrightarrow z, \quad w \leftrightarrow -w, \quad y \leftrightarrow -y.$$

But  $v = \frac{1}{2}(z - w)$  is mapped on  $v' = \frac{1}{2}(z + w)$  by this isometry. We have settled the present case.

We finish the proof by induction. By the existence of an orthogonal basis (Theorem 3.1), every subspace  $F$  of dimension  $> 1$  has an orthogonal decomposition into a sum of subspaces of smaller dimension. Let  $F = F_1 \perp F_2$  with  $\dim F_1$  and  $\dim F_2 \geq 1$ . Then

$$\sigma F = \sigma F_1 \perp \sigma F_2.$$

Let  $\sigma_1 = \sigma|F_1$  be the restriction of  $\sigma$  to  $F_1$ . By induction, we can extend  $\sigma_1$  to an isometry

$$\bar{\sigma}_1 : E \rightarrow E.$$

Then  $\bar{\sigma}_1(F_1^\perp) = (\sigma_1 F_1)^\perp$ . Since  $\sigma F_2$  is perpendicular to  $\sigma F_1 = \sigma_1 F_1$ , it follows that  $\sigma F_2$  is contained in  $\bar{\sigma}_1(F_1^\perp)$ . Let  $\sigma_2 = \sigma|F_2$ . Then the isometry

$$\sigma_2 : F_2 \rightarrow \sigma_2 F_2 = \sigma F_2$$

extends by induction to an isometry

$$\bar{\sigma}_2 : F_2^\perp \rightarrow \bar{\sigma}_1(F_1^\perp).$$

The pair  $(\sigma_1, \bar{\sigma}_2)$  gives us an isometry of  $F_1 \perp F_1^\perp = E$  onto itself, as desired.

**Corollary 10.3.** *Let  $E, E'$  be finite dimensional vector spaces with non-degenerate symmetric forms, and assume that they are isometric. Let  $F, F'$  be subspaces, and let  $\sigma : F \rightarrow F'$  be an isometry. Then  $\sigma$  can be extended to an isometry of  $E$  onto  $E'$ .*

*Proof.* Clear.

Let  $E$  be a space with a symmetric form  $g$ , and let  $F$  be a null subspace. Then by Lemma 10.1, we can embed  $F$  in a hyperbolic subspace  $H$  whose dimension is  $2 \dim F$ .

As applications of Theorem 10.2, we get several corollaries.

**Corollary 10.4.** *Let  $E$  be a finite dimensional vector space with a non-degenerate symmetric form. Let  $W$  be a maximal null subspace, and let  $W'$  be some null subspace. Then  $\dim W' \leq \dim W$ , and  $W'$  is contained in some maximal null subspace, whose dimension is the same as  $\dim W$ .*

*Proof.* That  $W'$  is contained in a maximal null subspace follows by Zorn's lemma. Suppose  $\dim W' \geq \dim W$ . We have an isometry of  $W$  onto a subspace of  $W'$  which we can extend to an isometry of  $E$  onto itself. Then  $\sigma^{-1}(W')$  is a null subspace containing  $W$ , hence is equal to  $W$ , whence  $\dim W = \dim W'$ . Our assertions follow by symmetry.

Let  $E$  be a vector space with a non-degenerate symmetric form. Let  $W$  be a null subspace. By Lemma 10.1 we can embed  $W$  in a hyperbolic subspace  $H$  of  $E$  such that  $W$  is the maximal null subspace of  $H$ , and  $H$  is non-degenerate. Any such  $H$  will be called a **hyperbolic enlargement** of  $W$ .

**Corollary 10.5.** *Let  $E$  be a finite dimensional vector space with a non-degenerate symmetric form. Let  $W$  and  $W'$  be maximal null subspaces. Let  $H$ ,  $H'$  be hyperbolic enlargements of  $W$ ,  $W'$  respectively. Then  $H$ ,  $H'$  are isometric and so are  $H^\perp$  and  $H'^\perp$ .*

*Proof.* We have obviously an isometry of  $H$  on  $H'$ , which can be extended to an isometry of  $E$  onto itself. This isometry maps  $H^\perp$  on  $H'^\perp$ , as desired.

**Corollary 10.6.** *Let  $g_1$ ,  $g_2$ ,  $h$  be symmetric forms on finite dimensional vector spaces over the field of  $k$ . If  $g_1 \oplus h$  is isometric to  $g_2 \oplus h$ , and if  $g_1$ ,  $g_2$  are non-degenerate, then  $g_1$  is isometric to  $g_2$ .*

*Proof.* Let  $g_1$  be a form on  $E_1$  and  $g_2$  a form on  $E_2$ . Let  $h$  be a form on  $F$ . Then we have an isometry between  $F \oplus E_1$  and  $F \oplus E_2$ . Extend the identity  $\text{id} : F \rightarrow F$  to an isometry  $\sigma$  of  $F \oplus E_1$  to  $F \oplus E_2$  by Corollary 10.3. Since  $E_1$  and  $E_2$  are the respective orthogonal complements of  $F$  in their two spaces, we must have  $\sigma(E_1) = E_2$ , which proves what we wanted.

If  $g$  is a symmetric form on  $E$ , we shall say that  $g$  is **definite** if  $g(x, x) \neq 0$  for any  $x \in E$ ,  $x \neq 0$  (i.e.  $x^2 \neq 0$  if  $x \neq 0$ ).

**Corollary 10.7.** *Let  $g$  be a symmetric form on  $E$ . Then  $g$  has a decomposition as an orthogonal sum*

$$g = g_0 \oplus g_{\text{hyp}} \oplus g_{\text{def}}$$

where  $g_0$  is a null form,  $g_{\text{hyp}}$  is hyperbolic, and  $g_{\text{def}}$  is definite. The form  $g_{\text{hyp}} \oplus g_{\text{def}}$  is non-degenerate. The forms  $g_0$ ,  $g_{\text{hyp}}$ , and  $g_{\text{def}}$  are uniquely determined up to isometries.

*Proof.* The decomposition  $g = g_0 \oplus g_1$  where  $g_0$  is a null form and  $g_1$  is non-degenerate is unique up to an isometry, since  $g_0$  corresponds to the kernel of  $g$ .

We may therefore assume that  $g$  is non-degenerate. If

$$g = g_h \oplus g_d$$

where  $g_h$  is hyperbolic and  $g_d$  is definite, then  $g_h$  corresponds to the hyperbolic enlargement of a maximal null subspace, and by Corollary 10.5 it follows that  $g_h$  is uniquely determined. Hence  $g_d$  is uniquely determined as the orthogonal complement of  $g_h$ . (By uniquely determined, we mean of course up to an isometry.)

We shall abbreviate  $g_{\text{hyp}}$  by  $g_h$  and  $g_{\text{def}}$  by  $g_d$ .

## §11. THE WITT GROUP

Let  $g, \varphi$  by symmetric forms on finite dimensional vector spaces over  $k$ . We shall say that they are **equivalent** if  $g_d$  is isometric to  $\varphi_d$ . The reader will verify at once that this is an equivalence relation. Furthermore the (orthogonal) sum of two null forms is a null form, and the sum of two hyperbolic forms is hyperbolic. However, the sum of two definite forms need not be definite. We write our equivalence  $g \sim \varphi$ . Equivalence is preserved under orthogonal sums, and hence equivalence classes of symmetric forms constitute a monoid.

**Theorem 11.1.** *The monoid of equivalence classes of symmetric forms (over the field  $k$ ) is a group.*

*Proof.* We have to show that every element has an additive inverse. Let  $g$  be a symmetric form, which we may assume definite. We let  $-g$  be the form such that  $(-g)(x, y) = -g(x, y)$ . We contend that  $g \oplus -g$  is equivalent to 0. Let  $E$  be the space on which  $g$  is defined. Then  $g \oplus -g$  is defined on  $E \oplus E$ . Let  $W$  be the subspace consisting of all pairs  $(x, x)$  with  $x \in E$ . Then  $W$  is a null space for  $g \oplus -g$ . Since  $\dim(E \oplus E) = 2 \dim W$ , it follows that  $W$  is a maximal null space, and that  $g \oplus -g$  is hyperbolic, as was to be shown.

The group of Theorem 11.1 will be called the **Witt group** of  $k$ , and will be denoted by  $WG(k)$ . It is of importance in the study of representations of elements of  $k$  by the quadratic form  $f$  arising from  $g$  [i.e.  $f(x) = g(x, x)$ ], for instance when one wants to classify the definite forms  $f$ .

We shall now define another group, which is of importance in more functorial studies of symmetric forms, for instance in studying the quadratic forms arising from manifolds in topology.

We observe that isometry classes of non-degenerate symmetric forms (over  $k$ ) constitute a monoid  $M(k)$ , the law of composition being the orthogonal sum. Furthermore, the cancellation law holds (Corollary 10.6). We let

$$\text{cl} : M(k) \rightarrow WG(k)$$

be the canonical map of  $M(k)$  into the Grothendieck group of this monoid, which we shall call the **Witt-Grothendieck** group over  $k$ . As we know, the cancellation law implies that  $\text{cl}$  is injective.

If  $g$  is a symmetric non-degenerate form over  $k$ , we define its dimension  $\dim g$  to be the dimension of the space  $E$  on which it is defined. Then it is clear that

$$\dim(g \oplus g') = \dim g + \dim g'.$$

Hence  $\dim$  factors through a homomorphism

$$\dim : WG(k) \rightarrow \mathbf{Z}.$$

This homomorphism splits since we have a non-degenerate symmetric form of dimension 1.

Let  $WG_0(k)$  be the kernel of our homomorphism  $\dim$ . If  $g$  is a symmetric non-degenerate form we can define its determinant  $\det(g)$  to be the determinant of a matrix  $G$  representing  $g$  relative to a basis, modulo squares. This is well defined as an element of  $k^*/k^{*2}$ . We define  $\det$  of the 0-form to be 1. Then  $\det$  is a homomorphism

$$\det : M(k) \rightarrow k^*/k^{*2},$$

and can therefore be factored through a homomorphism, again denoted by  $\det$ , of the Witt-Grothendieck group,  $\det : WG(k) \rightarrow k^*/k^{*2}$ .

Other properties of the Witt-Grothendieck group will be given in the exercises.

## EXERCISES

1. (a) Let  $E$  be a finite dimensional space over the complex numbers, and let

$$h : E \times E \rightarrow \mathbf{C}$$

be a hermitian form. Write

$$h(x, y) = g(x, y) + if(x, y)$$

where  $g, f$  are real valued. Show that  $g, f$  are  $\mathbf{R}$ -bilinear,  $g$  is symmetric,  $f$  is alternating.

- (b) Let  $E$  be finite dimensional over  $\mathbf{C}$ . Let  $g : E \times E \rightarrow \mathbf{C}$  be  $\mathbf{R}$ -bilinear. Assume that for all  $x \in E$ , the map  $y \mapsto g(x, y)$  is  $\mathbf{C}$ -linear, and that the  $\mathbf{R}$ -bilinear form

$$f(x, y) = g(x, y) - g(y, x)$$

is real-valued on  $E \times E$ . Show that there exists a hermitian form  $h$  on  $E$  and a symmetric  $\mathbf{C}$ -bilinear form  $\psi$  on  $E$  such that  $2ig = h + \psi$ . Show that  $h$  and  $\psi$  are uniquely determined.

2. Prove the real case of the unitary spectral theorem: If  $E$  is a non-zero finite dimensional space over  $\mathbf{R}$ , with a positive definite symmetric form, and  $U : E \rightarrow E$  is a unitary linear map, then  $E$  has an orthogonal decomposition into subspaces of dimension 1 or 2, invariant under  $U$ . If  $\dim E = 2$ , then the matrix of  $U$  with respect to any orthonormal basis is of the form

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix},$$

depending on whether  $\det(U) = 1$  or  $-1$ . Thus  $U$  is a rotation, or a rotation followed by a reflection.

3. Let  $E$  be a finite-dimensional, non-zero vector space over the reals, with a positive definite scalar product. Let  $T : E \rightarrow E$  be a unitary automorphism of  $E$ . Show that  $E$  is an orthogonal sum of subspaces

$$E = E_1 \perp \cdots \perp E_m$$

such that each  $E_i$  is  $T$ -invariant, and has dimension 1 or 2. If  $E$  has dimension 2, show that one can find a basis such that the matrix associated with  $T$  with respect to this basis is

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} -\cos \theta & \sin \theta \\ \sin \theta & \cos \theta \end{pmatrix},$$

according as  $\det T = 1$  or  $\det T = -1$ .

4. Let  $E$  be a finite dimensional non-zero vector space over  $\mathbf{C}$ , with a positive definite hermitian product. Let  $A, B : E \rightarrow E$  be a hermitian endomorphism. Assume that  $AB = BA$ . Prove that there exists a basis of  $E$  consisting of common eigenvectors for  $A$  and  $B$ .
5. Let  $E$  be a finite-dimensional space over the complex, with a positive definite hermitian form. Let  $S$  be a set of ( $\mathbf{C}$ -linear) endomorphisms of  $E$  having no invariant subspace except 0 and  $E$ . (This means that if  $F$  is a subspace of  $E$  and  $BF \subset F$  for all  $B \in S$ , then  $F = 0$  or  $F = E$ .) Let  $A$  be a hermitian map of  $E$  into itself such that  $AB = BA$  for all  $B \in S$ . Show that  $A = \lambda I$  for some real number  $\lambda$ . [Hint: Show that there exists exactly one eigenvalue of  $A$ . If there were two eigenvalues, say  $\lambda_1 \neq \lambda_2$ , one could find two polynomials  $f$  and  $g$  with real coefficients such that  $f(A) \neq 0$ ,  $g(A) \neq 0$  but  $f(A)g(A) = 0$ . Let  $F$  be the kernel of  $g(A)$  and get a contradiction.]
6. Let  $E$  be as in Exercise 5. Let  $T$  be a  $\mathbf{C}$ -linear map of  $E$  into itself. Let

$$A = \frac{1}{2}(T + T^*).$$

Show that  $A$  is hermitian. Show that  $T$  can be written in the form  $A + iB$  where  $A, B$  are hermitian, and are uniquely determined.

7. Let  $S$  be a commutative set of  $\mathbf{C}$ -linear endomorphisms of  $E$  having no invariant subspace unequal to 0 or  $E$ . Assume in addition that if  $B \in S$ , then  $B^* \in S$ . Show that each

element of  $S$  is of type  $\alpha I$  for some complex number  $\alpha$ . [Hint: Let  $B_0 \in S$ . Let

$$A = \frac{1}{2}(B_0 + B_0^*).$$

Show that  $A = \lambda I$  for some real  $\lambda$ .]

8. An endomorphism  $B$  of  $E$  is said to be **normal** if  $B$  commutes with  $B^*$ . State and prove a spectral theorem for normal endomorphisms.

### Symmetric endomorphisms

For Exercises 9, 10 and 11 we let  $E$  be a non-zero finite dimensional vector space over  $\mathbf{R}$ , with a symmetric positive definite scalar product  $g$ , which gives rise to a norm  $\| \cdot \|$  on  $E$ .

Let  $A : E \rightarrow E$  be a symmetric endomorphism of  $E$  with respect to  $g$ . Define  $A \geq 0$  to mean  $\langle Ax, x \rangle \geq 0$  for all  $x \in E$ .

9. (a) Show that  $A \geq 0$  if and only if all eigenvalues of  $A$  belonging to non-zero eigenvectors are  $\geq 0$ . Both in the hermitian case and the symmetric case, one says that  $A$  is **semipositive** if  $A \geq 0$ , and **positive definite** if  $\langle Ax, x \rangle > 0$  for all  $x \neq 0$ .  
 (b) Show that an automorphism  $A$  of  $E$  can be written in a unique way as a product  $A = UP$  where  $U$  is real unitary (that is,  $UU^* = I$ ), and  $P$  is symmetric positive definite. For two hermitian or symmetric endomorphisms  $A, B$ , define  $A \geq B$  to mean  $A - B \geq 0$ , and similarly for  $A > B$ . Suppose  $A > 0$ . Show that there are two real numbers  $\alpha > 0$  and  $\beta > 0$  such that  $\alpha I \leq A \leq \beta I$ .  
 10. If  $A$  is an endomorphism of  $E$ , define its norm  $|A|$  to be the greatest lower bound of all numbers  $C$  such that  $|Ax| \leq C|x|$  for all  $x \in E$ .  
 (a) Show that this norm satisfies the triangle inequality.  
 (b) Show that the series

$$\exp(A) = I + A + \frac{A^2}{2!} + \dots$$

converges, and if  $A$  commutes with  $B$ , then  $\exp(A + B) = \exp(A) \exp(B)$ . If  $A$  is sufficiently close to  $I$ , show that the series

$$\log(A) = \frac{(A - I)}{1} - \frac{(A - I)^2}{2} + \dots$$

converges, and if  $A$  commutes with  $B$ , then

$$\log(AB) = \log A + \log B.$$

- (c) Using the spectral theorem, show how to define  $\log P$  for arbitrary positive definite endomorphisms  $P$ .  
 11. Again, let  $E$  be non-zero finite dimensional over  $\mathbf{R}$ , and with a positive definite symmetric form. Let  $A : E \rightarrow E$  be a linear map. Prove:  
 (a) If  $A$  is symmetric (resp. alternating), then  $\exp(A)$  is symmetric positive definite (resp. real unitary).  
 (b) If  $A$  is a linear automorphism of  $E$  sufficiently close to  $I$ , and is symmetric

positive definite (resp. real unitary), then  $\log A$  is symmetric (resp. alternating).

- (c) More generally, if  $A$  is positive definite, then  $\log A$  is symmetric.
12. Let  $R$  be a commutative ring, let  $E, F$  be  $R$ -modules, and let  $f: E \rightarrow F$  be a mapping. Assume that multiplication by 2 in  $F$  is an invertible map. Show that  $f$  is homogeneous quadratic if and only if  $f$  satisfies the **parallelogram law**:

$$f(x + y) + f(x - y) = 2f(x) + 2f(y)$$

for all  $x, y \in E$ .

13. (Tate) Let  $E, F$  be complete normed vector spaces over the real numbers. Let  $f: E \rightarrow F$  be a map having the following property. There exists a number  $C > 0$  such that for all  $x, y \in E$  we have

$$|f(x + y) - f(x) - f(y)| \leq C.$$

Show that there exists a unique additive map  $g: E \rightarrow F$  such that  $|g - f|$  is bounded (i.e.  $|g(x) - f(x)|$  is bounded as a function of  $x$ ). Generalize to the bilinear case. [Hint: Let

$$g(x) = \lim_{n \rightarrow \infty} \frac{f(2^n x)}{2^n}.$$

14. (Tate) Let  $S$  be a set and  $f: S \rightarrow S$  a map of  $S$  into itself. Let  $h: S \rightarrow \mathbf{R}$  be a real valued function. Assume that there exists a real number  $d > 1$  such that  $h \circ f - df$  is bounded. Show that there exists a unique function  $h_f$  such that  $h_f - h$  is bounded, and  $h_f \circ f = dh_f$ . [Hint: Let  $h_f(x) = \lim h(f^n(x))/d^n$ .]
15. Define maps of degree  $> 2$ , from one module into another. [Hint: For degree 3, consider the expression

$$f(x + y + z) - f(x + y) - f(x + z) - f(y + z) + f(x) + f(y) + f(z).$$

Generalize the statement proved for quadratic maps to these higher-degree maps, i.e. the uniqueness of the various multilinear maps entering into their definitions.

## Alternating forms

16. Let  $E$  be a vector space over a field  $k$  and let  $g$  be a bilinear form on  $E$ . Assume that whenever  $x, y \in E$  are such that  $g(x, y) = 0$ , then  $g(y, x) = 0$ . Show that  $g$  is symmetric or alternating.
17. Let  $E$  be a module over  $\mathbf{Z}$ . Assume that  $E$  is free, of dimension  $n \geq 1$ , and let  $f$  be a bilinear alternating form on  $E$ . Show that there exists a basis  $\{e_i\}$  ( $i = 1, \dots, n$ ) and an integer  $r$  such that  $2r \leq n$ ,

$$e_1 \cdot e_2 = a_1, \quad e_3 \cdot e_4 = a_2, \dots, e_{2r-1} \cdot e_{2r} = a_r$$

where  $a_1, \dots, a_r \in \mathbf{Z}$ ,  $a_i \neq 0$ , and  $a_i$  divides  $a_{i+1}$  for  $i = 1, \dots, r-1$  and finally  $e_i \cdot e_j = 0$  for all other pairs of indices  $i \leq j$ . Show that the ideals  $\mathbf{Z}a_i$  are uniquely determined. [Hint: Consider the injective homomorphism  $\varphi_f: E \rightarrow E^\vee$  of  $E$  into the

dual space over  $\mathbf{Z}$ , viewing  $\varphi_f(E)$  as a free submodule of  $E^\vee$ .]. Generalize to principal rings when you know the basis theorem for modules over these rings.

**Remark.** A basis as in Exercise 18 is called a **symplectic basis**. For one use of such a basis, see the theory of theta functions, as in my *Introduction to Algebraic and Abelian Functions* (Second Edition, Springer Verlag), Chapter VI, §3.

18. Let  $E$  be a finite-dimensional vector space over the reals, and let  $\langle \cdot, \cdot \rangle$  be a symmetric positive definite form. Let  $\Omega$  be a non-degenerate alternating form on  $E$ . Show that there exists a direct sum decomposition

$$E = E_1 \oplus E_2$$

having the following property. If  $x, y \in E$  are written

$$x = (x_1, x_2) \quad \text{with} \quad x_1 \in E_1 \quad \text{and} \quad x_2 \in E_2,$$

$$y = (y_1, y_2) \quad \text{with} \quad y_1 \in E_1 \quad \text{and} \quad y_2 \in E_2,$$

then  $\Omega(x, y) = \langle x_1, y_2 \rangle - \langle x_2, y_1 \rangle$ . [Hint: Use Corollary 8.3, show that  $A$  is positive definite, and take its square root to transform the direct sum decomposition obtained in that corollary.]

19. Show that the pfaffian of an alternating  $n \times n$  matrix is 0 when  $n$  is odd.  
 20. Prove all the properties for the pfaffian stated in Artin's *Geometric Algebra* (Interscience, 1957), p. 142.

## The Witt group

21. Show explicitly how  $W(k)$  is a homomorphic image of  $WG(k)$ .  
 22. Show that  $WG(k)$  can be expressed as a homomorphic image of  $\mathbf{Z}[k^*/k^{*2}]$  [Hint: Use the existence of orthogonal bases.]  
 23. Witt's theorem is still true for alternating forms. Prove it or look it up in Artin (ref. in Exercise 20).

## $SL_n(\mathbf{R})$

There is a whole area of linear algebraic groups, giving rise to an extensive algebraic theory as well as the possibility of doing Fourier analysis on such groups. The group  $SL_n(\mathbf{R})$  (or  $SL_n(\mathbf{C})$ ) can serve as a prototype, and a number of basic facts can be easily verified. Some of them are listed below as exercises. Readers wanting to see solutions can look them up in [JoL 01], *Spherical Inversion on  $SL_n(\mathbf{R})$* , Chapter I.

24. **Iwasawa decomposition.** We start with  $GL_n(\mathbf{R})$ . Let:

$$G = GL_n(\mathbf{R});$$

$K$  = subgroup of real unitary  $n \times n$  matrices;

$U$  = group of real unipotent upper triangular matrices, that is having components 1 on the diagonal, arbitrary above the diagonal, and 0 below the diagonal;

$A$  = group of diagonal matrices with positive diagonal components.

Prove that the product map  $U \times A \times K \rightarrow UAK \subset G$  is actually a bijection. This amounts to Gram–Schmidt orthogonalization. Prove the similar statement in the complex case, that is, for  $G(\mathbb{C}) = GL_n(\mathbb{C})$ ,  $K(\mathbb{C})$  = complex unitary group,  $U(\mathbb{C})$  = complex unipotent upper triangular group, and  $A$  the same group of positive diagonal matrices as in the real case.

25. Let now  $G = SL_n(\mathbb{R})$ , and let  $K, A$  be the corresponding subgroups having determinant 1. Show that the product  $U \times A \times K \rightarrow UAK$  again gives a bijection with  $G$ .
26. Let  $\mathfrak{a}$  be the  $\mathbb{R}$ -vector space of real diagonal matrices with trace 0. Let  $\mathfrak{a}^\vee$  be the dual space. Let  $\alpha_i$  ( $i = 1, \dots, n-1$ ) be the functional defined on an element  $H = \text{diag}(h_1, \dots, h_n)$  by  $\alpha_i(H) = h_i - h_{i+1}$ . (a) Show that  $\{\alpha_1, \dots, \alpha_{n-1}\}$  is a basis of  $\mathfrak{a}^\vee$  over  $\mathbb{R}$ . (b) Let  $H_{i,i+1}$  be the diagonal matrix with  $h_i = 1$ ,  $h_{i+1} = -1$ , and  $h_j = 0$  for  $j \neq i, i+1$ . Show that  $\{H_{1,2}, \dots, H_{n-1,n}\}$  is a basis of  $\mathfrak{a}$ . (c) Abbreviate  $H_{i,i+1} = H_i$  ( $i = 1, \dots, n-1$ ). Let  $\alpha'_i \in \mathfrak{a}^\vee$  be the functional such that  $\alpha'_i(H_j) = \delta_{ij}$  ( $= 1$  if  $i = j$  and 0 otherwise). Thus  $\{\alpha'_1, \dots, \alpha'_{n-1}\}$  is the dual basis of  $\{H_1, \dots, H_{n-1}\}$ . Show that

$$\alpha'_i(H) = h_1 + \dots + h_i.$$

27. **The trace form.** Let  $\text{Mat}_n(\mathbb{R})$  be the vector space of real  $n \times n$  matrices. Define the **twisted trace form** on this space by

$$B_t(X, Y) = \text{tr}(X^t Y) = \langle X, Y \rangle_t.$$

As usual, ' $Y$ ' is the transpose of a matrix  $Y$ . Show that  $B_t$  is a symmetric positive definite bilinear form on  $\text{Mat}_n(\mathbb{R})$ . What is the analogous positive definite hermitian form on  $\text{Mat}_n(\mathbb{C})$ ?

28. **Positivity.** On  $\mathfrak{a}$  (real diagonal matrices with trace 0) the form of Exercise 27 can be defined by  $\text{tr}(XY)$ , since elements  $X, Y \in \mathfrak{a}$  are symmetric. Let  $\mathcal{A} = \{\alpha_1, \dots, \alpha_{n-1}\}$  denote the basis of Exercise 26. Define an element  $H \in \mathfrak{a}$  to be **semipositive** (written  $H \geqq 0$ ) if  $\alpha_i(H) \geqq 0$  for all  $i = 1, \dots, n-1$ . For each  $\alpha \in \mathfrak{a}^\vee$ , let  $H_\alpha \in \mathfrak{a}$  represent  $\alpha$  with respect to  $B_t$ , that is  $\langle H_\alpha, H \rangle = \alpha(H)$  for all  $H \in \mathfrak{a}$ . Show that  $H \geqq 0$  if and only if

$$H = \sum_{i=1}^{n-1} s_i H_{\alpha'_i} \quad \text{with } s_i \geqq 0.$$

Similarly, define  $H$  to be **positive** and formulate the similar condition with  $s_i > 0$ .

29. Show that the elements  $n\alpha'_i$  ( $i = 1, \dots, n-1$ ) can be expressed as linear combinations of  $\alpha_1, \dots, \alpha_{n-1}$  with positive coefficients in  $\mathbb{Z}$ .
30. Let  $W$  be the group of permutations of the diagonal elements in the vector space  $\mathfrak{a}$  of diagonal matrices. Show that  $\mathfrak{a}_{\geqq 0}$  is a fundamental domain for the action of  $W$  on  $\mathfrak{a}$  (i.e., given  $H \in \mathfrak{a}$ , there exists a unique  $H^+ \geqq 0$  such that  $H^+ = wH$  for some  $w \in W$ ).

---

# CHAPTER XVI

---

## The Tensor Product

Having considered bilinear maps, we now come to multilinear maps and basic theorems concerning their structure. There is a universal module representing multilinear maps, called the tensor product. We derive its basic properties, and postpone to Chapter XIX the special case of alternating products. The tensor product derives its name from the use made in differential geometry, when this product is applied to the tangent space or cotangent space of a manifold. The tensor product can be viewed also as providing a mechanism for “extending the base”; that is, passing from a module over a ring to a module over some algebra over the ring. This “extension” can also involve reduction modulo an ideal, because what matters is that we are given a ring homomorphism  $f: A \rightarrow B$ , and we pass from modules over  $A$  to modules over  $B$ . The homomorphism  $f$  can be of both types, an inclusion or a canonical map with  $B = A/J$  for some ideal  $J$ , or a composition of the two.

I have tried to provide the basic material which is immediately used in a variety of applications to many fields (topology, algebra, differential geometry, algebraic geometry, etc.).

---

### §1. TENSOR PRODUCT

Let  $R$  be a commutative ring. If  $E_1, \dots, E_n, F$  are modules, we denote by

$$L^n(E_1, \dots, E_n; F)$$

the module of  $n$ -multilinear maps

$$f: E_1 \times \dots \times E_n \rightarrow F.$$

We recall that a multilinear map is a map which is linear (i.e.,  $R$ -linear) in each variable. We use the words *linear* and *homomorphism* interchangeably. *Unless otherwise specified, modules, homomorphisms, linear, multilinear refer to the ring  $R$ .*

One may view the multilinear maps of a fixed set of modules  $E_1, \dots, E_n$  as the objects of a category. Indeed, if

$$f : E_1 \times \dots \times E_n \rightarrow F \quad \text{and} \quad g : E_1 \times \dots \times E_n \rightarrow G$$

are multilinear, we define a morphism  $f \rightarrow g$  to be a homomorphism  $h : F \rightarrow G$  which makes the following diagram commutative:

$$\begin{array}{ccc} & & F \\ & \nearrow f & \downarrow h \\ E_1 \times \dots \times E_n & & \searrow g \\ & & G \end{array}$$

A universal object in this category is called a **tensor product** of  $E_1, \dots, E_n$  (over  $R$ ).

We shall now prove that a tensor product exists, and in fact construct one in a natural way. By abstract nonsense, we know of course that a tensor product is uniquely determined, up to a unique isomorphism.

Let  $M$  be the free module generated by the set of all  $n$ -tuples  $(x_1, \dots, x_n)$ ,  $(x_i \in E_i)$ , i.e. generated by the set  $E_1 \times \dots \times E_n$ . Let  $N$  be the submodule generated by all the elements of the following type:

$$\begin{aligned} (x_1, \dots, x_i + x'_i, \dots, x_n) - (x_1, \dots, x_i, \dots, x_n) - (x_1, \dots, x'_i, \dots, x_n) \\ (x_1, \dots, ax_i, \dots, x_n) - a(x_1, \dots, x_n) \end{aligned}$$

for all  $x_i \in E_i$ ,  $x'_i \in E_i$ ,  $a \in R$ . We have the canonical injection

$$E_1 \times \dots \times E_n \rightarrow M$$

of our set into the free module generated by it. We compose this map with the canonical map  $M \rightarrow M/N$  on the factor module, to get a map

$$\varphi : E_1 \times \dots \times E_n \rightarrow M/N.$$

We contend that  $\varphi$  is multilinear and is a tensor product.

It is obvious that  $\varphi$  is multilinear—our definition was adjusted to this purpose. Let

$$f : E_1 \times \dots \times E_n \rightarrow G$$

be a multilinear map. By the definition of free module generated by

$$E_1 \times \dots \times E_n$$

we have an induced linear map  $M \rightarrow G$  which makes the following diagram commutative:

$$\begin{array}{ccc} & & M \\ & \swarrow & \downarrow \\ E_1 \times \cdots \times E_n & \xrightarrow{f} & G \end{array}$$

Since  $f$  is multilinear, the induced map  $M \rightarrow G$  takes on the value 0 on  $N$ . Hence by the universal property of factor modules, it can be factored through  $M/N$ , and we have a homomorphism  $f_*: M/N \rightarrow G$  which makes the following diagram commutative:

$$\begin{array}{ccc} & & M/N \\ & \swarrow \varphi & \downarrow f_* \\ E_1 \times \cdots \times E_n & \xrightarrow{f} & G \end{array}$$

Since the image of  $\varphi$  generates  $M/N$ , it follows that the induced map  $f_*$  is uniquely determined. This proves what we wanted.

The module  $M/N$  will be denoted by

$$E_1 \otimes \cdots \otimes E_n \quad \text{or also} \quad \bigotimes_{i=1}^n E_i.$$

We have constructed a specific tensor product in the isomorphism class of tensor products, and we shall call it **the tensor product of  $E_1, \dots, E_n$** . If  $x_i \in E_i$ , we write

$$\varphi(x_1, \dots, x_n) = x_1 \otimes \cdots \otimes x_n = x_1 \otimes_R \cdots \otimes_R x_n.$$

We have for all  $i$ ,

$$x_1 \otimes \cdots \otimes ax_i \otimes \cdots \otimes x_n = a(x_1 \otimes \cdots \otimes x_n),$$

$$\begin{aligned} x_1 \otimes \cdots \otimes (x_i + x'_i) \otimes \cdots \otimes x_n \\ = (x_1 \otimes \cdots \otimes x_n) + (x_1 \otimes \cdots \otimes x'_i \otimes \cdots \otimes x_n) \end{aligned}$$

for  $x_i, x'_i \in E_i$  and  $a \in R$ .

If we have two factors, say  $E \otimes F$ , then every element of  $E \otimes F$  can be written as a sum of terms  $x \otimes y$  with  $x \in E$  and  $y \in F$ , because such terms generate  $E \otimes F$  over  $R$ , and  $a(x \otimes y) = ax \otimes y$  for  $a \in R$ .

**Remark.** If an element of the tensor product is 0, then that element can already be expressed in terms of a finite number of the relations defining the tensor product. Thus if  $E$  is a direct limit of submodules  $E_i$  then

$$\varprojlim F \otimes E_i = F \otimes \varprojlim E_i = F \otimes E.$$

In particular, every module is a direct limit of finitely generated submodules, and one uses frequently the technique of testing whether an element of  $F \otimes E$  is 0 by testing whether the image of this element in  $F \otimes E_i$  is 0 when  $E_i$  ranges over the finitely generated submodules of  $E$ .

**Warning.** The tensor product can involve a great deal of collapsing between the modules. For instance, take the tensor product over  $\mathbf{Z}$  of  $\mathbf{Z}/m\mathbf{Z}$  and  $\mathbf{Z}/n\mathbf{Z}$  where  $m, n$  are integers  $> 1$  and are relatively prime. Then the tensor product

$$\mathbf{Z}/n\mathbf{Z} \otimes \mathbf{Z}/m\mathbf{Z} = 0.$$

Indeed, we have  $n(x \otimes y) = (nx) \otimes y = 0$  and  $m(x \otimes y) = x \otimes my = 0$ . Hence  $x \otimes y = 0$  for all  $x \in \mathbf{Z}/n\mathbf{Z}$  and  $y \in \mathbf{Z}/m\mathbf{Z}$ . Elements of type  $x \otimes y$  generate the tensor product, which is therefore 0. We shall see later conditions under which there is no collapsing.

In many subsequent results, we shall assert the existence of certain linear maps from a tensor product. This existence is proved by using the universal mapping property of bilinear maps factoring through the tensor product. The uniqueness follows by prescribing the value of the linear maps on elements of type  $x \otimes y$  (say for two factors) since such elements generate the tensor product.

We shall prove the associativity of the tensor product.

**Proposition 1.1.** *Let  $E_1, E_2, E_3$  be modules. Then there exists a unique isomorphism*

$$(E_1 \otimes E_2) \otimes E_3 \rightarrow E_1 \otimes (E_2 \otimes E_3)$$

*such that*

$$(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$$

*for  $x \in E_1, y \in E_2$  and  $z \in E_3$ .*

*Proof.* Since elements of type  $(x \otimes y) \otimes z$  generate the tensor product, the uniqueness of the desired linear map is obvious. To prove its existence, let  $x \in E_1$ . The map

$$\lambda_x : E_2 \times E_3 \rightarrow (E_1 \otimes E_2) \otimes E_3$$

such that  $\lambda_x(y, z) = (x \otimes y) \otimes z$  is clearly bilinear, and hence factors through a linear map of the tensor product

$$\bar{\lambda}_x: E_2 \otimes E_3 \rightarrow (E_1 \otimes E_2) \otimes E_3.$$

The map

$$E_1 \times (E_2 \otimes E_3) \rightarrow (E_1 \otimes E_2) \otimes E_3$$

such that

$$(x, \alpha) \mapsto \bar{\lambda}_x(\alpha)$$

for  $x \in E_1$  and  $\alpha \in E_2 \otimes E_3$  is then obviously bilinear, and factors through a linear map

$$E_1 \otimes (E_2 \otimes E_3) \rightarrow (E_1 \otimes E_2) \otimes E_3,$$

which has the desired property (clear from its construction).

**Proposition 1.2.** *Let  $E, F$  be modules. Then there is a unique isomorphism*

$$E \otimes F \rightarrow F \otimes E$$

such that  $x \otimes y \mapsto y \otimes x$  for  $x \in E$  and  $y \in F$ .

*Proof.* The map  $E \times F \rightarrow F \otimes E$  such that  $(x, y) \mapsto y \otimes x$  is bilinear, and factors through the tensor product  $E \otimes F$ , sending  $x \otimes y$  on  $y \otimes x$ . Since this last map has an inverse (by symmetry) we obtain the desired isomorphism.

The tensor product has various functorial properties. First, suppose that

$$f_i: E'_i \rightarrow E_i \quad (i = 1, \dots, n)$$

is a collection of linear maps. We get an induced map on the product,

$$\prod f_i: \prod E'_i \rightarrow \prod E_i.$$

If we compose  $\prod f_i$  with the canonical map into the tensor product, then we get an induced linear map which we may denote by  $T(f_1, \dots, f_n)$  which makes the following diagram commutative:

$$\begin{array}{ccc} E'_1 \times \cdots \times E'_n & \xrightarrow{\quad} & E'_1 \otimes \cdots \otimes E'_n \\ \Pi f_i \downarrow & & \downarrow T(f_1, \dots, f_n) \\ E_1 \times \cdots \times E_n & \xrightarrow{\quad} & E_1 \otimes \cdots \otimes E_n \end{array}$$

It is immediately verified that  $T$  is functorial, namely that if we have a composite of linear maps  $f_i \circ g_i$  ( $i = 1, \dots, n$ ) then

$$T(f_1 \circ g_1, \dots, f_n \circ g_n) = T(f_1, \dots, f_n) \circ T(g_1, \dots, g_n)$$

and

$$T(\text{id}, \dots, \text{id}) = \text{id}.$$

We observe that  $T(f_1, \dots, f_n)$  is the unique linear map whose effect on an element  $x'_1 \otimes \dots \otimes x'_n$  of  $E'_1 \otimes \dots \otimes E'_n$  is

$$x'_1 \otimes \dots \otimes x'_n \mapsto f_1(x'_1) \otimes \dots \otimes f_n(x'_n).$$

We may view  $T$  as a map

$$\prod_{i=1}^n L(E'_i, E_i) \rightarrow L\left(\bigotimes_{i=1}^n E'_i, \bigotimes_{i=1}^n E_i\right),$$

and the reader will have no difficulty in verifying that this map is multilinear. We shall write out what this means explicitly for two factors, so that our map can be written

$$(f, g) \mapsto T(f, g).$$

Given homomorphisms  $f : F' \rightarrow F$  and  $g_1, g_2 : E' \rightarrow E$ , then

$$T(f, g_1 + g_2) = T(f, g_1) + T(f, g_2),$$

$$T(f, ag_1) = aT(f, g_1).$$

In particular, select a fixed module  $F$ , and consider the functor  $\tau = \tau_F$  (from modules to modules) such that

$$\tau(E) = F \otimes E.$$

Then  $\tau$  gives rise to a linear map

$$\tau : L(E', E) \rightarrow L(\tau(E'), \tau(E))$$

for each pair of modules  $E', E$ , by the formula

$$\tau(f) = T(\text{id}, f).$$

**Remark.** By abuse of notation, it is sometimes convenient to write

$$f_1 \otimes \dots \otimes f_n \quad \text{instead of} \quad T(f_1, \dots, f_n).$$

This should not be confused with the tensor product of elements taken in the tensor product of the modules

$$L(E'_1, E_1) \otimes \cdots \otimes L(E'_n, E_n).$$

The context will always make our meaning clear.

## §2. BASIC PROPERTIES

The most basic relation relating linear maps, bilinear maps, and the tensor product is the following: For three modules  $E, F, G$ ,

$$L(E, L(F, G)) \approx L^2(E, F; G) \approx L(E \otimes F, G).$$

The isomorphisms involved are described in a natural way.

(i)  $L^2(E, F; G) \rightarrow L(E, L(F, G))$ .

If  $f: E \times F \rightarrow G$  is bilinear, and  $x \in E$ , then the map

$$f_x: F \rightarrow G$$

such that  $f_x(y) = f(x, y)$  is linear. Furthermore, the map  $x \mapsto f_x$  is linear, and is associated with  $f$  to get (i).

(ii)  $L(E, L(F, G)) \rightarrow L^2(E, F; G)$ .

Let  $\varphi \in L(E, L(F, G))$ . We let  $f_\varphi: E \times F \rightarrow G$  be the bilinear map such that

$$f_\varphi(x, y) = \varphi(x)(y).$$

Then  $\varphi \mapsto f_\varphi$  defines (ii).

It is clear that the homomorphisms of (i) and (ii) are inverse to each other and therefore give isomorphisms of the first two objects in the enclosed box.

(iii)  $L^2(E, F; G) \rightarrow L(E \otimes F, G)$ .

This is the map  $f \mapsto f_*$  which associates to each bilinear map  $f$  the induced linear map on the tensor product. The association  $f \mapsto f_*$  is injective (because  $f_*$  is uniquely determined by  $f$ ), and it is surjective, because any linear map of the tensor product composed with the canonical map  $E \times F \rightarrow E \otimes F$  gives rise to a bilinear map on  $E \times F$ .

**Proposition 2.1.** *Let  $E = \bigoplus_{i=1}^n E_i$  be a direct sum. Then we have an isomorphism*

$$F \otimes E \leftrightarrow \bigoplus_{i=1}^n (F \otimes E_i).$$

*Proof.* The isomorphism is given by abstract nonsense. We keep  $F$  fixed, and consider the functor  $\tau : X \mapsto F \otimes X$ . As we saw above,  $\tau$  is linear. We have projections  $\pi_i : E \rightarrow E$  of  $E$  on  $E_i$ . Then

$$\pi_i \circ \pi_i = \pi_i, \quad \pi_i \circ \pi_j = 0 \quad \text{if } i \neq j,$$

$$\sum_{i=1}^n \pi_i = \text{id}.$$

We apply the functor  $\tau$ , and see that  $\tau(\pi_i)$  satisfies the same relations, hence gives a direct sum decomposition of  $\tau(E) = F \otimes E$ . Note that  $\tau(\pi_i) = \text{id} \otimes \pi_i$ .

**Corollary 2.2.** *Let  $I$  be an indexing set, and  $E = \bigoplus_{i \in I} E_i$ . Then we have an isomorphism*

$$\left( \bigoplus_{i \in I} E_i \right) \otimes F \approx \bigoplus_{i \in I} (E_i \otimes F).$$

*Proof.* Let  $S$  be a finite subset of  $I$ . We have a sequence of maps

$$\left( \bigoplus_{i \in S} E_i \right) \times F \rightarrow \bigoplus_{i \in S} (E_i \otimes F) \rightarrow \bigoplus_{i \in I} (E_i \otimes F)$$

the first of which is bilinear, and the second is linear, induced by the inclusion of  $S$  in  $I$ . The first is the obvious map. If  $S \subset S'$ , then a trivial commutative diagram shows that the restriction of the map

$$\left( \bigoplus_{i \in S'} E_i \right) \times F \rightarrow \bigoplus_{i \in I} (E_i \otimes F)$$

induces our preceding map on the sum for  $i \in S$ . But we have an *injection*

$$\left( \bigoplus_{i \in S} E_i \right) \times F \rightarrow \left( \bigoplus_{i \in S'} E_i \right) \times F.$$

Hence by compatibility, we can define a bilinear map

$$\left( \bigoplus_{i \in I} E_i \right) \times F \rightarrow \bigoplus_{i \in I} (E_i \otimes F),$$

and consequently a linear map

$$\left( \bigoplus_{i \in I} E_i \right) \otimes F \rightarrow \bigoplus_{i \in I} (E_i \otimes F).$$

In a similar way, one defines a map in the opposite direction, and it is clear that these maps are inverse to each other, hence give an isomorphism.

Suppose now that  $E$  is free, of dimension 1 over  $R$ . Let  $\{v\}$  be a basis, and consider  $F \otimes E$ . Every element of  $F \otimes E$  can be written as a sum of terms  $y \otimes av$  with  $y \in F$  and  $a \in R$ . However,  $y \otimes av = ay \otimes v$ . In a sum of such terms, we can then use linearity on the left,

$$\sum_{i=1}^n (y_i \otimes v) = \left( \sum_{i=1}^n y_i \right) \otimes v, \quad y_i \in F.$$

Hence every element is in fact of type  $y \otimes v$  with some  $y \in F$ .

We have a bilinear map

$$F \times E \rightarrow F$$

such that  $(y, av) \mapsto ay$ , inducing a linear map

$$F \otimes E \mapsto F.$$

We also have a linear map  $F \rightarrow F \otimes E$  given by  $y \mapsto y \otimes v$ . It is clear that these maps are inverse to each other, and hence that we have an isomorphism

$$F \otimes E \approx F.$$

Thus every element of  $F \otimes E$  can be written *uniquely* in the form  $y \otimes v$ ,  $y \in F$ .

**Proposition 2.3.** *Let  $E$  be free over  $R$ , with basis  $\{v_i\}_{i \in I}$ . Then every element of  $F \otimes E$  has a unique expression of the form*

$$\sum_{i \in I} y_i \otimes v_i, \quad y_i \in F$$

*with almost all  $y_i = 0$ .*

*Proof.* This follows at once from the discussion of the 1-dimensional case, and the corollary of Proposition 2.1.

**Corollary 2.4.** *Let  $E, F$  be free over  $R$ , with bases  $\{v_i\}_{i \in I}$  and  $\{w_j\}_{j \in J}$  respectively. Then  $E \otimes F$  is free, with basis  $\{v_i \otimes w_j\}$ . We have*

$$\dim(E \otimes F) = (\dim E)(\dim F).$$

*Proof.* Immediate from the proposition.

We see that when  $E$  is free over  $R$ , then there is no collapsing in the tensor product. Every element of  $F \otimes E$  can be viewed as a “formal” linear combination of elements in a basis of  $E$  with coefficients in  $F$ .

In particular, we see that  $R \otimes E$  (or  $E \otimes R$ ) is isomorphic to  $E$ , under the correspondence  $x \mapsto x \otimes 1$ .

**Proposition 2.5.** *Let  $E, F$  be free of finite dimension over  $R$ . Then we have an isomorphism*

$$\text{End}_R(E) \otimes \text{End}_R(F) \rightarrow \text{End}_R(E \otimes F)$$

which is the unique linear map such that

$$f \otimes g \mapsto T(f, g)$$

for  $f \in \text{End}_R(E)$  and  $g \in \text{End}_R(F)$ .

[We note that the tensor product on the left is here taken in the tensor product of the two modules  $\text{End}_R(E)$  and  $\text{End}_R(F)$ .]

*Proof.* Let  $\{v_i\}$  be a basis of  $E$  and let  $\{w_j\}$  be a basis of  $F$ . Then  $\{v_i \otimes w_j\}$  is a basis of  $E \otimes F$ . For each pair of indices  $(i', j')$  there exists a unique endomorphism  $f = f_{i, i'}$  of  $E$  and  $g = g_{j, j'}$  of  $F$  such that

$$\begin{aligned} f(v_i) &= v_{i'} \quad \text{and} \quad f(v_v) = 0 \quad \text{if } v \neq i \\ g(w_j) &= w_{j'} \quad \text{and} \quad g(w_\mu) = 0 \quad \text{if } \mu \neq j. \end{aligned}$$

Furthermore, the families  $\{f_{i, i'}\}$  and  $\{g_{j, j'}\}$  are bases of  $\text{End}_R(E)$  and  $\text{End}_R(F)$  respectively. Then

$$T(f, g)(v_v \otimes w_\mu) = \begin{cases} v_{i'} \otimes w_{j'} & \text{if } (v, \mu) = (i, j) \\ 0 & \text{if } (v, \mu) \neq (i, j). \end{cases}$$

Thus the family  $\{T(f_{i, i'}, g_{j, j'})\}$  is a basis of  $\text{End}_R(E \otimes F)$ . Since the family  $\{f_{i, i'} \otimes g_{j, j'}\}$  is a basis of  $\text{End}_R(E) \otimes \text{End}_R(F)$ , the assertion of our proposition is now clear.

In Proposition 2.5, we see that the ambiguity of the tensor sign in  $f \otimes g$  is in fact unambiguous in the important special case of free, finite dimensional modules. We shall see later an important application of Proposition 2.5 when we discuss the tensor algebra of a module.

**Proposition 2.6.** *Let*

$$0 \rightarrow E' \xrightarrow{\varphi} E \xrightarrow{\psi} E'' \rightarrow 0$$

be an exact sequence, and  $F$  any module. Then the sequence

$$F \otimes E' \rightarrow F \otimes E \rightarrow F \otimes E'' \rightarrow 0$$

is exact.

*Proof.* Given  $x'' \in E''$  and  $y \in F$ , there exists  $x \in E$  such that  $x'' = \psi(x)$ , and hence  $y \otimes x''$  is the image of  $y \otimes x$  under the linear map

$$F \otimes E \rightarrow F \otimes E''.$$

Since elements of type  $y \otimes x''$  generate  $F \otimes E''$ , we conclude that the preceding linear map is surjective. One also verifies trivially that the image of

$$F \otimes E' \rightarrow F \otimes E$$

is contained in the kernel of

$$F \otimes E \rightarrow F \otimes E''.$$

Conversely, let  $I$  be the image of  $F \otimes E' \rightarrow F \otimes E$ , and let

$$f : (F \otimes E)/I \rightarrow F \otimes E''$$

be the canonical map. We shall define a linear map

$$g : F \otimes E'' \rightarrow (F \otimes E)/I$$

such that  $g \circ f = \text{id}$ . This obviously will imply that  $f$  is injective, and hence will prove the desired converse.

Let  $y \in F$  and  $x'' \in E''$ . Let  $x \in E$  be such that  $\psi(x) = x''$ . We define a map  $F \times E'' \rightarrow (F \otimes E)/I$  by letting

$$(y, x'') \mapsto y \otimes x \pmod{I},$$

and contend that this map is well defined, i.e. independent of the choice of  $x$  such that  $\psi(x) = x''$ . If  $\psi(x_1) = \psi(x_2) = x''$ , then  $\psi(x_1 - x_2) = 0$ , and by hypothesis,  $x_1 - x_2 = \varphi(x')$  for some  $x' \in E'$ . Then

$$y \otimes x_1 - y \otimes x_2 = y \otimes (x_1 - x_2) = y \otimes \varphi(x').$$

This shows that  $y \otimes x_1 \equiv y \otimes x_2 \pmod{I}$ , and proves that our map is well defined. It is obviously bilinear, and hence factors through a linear map  $g$ , on the tensor product. It is clear that the restriction of  $g \circ f$  on elements of type  $y \otimes x$  is the identity. Since these elements generate  $F \otimes E$ , we conclude that  $f$  is injective, as was to be shown.

*It is not always true that the sequence*

$$0 \rightarrow F \otimes E' \rightarrow F \otimes E \rightarrow F \otimes E'' \rightarrow 0$$

*is exact.* It is exact if the first sequence in Proposition 2.6 splits, i.e. if  $E$  is essentially the direct sum of  $E'$  and  $E''$ . This is a trivial consequence of Proposition 2.1, and the reader should carry out the details to get accustomed to the formalism of the tensor product.

**Proposition 2.7.** *Let  $\mathfrak{a}$  be an ideal of  $R$ . Let  $E$  be a module. Then the map  $(R/\mathfrak{a}) \times E \rightarrow E/\mathfrak{a}E$  induced by*

$$(a, x) \mapsto ax \pmod{\mathfrak{a}E}, \quad a \in R, x \in E$$

*is bilinear and induces an isomorphism*

$$(R/\mathfrak{a}) \otimes E \xrightarrow{\cong} E/\mathfrak{a}E.$$

*Proof.* Our map  $(a, x) \mapsto ax \pmod{\mathfrak{a}E}$  clearly induces a bilinear map of  $R/\mathfrak{a} \times E$  onto  $E/\mathfrak{a}E$ , and hence a linear map of  $R/\mathfrak{a} \otimes E$  onto  $E/\mathfrak{a}E$ . We can construct an inverse, for we have a well-defined linear map

$$E \rightarrow R/\mathfrak{a} \otimes E$$

such that  $x \mapsto \bar{1} \otimes x$  (where  $\bar{1}$  is the residue class of 1 in  $R/\mathfrak{a}$ ). It is clear that  $\mathfrak{a}E$  is contained in the kernel of this last linear map, and thus that we obtain a homomorphism

$$E/\mathfrak{a}E \rightarrow R/\mathfrak{a} \otimes E,$$

which is immediately verified to be inverse to the homomorphism described in the statement of the proposition.

The association  $E \mapsto E/\mathfrak{a}E \approx R/\mathfrak{a} \otimes E$  is often called a **reduction map**. In §4, we shall interpret this reduction map as an extension of the base.

### §3. FLAT MODULES

The question under which conditions the left-hand arrow in Proposition 2.6 is an injection gives rise to the theory of those modules for which it is, and we follow Serre in calling them flat. Thus formally, the following conditions are equivalent, and define a **flat** module  $F$ , which should be called **tensor exact**.

**F 1.** For every exact sequence

$$E' \rightarrow E \rightarrow E''$$

the sequence

$$F \otimes E' \rightarrow F \otimes E \rightarrow F \otimes E''$$

is exact.

**F 2.** For every short exact sequence

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

the sequence

$$0 \rightarrow F \otimes E' \rightarrow F \otimes E \rightarrow F \otimes E'' \rightarrow 0$$

is exact.

**F 3.** For every injection  $0 \rightarrow E' \rightarrow E$  the sequence

$$0 \rightarrow F \otimes E' \rightarrow F \otimes E$$

is exact.

It is immediate that **F 1** implies **F 2** implies **F 3**. Finally, we see that **F 3** implies **F 1** by writing down the kernel and image of the map  $E' \rightarrow E$  and applying **F 3**. We leave the details to the reader.

The following proposition gives tests for flatness, and also examples.

**Proposition 3.1.**

- (i) *The ground ring is flat as module over itself.*
- (ii) *Let  $F = \bigoplus F_i$  be a direct sum. Then  $F$  is flat if and only if each  $F_i$  is flat.*
- (iii) *A projective module is flat.*

The properties expressed in this proposition are basically categorical, cf. the comments on abstract nonsense at the end of the section. In another vein, we have the following tests having to do with localization.

**Proposition 3.2.**

- (i) *Let  $S$  be a multiplicative subset of  $R$ . Then  $S^{-1}R$  is flat over  $R$ .*
- (ii) *A module  $M$  is flat over  $R$  if and only if the localization  $M_{\mathfrak{p}}$  is flat over  $R_{\mathfrak{p}}$  for each prime ideal  $\mathfrak{p}$  of  $R$ .*
- (iii) *Let  $R$  be a principal ring. A module  $F$  is flat if and only if  $F$  is torsion free.*

The proofs are simple, and will be left to the reader. More difficult tests for flatness will be proved below, however.

**Examples of non-flatness.** If  $R$  is an entire ring, and a module  $M$  over  $R$  has torsion, then  $M$  is not flat. (Prove this, which is immediate.)

There is another type of example which illustrates another bad phenomenon. Let  $R$  be some ring in a finite extension  $K$  of  $\mathbf{Q}$ , and such that  $R$  is a finite module over  $\mathbf{Z}$  but not integrally closed. Let  $R'$  be its integral closure. Let  $\mathfrak{p}$  be a maximal ideal of  $R$  and suppose that  $\mathfrak{p}R'$  is contained in two distinct maximal ideals  $\mathfrak{P}_1$  and  $\mathfrak{P}_2$ . Then it can be shown that  $R'$  is not flat over  $R$ , otherwise  $R'$  would be free over the local ring  $R_{\mathfrak{p}}$ , and the rank would have to be 1, thus precluding the possibility of the two primes  $\mathfrak{P}_1$  and  $\mathfrak{P}_2$ . It is good practice for the reader actually to construct a numerical example of this situation. The same type of example can be constructed with a ring  $R = k[x, y]$ , where  $k$  is an algebraically closed field, even of characteristic 0, and  $x, y$  are related by an irreducible polynomial equation  $f(x, y) = 0$  over  $k$ . We take  $R$  not integrally closed, such that its integral closure exhibits the same splitting of a prime  $\mathfrak{p}$  of  $R$  into two primes. In each one of these similar cases, one says that there is a singularity at  $\mathfrak{p}$ .

As a third example, let  $R$  be the power series ring in more than one variable over a field  $k$ . Let  $\mathfrak{m}$  be the maximal ideal. Then  $\mathfrak{m}$  is not flat, because otherwise, by Theorem 3.8 below,  $\mathfrak{m}$  would be free, and if  $R = k[[x_1, \dots, x_n]]$ , then  $x_1, \dots, x_n$  would be a basis for  $\mathfrak{m}$  over  $R$ , which is obviously not the case, since  $x_1, x_2$  are linearly dependent over  $R$  when  $n \geq 2$ . The same argument, of course, applies to any local ring  $R$  such that  $\mathfrak{m}/\mathfrak{m}^2$  has dimension  $\geq 2$  over  $R/\mathfrak{m}$ .

Next we come to further criteria when a module is flat. For the proofs, we shall snake it all over the place. Cf. the remark at the end of the section.

**Lemma 3.3.** *Let  $F$  be flat, and suppose that*

$$0 \rightarrow N \rightarrow M \rightarrow F \rightarrow 0$$

*is an exact sequence. Then for any  $E$ , we have an exact sequence*

$$0 \rightarrow N \otimes E \rightarrow M \otimes E \rightarrow F \otimes E \rightarrow 0.$$

*Proof.* Represent  $E$  as a quotient of a flat  $L$  by an exact sequence

$$0 \rightarrow K \rightarrow L \rightarrow E \rightarrow 0.$$

Then we have the following exact and commutative diagram:

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \downarrow & & \\
 & & N \otimes K & \longrightarrow & M \otimes K & \longrightarrow & F \otimes K \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & N \otimes L & \longrightarrow & M \otimes L & \longrightarrow & F \otimes L \\
 & & \downarrow & & \downarrow & & \\
 & & N \otimes E & \longrightarrow & M \otimes E & & \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 
 \end{array}$$

The top right 0 comes by hypothesis that  $F$  is flat. The 0 on the left comes from the fact that  $L$  is flat. The snake lemma yields the exact sequence

$$0 \rightarrow N \otimes E \rightarrow M \otimes E$$

which proves the lemma.

**Proposition 3.4.** *Let*

$$0 \rightarrow F' \rightarrow F \rightarrow F'' \rightarrow 0$$

*be an exact sequence, and assume that  $F''$  is flat. Then  $F$  is flat if and only if  $F'$  is flat. More generally, let*

$$0 \rightarrow F^0 \rightarrow F^1 \rightarrow \cdots \rightarrow F^n \rightarrow 0$$

*be an exact sequence such that  $F^1, \dots, F^n$  are flat. Then  $F^0$  is flat.*

*Proof.* Let  $0 \rightarrow E' \rightarrow E$  be an injection. We have an exact and commutative diagram:

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \downarrow & & \\
 0 & \longrightarrow & F' \otimes E' & \longrightarrow & F \otimes E' & \longrightarrow & F'' \otimes E' \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & F' \otimes E & \longrightarrow & F \otimes E & \longrightarrow & F'' \otimes E
 \end{array}$$

The 0 on top is by hypothesis that  $F''$  is flat, and the two zeros on the left are justified by Lemma 3.3. If  $F'$  is flat, then the first vertical map is an injection, and the snake lemma shows that  $F$  is flat. If  $F$  is flat, then the middle column is an injection. Then the two zeros on the left and the commutativity of the left square show that the map  $F' \otimes E' \rightarrow F' \otimes E$  is an injection, so  $F'$  is flat. This proves the first statement.

The proof of the second statement is done by induction, introducing kernels and cokernels at each step as in dimension shifting, and apply the first statement at each step. This proves the proposition

To give flexibility in testing for flatness, the next two lemmas are useful, in relating the notion of flatness to a specific module. Namely, we say that  $F$  is  **$E$ -flat** or **flat for  $E$** , if for every monomorphism

$$0 \rightarrow E' \rightarrow E$$

the tensored sequence

$$0 \rightarrow F \otimes E' \rightarrow F \otimes E$$

is also exact.

**Lemma 3.5.** *Assume that  $F$  is  $E$ -flat. Then  $F$  is also flat for every submodule and every quotient module of  $E$ .*

*Proof.* The submodule part is immediate because if  $E'_1 \subset E'_2 \subset E$  are submodules, and  $F \otimes E'_1 \rightarrow F \otimes E$  is a monomorphism so is  $F \otimes E'_1 \rightarrow F \otimes E'_2$  since the composite map with  $F \otimes E'_2 \rightarrow F \otimes E$  is a monomorphism. The only question lies with a factor module. Suppose we have an exact sequence

$$0 \rightarrow N \rightarrow E \rightarrow M \rightarrow 0.$$

Let  $M'$  be a submodule of  $M$  and  $E'$  its inverse image in  $E$ . Then we have a

commutative diagram of exact sequences:

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & E' & \longrightarrow & M' & \longrightarrow 0 \\ & & \parallel & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M & \longrightarrow 0. \end{array}$$

We tensor with  $F$  to get the exact and commutative diagram

$$\begin{array}{ccccccc} & & 0 & & K & & \\ & & \downarrow & & \downarrow & & \\ & & F \otimes N & \longrightarrow & F \otimes E' & \longrightarrow & F \otimes M' & \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & F \otimes N & \longrightarrow & F \otimes E & \longrightarrow & F \otimes M & \longrightarrow 0 \\ & & \downarrow & & & & & \\ & & 0 & & & & & \end{array}$$

where  $K$  is the questionable kernel which we want to prove is 0. But the snake lemma yields the exact sequence

$$0 \rightarrow K \rightarrow 0$$

which concludes the proof.

**Lemma 3.6.** *Let  $\{E_i\}$  be a family of modules, and suppose that  $F$  is flat for each  $E_i$ . Then  $F$  is flat for their direct sum.*

*Proof.* Let  $E = \bigoplus E_i$  be their direct sum. We have to prove that given any submodule  $E'$  of  $E$ , the sequence

$$0 \rightarrow F \otimes E' \rightarrow F \otimes E = \bigoplus F \otimes E_i$$

is exact. Note that if an element of  $F \otimes E'$  becomes 0 when mapped into the direct sum, then it becomes 0 already in a finite subsum, so without loss of generality we may assume that the set of indices is finite. Then by induction, we can assume that the set of indices consists of two elements, so we have two modules  $E_1$  and  $E_2$ , and  $E = E_1 \oplus E_2$ . Let  $N$  be a submodule of  $E$ . Let  $N_1 = N \cap E_1$  and let  $N_2$  be the image of  $N$  under the projection on  $E_2$ . Then

we have the following commutative and exact diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 N_1 & \longrightarrow & N & \longrightarrow & N_2 & \longrightarrow & 0 \\
 \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & E_1 & \longrightarrow & E & \longrightarrow & E_2
 \end{array}$$

Tensoring with  $F$  we get the exact and commutative diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 F \otimes N_1 & \longrightarrow & F \otimes N & \longrightarrow & F \otimes N_2 & \longrightarrow & 0 \\
 \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & F \otimes E_1 & \longrightarrow & F \otimes E & \longrightarrow & F \otimes E_2
 \end{array}$$

The lower left exactness is due to the fact that  $E = E_1 \oplus E_2$ . Then the snake lemma shows that the kernel of the middle vertical map is 0. This proves the lemma.

The next proposition shows that to test for flatness, it suffices to do so only for a special class of exact sequences arising from ideals.

**Proposition 3.7.**  *$F$  is flat if and only if for every ideal  $\mathfrak{a}$  of  $R$  the natural map*

$$\mathfrak{a} \otimes F \rightarrow \mathfrak{a}F$$

*is an isomorphism. In fact,  $F$  is flat if and only for every ideal  $\mathfrak{a}$  of  $R$  tensoring the sequence*

$$0 \rightarrow \mathfrak{a} \rightarrow R \rightarrow R/\mathfrak{a} \rightarrow 0$$

*with  $F$  yields an exact sequence.*

*Proof.* If  $F$  is flat, then tensoring with  $F$  and using Proposition 2.7 shows that the natural map is an isomorphism, because  $\mathfrak{a}M$  is the kernel of  $M \rightarrow M/\mathfrak{a}M$ . Conversely, assume that this map is an isomorphism for all ideals  $\mathfrak{a}$ . This means

that  $F$  is  $R$ -flat. By Lemma 3.6 it follows that  $F$  is flat for an arbitrary direct sum of  $R$  with itself, and since any module  $M$  is a quotient of such a direct sum, Lemma 3.5 implies that  $F$  is  $M$ -flat, thus concluding the proof.

**Remark on abstract nonsense.** The proofs of Proposition 3.1(i), (ii), (iii), and Propositions 3.3 through 3.7 are basically rooted in abstract nonsense, and depend only on arrow theoretic arguments. Specifically, as in Chapter XX, §8, suppose that we have a bifunctor  $T$  on two distinct abelian categories  $\mathfrak{Q}$  and  $\mathfrak{G}$  such that for each  $A$ , the functor  $B \mapsto T(A, B)$  is right exact and for each  $B$  the functor  $A \mapsto T(A, B)$  is right exact. Instead of “flat” we call an object  $A$  of  $\mathfrak{Q}$   $T$ -exact if  $B \mapsto T(A, B)$  is an exact functor; and we call an object  $L$  of  $\mathfrak{G}$   $'T$ -exact if  $A \mapsto T(A, L)$  is exact. Then the references to the base ring and free modules can be replaced by abstract nonsense conditions as follows.

In the use of  $L$  in Lemma 3.3, we need to assume that for every object  $E$  of  $\mathfrak{G}$  there is a  $'T$ -exact  $L$  and an epimorphism

$$L \rightarrow E \rightarrow 0.$$

For the analog of Proposition 3.7, we need to assume that there is some object  $R$  in  $\mathfrak{G}$  for which  $F$  is  $R$ -exact, that is given an exact sequence

$$0 \rightarrow \mathfrak{a} \rightarrow R$$

then  $0 \rightarrow T(F, \mathfrak{a}) \rightarrow T(F, R)$  is exact; and we also need to assume that  $R$  is a generator in the sense that every object  $B$  is the quotient of a direct sum of  $R$  with itself, taken over some family of indices, and  $T$  respects direct sums.

The snake lemma is valid in arbitrary abelian categories, either because its proof is “functorial,” or by using a representation functor to reduce it to the category of abelian groups. Take your pick.

In particular, we really don’t need to have a commutative ring as base ring, this was done only for simplicity of language.

We now pass to somewhat different considerations.

**Theorem 3.8.** *Let  $R$  be a commutative local ring, and let  $M$  be a finite flat module over  $R$ . Then  $M$  is free. In fact, if  $x_1, \dots, x_n \in M$  are elements of  $M$  whose residue classes are a basis of  $M/\mathfrak{m}M$  over  $R/\mathfrak{m}$ , then  $x_1, \dots, x_n$  form a basis of  $M$  over  $R$ .*

*Proof.* Let  $R^{(n)} \rightarrow M$  be the map which sends the unit vectors of  $R^{(n)}$  on  $x_1, \dots, x_n$  respectively, and let  $N$  be its kernel. We get an exact sequence

$$0 \rightarrow N \rightarrow R^{(n)} \rightarrow M,$$

whence a commutative diagram

$$\begin{array}{ccccccc}
 \mathfrak{m} \otimes N & \longrightarrow & \mathfrak{m} \otimes R^{(n)} & \longrightarrow & \mathfrak{m} \otimes M & & \\
 \downarrow f & & \downarrow g & & \downarrow h & & \\
 0 & \longrightarrow & N & \longrightarrow & R^{(n)} & \longrightarrow & M
 \end{array}$$

in which the rows are exact. Since  $M$  is assumed flat, the map  $h$  is an injection. By the snake lemma one gets an exact sequence

$$0 \rightarrow \text{coker } f \rightarrow \text{coker } g \rightarrow \text{coker } h,$$

and the arrow on the right is merely

$$R^{(n)}/\mathfrak{m}R^{(n)} \rightarrow M/\mathfrak{m}M,$$

which is an isomorphism by the assumption on  $x_1, \dots, x_n$ . It follows that  $\text{coker } f = 0$ , whence  $\mathfrak{m}N = N$ , whence  $N = 0$  by Nakayama if  $R$  is Noetherian, so  $N$  is finitely generated. If  $R$  is not assumed Noetherian, then one has to add a slight argument as follows in case  $M$  is finitely presented.

**Lemma 3.9.** *Assume that  $M$  is finitely presented, and let*

$$0 \rightarrow N \rightarrow E \rightarrow M \rightarrow 0$$

*be exact, with  $E$  finite free. Then  $N$  is finitely generated.*

*Proof.* Let

$$L_1 \rightarrow L_2 \rightarrow M \rightarrow 0$$

be a finite presentation of  $M$ , that is an exact sequence with  $L_1, L_2$  finite free. Using the freeness, there exists a commutative diagram

$$\begin{array}{ccccccc}
 L_1 & \longrightarrow & L_2 & \longrightarrow & M & \longrightarrow & 0 \\
 \downarrow & & \downarrow & & \downarrow \text{id} & & \\
 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M \longrightarrow 0
 \end{array}$$

such that  $L_2 \rightarrow E$  is surjective. Then the snake lemma gives at once the exact sequence

$$0 \rightarrow \text{coker}(L_1 \rightarrow N) \rightarrow 0,$$

so  $\text{coker}(L_1 \rightarrow N) = 0$ , whence  $N$  is an image of  $L_1$  and is therefore finitely generated, thereby proving the lemma, and also completing the proof of Theorem 3.8 when  $M$  is finitely presented.

We still have not proved Theorem 3.8 in the fully general case. For this we use Matsumura's proof (see his *Commutative Algebra*, Chapter 2), based on the following lemma.

**Lemma 3.10.** *Assume that  $M$  is flat over  $R$ . Let  $a_i \in A$ ,  $x_i \in M$  for  $i = 1, \dots, n$ , and suppose that we have the relation*

$$\sum_{i=1}^n a_i x_i = 0.$$

*Then there exists an integer  $s$  and elements  $b_{ij} \in A$  and  $y_j \in M$  ( $j = 1, \dots, s$ ) such that*

$$\sum_i a_i b_{ij} = 0 \quad \text{for all } j \quad \text{and} \quad x_i = \sum_j b_{ij} y_j \quad \text{for all } i.$$

*Proof.* We consider the exact sequence

$$0 \rightarrow K \rightarrow R^{(n)} \rightarrow R$$

where the map  $R^{(n)} \rightarrow R$  is given by

$$(b_1, \dots, b_n) \mapsto \sum_{i=1}^n a_i b_i,$$

and  $K$  is its kernel. Since  $M$  is flat it follows that

$$K \otimes M \rightarrow M^{(n)} \xrightarrow{f_M} M$$

is exact, where  $f_M$  is given by

$$f_M(z_1, \dots, z_n) = \sum_{i=1}^n a_i z_i.$$

Therefore there exist elements  $\beta_j \in K$  and  $y_j \in M$  such that

$$(x_1, \dots, x_n) = \sum_{j=1}^s \beta_j y_j.$$

Write  $\beta_j = (b_{1j}, \dots, b_{nj})$  with  $b_{ij} \in R$ . This proves the lemma.

We may now apply the lemma to prove the theorem in exactly the same way we proved that a finite projective module over a local ring is free in Chapter X, Theorem 4.4, by induction. This concludes the proof.

**Remark.** In the applications I know of, the base ring is Noetherian, and so one gets away with the very simple proof given at first. I did not want to obstruct the simplicity of this proof, and that is the reason I gave the additional technicalities in increasing order of generality.

**Applications of homology.** We end this section by pointing out a connection between the tensor product and the homological considerations of Chapter XX, §8 for those readers who want to pursue this trend of thoughts. The tensor product is a bifunctor to which we can apply the considerations of Chapter XX, §8. Let  $M, N$  be modules. Let

$$\cdots \rightarrow E_i \rightarrow E_{i-1} \rightarrow E_0 \rightarrow M \rightarrow 0$$

be a free or projective resolution of  $M$ , i.e. an exact sequence where  $E_i$  is free or projective for all  $i \geq 0$ . We write this sequence as

$$E_M \rightarrow M \rightarrow 0.$$

Then by definition,

$\text{Tor}_i(M, N) = i\text{-th homology of the complex } E \otimes N\text{, that is of}$

$$\cdots \rightarrow E_i \otimes N \rightarrow E_{i-1} \otimes N \rightarrow \cdots \rightarrow E_0 \otimes N \rightarrow 0.$$

This homology is determined up to a unique isomorphism. I leave to the reader to pick whatever convention is agreeable to fix one resolution to determine a fixed representation of  $\text{Tor}_i(M, N)$ , to which all others are isomorphic by a unique isomorphism.

Since we have a bifunctorial isomorphism  $M \otimes N \approx N \otimes M$ , we also get a bifunctorial isomorphism

$$\text{Tor}_i(M, N) \approx \text{Tor}_i(N, M)$$

for all  $i$ . See Propositions 8.2 and 8.2' of Chapter XX.

Following general principles, we say that  $M$  has **Tor-dimension**  $\leq d$  if  $\text{Tor}_i(M, N) = 0$  for all  $i > d$  and all  $N$ . From Chapter XX, §8 we get the following result, which merely replaces  $T$ -exact by flat.

**Theorem 3.11.** *The following three conditions are equivalent concerning a module  $M$ .*

- (i)  $M$  is flat.
- (ii)  $\text{Tor}_1(M, N) = 0$  for all  $N$ .
- (iii)  $\text{Tor}_i(M, N) = 0$  for all  $i \geq 1$  and all  $N$ , in other words,  $M$  has Tor-dimension 0.

**Remark.** Readers willing to use this characterization can replace some of the preceding proofs from 3.3 to 3.6 by a Tor-dimension argument, which is more formal, or at least formal in a different way, and may seem more rapid. The snake lemma was used ad hoc in each case to prove the desired result. The general homology theory simply replaces this use by the corresponding formal homological step, once the general theory of the derived functor has been carried out.

---

## §4. EXTENSION OF THE BASE

Let  $R$  be a commutative ring and let  $E$  be a  $R$ -module. We specify  $R$  since we are going to work with several rings in a moment. Let  $R \rightarrow R'$  be a homomorphism of commutative rings, so that  $R'$  is an  $R$ -algebra, and may be viewed as an  $R$ -module also. We have a 3-multilinear map

$$R' \times R' \times E \rightarrow R' \otimes E$$

defined by the rule

$$(a, b, x) \mapsto ab \otimes x.$$

This induces therefore a  $R$ -linear map

$$R' \otimes (R' \otimes E) \rightarrow R' \otimes E$$

and hence a  $R$ -bilinear map  $R' \times (R' \otimes E) \rightarrow R' \otimes E$ . It is immediately verified that our last map makes  $R' \otimes E$  into a  $R'$ -module, which we shall call the **extension of  $E$  over  $R'$** , and denote by  $E_{R'}$ . We also say that  $E_{R'}$  is obtained by **extension of the base** ring from  $R$  to  $R'$ .

**Example 1.** Let  $\mathfrak{a}$  be an ideal of  $R$  and let  $R \rightarrow R/\mathfrak{a}$  be the canonical homomorphism. Then the extension of  $E$  to  $R/\mathfrak{a}$  is also called the **reduction** of  $E$  modulo  $\mathfrak{a}$ . This happens often over the integers, when we reduce modulo a prime  $p$  (i.e. modulo the prime ideal  $(p)$ ).

**Example 2.** Let  $R$  be a field and  $R'$  an extension field. Then  $E$  is a vector space over  $R$ , and  $E_{R'}$  is a vector space over  $R'$ . In terms of a basis, we see that our extension gives what was alluded to in the preceding chapter. This example will be expanded in the exercises.

We draw the same diagrams as in field theory:

$$\begin{array}{ccc} & E_{R'} & \\ / \quad \backslash & & \backslash \quad / \\ E & & R' \\ / \quad \backslash & & \backslash \quad / \\ & R & \end{array}$$

to visualize an extension of the base. From Proposition 2.3, we conclude:

**Proposition 4.1.** *Let  $E$  be a free module over  $R$ , with basis  $\{v_i\}_{i \in I}$ . Let  $v'_i = 1 \otimes v_i$ . Then  $E_{R'}$  is a free module over  $R'$ , with basis  $\{v'_i\}_{i \in I}$ .*

We had already used a special case of this proposition when we observed that the dimension of a free module is defined, i.e. that two bases have the same

cardinality. Indeed, in that case, we reduced modulo a maximal ideal of  $R$  to reduce the question to a vector space over a field.

When we start changing rings, it is desirable to indicate  $R$  in the notation for the tensor product. Thus we write

$$E_{R'} = R' \otimes E = R' \otimes_R E.$$

*Then we have transitivity of the extension of the base*, namely, if  $R \rightarrow R' \rightarrow R''$  is a succession of homomorphisms of commutative rings, then we have an isomorphism

$$R'' \otimes_R E \approx R'' \otimes_{R'} (R' \otimes_R E)$$

and this isomorphism is one of  $R''$ -modules. The proof is trivial and will be left to the reader.

If  $E$  has a multiplicative structure, we can extend the base also for this multiplication. Let  $R \rightarrow A$  be a ring-homomorphism such that every element in the image of  $R$  in  $A$  commutes with every element in  $A$  (i.e. an  $R$ -algebra). Let  $R \rightarrow R'$  be a homomorphism of commutative rings. We have a 4-multilinear map

$$R' \times A \times R' \times A \rightarrow R' \otimes A$$

defined by

$$(a, x, b, y) \mapsto ab \otimes xy.$$

We get an induced  $R$ -linear map

$$R' \otimes A \otimes R' \otimes A \rightarrow R' \otimes A$$

and hence an induced  $R$ -bilinear map

$$(R' \otimes A) \times (R' \otimes A) \rightarrow R' \otimes A.$$

It is trivially verified that the law of composition on  $R' \otimes A$  we have just defined is associative. There is a unit element in  $R' \otimes A$ , namely,  $1 \otimes 1$ . We have a ring-homomorphism of  $R'$  into  $R' \otimes A$ , given by  $a \mapsto a \otimes 1$ . In this way one sees at once that  $R' \otimes A = A_{R'}$  is an  $R'$ -algebra. We note that the map

$$x \mapsto 1 \otimes x$$

is a ring-homomorphism of  $A$  into  $R' \otimes A$ , and that we get a commutative diagram of ring homomorphisms,

$$\begin{array}{ccccc} & & R' \otimes A = A_{R'} & & \\ & \swarrow & & \searrow & \\ A & & & & R' \\ & \nwarrow & & \nearrow & \\ & & R & & \end{array}$$

For the record, we give some routine tests for flatness in the context of base extension.

**Proposition 4.2.** *Let  $R \rightarrow A$  be an  $R$ -algebra, and assume  $A$  commutative.*

- (i) **Base change.** *If  $F$  is a flat  $R$ -module, then  $A \otimes_R F$  is a flat  $A$ -module.*
- (ii) **Transitivity.** *If  $A$  is a flat commutative  $R$ -algebra and  $M$  is a flat  $A$ -module, then  $M$  is flat as  $R$ -module.*

The proofs are immediate, and will be left to the reader.

## §5. SOME FUNCTORIAL ISOMORPHISMS

We recall an abstract definition. Let  $\mathfrak{A}, \mathfrak{B}$  be two categories. The functors of  $\mathfrak{A}$  into  $\mathfrak{B}$  (say covariant, and in one variable) can be viewed as the objects of a category, whose morphisms are defined as follows. If  $L, M$  are two such functors, a morphism  $H: L \rightarrow M$  is a rule which to each object  $X$  of  $\mathfrak{A}$  associates a morphism  $H_X: L(X) \rightarrow M(X)$  in  $\mathfrak{B}$ , such that for any morphism  $f: X \rightarrow Y$  in  $\mathfrak{A}$ , the following diagram is commutative:

$$\begin{array}{ccc} L(X) & \xrightarrow{H_X} & M(X) \\ L(f) \downarrow & & \downarrow M(f) \\ L(Y) & \xrightarrow{H_Y} & M(Y) \end{array}$$

We can therefore speak of isomorphisms of functors. We shall see examples of these in the theory of tensor products below. In our applications, our categories are additive, that is, the set of morphisms is an additive group, and the composition law is  $\mathbf{Z}$ -bilinear. In that case, a functor  $L$  is called **additive** if

$$L(f + g) = L(f) + L(g).$$

We let  $R$  be a commutative ring, and we shall consider additive functors from the category of  $R$ -modules into itself. For instance we may view the dual module as a functor,

$$E \mapsto E^\vee = L(E, R) = \text{Hom}_R(E, R).$$

Similarly, we have a functor in two variables,

$$(E, F) \mapsto L(E, F) = \text{Hom}_R(E, F),$$

contravariant in the first, covariant in the second, and bi-additive.

We shall give several examples of functorial isomorphisms connected with the tensor product, and for this it is most convenient to state a general theorem, giving us a criterion when a morphism of functors is in fact an isomorphism.

**Proposition 5.1.** *Let  $L, M$  be two functors (both covariant or both contravariant) from the category of  $R$ -modules into itself. Assume that both functors are additive. Let  $H: L \rightarrow M$  be a morphism of functors. If  $H_E: L(E) \rightarrow M(E)$  is an isomorphism for every 1-dimensional free module  $E$  over  $R$ , then  $H_E$  is an isomorphism for every finite-dimensional free module over  $R$ .*

*Proof.* We begin with a lemma.

**Lemma 5.2.** *Let  $E$  and  $E_i$  ( $i = 1, \dots, m$ ) be modules over a ring. Let  $\varphi_i: E_i \rightarrow E$  and  $\psi_i: E \rightarrow E_i$  be homomorphisms having the following properties:*

$$\psi_i \circ \varphi_i = \text{id}, \quad \psi_i \circ \varphi_j = 0 \quad \text{if } i \neq j$$

$$\sum_{i=1}^m \varphi_i \circ \psi_i = \text{id},$$

*Then the map*

$$x \mapsto (\psi_1 x, \dots, \psi_m x)$$

*is an isomorphism of  $E$  onto the direct product  $\prod_{i=1}^m E_i$ , and the map*

$$(x_1, \dots, x_m) \mapsto \varphi_1 x_1 + \dots + \varphi_m x_m$$

*is an isomorphism of the product onto  $E$ . Conversely, if  $E$  is equal to the direct sum of submodules  $E_i$  ( $i = 1, \dots, m$ ), if we let  $\psi_i$  be the inclusion of  $E_i$  in  $E$ , and  $\varphi_i$  the projection of  $E$  on  $E_i$ , then these maps satisfy the above-mentioned properties.*

*Proof.* The proof is routine, and is essentially the same as that of Proposition 3.1 of Chapter III. We shall leave it as an exercise to the reader.

We observe that the families  $\{\varphi_i\}$  and  $\{\psi_i\}$  satisfying the properties of the lemma behave functorially: If  $T$  is an additive contravariant functor, say, then the families  $\{T(\psi_i)\}$  and  $\{T(\varphi_i)\}$  also satisfy the properties of the lemma. Similarly if  $T$  is a covariant functor.

To apply the lemma, we take the modules  $E_i$  to be the 1-dimensional components occurring in a decomposition of  $E$  in terms of a basis. Let us assume for instance that  $L, M$  are both covariant. We have for each module  $E$  a com-

mutative diagram

$$\begin{array}{ccc}
 L(E) & \xrightarrow{H_E} & M(E) \\
 \uparrow L(\varphi_i) & & \uparrow M(\varphi_i) \\
 L(E_i) & \xrightarrow{H_{E_i}} & M(E_i)
 \end{array}$$

and a similar diagram replacing  $\varphi_i$  by  $\psi_i$ , reversing the two vertical arrows. Hence we get a direct sum decomposition of  $L(E)$  in terms of  $L(\psi_i)$  and  $L(\varphi_i)$ , and similarly for  $M(E)$ , in terms of  $M(\psi_i)$  and  $M(\varphi_i)$ . By hypothesis,  $H_{E_i}$  is an isomorphism. It then follows trivially that  $H_E$  is an isomorphism. For instance, to prove injectivity, we write an element  $v \in L(E)$  in the form

$$v = \sum L(\varphi_i)v_i,$$

with  $v_i \in L(E_i)$ . If  $H_E v = 0$ , then

$$0 = \sum H_E L(\varphi_i)v_i = \sum M(\varphi_i)H_{E_i}v_i,$$

and since the maps  $M(\varphi_i)$  ( $i = 1, \dots, m$ ) give a direct sum decomposition of  $M(E)$ , we conclude that  $H_{E_i}v_i = 0$  for all  $i$ , whence  $v_i = 0$ , and  $v = 0$ . The surjectivity is equally trivial.

When dealing with a functor of several variables, additive in each variable, one can keep all but one of the variables fixed, and then apply the proposition. We shall do this in the following corollaries.

**Corollary 5.3.** *Let  $E', E, F', F$  be free and finite dimensional over  $R$ . Then we have a functorial isomorphism*

$$L(E', E) \otimes L(F', F) \rightarrow L(E' \otimes F', E \otimes F)$$

such that

$$f \otimes g \mapsto T(f, g).$$

*Proof.* Keep  $E, F', F$  fixed, and view  $L(E', E) \otimes L(F', F)$  as a functor in the variable  $E'$ . Similarly, view

$$L(E' \otimes F', E \otimes F)$$

as a functor in  $E'$ . The map  $f \otimes g \mapsto T(f, g)$  is functorial, and thus by the lemma, it suffices to prove that it yields an isomorphism when  $E'$  has dimension 1. Assume now that this is the case; fix  $E'$  of dimension 1, and view the two expressions in the corollary as functors of the variable  $E$ . Applying the lemma

again, it suffices to prove that our arrow is an isomorphism when  $E$  has dimension 1. Similarly, we may assume that  $F, F'$  have dimension 1. In that case the verification that the arrow is an isomorphism is a triviality, as desired.

**Corollary 5.4.** *Let  $E, F$  be free and finite dimensional. Then we have a natural isomorphism*

$$\text{End}_R(E) \otimes \text{End}_R(F) \rightarrow \text{End}_R(E \otimes F).$$

*Proof.* Special case of Corollary 5.3.

Note that Corollary 5.4 had already been proved before, and that we mention it here only to see how it fits with the present point of view.

**Corollary 5.5.** *Let  $E, F$  be free finite dimensional over  $R$ . There is a functorial isomorphism*

$$E^\vee \otimes F \rightarrow L(E, F)$$

given for  $\lambda \in E^\vee$  and  $y \in F$  by the map

$$\lambda \otimes y \mapsto A_{\lambda, y}$$

where  $A_{\lambda, y}$  is such that for all  $x \in E$ , we have  $A_{\lambda, y}(x) = \lambda(x)y$ .

The inverse isomorphism of Corollary 5.5 can be described as follows. Let  $\{v_1, \dots, v_n\}$  be a basis of  $E$ , and let  $\{v'_1, \dots, v'_n\}$  be the dual basis. If  $A \in L(E, F)$ , then the element

$$\sum_{i=1}^n v'_i \otimes A(v_i) \in E^\vee \otimes F$$

maps to  $A$ . In particular, if  $E = F$ , then the element mapping to the identity  $\text{id}_E$  is called the **Casimir element**

$$\sum_{i=1}^n v'_i \otimes v_i,$$

independent of the choice of basis. Cf. Exercise 14.

To prove Corollary 5.5, justify that there is a well-defined homomorphism of  $E^\vee \otimes F$  to  $L(E, F)$ , by the formula written down. Verify that this homomorphism is both injective and surjective. We leave the details as exercises.

Differential geometers are very fond of the isomorphism

$$L(E, E) \rightarrow E^\vee \otimes E,$$

and often use  $E^\vee \otimes E$  when they think geometrically of  $L(E, E)$ , thereby emphasizing an unnecessary dualization, and an irrelevant formalism, when it is easier to deal directly with  $L(E, E)$ . In differential geometry, one applies various functors  $L$  to the tangent space at a point on a manifold, and elements of the spaces thus obtained are called **tensors** (of type  $L$ ).

**Corollary 5.6.** *Let  $E, F$  be free and finite dimensional over  $R$ . There is a functorial isomorphism*

$$E^\vee \otimes F^\vee \rightarrow (E \otimes F)^\vee.$$

*given for  $\lambda \in E^\vee$  and  $\mu \in F^\vee$  by the map*

$$\lambda \otimes \mu \mapsto \Lambda,$$

*where  $\Lambda$  is such that, for all  $x \in E$  and  $y \in F$ ,*

$$\Lambda(x \otimes y) = \lambda(x)\mu(y)$$

*Proof.* As before.

Finally, we leave the following results as an exercise.

**Proposition 5.7.** *Let  $E$  be free and finite dimensional over  $R$ . The trace function on  $L(E, E)$  is equal to the composite of the two maps*

$$L(E, E) \rightarrow E^\vee \otimes E \rightarrow R,$$

*where the first map is the inverse of the isomorphism described in Corollary 5.5, and the second map is induced by the bilinear map*

$$(\lambda, x) \mapsto \lambda(x).$$

Of course, it is precisely in a situation involving the trace that the isomorphism of Corollary 5.5 becomes important, and that the finite dimensionality of  $E$  is used. In many applications, this finite dimensionality plays no role, and it is better to deal with  $L(E, E)$  directly.

## §6. TENSOR PRODUCT OF ALGEBRAS

In this section, we again let  $R$  be a commutative ring. By an  **$R$ -algebra** we mean a ring homomorphism  $R \rightarrow A$  into a ring  $A$  such that the image of  $R$  is contained in the center of  $A$ .

Let  $A, B$  be  $R$ -algebras. We shall make  $A \otimes B$  into an  $R$ -algebra. Given  $(a, b) \in A \times B$ , we have an  $R$ -bilinear map

$$M_{a,b}: A \times B \rightarrow A \otimes B \text{ such that } M_{a,b}(a', b') = aa' \otimes bb'.$$

Hence  $M_{a,b}$  induces an  $R$ -linear map  $m_{a,b}: A \otimes B \rightarrow A \otimes B$  such that  $m_{a,b}(a', b') = aa' \otimes bb'$ . But  $m_{a,b}$  depends bilinearly on  $a$  and  $b$ , so we obtain finally a unique  $R$ -bilinear map

$$A \otimes B \times A \otimes B \rightarrow A \otimes B$$

such that  $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ . This map is obviously associative, and we have a natural ring homomorphism

$$R \rightarrow A \otimes B \quad \text{given by} \quad c \mapsto 1 \otimes c = c \otimes 1.$$

Thus  $A \otimes B$  is an  $R$ -algebra, called the **ordinary tensor product**.

### Application: commutative rings

We shall now see the implication of the above for commutative rings.

**Proposition 6.1.** *Finite coproducts exist in the category of commutative rings, and in the category of commutative algebras over a commutative ring. If  $R \rightarrow A$  and  $R \rightarrow B$  are two homomorphisms of commutative rings, then their coproduct over  $R$  is the homomorphism  $R \rightarrow A \otimes B$  given by*

$$a \mapsto a \otimes 1 = 1 \otimes a.$$

*Proof.* We shall limit our proof to the case of the coproduct of two ring homomorphisms  $R \rightarrow A$  and  $R \rightarrow B$ . One can use induction.

Let  $A, B$  be commutative rings, and assume given ring-homomorphisms into a commutative ring  $C$ ,

$$\varphi : A \rightarrow C \quad \text{and} \quad \psi : B \rightarrow C.$$

Then we can define a  $\mathbf{Z}$ -bilinear map

$$A \times B \rightarrow C$$

by  $(x, y) \mapsto \varphi(x)\psi(y)$ . From this we get a unique additive homomorphism

$$A \otimes B \rightarrow C$$

such that  $x \otimes y \mapsto \varphi(x)\psi(y)$ . We have seen above that we can define a ring structure on  $A \otimes B$ , such that

$$(a \otimes b)(c \otimes d) = ac \otimes bd.$$

It is then clear that our map  $A \otimes B \rightarrow C$  is a ring-homomorphism. We also have two ring-homomorphisms

$$A \xrightarrow{f} A \otimes B \quad \text{and} \quad B \xrightarrow{g} A \otimes B$$

given by

$$x \mapsto x \otimes 1 \quad \text{and} \quad y \mapsto 1 \otimes y.$$

The universal property of the tensor product shows that  $(A \otimes B, f, g)$  is a coproduct of our rings  $A$  and  $B$ .

If  $A, B, C$  are  $R$ -algebras, and if  $\varphi, \psi$  make the following diagram com-

mutative,

$$\begin{array}{ccccc}
 & & C & & \\
 & \swarrow \varphi & & \searrow \psi & \\
 A & & & & B \\
 & \nwarrow & & \uparrow & \\
 & & R & &
 \end{array}$$

then  $A \otimes B$  is also an  $R$ -algebra (it is in fact an algebra over  $R$ , or  $A$ , or  $B$ , depending on what one wants to use), and the map  $A \otimes B \rightarrow C$  obtained above gives a homomorphism of  $R$ -algebras.

A commutative ring can always be viewed as a  $\mathbf{Z}$ -algebra (i.e. as an algebra over the integers). Thus one sees the coproduct of commutative rings as a special case of the coproduct of  $R$ -algebras.

**Graded Algebras.** Let  $G$  be a commutative monoid, written additively. By a  **$G$ -graded ring**, we shall mean a ring  $A$ , which as an additive group can be expressed as a direct sum.

$$A = \bigoplus_{r \in G} A_r,$$

and such that the ring multiplication maps  $A_r \times A_s$  into  $A_{r+s}$ , for all  $r, s \in G$ .

In particular, we see that  $A_0$  is a subring.

The elements of  $A_r$  are called the **homogeneous elements of degree  $r$** .

We shall construct several examples of graded rings, according to the following pattern. Suppose given for each  $r \in G$  an abelian group  $A_r$  (written additively), and for each pair  $r, s \in G$  a map  $A_r \times A_s \rightarrow A_{r+s}$ . Assume that  $A_0$  is a commutative ring, and that composition under these maps is associative and  $A_0$ -bilinear. Then the direct sum  $A = \bigoplus_{r \in G} A_r$  is a ring: We can define multiplication in the obvious way, namely

$$\left( \sum_{r \in G} x_r \right) \left( \sum_{s \in G} y_s \right) = \sum_{t \in G} \left( \sum_{r+s=t} x_r y_s \right).$$

The above product is called the **ordinary product**. However, there is another way. Suppose the grading is in  $\mathbf{Z}$  or  $\mathbf{Z}/2\mathbf{Z}$ . We define the **super product** of  $x \in A_r$ , and  $y \in A_s$  to be  $(-1)^{rs}xy$ , where  $xy$  is the given product. It is easily verified that this product is associative, and extends to what is called the **super product**  $A \otimes A \rightarrow A$  associated with the bilinear maps. If  $R$  is a commutative ring such that  $A$  is a graded  $R$ -algebra, i.e.  $RA_r \subset A_r$  for all  $r$  (in addition to the condition that  $A$  is a graded ring), then with the super product,  $A$  is also an  $R$ -algebra, which will be denoted by  $A_{su}$ , and will be called the **super algebra** associated with  $A$ .

**Example.** In the next section, we shall meet the tensor algebra  $T(E)$ , which will be graded as the direct sum of  $T^r(E)$ , and so we get the associated super tensor algebra  $T_{\text{su}}(E)$  according to the above recipe.

Similarly, let  $A, B$  be graded algebras (graded by the natural numbers as above). We define their **super tensor product**

$$A \otimes_{\text{su}} B$$

to be the ordinary tensor product as graded module, but with the **super product**

$$(a \otimes b)(a' \otimes b') = (-1)^{(\deg b)(\deg a')} aa' \otimes bb'$$

if  $b, a'$  are homogeneous elements of  $B$  and  $A$  respectively. It is routinely verified that  $A \otimes_{\text{su}} B$  is then a ring which is also a graded algebra. Except for the sign, the product is the same as the ordinary one, but it is necessary to verify associativity explicitly. Suppose  $a' \in A_i, b \in B_j, a'' \in A_s$ , and  $b' \in B_r$ . Then the reader will find at once that the sign which comes out by computing

$$(a \otimes_{\text{su}} b)(a' \otimes_{\text{su}} b')(a'' \otimes_{\text{su}} b'')$$

in two ways turns out to be the same, namely  $(-1)^{ij+js+sr}$ . Since bilinearity is trivially satisfied, it follows that  $A \otimes_{\text{su}} B$  is indeed an algebra.

The super product in many ways is more natural than what we called the ordinary product. For instance, it is the natural product of cohomology in topology. Cf. Greenberg-Harper, *Algebraic Topology*, Chapter 29. For a similar construction with  $\mathbf{Z}/2\mathbf{Z}$ -grading, see Chapter XIX, §4.

## §7. THE TENSOR ALGEBRA OF A MODULE

Let  $R$  be a commutative ring as before, and let  $E$  be a module (i.e. an  $R$ -module). For each integer  $r \geq 0$ , we let

$$T^r(E) = \bigotimes_{i=1}^r E \quad \text{and} \quad T^0(E) = R.$$

Thus  $T^r(E) = E \otimes \cdots \otimes E$  (tensor product taken  $r$  times). Then  $T^r$  is a functor, whose effect on linear maps is given as follows. If  $f : E \rightarrow F$  is a linear map, then

$$T^r(f) = T(f, \dots, f)$$

in the sense of §1.

From the associativity of the tensor product, we obtain a bilinear map

$$T^r(E) \times T^s(E) \rightarrow T^{r+s}(E),$$

which is associative. Consequently, by means of this bilinear map, we can define a ring structure on the direct sum

$$T(E) = \bigoplus_{r=0}^{\infty} T^r(E),$$

and in fact an algebra structure (mapping  $R$  on  $T^0(E) = R$ ). We shall call  $T(E)$  the **tensor algebra** of  $E$ , over  $R$ . It is in general *not* commutative. If  $x, y \in T(E)$ , we shall again write  $x \otimes y$  for the ring operation in  $T(E)$ .

Let  $f : E \rightarrow F$  be a linear map. Then  $f$  induces a linear map

$$T^r(f) : T^r(E) \rightarrow T^r(F)$$

for each  $r \geq 0$ , and in this way induces a map which we shall denote by  $T(f)$  on  $T(E)$ . (There can be no ambiguity with the map of §1, which should now be written  $T^1(f)$ , and is in fact equal to  $f$  since  $T^1(E) = E$ .) It is clear that  $T(f)$  is the unique linear map such that for  $x_1, \dots, x_r \in E$  we have

$$T(f)(x_1 \otimes \cdots \otimes x_r) = f(x_1) \otimes \cdots \otimes f(x_r).$$

Indeed, the elements of  $T^1(E) = E$  are algebra-generators of  $T(E)$  over  $R$ . We see that  $T(f)$  is an algebra-homomorphism. *Thus  $T$  may be viewed as a functor from the category of modules to the category of graded algebras,  $T(f)$  being a homomorphism of degree 0.*

When  $E$  is free and finite dimensional over  $R$ , we can determine the structure of  $T(E)$  completely, using Proposition 2.3. Let  $P$  be an algebra over  $k$ . We shall say that  $P$  is a **non-commutative polynomial algebra** if there exist elements  $t_1, \dots, t_n \in P$  such that the elements

$$M_{(i)}(t) = t_{i_1} \cdots t_{i_s}$$

with  $1 \leq i_v \leq n$  form a basis of  $P$  over  $R$ . We may call these elements non-commutative monomials in  $(t)$ . As usual, by convention, when  $r = 0$ , the corresponding monomial is the unit element of  $P$ . We see that  $t_1, \dots, t_n$  generate  $P$  as an algebra over  $k$ , and that  $P$  is in fact a graded algebra, where  $P_r$  consists of linear combinations of monomials  $t_{i_1} \cdots t_{i_r}$  with coefficients in  $R$ . It is natural to say that  $t_1, \dots, t_n$  are **independent non-commutative variables** over  $R$ .

**Proposition 7.1.** *Let  $E$  be free of dimension  $n$  over  $R$ . Then  $T(E)$  is isomorphic to the non-commutative polynomial algebra on  $n$  variables over  $R$ . In other words, if  $\{v_1, \dots, v_n\}$  is a basis of  $E$  over  $R$ , then the elements*

$$M_{(i)}(v) = v_{i_1} \otimes \cdots \otimes v_{i_n}, \quad 1 \leq i_v \leq n$$

*form a basis of  $T^r(E)$ , and every element of  $T(E)$  has a unique expression as a finite sum*

$$\sum_{(i)} a_{(i)} M_{(i)}(v), \quad a_{(i)} \in R$$

with almost all  $a_{(i)}$  equal to 0.

*Proof.* This follows at once from Proposition 2.3.

The tensor product of linear maps will now be interpreted in the context of the tensor algebra.

For convenience, we shall denote the module of endomorphisms  $\text{End}_R(E)$  by  $L(E)$  for the rest of this section.

We form the direct sum

$$(LT)(E) = \bigoplus_{r=0}^{\infty} L(T^r(E)),$$

which we shall also write  $LT(E)$  for simplicity. (Of course,  $LT(E)$  is not equal to  $\text{End}_R(T(E))$ , so we must view  $LT$  as a single symbol.) We shall see that  $LT$  is a functor from modules to graded algebras, by defining a suitable multiplication on  $LT(E)$ . Let  $f \in L(T^r(E))$ ,  $g \in L(T^s(E))$ ,  $h \in L(T^m(E))$ . We define the product  $fg \in L(T^{r+s}(E))$  to be  $T(f, g)$ , in the notation of §1, in other words to be the unique linear map whose effect on an element  $x \otimes y$  with  $x \in T^r(E)$  and  $y \in T^s(E)$  is

$$x \otimes y \mapsto f(x) \otimes g(y).$$

In view of the associativity of the tensor product, we obtain at once the associativity  $(fg)h = f(gh)$ , and we also see that our product is bilinear. Hence  $LT(E)$  is a  $k$ -algebra.

We have an algebra-homomorphism

$$T(L(E)) \rightarrow LT(E)$$

given in each dimension  $r$  by the linear map

$$f_1 \otimes \cdots \otimes f_r \mapsto T(f_1, \dots, f_r) = f_1 \cdots f_r.$$

We specify here that the tensor product on the left is taken in

$$L(E) \otimes \cdots \otimes L(E).$$

We also note that the homomorphism is in general neither surjective nor injective. When  $E$  is free finite dimensional over  $R$ , the homomorphism turns out to be both, and thus we have a clear picture of  $LT(E)$  as a non-commutative polynomial algebra, generated by  $L(E)$ . Namely, from Proposition 2.5, we obtain:

**Proposition 7.2.** *Let  $E$  be free, finite dimensional over  $R$ . Then we have an algebra-isomorphism*

$$T(L(E)) = T(\text{End}_R(E)) \rightarrow LT(E) = \bigoplus_{r=0}^{\infty} \text{End}_R(T^r(E))$$

given by

$$f \otimes g \mapsto T(f, g).$$

*Proof.* By Proposition 2.5, we have a linear isomorphism in each dimension, and it is clear that the map preserves multiplication.

In particular, we see that  $LT(E)$  is a noncommutative polynomial algebra.

## §8. SYMMETRIC PRODUCTS

Let  $\mathfrak{S}_n$  denote the symmetric group on  $n$  letters, say operating on the integers  $(1, \dots, n)$ . An  $r$ -multilinear map

$$f : E^{(r)} \rightarrow F$$

is said to be **symmetric** if  $f(x_1, \dots, x_r) = f(x_{\sigma(1)}, \dots, x_{\sigma(r)})$  for all  $\sigma \in \mathfrak{S}_r$ .

In  $T'(E)$ , we let  $\mathfrak{b}_r$  be the submodule generated by all elements of type

$$x_1 \otimes \cdots \otimes x_r - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(r)}$$

for all  $x_i \in E$  and  $\sigma \in \mathfrak{S}_r$ . We define the factor module

$$S'(E) = T'(E)/\mathfrak{b}_r,$$

and let

$$S(E) = \bigoplus_{r=0}^{\infty} S'(E)$$

be the direct sum. It is immediately obvious that the direct sum

$$\mathfrak{b} = \bigoplus_{r=0}^{\infty} \mathfrak{b}_r$$

is an ideal in  $T(E)$ , and hence that  $S(E)$  is a graded  $R$ -algebra, which is called the **symmetric algebra** of  $E$ .

Furthermore, the canonical map

$$E^{(r)} \rightarrow S'(E)$$

obtained by composing the maps

$$E^{(r)} \rightarrow T'(E) \rightarrow T'(E)/\mathfrak{b}_r = S'(E)$$

is universal for  $r$ -multilinear symmetric maps.

We observe that  $S$  is a functor, from the category of modules to the category of graded  $R$ -algebras. The image of  $(x_1, \dots, x_r)$  under the canonical map

$$E^{(r)} \rightarrow S^r(E)$$

will be denoted simply by  $x_1 \cdots x_r$ .

**Proposition 8.1.** *Let  $E$  be free of dimension  $n$  over  $R$ . Let  $\{v_1, \dots, v_n\}$  be a basis of  $E$  over  $k$ . Viewed as elements of  $S^1(E)$  in  $S(E)$ , these basis elements are algebraically independent over  $R$ , and  $S(E)$  is therefore isomorphic to the polynomial algebra in  $n$  variables over  $R$ .*

*Proof.* Let  $t_1, \dots, t_n$  be algebraically independent variables over  $R$ , and form the polynomial algebra  $R[t_1, \dots, t_n]$ . Let  $P_r$  be the  $R$ -module of homogeneous polynomials of degree  $r$ . We define a map of  $E^{(r)} \rightarrow P_r$  as follows. If  $w_1, \dots, w_r$  are elements of  $E$  which can be written

$$w_i = \sum_{v=1}^n a_{iv} v, \quad i = 1, \dots, r,$$

then our map is given by

$$(w_1, \dots, w_r) \mapsto (a_{11}t_1 + \cdots + a_{1n}t_n) \cdots (a_{r1}t_1 + \cdots + a_{rn}t_n).$$

It is obvious that this map is multilinear and symmetric. Hence it factors through a linear map of  $S^r(E)$  into  $P_r$ :

$$\begin{array}{ccc} E^{(r)} & \longrightarrow & S^r(E) \\ & \searrow & \swarrow \\ & P_r & \end{array}$$

From the commutativity of our diagram, it is clear that the element  $v_{i_1} \cdots v_{i_s}$  in  $S^r(E)$  maps on  $t_{i_1} \cdots t_{i_s}$  in  $P_r$  for each  $r$ -tuple of integers  $(i) = (i_1, \dots, i_r)$ . Since the monomials  $M_{(i)}(t)$  of degree  $r$  are linearly independent over  $k$ , it follows that the monomials  $M_{(i)}(v)$  in  $S^r(E)$  are also linearly independent over  $R$ , and that our map  $S^r(E) \rightarrow P_r$  is an isomorphism. One verifies at once that the multiplication in  $S(E)$  corresponds to the multiplication of polynomials in  $R[t]$ , and thus that the map of  $S(E)$  into the polynomial algebra described as above for each component  $S^r(E)$  induces an algebra-isomorphism of  $S(E)$  onto  $R[t]$ , as desired.

**Proposition 8.2.** *Let  $E = E' \oplus E''$  be a direct sum of finite free modules. Then there is a natural isomorphism*

$$S^n(E' \oplus E'') \approx \bigoplus_{p+q=n} S^p E' \otimes S^q E''.$$

*In fact, this is but the  $n$ -part of a graded isomorphism*

$$S(E' \oplus E'') \approx SE' \otimes SE''.$$

*Proof.* The isomorphism comes from the following maps. The inclusions of  $E'$  and  $E''$  into their direct sum give rise to the functorial maps

$$SE' \otimes SE'' \rightarrow SE,$$

and the claim is that this is a graded isomorphism. Note that  $SE'$  and  $SE''$  are commutative rings, and so their tensor product is just the tensor product of commutative rings discussed in §6. The reader can either give a functorial map backward to prove the desired isomorphism, or more concretely,  $SE'$  is the polynomial ring on a finite family of variables,  $SE''$  is the polynomial ring in another family of variables, and their tensor product is just the polynomial ring in the two families of variables. The matter is easy no matter what, and the formal proof is left to the reader.

## EXERCISES

1. Let  $k$  be a field and  $k(\alpha)$  a finite extension. Let  $f(X) = \text{Irr}(\alpha, k, X)$ , and suppose that  $f$  is separable. Let  $k'$  be any extension of  $k$ . Show that  $k(\alpha) \otimes k'$  is a direct sum of fields. If  $k'$  is algebraically closed, show that these fields correspond to the embeddings of  $k(\alpha)$  in  $k'$ .
2. Let  $k$  be a field,  $f(X)$  an irreducible polynomial over  $k$ , and  $\alpha$  a root of  $f$ . Show that  $k(\alpha) \otimes k'$  is isomorphic, as a  $k'$ -algebra, to  $k'[X]/(f(X))$ .
3. Let  $E$  be a finite extension of a field  $k$ . Show that  $E$  is separable over  $k$  if and only if  $E \otimes_k L$  has no nilpotent elements for all extensions  $L$  of  $k$ , and also when  $L = k^a$ .
4. Let  $\varphi : A \rightarrow B$  be a commutative ring homomorphism. Let  $E$  be an  $A$ -module and  $F$  a  $B$ -module. Let  $F_A$  be the  $A$ -module obtained from  $F$  via the operation of  $A$  on  $F$  through  $\varphi$ , that is for  $y \in F_A$  and  $a \in A$  this operation is given by

$$(a, y) \mapsto \varphi(a)y.$$

Show that there is a natural isomorphism

$$\text{Hom}_B(B \otimes_A E, F) \approx \text{Hom}_A(E, F_A).$$

5. **The norm.** Let  $B$  be a commutative algebra over the commutative ring  $R$  and assume that  $B$  is free of rank  $r$ . Let  $A$  be any commutative  $R$ -algebra. Then  $A \otimes B$  is both an  $A$ -algebra and a  $B$ -algebra. We view  $A \otimes B$  as an  $A$ -algebra, which is also free of rank  $r$ . If  $\{e_1, \dots, e_r\}$  is a basis of  $B$  over  $R$ , then

$$1_A \otimes e_1, \dots, 1_A \otimes e_r$$

is a basis of  $A \otimes B$  over  $A$ . We may then define the **norm**

$$N = N_{A \otimes B, A} : A \otimes B \rightarrow A$$

as the unique map which coincides with the determinant of the regular representation.

In other words, if  $b \in B$  and  $b_B$  denotes multiplication by  $b$ , then

$$N_{B, R}(b) = \det(b_B);$$

and similarly after extension of the base. Prove:

- (a) Let  $\varphi : A \rightarrow C$  be a homomorphism of  $R$ -algebras. Then the following diagram is commutative:

$$\begin{array}{ccc} A \otimes B & \xrightarrow{\varphi \otimes \text{id}} & C \otimes B \\ \downarrow N & & \downarrow N \\ A & \xrightarrow{\varphi} & C \end{array}$$

- (b) Let  $x, y \in A \otimes B$ . Then  $N(x \otimes_B y) = N(x) \otimes N(y)$ . [Hint: Use the commutativity relations  $e_i e_j = e_j e_i$  and the associativity.]

### A little flatness

6. Let  $M, N$  be flat. Show that  $M \otimes N$  is flat.
7. Let  $F$  be a flat  $R$ -module, and let  $a \in R$  be an element which is not a zero-divisor. Show that if  $ax = 0$  for some  $x \in F$  then  $x = 0$ .
8. Prove Proposition 3.2.

### Faithfully flat

9. We continue to assume that rings are commutative. Let  $M$  be an  $A$ -module. We say that  $M$  is **faithfully flat** if  $M$  is flat, and if the functor

$$T_M : E \mapsto M \otimes_A E.$$

is faithful, that is  $E \neq 0$  implies  $M \otimes_A E \neq 0$ . Prove that the following conditions are equivalent.

- (i)  $M$  is faithfully flat.
- (ii)  $M$  is flat, and if  $u : F \rightarrow E$  is a homomorphism of  $A$ -modules,  $u \neq 0$ , then  $T_M(u) : M \otimes_A F \rightarrow M \otimes_A E$  is also  $\neq 0$ .
- (iii)  $M$  is flat, and for all maximal ideals  $\mathfrak{m}$  of  $A$ , we have  $\mathfrak{m}M \neq M$ .
- (iv) A sequence of  $A$ -modules  $N' \rightarrow N \rightarrow N''$  is exact if and only if the sequence tensored with  $M$  is exact.
10. (a) Let  $A \rightarrow B$  be a ring-homomorphism. If  $M$  is faithfully flat over  $A$ , then  $B \otimes_A M$  is faithfully flat over  $B$ .
- (b) Let  $M$  be faithfully flat over  $B$ . Then  $M$  viewed as  $A$ -module via the homomorphism  $A \rightarrow B$  is faithfully flat over  $A$  if  $B$  is faithfully flat over  $A$ .
11. Let  $P, M, E$  be modules over the commutative ring  $A$ . If  $P$  is finitely generated (resp. finitely presented) and  $E$  is flat, show that the natural homomorphism

$$\text{Hom}_A(P, M) \otimes_A E \rightarrow \text{Hom}_A(P, M \otimes_A E)$$

is a monomorphism (resp. an isomorphism).

[Hint: Let  $F_1 \rightarrow F_0 \rightarrow P \rightarrow 0$  be a finite presentation, say. Consider the diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{Hom}_A(P, M) \otimes_A E & \longrightarrow & \text{Hom}_A(F_0, M) \otimes_A E & \longrightarrow & \text{Hom}_A(F_1, M) \otimes_A E \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \text{Hom}_A(P, M \otimes_A E) & \longrightarrow & \text{Hom}_A(F_0, M \otimes_A E) & \longrightarrow & \text{Hom}_A(F_1, M \otimes_A E).
 \end{array}$$

### Tensor products and direct limits

12. Show that the tensor product commutes with direct limits. In other words, if  $\{E_i\}$  is a directed family of modules, and  $M$  is any module, then there is a natural isomorphism

$$\varinjlim(E_i \otimes_A M) \approx (\varinjlim E_i) \otimes_A M.$$

13. (D. Lazard) Let  $E$  be a module over a commutative ring  $A$ . Tensor products are all taken over that ring. Show that the following conditions are equivalent:

(i) There exists a direct family  $\{F_i\}$  of free modules of finite type such that

$$E \approx \varinjlim F_i.$$

(ii)  $E$  is flat.

(iii) For every finitely presented module  $P$  the natural homomorphism

$$\text{Hom}_A(P, A) \otimes_A E \rightarrow \text{Hom}_A(P, E)$$

is surjective.

(iv) For every finitely presented module  $P$  and homomorphism  $f: P \rightarrow E$  there exists a free module  $F$ , finitely generated, and homomorphisms

$$g: P \rightarrow F \quad \text{and} \quad h: F \rightarrow E$$

such that  $f = h \circ g$ .

**Remark.** The point of Lazard's theorem lies in the first two conditions:  $E$  is flat if and only if  $E$  is a direct limit of free modules of finite type.

[Hint: Since the tensor product commutes with direct limits, that (i) implies (ii) comes from the preceding exercise and the definition of flat.

To show that (ii) implies (iii), use Exercise 11.

To show that (iii) implies (iv) is easy from the hypothesis.

To show that (iv) implies (i), use the fact that a module is a direct limit of finitely presented modules (an exercise in Chapter III), and (iv) to get the free modules instead. For complete details, see for instance Bourbaki, *Algèbre*, Chapter X, §1, Theorem 1, p. 14.]

### The Casimir element

14. Let  $k$  be a commutative field and let  $E$  be a vector space over  $k$ , of finite dimension  $n$ . Let  $B$  be a nondegenerate symmetric bilinear form on  $E$ , inducing an iso-

morphism  $E \rightarrow E^\vee$  of  $E$  with its dual space. Let  $\{v_1, \dots, v_n\}$  be a basis of  $E$ . The  $B$ -dual basis  $\{v'_1, \dots, v'_n\}$  consists of the elements of  $E$  such that  $B(v_i, v'_j) = \delta_{ij}$ .

- (a) Show that the element  $\sum v_i \otimes v'_i$  in  $E \otimes E$  is independent of the choice of basis. We call this element the **Casimir element** (see below).
- (b) In the symmetric algebra  $S(E)$ , let  $Q_B = \sum v_i v'_i$ . Show that  $Q_B$  is independent of the choice of basis. We call  $Q_B$  the **Casimir polynomial**. It depends on  $B$ , of course.
- (c) More generally, let  $\mathbf{D}$  be an (associative) algebra over  $k$ , let  $\mathcal{D}: E \rightarrow \mathbf{D}$  be an injective linear map of  $E$  into  $\mathbf{D}$ . Show that the element  $\sum \mathcal{D}(v_i) \mathcal{D}(v'_i) = \omega_{B, \mathcal{D}}$  is independent of the choice of basis. We call it the **Casimir element** in  $\mathbf{D}$ , determined by  $\mathcal{D}$  and  $B$ .

**Remark.** The terminology of the Casimir element is determined by the classical case, when  $G$  is a Lie group,  $E = \mathfrak{g} = \text{Lie}(G)$  is the Lie algebra of  $G$  (tangent space at the origin with the Lie algebra product determined by the Lie derivative), and  $\mathcal{D}(v)$  is the differential operator associated with  $v$  (Lie derivative in the direction of  $v$ ). The Casimir element is then a partial differential operator in the algebra of all differential operators on  $G$ . Cf. basic books on manifolds and Lie theory, for instance [JoL 01], Chapter II, §1 and Chapter VII, §2.

15. Let  $E = \mathfrak{sl}_n(k) =$  subspace of  $\text{Mat}_n(k)$  consisting of matrices with trace 0. Let  $B$  be the bilinear form defined by  $B(X, Y) = \text{tr}(XY)$ . Let  $G = \text{SL}_n(k)$ . Prove:
- (a)  $B$  is  $c(G)$ -invariant, where  $c(g)$  is conjugation by an element  $g \in G$ .
  - (b)  $B$  is invariant under the transpose  $(X, Y) \mapsto ({}^t X, {}^t Y)$ .
  - (c) Let  $k = \mathbb{R}$ . Then  $B$  is positive definite on the symmetric matrices and negative definite on the skew-symmetric matrices.
  - (d) Suppose  $G$  is given with an action on the algebra  $\mathbf{D}$  of Exercise 14, and that the linear map  $\mathcal{D}: E \rightarrow \mathbf{D}$  is  $G$ -linear. Show that the Casimir element is  $G$ -invariant (for the conjugation action on  $S(E)$ , and the given action on  $\mathbf{D}$ ).

---

# CHAPTER XVII

---

## Semisimplicity

In many applications, a module decomposes as a direct sum of simple submodules, and then one can develop a fairly precise structure theory, both under general assumptions, and particular applications. This chapter is devoted to those results which can be proved in general. In the next chapter, we consider those additional results which can be proved in a classical and important special case.

I have more or less followed Bourbaki in the proof of Jacobson's density theorem.

---

### §1. MATRICES AND LINEAR MAPS OVER NON-COMMUTATIVE RINGS

In Chapter XIII, we considered exclusively matrices over commutative rings. For our present purposes, it is necessary to consider a more general situation.

Let  $K$  be a ring. We define a matrix  $(\varphi_{ij})$  with coefficients in  $K$  just as we did for commutative rings. The product of matrices is defined by the same formula. Then we again have associativity and distributivity, whenever the size of the matrices involved in the operations makes the operations defined. In particular, the square  $n \times n$  matrices over  $K$  form a ring, again denoted by  $\text{Mat}_n(K)$ . We have a ring-homomorphism

$$K \rightarrow \text{Mat}_n(K)$$

on the diagonal.

By a **division ring** we shall mean a ring with  $1 \neq 0$ , and such that every non-zero element has a multiplicative inverse.

If  $K$  is a division ring, then every non-zero  $K$ -module has a basis, and the cardinalities of two bases are equal. The proof is the same as in the commutative case; we never needed commutativity in the arguments. This cardinality is again called the dimension of the module over  $K$ , and a module over a division ring is called a vector space.

We can associate a matrix with linear maps, depending on the choice of a finite basis, just as in the commutative case. However, we shall consider a somewhat different situation which we want to apply to semisimple modules.

Let  $R$  be a ring, and let

$$E = E_1 \oplus \cdots \oplus E_n, \quad F = F_1 \oplus \cdots \oplus F_m$$

be  $R$ -modules, expressed as direct sums of  $R$ -submodules. We wish to describe the most general  $R$ -homomorphism of  $E$  into  $F$ .

Suppose first  $F = F_1$  has one component. Let

$$\varphi : E_1 \oplus \cdots \oplus E_n \rightarrow F$$

be a homomorphism. Let  $\varphi_j : E_j \rightarrow F$  be the restriction of  $\varphi$  to the factor  $E_j$ . Every element  $x \in E$  has a unique expression  $x = x_1 + \cdots + x_n$ , with  $x_j \in E_j$ . We may therefore associate with  $x$  the column vector  $X = {}^t(x_1, \dots, x_n)$ , whose components are in  $E_1, \dots, E_n$  respectively. We can associate with  $\varphi$  the row vector  $(\varphi_1, \dots, \varphi_n)$ ,  $\varphi_j \in \text{Hom}_R(E_j, F)$ , and the effect of  $\varphi$  on the element  $x$  of  $E$  is described by matrix multiplication, of the row vector times the column vector.

More generally, consider a homomorphism

$$\varphi : E_1 \oplus \cdots \oplus E_n \rightarrow F_1 \oplus \cdots \oplus F_m.$$

Let  $\pi_i : F_1 \oplus \cdots \oplus F_m \rightarrow F_i$  be the projection on the  $i$ -th factor. Then we can apply our previous remarks to  $\pi_i \circ \varphi$ , for each  $i$ . In this way, we see that there exist unique elements  $\varphi_{ij} \in \text{Hom}_R(E_j, F_i)$ , such that  $\varphi$  has a matrix representation

$$M(\varphi) = \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix}$$

whose effect on an element  $x$  is given by matrix multiplication, namely

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Conversely, given a matrix  $(\varphi_{ij})$  with  $\varphi_{ij} \in \text{Hom}_R(E_j, F_i)$ , we can define an element of  $\text{Hom}_R(E, F)$  by means of this matrix. We have an additive group-isomorphism between  $\text{Hom}_R(E, F)$  and this group of matrices.

*In particular, let  $E$  be a fixed  $R$ -module, and let  $K = \text{End}_R(E)$ . Then we have a ring-isomorphism*

$$\text{End}_R(E^{(n)}) \rightarrow \text{Mat}_n(K)$$

*which to each  $\varphi \in \text{End}_R(E^{(n)})$  associates the matrix*

$$\begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \vdots \\ \varphi_{n1} & \cdots & \varphi_{nn} \end{pmatrix}$$

*determined as before, and operating on the left on column vectors of  $E^{(n)}$ , with components in  $E$ .*

**Remark.** Let  $E$  be a 1-dimensional vector space over a division ring  $D$ , and let  $\{v\}$  be a basis. For each  $a \in D$ , there exists a unique  $D$ -linear map  $f_a : E \rightarrow E$  such that  $f_a(v) = av$ . Then we have the rule

$$f_a f_b = f_{ba}.$$

Thus when we associate a matrix with a linear map, depending on a basis, the multiplication gets twisted. Nevertheless, the statement we just made preceding this remark is correct!! The point is that we took the  $\varphi_{ij}$  in  $\text{End}_R(E)$ , and not in  $D$ , in the special case that  $R = D$ . Thus  $K$  is not isomorphic to  $D$  (in the non-commutative case), but anti-isomorphic. This is the only point of difference of the formal elementary theory of linear maps in the commutative or non-commutative case.

We recall that an  $R$ -module  $E$  is said to be **simple** if it is  $\neq 0$  and if it has no submodule other than 0 or  $E$ .

**Proposition 1.1. Schur's Lemma.** *Let  $E, F$  be simple  $R$ -modules. Every non-zero homomorphism of  $E$  into  $F$  is an isomorphism. The ring  $\text{End}_R(E)$  is a division ring.*

*Proof.* Let  $f : E \rightarrow F$  be a non-zero homomorphism. Its image and kernel are submodules, hence  $\text{Ker } f = 0$  and  $\text{Im } f = F$ . Hence  $f$  is an isomorphism. If  $E = F$ , then  $f$  has an inverse, as desired.

The next proposition describes completely the ring of endomorphisms of a direct sum of simple modules.

**Proposition 1.2.** *Let  $E = E_1^{(n_1)} \oplus \cdots \oplus E_r^{(n_r)}$  be a direct sum of simple modules, the  $E_i$  being non-isomorphic, and each  $E_i$  being repeated  $n_i$  times in*

the sum. Then, up to a permutation,  $E_1, \dots, E_r$  are uniquely determined up to isomorphisms, and the multiplicities  $n_1, \dots, n_r$  are uniquely determined. The ring  $\text{End}_R(E)$  is isomorphic to a ring of matrices, of type

$$\begin{pmatrix} M_1 & & \cdots & 0 \\ \vdots & M_2 & \ddots & \vdots \\ 0 & & \cdots & M_r \end{pmatrix}$$

where  $M_i$  is an  $n_i \times n_i$  matrix over  $\text{End}_R(E_i)$ . (The isomorphism is the one with respect to our direct sum decomposition.)

*Proof.* The last statement follows from our previous considerations, taking into account Proposition 1.1.

Suppose now that we have two  $R$ -modules, with direct sum decompositions into simple submodules, and an isomorphism

$$E_1^{(n_1)} \oplus \cdots \oplus E_r^{(n_r)} \rightarrow F_1^{(m_1)} \oplus \cdots \oplus F_s^{(m_s)},$$

such that the  $E_i$  are non-isomorphic, and the  $F_j$  are non-isomorphic. From Proposition 1.1, we conclude that each  $E_i$  is isomorphic to some  $F_j$ , and conversely. It follows that  $r = s$ , and that after a permutation,  $E_i \approx F_i$ . Furthermore, the isomorphism must induce an isomorphism

$$E_i^{(n_i)} \rightarrow F_i^{(m_i)}$$

for each  $i$ . Since  $E_i \approx F_i$ , we may assume without loss of generality that in fact  $E_i = F_i$ . Thus we are reduced to proving: If a module is isomorphic to  $E^{(n)}$  and to  $E^{(m)}$ , with some simple module  $E$ , then  $n = m$ . But  $\text{End}_R(E^{(n)})$  is isomorphic to the  $n \times n$  matrix ring over the division ring  $\text{End}_R(E) = K$ . Furthermore this isomorphism is verified at once to be an isomorphism as  $K$ -vector space. The dimension of the space of  $n \times n$  matrices over  $K$  is  $n^2$ . This proves that the multiplicity  $n$  is uniquely determined, and proves our proposition.

When  $E$  admits a (finite) direct sum decomposition of simple submodules, the number of times that a simple module of a given isomorphism class occurs in a decomposition will be called the **multiplicity** of the simple module (or of the isomorphism class of the simple module).

Furthermore, if

$$E = E_1^{(n_1)} \oplus \cdots \oplus E_r^{(n_r)}$$

is expressed as a sum of simple submodules, we shall call  $n_1 + \cdots + n_r$  the **length** of  $E$ . In many applications, we shall also write

$$E = n_1 E_1 \oplus \cdots \oplus n_r E_r = \bigoplus_{i=1}^r n_i E_i.$$

---

## §2. CONDITIONS DEFINING SEMISIMPLICITY

Let  $R$  be a ring. Unless otherwise specified in this section all modules and homomorphisms will be  $R$ -modules and  $R$ -homomorphisms.

The following conditions on a module  $E$  are equivalent:

**SS 1.**  $E$  is the sum of a family of simple submodules.

**SS 2.**  $E$  is the direct sum of a family of simple submodules.

**SS 3.** Every submodule  $F$  of  $E$  is a direct summand, i.e. there exists a submodule  $F'$  such that  $E = F \oplus F'$ .

We shall now prove that these three conditions are equivalent.

**Lemma 2.1.** *Let  $E = \sum_{i \in I} E_i$  be a sum (not necessarily direct) of simple submodules. Then there exists a subset  $J \subset I$  such that  $E$  is the direct sum  $\bigoplus_{j \in J} E_j$ .*

*Proof.* Let  $J$  be a maximal subset of  $I$  such that the sum  $\sum_{j \in J} E_j$  is direct.

We contend that this sum is in fact equal to  $E$ . It will suffice to prove that each  $E_i$  is contained in this sum. But the intersection of our sum with  $E_i$  is a submodule of  $E_i$ , hence equal to 0 or  $E_i$ . If it is equal to 0, then  $J$  is not maximal, since we can adjoin  $i$  to it. Hence  $E_i$  is contained in the sum, and our lemma is proved.

The lemma shows that **SS 1** implies **SS 2**. To see that **SS 2** implies **SS 3**, take a submodule  $F$ , and let  $J$  be a maximal subset of  $I$  such that the sum  $F + \bigoplus_{j \in J} E_j$  is direct. The same reasoning as before shows that this sum is equal to  $E$ .

Finally assume **SS3**. To show **SS 1**, we shall first prove that every non-zero submodule of  $E$  contains a simple submodule. Let  $v \in E$ ,  $v \neq 0$ . Then by definition,  $Rv$  is a principal submodule, and the kernel of the homomorphism

$$R \rightarrow Rv$$

is a left ideal  $L \neq R$ . Hence  $L$  is contained in a maximal left ideal  $M \neq R$  (by Zorn's lemma). Then  $M/L$  is a maximal submodule of  $R/L$  (unequal to  $R/L$ ), and hence  $Mv$  is a maximal submodule of  $Rv$ , unequal to  $Rv$ , corresponding to  $M/L$  under the isomorphism

$$R/L \rightarrow Rv.$$

We can write  $E = Mv \oplus M'$  with some submodule  $M'$ . Then

$$Rv = Mv \oplus (M' \cap Cv),$$

because every element  $x \in Cv$  can be written uniquely as a sum  $x = \alpha v + x'$  with  $\alpha \in M$  and  $x' \in M'$ , and  $x' = x - \alpha v$  lies in  $Cv$ . Since  $Mv$  is maximal in  $Cv$ , it follows that  $M' \cap Cv$  is simple, as desired.

Let  $E_0$  be the submodule of  $E$  which is the sum of all simple submodules of  $E$ . If  $E_0 \neq E$ , then  $E = E_0 \oplus F$  with  $F \neq 0$ , and there exists a simple submodule of  $F$ , contradicting the definition of  $E_0$ . This proves that **SS 3** implies **SS 1**.

A module  $E$  satisfying our three conditions is said to be **semisimple**.

**Proposition 2.2.** *Every submodule and every factor module of a semisimple module is semisimple.*

*Proof.* Let  $F$  be a submodule. Let  $F_0$  be the sum of all simple submodules of  $F$ . Write  $F = F_0 \oplus F'$ . Every element  $x$  of  $F$  has a unique expression  $x = x_0 + x'_0$  with  $x_0 \in F_0$  and  $x'_0 \in F'$ . But  $x'_0 = x - x_0 \in F$ . Hence  $F$  is the direct sum

$$F = F_0 \oplus (F \cap F').$$

We must therefore have  $F_0 = F$ , which is semisimple. As for the factor module, write  $E = F \oplus F'$ . Then  $F'$  is a sum of its simple submodules, and the canonical map  $E \rightarrow E/F$  induces an isomorphism of  $F'$  onto  $E/F$ . Hence  $E/F$  is semisimple.

### §3. THE DENSITY THEOREM

Let  $E$  be a semisimple  $R$ -module. Let  $R' = R'(E)$  be the ring  $\text{End}_R(E)$ . Then  $E$  is also a  $R'$ -module, the operation of  $R'$  on  $E$  being given by

$$(\varphi, x) \mapsto \varphi(x)$$

for  $\varphi \in R'$  and  $x \in E$ . Each  $\alpha \in R$  induces a  $R'$ -homomorphism  $f_\alpha: E \rightarrow E$  by the map  $f_\alpha(x) = \alpha x$ . This is what is meant by the condition

$$\varphi(\alpha x) = \alpha \varphi(x).$$

We let  $R'' = R''(E) = \text{End}_{R'}(E)$ . We call  $R'$  the **commutant** of  $R$  and  $R''$  the **bicommutant**. Thus we get a ring-homomorphism

$$R \rightarrow \text{End}_{R'}(E) = R''(E) = R''$$

by  $\alpha \mapsto f_\alpha$ . We now ask how big is the image of this ring-homomorphism. The density theorem states that it is quite big.

**Lemma 3.1.** *Let  $E$  be semisimple over  $R$ . Let  $R' = \text{End}_R(E)$ ,  $f \in \text{End}_{R'}(E)$  as above. Let  $x \in R$ . There exists an element  $\alpha \in R$  such that  $\alpha x = f(x)$ .*

*Proof.* Since  $E$  is semisimple, we can write an  $R$ -direct sum

$$E = Rx \oplus F$$

with some submodule  $F$ . Let  $\pi: E \rightarrow Rx$  be the projection. Then  $\pi \in R'$ , and hence

$$f(x) = f(\pi x) = \pi f(x).$$

This shows that  $f(x) \in Rx$ , as desired.

The density theorem generalizes the lemma by dealing with a finite number of elements of  $E$  instead of just one. For the proof, we use a diagonal trick.

**Theorem 3.2. (Jacobson).** *Let  $E$  be semisimple over  $R$ , and let  $R' = \text{End}_R(E)$ . Let  $f \in \text{End}_{R'}(E)$ . Let  $x_1, \dots, x_n \in E$ . Then there exists an element  $\alpha \in R$  such that*

$$\alpha x_i = f(x_i) \quad \text{for } i = 1, \dots, n.$$

*If  $E$  is finitely generated over  $R'$ , then the natural map  $R \rightarrow \text{End}_{R'}(E)$  is surjective.*

*Proof.* For clarity of notation, we shall first carry out the proof in case  $E$  is simple. Let  $f^{(n)}: E^{(n)} \rightarrow E^{(n)}$  be the product map, so that

$$f^{(n)}(y_1, \dots, y_n) = (f(y_1), \dots, f(y_n)).$$

Let  $R'_n = \text{End}_R(E^{(n)})$ . Then  $R'_n$  is none other than the ring of matrices with coefficients in  $R'$ . Since  $f$  commutes with elements of  $R'$  in its action on  $E$ , one sees immediately that  $f^{(n)}$  is in  $\text{End}_{R'_n}(E^{(n)})$ . By the lemma, there exists an element  $\alpha \in R$  such that

$$(\alpha x_1, \dots, \alpha x_n) = (f(x_1), \dots, f(x_n)),$$

which is what we wanted to prove.

When  $E$  is not simple, suppose that  $E$  is equal to a finite direct sum of simple submodules  $E_i$  (non-isomorphic), with multiplicities  $n_i$ :

$$E = E_1^{(n_1)} \oplus \cdots \oplus E_r^{(n_r)} \quad (E_i \not\approx E_j \quad \text{if } i \neq j),$$

then the matrices representing the ring of endomorphisms split according to blocks corresponding to the non-isomorphic simple components in our direct sum decomposition. Hence here again the argument goes through as before.

The main point is that  $f^{(n)}$  lies in  $\text{End}_{R'}(E^{(n)})$ , and that we can apply the lemma.

We add the observation that if  $E$  is finitely generated over  $R'$ , then an element  $f \in \text{End}_{R'}(E)$  is determined by its value on a finite number of elements of  $E$ , so the asserted surjectivity  $R \rightarrow \text{End}_{R'}(E)$  follows at once. In the applications below,  $E$  will be a finite dimensional vector space over a field  $k$ , and  $R$  will be a  $k$ -algebra, so the finiteness condition is automatically satisfied.

The argument when  $E$  is an infinite direct sum would be similar, but the notation is disagreeable. However, in the applications we shall never need the theorem in any case other than the case when  $E$  itself is a finite direct sum of simple modules, and this is the reason why we first gave the proof in that case, and let the reader write out the formal details in the other cases, if desired.

**Corollary 3.3. (Burnside's Theorem).** *Let  $E$  be a finite-dimensional vector space over an algebraically closed field  $k$ , and let  $R$  be a subalgebra of  $\text{End}_k(E)$ . If  $E$  is a simple  $R$ -module, then  $R = \text{End}_{R'}(E)$ .*

*Proof.* We contend that  $\text{End}_R(E) = k$ . At any rate,  $\text{End}_R(E)$  is a division ring  $R'$ , containing  $k$  as a subring and every element of  $k$  commutes with every element of  $R'$ . Let  $\alpha \in R'$ . Then  $k(\alpha)$  is a field. Furthermore,  $R'$  is contained in  $\text{End}_k(E)$  as a  $k$ -subspace, and is therefore finite dimensional over  $k$ . Hence  $k(\alpha)$  is finite over  $k$ , and therefore equal to  $k$  since  $k$  is algebraically closed. This proves that  $\text{End}_R(E) = k$ . Let now  $\{v_1, \dots, v_n\}$  be a basis of  $E$  over  $k$ . Let  $A \in \text{End}_k(E)$ . According to the density theorem, there exists  $\alpha \in R$  such that

$$\alpha v_i = A v_i \quad \text{for } i = 1, \dots, n.$$

Since the effect of  $A$  is determined by its effect on a basis, we conclude that  $R = \text{End}_k(E)$ .

Corollary 3.3 is used in the following situation as in Exercise 8. Let  $E$  be a finite-dimensional vector space over field  $k$ . Let  $G$  be a submonoid of  $GL(E)$  (multiplicative). A  **$G$ -invariant** subspace  $F$  of  $E$  is a subspace such that  $\sigma F \subset F$  for all  $\sigma \in G$ . We say that  $E$  is  **$G$ -simple** if it has no  $G$ -invariant subspace other than 0 and  $E$  itself, and  $E \neq 0$ . Let  $R = k[G]$  be the subalgebra of  $\text{End}_k(E)$  generated by  $G$  over  $k$ . Since we assumed that  $G$  is a monoid, it follows that  $R$  consists of linear combinations

$$\sum a_i \sigma_i$$

with  $a_i \in k$  and  $\sigma_i \in G$ . Then we see that a subspace  $F$  of  $E$  is  $G$ -invariant if and only if it is  $R$ -invariant. Thus  $E$  is  $G$ -simple if and only if it is simple over  $R$  in the sense which we have been considering. We can then restate Burnside's theorem as he stated it:

**Corollary 3.4.** *Let  $E$  be a finite dimensional vector space over an algebraically closed field  $k$ , and let  $G$  be a (multiplicative) submonoid of  $GL(E)$ .*

If  $E$  is  $G$ -simple, then  $k[G] = \text{End}_k(E)$ .

When  $k$  is not algebraically closed, then we still get some result. Quite generally, let  $R$  be a ring and  $E$  a simple  $R$ -module. We have seen that  $\text{End}_R(E)$  is a division ring, which we denote by  $D$ , and  $E$  is a vector space over  $D$ .

Let  $R$  be a ring, and  $E$  any  $R$ -module. We shall say that  $E$  is a **faithful** module if the following condition is satisfied. Given  $\alpha \in R$  such that  $\alpha x = 0$  for all  $x \in E$ , we have  $\alpha = 0$ . In the applications,  $E$  is a vector space over a field  $k$ , and we have a ring-homomorphism of  $R$  into  $\text{End}_k(E)$ . In this way,  $E$  is an  $R$ -module, and it is faithful if and only if this homomorphism is injective.

**Corollary 3.5. (Wedderburn's Theorem).** *Let  $R$  be a ring, and  $E$  a simple, faithful module over  $R$ . Let  $D = \text{End}_R(E)$ , and assume that  $E$  is finite dimensional over  $D$ . Then  $R = \text{End}_D(E)$ .*

*Proof.* Let  $\{v_1, \dots, v_n\}$  be a basis of  $E$  over  $D$ . Given  $A \in \text{End}_D(E)$ , by Theorem 3.2 there exists  $\alpha \in R$  such that

$$\alpha v_i = Av_i \quad \text{for } i = 1, \dots, n.$$

Hence the map  $R \rightarrow \text{End}_D(E)$  is surjective. Our assumption that  $E$  is faithful over  $R$  implies that it is injective, and our corollary is proved.

**Example.** Let  $R$  be a finite-dimensional algebra over a field  $k$ , and assume that  $R$  has a unit element, so is a ring. If  $R$  does not have any two-sided ideals other than 0 and  $R$  itself, then any nonzero module  $E$  over  $R$  is faithful, because the kernel of the homomorphism

$$R \rightarrow \text{End}_k(E)$$

is a two-sided ideal  $\neq R$ . If  $E$  is simple, then  $E$  is finite dimensional over  $k$ . Then  $D$  is a finite-dimensional division algebra over  $k$ . Wedderburn's theorem gives a representation of  $R$  as the ring of  $D$ -endomorphisms of  $E$ .

Under the assumption that  $R$  is finite dimensional, one can find a simple module simply by taking a minimal left ideal  $\neq 0$ . Such an ideal exists merely by taking a left ideal of minimal non-zero dimension over  $k$ . An even shorter proof of Wedderburn's theorem will be given below (Rieffel's theorem) in this case.

**Corollary 3.6.** *Let  $R$  be a ring, finite dimensional algebra over a field  $k$  which is algebraically closed. Let  $V$  be a finite dimensional vector space over  $k$ , with a simple faithful representation  $\rho: R \rightarrow \text{End}_k(V)$ . Then  $\rho$  is an isomorphism, in other words,  $R \approx \text{Mat}_n(k)$ .*

*Proof.* We apply Corollary 3.5, noting that  $D$  is finite dimensional over  $k$ . Given  $\alpha \in D$ , we note that  $k(\alpha)$  is a commutative subfield of  $D$ , whence  $k(\alpha) = k$  by assumption that  $k$  is algebraically closed, and the corollary follows.

**Note.** The corollary applies to simple rings, which will be defined below.

Suppose next that  $V_1, \dots, V_m$  are finite dimensional vector spaces over a field  $k$ , and that  $R$  is a  $k$ -algebra with representations

$$R \rightarrow \text{End}_k(V_i), \quad i = 1, \dots, m,$$

so  $V_i$  is an  $R$ -module. If we let

$$E = V_1 \oplus \dots \oplus V_m,$$

then  $E$  is finite over  $R'(E)$ , so we get the following consequence of Jacobson's density theorem.

**Theorem 3.7. Existence of projection operators.** *Let  $k$  be a field,  $R$  a  $k$ -algebra, and  $V_1, \dots, V_m$  finite dimensional  $k$ -spaces which are also simple  $R$ -modules, and such that  $V_i$  is not  $R$ -isomorphic to  $V_j$  for  $i \neq j$ . Then there exist elements  $e_i \in R$  such that  $e_i$  acts as the identity on  $V_i$  and  $e_i V_j = 0$  if  $j \neq i$ .*

*Proof.* We observe that the projection  $f_i$  from the direct sum  $E$  to the  $i$ -th factor is in  $\text{End}_{R'}(E)$ , because if  $\varphi \in R'$  then  $\varphi(V_j) \subset V_j$  for all  $j$ . We may therefore apply the density theorem to conclude the proof.

**Corollary 3.8. (Bourbaki).** *Let  $k$  be a field of characteristic 0. Let  $R$  be a  $k$ -algebra, and let  $E, F$  be semisimple  $R$ -modules, finite dimensional over  $k$ . For each  $\alpha \in R$ , let  $\alpha_E, \alpha_F$  be the corresponding  $k$ -endomorphisms on  $E$  and  $F$  respectively. Suppose that the traces are equal; that is,*

$$\text{tr}(\alpha_E) = \text{tr}(\alpha_F) \text{ for all } \alpha \in R.$$

*Then  $E$  is isomorphic to  $F$  as  $R$ -module.*

*Proof.* Each of  $E$  and  $F$  is isomorphic to a finite direct sum of simple  $R$ -modules, with certain multiplicities. Let  $V$  be a simple  $R$ -module, and suppose

$$E = V^{(n)} \oplus \text{direct summands not isomorphic to } V$$

$$F = V^{(m)} \oplus \text{direct summands not isomorphic to } V.$$

It will suffice to prove that  $m = n$ . Let  $e_V$  be the element of  $R$  found in Theorem 3.7 such that  $e_V$  acts as the identity on  $V$ , and is 0 on the other direct summands of  $E$  and  $F$ . Then

$$\text{tr}(e_E) = n \dim_k(V) \quad \text{and} \quad \text{tr}(e_F) = m \dim_k(V).$$

Since the traces are equal by assumption, it follows that  $m = n$ , thus concluding the proof. Note that the characteristic 0 is used here, because the values of the trace are in  $k$ .

**Example.** In the language of representations, suppose  $G$  is a monoid, and

we have two semisimple representations into finite dimensional  $k$ -spaces

$$\rho : G \rightarrow \text{End}_k(E) \quad \text{and} \quad \rho' : G \rightarrow \text{End}_k(F)$$

(so  $\rho$  and  $\rho'$  map  $G$  into the multiplicative monoid of  $\text{End}_k$ ). Assume that  $\text{tr } \rho(\sigma) = \text{tr } \rho'(\sigma)$  for all  $\sigma \in G$ . Then  $\rho$  and  $\rho'$  are isomorphic. Indeed, we let  $R = k[G]$ , so that  $\rho$  and  $\rho'$  extend to representations of  $R$ . By linearity, one has that  $\text{tr } \rho(\alpha) = \text{tr } \rho'(\alpha)$  for all  $\alpha \in R$ , so one can apply Corollary 3.8.

## §4. SEMISIMPLE RINGS

A ring  $R$  is called **semisimple** if  $1 \neq 0$ , and if  $R$  is semisimple as a left module over itself.

**Proposition 4.1.** *If  $R$  is semisimple, then every  $R$ -module is semisimple.*

*Proof.* An  $R$ -module is a factor module of a free module, and a free module is a direct sum of  $R$  with itself a certain number of times. We can apply Proposition 2.2 to conclude the proof.

**Examples.** 1) Let  $k$  be a field and let  $R = \text{Mat}_n(k)$  be the algebra of  $n \times n$  matrices over  $k$ . Then  $R$  is semisimple, and actually simple, as we shall define and prove in §5, Theorem 5.5.

2) Let  $G$  be a finite group and suppose that the characteristic of  $k$  does not divide  $\#(G)$ . Then the group ring  $k[G]$  is semisimple, as we shall prove in Chapter XVIII, Theorem 1.2.

3) The Clifford algebras  $C_n$  over the real numbers are semisimple. See Exercise 19 of Chapter XIX.

A left ideal of  $R$  is an  $R$ -module, and is thus called simple if it is simple as a module. Two ideals  $L, L'$  are called isomorphic if they are isomorphic as modules.

We shall now decompose  $R$  as a sum of its simple left ideals, and thereby get a structure theorem for  $R$ .

Let  $\{L_i\}_{i \in I}$  be a family of simple left ideals, no two of which are isomorphic, and such that each simple left ideal is isomorphic to one of them. We say that this family is a family of representatives for the isomorphism classes of simple left ideals.

**Lemma 4.2.** *Let  $L$  be a simple left ideal, and let  $E$  be a simple  $R$ -module. If  $L$  is not isomorphic to  $E$ , then  $LE = 0$ .*

*Proof.* We have  $RLE = LE$ , and  $LE$  is a submodule of  $E$ , hence equal to

0 or  $E$ . Suppose  $LE = E$ . Let  $y \in E$  be such that

$$Ly \neq 0.$$

Since  $Ly$  is a submodule of  $E$ , it follows that  $Ly = E$ . The map  $\alpha \mapsto \alpha y$  of  $L$  into  $E$  is a homomorphism of  $L$  into  $E$ , which is surjective, and hence nonzero. Since  $L$  is simple, this homomorphism is an isomorphism.

Let

$$R_i = \sum_{L \cong L_i} L$$

be the sum of all simple left ideals isomorphic to  $L_i$ . From the lemma, we conclude that  $R_i R_j = 0$  if  $i \neq j$ . This will be used constantly in what follows. We note that  $R_i$  is a left ideal, and that  $R$  is the sum

$$R = \sum_{i \in I} R_i,$$

because  $R$  is a sum of simple left ideals. Hence for any  $j \in I$ ,

$$R_j \subset R_j R = R_j R_j \subset R_j,$$

the first inclusion because  $R$  contains a unit element, and the last because  $R_j$  is a left ideal. We conclude that  $R_j$  is also a right ideal, i.e.  $R_j$  is a two-sided ideal for all  $j \in I$ .

We can express the unit element 1 of  $R$  as a sum

$$1 = \sum_{i \in I} e_i$$

with  $e_i \in R_i$ . This sum is actually finite, almost all  $e_i = 0$ . Say  $e_i \neq 0$  for indices  $i = 1, \dots, s$ , so that we write

$$1 = e_1 + \dots + e_s.$$

For any  $x \in R$ , write

$$x = \sum_{i \in I} x_i, \quad x_i \in R_i.$$

For  $j = 1, \dots, s$  we have  $e_j x = e_j x_j$  and also

$$x_j = 1 \cdot x_j = e_1 x_j + \dots + e_s x_j = e_j x_j.$$

Furthermore,  $x = e_1 x + \dots + e_s x$ . This proves that there is no index  $i$  other than  $i = 1, \dots, s$  and also that the  $i$ -th component  $x_i$  of  $x$  is uniquely determined as  $e_i x = e_i x_i$ . Hence the sum  $R = R_1 + \dots + R_s$  is direct, and furthermore,  $e_i$  is a unit element for  $R_i$ , which is therefore a ring. Since

$R_i R_j = 0$  for  $i \neq j$ , we find that in fact

$$R = \prod_{i=1}^s R_i$$

is a direct product of the rings  $R_i$ .

A ring  $R$  is said to be **simple** if it is semisimple, and if it has only one isomorphism class of simple left ideals. We see that we have proved a structure theorem for semisimple rings:

**Theorem 4.3.** *Let  $R$  be semisimple. Then there is only a finite number of non-isomorphic simple left ideals, say  $L_1, \dots, L_s$ . If*

$$R_i = \sum_{L \approx L_i} L$$

*is the sum of all simple left ideals isomorphic to  $L_i$ , then  $R_i$  is a two-sided ideal, which is also a ring (the operations being those induced by  $R$ ), and  $R$  is ring isomorphic to the direct product*

$$R = \prod_{i=1}^s R_i.$$

*Each  $R_i$  is a simple ring. If  $e_i$  is its unit element, then  $1 = e_1 + \dots + e_s$ , and  $R_i = Re_i$ . We have  $e_i e_j = 0$  if  $i \neq j$ .*

We shall now discuss modules.

**Theorem 4.4.** *Let  $R$  be semisimple, and let  $E$  be an  $R$ -module  $\neq 0$ . Then*

$$E = \bigoplus_{i=1}^s R_i E = \bigoplus_{i=1}^s e_i E,$$

*and  $R_i E$  is the submodule of  $E$  consisting of the sum of all simple submodules isomorphic to  $L_i$ .*

*Proof.* Let  $E_i$  be the sum of all simple submodules of  $E$  isomorphic to  $L_i$ . If  $V$  is a simple submodule of  $E$ , then  $RV = V$ , and hence  $L_i V = V$  for some  $i$ . By a previous lemma, we have  $L_i \approx V$ . Hence  $E$  is the direct sum of  $E_1, \dots, E_s$ . It is then clear that  $R_i E = E_i$ .

**Corollary 4.5.** *Let  $R$  be semisimple. Every simple module is isomorphic to one of the simple left ideals  $L_i$ .*

**Corollary 4.6.** *A simple ring has exactly one simple module, up to isomorphism.*

Both these corollaries are immediate consequences of Theorems 4.3 and 4.4.

**Proposition 4.7.** *Let  $k$  be a field and  $E$  a finite dimensional vector space over  $k$ . Let  $S$  be a subset of  $\text{End}_k(E)$ . Let  $R$  be the  $k$ -algebra generated by the elements of  $S$ . Then  $R$  is semisimple if and only if  $E$  is a semisimple  $R$  (or  $S$ ) module.*

*Proof.* If  $R$  is semisimple, then  $E$  is semisimple by Proposition 4.1. Conversely, assume  $E$  semisimple as  $S$ -module. Then  $E$  is semisimple as  $R$ -module, and so is a direct sum

$$E = \bigoplus_{i=1}^n E_i$$

where each  $E_i$  is simple. Then for each  $i$  there exists an element  $v_i \in E_i$  such that  $E_i = Rv_i$ . The map

$$x \mapsto (xv_1, \dots, xv_n)$$

is a  $R$ -homomorphism of  $R$  into  $E$ , and is an injection since  $R$  is contained in  $\text{End}_k(E)$ . Since a submodule of a semisimple module is semisimple by Proposition 2.2, the desired result follows.

## §5. SIMPLE RINGS

**Lemma 5.1.** *Let  $R$  be a ring, and  $\psi \in \text{End}_R(R)$  a homomorphism of  $R$  into itself, viewed as  $R$ -module. Then there exists  $\alpha \in R$  such that  $\psi(x) = x\alpha$  for all  $x \in R$ .*

*Proof.* We have  $\psi(x) = \psi(x \cdot 1) = x\psi(1)$ . Let  $\alpha = \psi(1)$ .

**Theorem 5.2.** *Let  $R$  be a simple ring. Then  $R$  is a finite direct sum of simple left ideals. There are no two-sided ideals except  $0$  and  $R$ . If  $L, M$  are simple left ideals, then there exists  $\alpha \in R$  such that  $L\alpha = M$ . We have  $LR = R$ .*

*Proof.* Since  $R$  is by definition also semisimple, it is a direct sum of simple left ideals, say  $\bigoplus_{j \in J} L_j$ . We can write  $1$  as a finite sum  $1 = \sum_{j=1}^m \beta_j$ , with  $\beta_j \in L_j$ .

Then

$$R = \bigoplus_{j=1}^m R\beta_j = \bigoplus_{j=1}^m L_j.$$

This proves our first assertion. As to the second, it is a consequence of the third. Let therefore  $L$  be a simple left ideal. Then  $LR$  is a left ideal, because  $RLR = LR$ , hence ( $R$  being semisimple) is a direct sum of simple left ideals, say

$$LR = \bigoplus_{j=1}^m L_j, \quad L = L_1.$$

Let  $M$  be a simple left ideal. We have a direct sum decomposition  $R = L \oplus L'$ . Let  $\pi: R \rightarrow L$  be the projection. It is an  $R$ -endomorphism. Let  $\sigma: L \rightarrow M$  be an isomorphism (it exists by Theorem 4.3). Then  $\sigma \circ \pi: R \rightarrow R$  is an  $R$ -endomorphism. By the lemma, there exists  $\alpha \in R$  such that

$$\sigma \circ \pi(x) = x\alpha \quad \text{for all } x \in R.$$

Apply this to elements  $x \in L$ . We find

$$\sigma(x) = x\alpha \quad \text{for all } x \in L.$$

The map  $x \mapsto x\alpha$  is a  $R$ -homomorphism of  $L$  into  $M$ , is non-zero, hence is an isomorphism. From this it follows at once that  $LR = R$ , thereby proving our theorem.

**Corollary 5.3.** *Let  $R$  be a simple ring. Let  $E$  be a simple  $R$ -module, and  $L$  a simple left ideal of  $R$ . Then  $LE = E$  and  $E$  is faithful.*

*Proof.* We have  $LE = L(RE) = (LR)E = RE = E$ . Suppose  $\alpha E = 0$  for some  $\alpha \in R$ . Then  $R\alpha RE = R\alpha E = 0$ . But  $R\alpha R$  is a two-sided ideal. Hence  $R\alpha R = 0$ , and  $\alpha = 0$ . This proves that  $E$  is faithful.

**Theorem 5.4.** (Rieffel). *Let  $R$  be a ring without two-sided ideals except 0 and  $R$ . Let  $L$  be a nonzero left ideal,  $R' = \text{End}_R(L)$  and  $R'' = \text{End}_{R'}(L)$ . Then the natural map  $\lambda: R \rightarrow R''$  is an isomorphism.*

*Proof.* The kernel of  $\lambda$  is a two-sided ideal, so  $\lambda$  is injective. Since  $LR$  is a two-sided ideal, we have  $LR = R$  and  $\lambda(L)\lambda(R) = \lambda(R)$ . For any  $x, y \in L$ , and  $f \in R''$ , we have  $f(xy) = f(x)y$ , because right multiplication by  $y$  is an  $R$ -endomorphism of  $L$ . Hence  $\lambda(L)$  is a left ideal of  $R''$ , so

$$R'' = R''\lambda(R) = R''\lambda(L)\lambda(R) = \lambda(L)\lambda(R) = \lambda(R),$$

as was to be shown.

In Rieffel's theorem, we do not need to assume that  $L$  is a simple module.

On the other hand,  $L$  is an ideal. So this theorem is not equivalent with previous ones of the same nature. In §7, we shall give a very general condition under which the canonical homomorphism

$$R \rightarrow R''$$

of a ring into the double endomorphism ring of a module is an isomorphism. This will cover all the previous cases.

As pointed out in the example following Wedderburn's theorem, Rieffel's theorem applies to give another proof when  $R$  is a finite-dimensional algebra (with unit) over a field  $k$ .

The next theorem gives a converse, showing that matrix rings over division algebras are simple.

**Theorem 5.5.** *Let  $D$  be a division ring, and  $E$  a finite-dimensional vector space over  $D$ . Let  $R = \text{End}_D(E)$ . Then  $R$  is simple and  $E$  is a simple  $R$ -module. Furthermore,  $D = \text{End}_R(E)$ .*

*Proof.* We first show that  $E$  is a simple  $R$ -module. Let  $v \in E$ ,  $v \neq 0$ . Then  $v$  can be completed to a basis of  $E$  over  $D$ , and hence, given  $w \in E$ , there exists  $\alpha \in R$  such that  $\alpha v = w$ . Hence  $E$  cannot have any invariant subspaces other than 0 or itself, and is simple over  $R$ . It is clear that  $E$  is faithful over  $R$ . Let  $\{v_1, \dots, v_m\}$  be a basis of  $E$  over  $D$ . The map

$$\alpha \mapsto (\alpha v_1, \dots, \alpha v_m)$$

of  $R$  into  $E^{(m)}$  is an  $R$ -homomorphism of  $R$  into  $E^{(m)}$ , and is injective. Given  $(w_1, \dots, w_m) \in E^{(m)}$ , there exists  $\alpha \in R$  such that  $\alpha v_i = w_i$  and hence  $R$  is  $R$ -isomorphic to  $E^{(m)}$ . This shows that  $R$  (as a module over itself) is isomorphic to a direct sum of simple modules and is therefore semisimple. Furthermore, all these simple modules are isomorphic to each other, and hence  $R$  is simple by Theorem 4.3.

There remains to prove that  $D = \text{End}_R(E)$ . We note that  $E$  is a semisimple module over  $D$  since it is a vector space, and every subspace admits a complementary subspace. We can therefore apply the density theorem (the roles of  $R$  and  $D$  are now permuted!). Let  $\varphi \in \text{End}_R(E)$ . Let  $v \in E$ ,  $v \neq 0$ . By the density theorem, there exists an element  $a \in D$  such that  $\varphi(v) = av$ . Let  $w \in E$ . There exists an element  $f \in R$  such that  $f(v) = w$ . Then

$$\varphi(w) = \varphi(f(v)) = f(\varphi(v)) = f(av) = af(v) = aw.$$

Therefore  $\varphi(w) = aw$  for all  $w \in E$ . This means that  $\varphi \in D$ , and concludes our proof.

**Theorem 5.6.** *Let  $k$  be a field and  $E$  a finite-dimensional vector space of*

dimension  $m$  over  $k$ . Let  $R = \text{End}_k(E)$ . Then  $R$  is a  $k$ -space, and

$$\dim_k R = m^2.$$

Furthermore,  $m$  is the number of simple left ideals appearing in a direct sum decomposition of  $R$  as such a sum.

*Proof.* The  $k$ -space of  $k$ -endomorphisms of  $E$  is represented by the space of  $m \times m$  matrices in  $k$ , so the dimension of  $R$  as a  $k$ -space is  $m^2$ . On the other hand, the proof of Theorem 5.5 showed that  $R$  is  $R$ -isomorphic as an  $R$ -module to the direct sum  $E^{(m)}$ . We know the uniqueness of the decomposition of a module into a direct sum of simple modules (Proposition 1.2), and this proves our assertion.

In the terminology introduced in §1, we see that the integer  $m$  in Theorem 5.6 is the length of  $R$ .

We can identify  $R = \text{End}_k(E)$  with the ring of matrices  $\text{Mat}_m(k)$ , once a basis of  $E$  is selected. In that case, we can take the simple left ideals to be the ideals  $L_i$  ( $i = 1, \dots, m$ ) where a matrix in  $L_i$  has coefficients equal to 0 except in the  $i$ -th column. An element of  $L_1$  thus looks like

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ a_{m1} & 0 & \cdots & 0 \end{pmatrix}$$

We see that  $R$  is the direct sum of the  $m$  columns.

We also observe that Theorem 5.5 implies the following:

*If a matrix  $M \in \text{Mat}_m(k)$  commutes with all elements of  $\text{Mat}_m(k)$ , then  $M$  is a scalar matrix.*

Indeed, such a matrix  $M$  can then be viewed as an  $R$ -endomorphism of  $E$ , and we know by Theorem 5.5 that such an endomorphism lies in  $k$ . Of course, one can also verify this directly by a brute force computation.

---

## §6. THE JACOBSON RADICAL, BASE CHANGE, AND TENSOR PRODUCTS

Let  $R$  be a ring and let  $M$  be a maximal left ideal. Then  $R/M$  is an  $R$ -module, and actually  $R/M$  is simple. Indeed, let  $\bar{J}$  be a submodule of  $R/M$  with  $\bar{J} \neq R/M$ . Let  $J$  be its inverse image in  $R$  under the canonical homomorphism.

Then  $J$  is a left ideal  $\neq M$  because  $\bar{J} \neq R/M$ , so  $J = R$  and  $\bar{J} = 0$ . Conversely, let  $E$  be a simple  $R$ -module and let  $v \in E$ ,  $v \neq 0$ . Then  $Rv$  is a submodule  $\neq 0$  of  $E$ , and hence  $Rv = E$ . Let  $M$  be the kernel of the homomorphism  $x \mapsto xv$ . Then  $M$  is a left ideal, and  $M$  is maximal; otherwise there is a left ideal  $M'$  with  $R \supset M' \supset M$  and  $M' \neq R, \neq M$ . Then  $R/M \approx E$  and  $R/M'$  is a non-zero homomorphic image of  $E$ , which cannot exist since  $E$  is simple (Schur's lemma, Proposition 1.1). Thus we obtain a bijection between maximal left ideals and simple  $R$ -modules (up to isomorphism).

We define the **Jacobson radical** of  $R$  to be the left ideal  $N$  which is the intersection of all maximal left ideals of  $R$ . We may also denote  $N = \text{Rad}(R)$ .

- Theorem 6.1.** (a) *For every simple  $R$ -module we have  $NE = 0$ .*  
 (b) *The radical  $N$  is a two-sided ideal, containing all nilpotent two-sided ideals.*  
 (c) *Let  $R$  be a finite dimensional algebra over field  $k$ . Its radical is  $\{0\}$ , if and only if  $R$  is semisimple.*  
 (d) *If  $R$  is a finite dimensional algebra over a field  $k$ , then its radical  $N$  is nilpotent (i.e.  $N^r = 0$  for some positive integer  $r$ ).*

These statements are easy to prove, and hints will be given appropriately. See Exercises 1 through 5.

Observe that under finite dimensionality conditions, the radical's being 0 gives us a useful criterion for a ring to be semisimple, which we shall use in the next result.

- Theorem 6.2.** *Let  $A$  be a semisimple algebra, finite dimensional over a field  $k$ . Let  $K$  be a finite separable extension of  $k$ . Then  $K \otimes_k A$  is a semisimple over  $K$ .*

*Proof.* In light of the radical criterion for semisimplicity, it suffices to prove that  $K \otimes_k A$  has zero radical, and it suffices to do so for an even larger extension than  $K$ , so that we may assume  $K$  is Galois over  $k$ , say with Galois group  $G$ . Then  $G$  operates on  $K \otimes A$  by

$$\sigma(x \otimes a) = \sigma x \otimes a \quad \text{for } x \in K \quad \text{and} \quad a \in A.$$

Let  $N$  be the radical of  $K \otimes A$ . Since  $N$  is nilpotent, it follows that  $\sigma N$  is also nilpotent for all  $\sigma \in G$ , whence  $\sigma N = N$  because  $N$  is the maximal nilpotent ideal (Exercise 5). Let  $\{\alpha_1, \dots, \alpha_m\}$  be a basis of  $A$  over  $k$ . Suppose  $N$  contains the element

$$\xi = \sum x_i \otimes \alpha_i \neq 0 \quad \text{with} \quad x_i \in K.$$

For every  $y \in K$  the element  $(y \otimes 1)\xi = \sum yx_i \otimes \alpha_i$  also lies in  $N$ . Then

$$\text{trace}((y \otimes 1)\xi) = \sum \sigma \xi = \sum \text{Tr}(yx_i) \otimes \alpha_i = \sum 1 \otimes \alpha_i \text{Tr}(yx_i)$$

also lies in  $N$ , and lies in  $1 \otimes A \approx A$ , thus proving the theorem.

**Remark.** For the case when  $A$  is a finite extension of  $k$ , compare with Exercises 1, 2, 3 of Chapter XVI.

Let  $A$  be a semisimple algebra, finite dimensional over a field  $k$ . Then by Theorem 6.2 the extension of scalars  $A \otimes_k k^a$  is semisimple if  $k$  is perfect. In general, an algebra  $A$  over  $k$  is said to be **absolutely semisimple** if  $A \otimes_k k^a$  is semisimple.

We now look at semisimple algebras over an algebraically closed field.

**Theorem 6.3.** *Let  $A, B$  be simple algebras, finite dimensional over a field  $k$  which is algebraically closed. Then  $A \otimes_k B$  is also simple. We have  $A \approx \text{End}_k(V)$  and  $B \approx \text{End}_k(W)$  where  $V, W$  are finite dimensional vector spaces over  $k$ , and there is a natural isomorphism*

$$A \otimes_k B \approx \text{End}_k(V \otimes_k W) \approx \text{End}_k(V) \otimes_k \text{End}_k(W).$$

*Proof.* The formula is a special case of Theorem 2.5 of Chapter XVI, and the isomorphisms  $A \approx \text{End}_k(V)$ ,  $B \approx \text{End}_k(W)$  exist by Wedderburn's theorem or its corollaries.

Let  $A$  be an algebra over  $k$  and let  $F$  be an extension field of  $k$ . We denote by  $A_F$  the extension of scalars

$$A_F = A \otimes_k F.$$

Thus  $A_F$  is an algebra over  $F$ . As an exercise, prove that if  $k$  is the center of  $A$ , then  $F$  is the center of  $A_F$ . (Here we identify  $F$  with  $1 \otimes F$ .)

Let  $A, B$  be algebras over  $k$ . We leave to the reader the proof that for every extension field  $F$  of  $k$ , we have a natural isomorphism

$$(A \otimes_k B)_F = A_F \otimes_F B_F.$$

We apply the above considerations to the tensor product of semisimple algebras.

**Theorem 6.4.** *Let  $A, B$  be absolutely semisimple algebras finite dimensional over a field  $k$ . Then  $A \otimes_k B$  is absolutely semisimple.*

*Proof.* Let  $F = k^a$ . Then  $A_F$  is semisimple by hypothesis, so it is a direct product of simple algebras, which are matrix algebras, and in particular we can apply Theorem 6.3 to see that  $A_F \otimes_F B_F$  has no radical. Hence  $A \otimes_k B$  has no radical (because if  $N$  is its radical, then  $N \otimes_k F = N_F$  is a nilpotent ideal of  $A_F \otimes_F B_F$ ), whence  $A \otimes_k B$  is semisimple by Theorem 6.1(c).

**Remark.** We have proved the above tensor product theorems rapidly in special cases, which are already important in various applications. For a more general treatment, I recommend Bourbaki's *Algebra*, Chapter VIII, which gives an exhaustive treatment of tensor products of semisimple and simple algebras.

---

## §7. BALANCED MODULES

Let  $R$  be a ring and  $E$  a module. We let  $R'(E) = \text{End}_R(E)$  and

$$R''(E) = \text{End}_{R'}(E).$$

Let  $\lambda: R \rightarrow R''$  be the natural homomorphism such that  $\lambda_x(v) = xv$  for  $x \in R$  and  $v \in E$ . If  $\lambda$  is an isomorphism, we shall say that  $E$  is **balanced**. We shall say that  $E$  is a **generator** (for  $R$ -modules) if every module is a homomorphic image of a (possibly infinite) direct sum of  $E$  with itself. For example,  $R$  is a generator.

More interestingly, in Rieffel's Theorem 5.4, the left ideal  $L$  is a generator, because  $LR = R$  implies that there is a surjective homomorphism  $L \times \cdots \times L \rightarrow R$  since we can write 1 as a finite combination

$$1 = x_1a_1 + \cdots + x_na_n \text{ with } x_i \in L \text{ and } a_i \in R.$$

The map  $(x_1, \dots, x_n) \mapsto x_1a_1 + \cdots + x_na_n$  is a  $R$ -homomorphism of left module onto  $R$ .

If  $E$  is a generator, then there is a surjective homomorphism  $E^{(n)} \rightarrow R$  (we can take  $n$  finite since  $R$  is finitely generated, by one element 1).

**Theorem 7.1. (Morita).** *Let  $E$  be an  $R$ -module. Then  $E$  is a generator if and only if  $E$  is balanced and finitely generated projective over  $R'(E)$ .*

*Proof.* We shall prove half of the theorem, leaving the other half to the reader, using similar ideas (see Exercise 12). So we assume that  $E$  is a generator, and we prove that it satisfies the other properties by arguments due to Faith.

We first prove that for any module  $F$ ,  $R \oplus F$  is balanced. We identify  $R$  and  $F$  as the submodules  $R \oplus 0$  and  $0 \oplus F$  of  $R \oplus F$ , respectively. For  $w \in F$ , let  $\psi_w: R \oplus F \rightarrow F$  be the map  $\psi_w(x + v) = xw$ . Then any  $f \in R''(R \oplus F)$  commutes with  $\pi_1$ ,  $\pi_2$ , and each  $\psi_w$ . From this we see at once that  $f(x + v) = f(1)(x + v)$  and hence that  $R \oplus F$  is balanced. Let  $E$  be a generator, and  $E^{(n)} \rightarrow R$  a surjective homomorphism. Since  $R$  is free, we can write  $E^{(n)} \approx R \oplus F$  for some module  $F$ , so that  $E^{(n)}$  is balanced. Let  $g \in R'(E)$ . Then  $g^{(n)}$  commutes with every element  $\varphi = (\varphi_{ij})$  in  $R'(E^{(n)})$  (with components  $\varphi_{ij} \in R'(E)$ ), and hence there is some  $x \in R$  such that  $g^{(n)} = \lambda_x^{(n)}$ . Hence  $g = \lambda_x$ , thereby proving that  $E$  is balanced, since  $\lambda$  is obviously injective.

To prove that  $E$  is finitely generated over  $R'(E)$ , we have

$$R'(E)^{(n)} \approx \text{Hom}_R(E^{(n)}, E) \approx \text{Hom}_R(R, E) \oplus \text{Hom}_R(F, E)$$

as additive groups. This relation also obviously holds as  $R'$ -modules if we define the operation of  $R'$  to be composition of mappings (on the left). Since  $\text{Hom}_R(R, E)$  is  $R'$ -isomorphic to  $E$  under the map  $h \mapsto h(1)$ , it follows that  $E$  is an  $R'$ -homomorphic image of  $R'^{(n)}$ , whence finitely generated over  $R'$ . We also see that  $E$  is a direct summand of the free  $R'$ -module  $R'^{(n)}$  and is therefore projective over  $R'(E)$ . This concludes the proof.

---

**EXERCISES**
**The radical**

1. (a) Let  $R$  be a ring. We define the **radical** of  $R$  to be the left ideal  $N$  which is the intersection of all maximal left ideals of  $R$ . Show that  $NE = 0$  for every simple  $R$ -module  $E$ . Show that  $N$  is a two-sided ideal. (b) Show that the radical of  $R/N$  is 0.
2. A ring is said to be **Artinian** if every descending sequence of left ideals  $J_1 \supset J_2 \supset \dots$  with  $J_i \neq J_{i+1}$  is finite. (a) Show that a finite dimensional algebra over a field is Artinian. (b) If  $R$  is Artinian, show that every non-zero left ideal contains a simple left ideal. (c) If  $R$  is Artinian, show that every non-empty set of ideals contains a minimal ideal.
3. Let  $R$  be Artinian. Show that its radical is 0 if and only if  $R$  is semisimple. [*Hint:* Get an injection of  $R$  into a direct sum  $\bigoplus R/M_i$  where  $\{M_i\}$  is a finite set of maximal left ideals.]
4. **Nakayama's lemma.** Let  $R$  be any ring and  $M$  a finitely generated module. Let  $N$  be the radical of  $R$ . If  $NM = M$  show that  $M = 0$ . [*Hint:* Observe that the proof of Nakayama's lemma still holds.]
5. (a) Let  $J$  be a two-sided nilpotent ideal of  $R$ . Show that  $J$  is contained in the radical. (b) Conversely, assume that  $R$  is Artinian. Show that its radical is nilpotent, i.e., that there exists an integer  $r \geq 1$  such that  $N^r = 0$ . [*Hint:* Consider the descending sequence of powers  $N^r$ , and apply Nakayama to a minimal finitely generated left ideal  $L \subset N^\infty$  such that  $N^\infty L \neq 0$ .
6. Let  $R$  be a semisimple commutative ring. Show that  $R$  is a direct product of fields.
7. Let  $R$  be a finite dimensional commutative algebra over a field  $k$ . If  $R$  has no nilpotent element  $\neq 0$ , show that  $R$  is semisimple.
8. (Kolchin) Let  $E$  be a finite-dimensional vector space over a field  $k$ . Let  $G$  be a subgroup of  $GL(E)$  such that every element  $A \in G$  is of type  $I + N$  where  $N$  is nilpotent. Assume  $E \neq 0$ . Show that there exists an element  $v \in E, v \neq 0$  such that  $Av = v$  for all  $A \in G$ . [*Hint:* First reduce the question to the case when  $k$  is algebraically closed by showing that the problem amounts to solving linear equations. Secondly, reduce it to the case when  $E$  is a simple  $k[G]$ -module. Combining Burnside's theorem with the fact that  $\text{tr}(A) = \text{tr}(I)$  for all  $A \in G$ , show that if  $A_0 \in G, A_0 = I + N$ , then  $\text{tr}(NX) = 0$  for all  $X \in \text{End}_k(E)$ , and hence that  $N = 0, A_0 = I$ .]

**Semisimple operations**

9. Let  $E$  be a finite dimensional vector space over a field  $k$ . Let  $R$  be a semisimple subalgebra of  $\text{End}_k(E)$ . Let  $a, b \in R$ . Assume that

$$\text{Ker } b_E \supset \text{Ker } a_E,$$

where  $b_E$  is multiplication by  $b$  on  $E$  and similarly for  $a_E$ . Show that there exists an element  $s \in R$  such that  $sa = b$ . [*Hint:* Reduce to  $R$  simple. Then  $R = \text{End}_D(E_0)$  and  $E = E_0^{(n)}$ . Let  $v_1, \dots, v_r \in E$  be a  $D$ -basis for  $aE$ . Define  $s$  by  $s(av_i) = bv_i$  and

extend  $s$  by  $D$ -linearity. Then  $sa_E = b_E$ , so  $sa = b$ .]

10. Let  $E$  be a finite-dimensional vector space over a field  $k$ . Let  $A \in \text{End}_k(E)$ . We say that  $A$  is **semisimple** if  $E$  is a semisimple  $A$ -space, or equivalently, let  $R$  be the  $k$ -algebra generated by  $A$ , then  $E$  is semisimple over  $R$ . Show that  $A$  is semisimple if and only if its minimal polynomial has no factors of multiplicity  $> 1$  over  $k$ .
11. Let  $E$  be a finite-dimensional vector space over a field  $k$ , and let  $S$  be a commutative set of endomorphisms of  $E$ . Let  $R = k[S]$ . Assume that  $R$  is semisimple. Show that every subset of  $S$  is semisimple.
12. Prove that an  $R$ -module  $E$  is a generator if and only if it is balanced, and finitely generated projective over  $R'(E)$ . Show that Theorem 5.4 is a consequence of Theorem 7.1.
13. Let  $A$  be a principal ring with quotient field  $K$ . Let  $A^n$  be  $n$ -space over  $A$ , and let

$$T = A^n \oplus A^n \oplus \cdots \oplus A^n$$

be the direct sum of  $A^n$  with itself  $r$  times. Then  $T$  is free of rank  $nr$  over  $A$ . If we view elements of  $A^n$  as column vectors, then  $T$  is the space of  $n \times r$  matrices over  $A$ . Let  $M = \text{Mat}_n(A)$  be the ring of  $n \times n$  matrices over  $A$ , operating on the left of  $T$ . By a **lattice**  $L$  in  $T$  we mean an  $A$ -submodule of rank  $nr$  over  $A$ . Prove that any such lattice which is  $M$ -stable is  $M$ -isomorphic to  $T$  itself. Thus there is just one  $M$ -isomorphism class of lattices. [Hint: Let  $g \in M$  be the matrix with 1 in the upper left corner and 0 everywhere else, so  $g$  is a projection of  $A^n$  on a 1-dimensional subspace. Then multiplication on the left  $g: T \rightarrow A_r$  maps  $T$  on the space of  $n \times r$  matrices with arbitrary first row and 0 everywhere else. Furthermore, for any lattice  $L$  in  $T$  the image  $gL$  is a lattice in  $A_r$ , that is a free  $A$ -submodule of rank  $r$ . By elementary divisors there exists an  $r \times r$  matrix  $Q$  such that

$$gL = A_r Q \quad (\text{multiplication on the right}).$$

Then show that  $TQ = L$  and that multiplication by  $Q$  on the right is an  $M$ -isomorphism of  $T$  with  $L$ .]

14. Let  $F$  be a field. Let  $\mathfrak{n} = \mathfrak{n}(F)$  be the vector space of strictly upper triangular  $n \times n$  matrices over  $F$ . Show that  $\mathfrak{n}$  is actually an algebra, and all elements of  $\mathfrak{n}$  are nilpotent (some positive integral power is 0).
15. **Conjugation representation.** Let  $A$  be the multiplicative group of diagonal matrices in  $F$  with non-zero diagonal components. For  $a \in A$ , the **conjugation action** of  $a$  on  $\text{Mat}_n(F)$  is denoted by  $\mathbf{c}(a)$ , so  $\mathbf{c}(a)M = aMa^{-1}$  for  $M \in \text{Mat}_n(F)$ . (a) Show that  $\mathfrak{n}$  is stable under this action. (b) Show that  $\mathfrak{n}$  is semisimple under this action. More precisely, for  $1 \leq i < j \leq n$ , let  $E_{ij}$  be the matrix with  $(ij)$ -component 1, and all other components 0. Then these matrices  $E_{ij}$  form a basis for  $\mathfrak{n}$  over  $F$ , and each  $E_{ij}$  is an eigenvector for the conjugation action, namely for  $a = \text{diag}(a_1, \dots, a_n)$ , we have

$$aE_{ij}a^{-1} = (a_i/a_j)E_{ij},$$

so the corresponding character  $\chi_{ij}$  is given by  $\chi_{ij}(a) = a_i/a_j$ . (c) Show that  $\text{Mat}_n(F)$  is semisimple, and in fact is equal to  $\mathfrak{d} \oplus \mathfrak{n} \oplus {}' \mathfrak{n}$ , where  $\mathfrak{d}$  is the space of diagonal matrices.

---

## CHAPTER XVIII

---

# Representations of Finite Groups

The theory of group representations occurs in many contexts. First, it is developed for its own sake: determine all irreducible representations of a given group. See for instance Curtis-Reiner's *Methods of Representation Theory* (Wiley-Interscience, 1981). It is also used in classifying finite simple groups. But already in this book we have seen applications of representations to Galois theory and the determination of the Galois group over the rationals. In addition, there is an analogous theory for topological groups. In this case, the closest analogy is with compact groups, and the reader will find a self-contained treatment of the compact case entirely similar to §5 of this chapter in my book  $\mathbf{SL}_2(\mathbf{R})$  (Springer Verlag), Chapter II, §2. Essentially, finite sums are replaced by integrals, otherwise the formalism is the same. The analysis comes only in two places. One of them is to show that every irreducible representation of a compact group is finite dimensional; the other is Schur's lemma. The details of these extra considerations are carried out completely in the above-mentioned reference. I was careful to write up §5 with the analogy in mind.

Similarly, readers will find analogous material on induced representations in  $\mathbf{SL}_2(\mathbf{R})$ , Chapter III, §2 (which is also self-contained).

Examples of the general theory come in various shapes. Theorem 8.4 may be viewed as an example, showing how a certain representation can be expressed as a direct sum of induced representations from 1-dimensional representations. Examples of representations of  $S_3$  and  $S_4$  are given in the exercises. The entire last section works out completely the simple characters for the group  $GL_2(\mathbf{F})$  when  $\mathbf{F}$  is a finite field, and shows how these characters essentially come from induced characters.

For other examples also leading into Lie groups, see W. Fulton and J. Harris, *Representation Theory*, Springer Verlag 1991.

---

## §1. REPRESENTATIONS AND SEMISIMPLICITY

Let  $R$  be a commutative ring and  $G$  a group. We form the group algebra  $R[G]$ . As explained in Chapter II, §3 it consists of all formal linear combinations

$$\sum_{\sigma \in G} a_{\sigma} \sigma$$

with coefficients  $a_{\sigma} \in R$ , almost all of which are 0. The product is taken in the natural way,

$$\left( \sum_{\sigma \in G} a_{\sigma} \sigma \right) \left( \sum_{\tau \in G} b_{\tau} \tau \right) = \sum_{\sigma, \tau} a_{\sigma} b_{\tau} \sigma \tau.$$

Let  $E$  be an  $R$ -module. Every algebra-homomorphism

$$R[G] \rightarrow \text{End}_R(E)$$

induces a group-homomorphism

$$G \rightarrow \text{Aut}_R(E),$$

and thus a representation of the ring  $R[G]$  in  $E$  gives rise to a representation of the group. Given such representations, we also say that  $R[G]$ , or  $G$ , **operate** on  $E$ . We note that the representation makes  $E$  into a module over the ring  $R[G]$ .

Conversely, given a representation of the group, say  $\rho : G \rightarrow \text{Aut}_R(E)$ , we can extend  $\rho$  to a representation of  $R[G]$  as follows. Let  $\alpha = \sum a_{\sigma} \sigma$  and  $x \in E$ . We define

$$\rho(\alpha)x = \sum a_{\sigma} \rho(\sigma)x.$$

It is immediately verified that  $\rho$  has been extended to a ring-homomorphism of  $R[G]$  into  $\text{End}_R(E)$ . We say that  $\rho$  is **faithful** on  $G$  if the map  $\rho : G \rightarrow \text{Aut}_R(E)$  is injective. The extension of  $\rho$  to  $R[G]$  may not be faithful, however.

Given a representation of  $G$  on  $E$ , we often write simply  $\sigma x$  instead of  $\rho(\sigma)x$ , whenever we deal with a fixed representation throughout a discussion.

An  $R$ -module  $E$ , together with a representation  $\rho$ , will be called a  **$G$ -module**, or  **$G$ -space**, or also a  $(G, R)$ -module if we wish to specify the ring  $R$ . If  $E, F$  are  $G$ -modules, we recall that a  $G$ -homomorphism  $f : E \rightarrow F$  is an  $R$ -linear map such that  $f(\sigma x) = \sigma f(x)$  for all  $x \in E$  and  $\sigma \in G$ .

Given a  $G$ -homomorphism  $f : E \rightarrow F$ , we note that the kernel of  $f$  is a  $G$ -submodule of  $E$ , and that the  $R$ -factor module  $F/f(E)$  admits an operation of  $G$  in a unique way such that the canonical map  $F \rightarrow F/f(E)$  is a  $G$ -homomorphism.

By a **trivial** representation  $\rho : G \rightarrow \text{Aut}_R(E)$ , we shall mean the representation such that  $\rho(G) = 1$ . A representation is trivial if and only if  $\sigma x = x$  for all  $x \in E$ . We also say in that case that  $G$  **operates trivially**.

We make  $R$  into a  $G$ -module by making  $G$  act trivially on  $R$ .

We shall now discuss systematically the representations which arise from a given one, on Hom, the dual, and the tensor product. This pattern will be repeated later when we deal with induced representations.

First,  $\text{Hom}_R(E, F)$  is a  $G$ -module under the action defined for  $f \in \text{Hom}_R(E, F)$  by

$$([\sigma]f)(x) = \sigma f(\sigma^{-1}x).$$

The conditions for an operation are trivially verified. Note the  $\sigma^{-1}$  inside the expression. We shall usually omit parentheses, and write simply  $[\sigma]f(x)$  for the left-hand side. We note that  $f$  is a  $G$ -homomorphism if and only if  $[\sigma]f = f$  for all  $\sigma \in G$ .

We are particularly concerned when  $F = R$  (so with trivial action), in which case  $\text{Hom}_R(E, R) = E^\vee$  is the dual module. In the terminology of representations, if  $\rho: G \rightarrow \text{Aut}_R(E)$  is a representation of  $G$  on  $E$ , then the action we have just described gives a representation denoted by

$$\rho^\vee: G \rightarrow \text{Aut}_R(E^\vee),$$

and called the **dual representation** (also called contragredient (ugh!) in the literature).

Suppose now that the modules  $E, F$  are free and finite dimensional over  $R$ . Let  $\rho$  be representation of  $G$  on  $E$ . Let  $M$  be the matrix of  $\rho(\sigma)$  with respect to a basis, and let  $M^\vee$  be the matrix of  $\rho^\vee(\sigma)$  with respect to the dual basis. Then it is immediately verified that

$$(1) \quad M^\vee = {}^t M^{-1}.$$

Next we consider the tensor product instead of Hom. Let  $E, E'$  be  $(G, R)$ -modules. We can form their tensor product  $E \otimes E'$ , always taken over  $R$ . Then there is a unique action of  $G$  on  $E \otimes E'$  such that for  $\sigma \in G$  we have

$$\sigma(x \otimes x') = \sigma x \otimes \sigma x'.$$

Suppose that  $E, F$  are finite free over  $R$ . Then the  $R$ -isomorphism

$$(2) \quad E^\vee \otimes F \approx \text{Hom}_R(E, F)$$

of Chapter XVI, Corollary 5.5, is immediately verified to be a  $G$ -isomorphism.

Whether  $E$  is free or not, we define the  **$G$ -invariant submodule** of  $E$  to be  $\text{inv}_G(E) = R$ -submodule of elements  $x \in E$  such that  $\sigma x = x$  for all  $\sigma \in G$ . If  $E, F$  are free then we have an  $R$ -isomorphism

$$(3) \quad \text{inv}_G(E^\vee \otimes F) \approx \text{Hom}_G(E, F).$$

If  $\rho: G \rightarrow \text{Aut}_R(E)$  and  $\rho': G \rightarrow \text{Aut}_R(E')$  are representations of  $G$  on  $E$  and  $E'$  respectively, then we define their **sum**  $\rho \oplus \rho'$  to be the representation on the direct sum  $E \oplus E'$ , with  $\sigma \in G$  acting componentwise. Observe that  $G$ -isomorphism classes of representations have an additive monoid structure under this direct sum, and also have an associative multiplicative structure under the tensor product. With the notation of representations, we denote this product by  $\rho \otimes \rho'$ . This product is distributive with respect to the addition (direct sum).

If  $G$  is a finite group, and  $E$  is a  $G$ -module, then we can define the **trace**  $\text{Tr}_G: E \rightarrow E$  which is an  $R$ -homomorphism, namely

$$\text{Tr}_G(x) = \sum_{\sigma \in G} \sigma x.$$

We observe that  $\text{Tr}_G(x)$  lies in  $\text{inv}_G(E)$ , i.e. is fixed under the operation of all elements of  $G$ . This is because

$$\tau \text{Tr}_G(x) = \sum_{\sigma \in G} \tau \sigma x,$$

and multiplying by  $\tau$  on the left permutes the elements of  $G$ .

In particular, if  $f: E \rightarrow F$  is an  $R$ -homomorphism of  $G$ -modules, then  $\text{Tr}_G(f): E \rightarrow F$  is a  $G$ -homomorphism.

**Proposition 1.1.** *Let  $G$  be a finite group and let  $E', E, F, F'$  be  $G$ -modules. Let*

$$E' \xrightarrow{\varphi} E \xrightarrow{f} F \xrightarrow{\psi} F'$$

*be  $R$ -homomorphisms, and assume that  $\varphi, \psi$  are  $G$ -homomorphisms. Then*

$$\text{Tr}_G(\psi \circ f \circ \varphi) = \psi \circ \text{Tr}_G(f) \circ \varphi.$$

*Proof.* We have

$$\begin{aligned} \text{Tr}_G(\psi \circ f \circ \varphi) &= \sum_{\sigma \in G} \sigma(\psi \circ f \circ \varphi) = \sum_{\sigma \in G} (\sigma\psi) \circ (\sigma f) \circ (\sigma\varphi) \\ &= \psi \circ \left( \sum_{\sigma \in G} \sigma f \right) \circ \varphi = \psi \circ \text{Tr}_G(f) \circ \varphi. \end{aligned}$$

**Theorem 1.2.** (Maschke). *Let  $G$  be a finite group of order  $n$ , and let  $k$  be a field whose characteristic does not divide  $n$ . Then the group ring  $k[G]$  is semisimple.*

*Proof.* Let  $E$  be a  $G$ -module, and  $F$  a  $G$ -submodule. Since  $k$  is a field, there exists a  $k$ -subspace  $F'$  such that  $E$  is the  $k$ -direct sum of  $F$  and  $F'$ . We let the  $k$ -linear map  $\pi: E \rightarrow F$  be the projection on  $F$ . Then  $\pi(x) = x$  for all  $x \in F$ .

Let

$$\varphi = \frac{1}{n} \operatorname{Tr}_G(\pi).$$

We have then two  $G$ -homomorphisms

$$0 \rightarrow F \xrightarrow{j} E$$

such that  $j$  is the inclusion, and  $\varphi \circ j = \operatorname{id}$ . It follows that  $E$  is the  $G$ -direct sum of  $F$  and  $\operatorname{Ker} \varphi$ , thereby proving that  $k[G]$  is semisimple.

**Except in §7 we denote by  $G$  a finite group, and we denote  $E, F$  finite dimensional  $k$ -spaces, where  $k$  is a field of characteristic not dividing  $\#(G)$ . We usually denote  $\#(G)$  by  $n$ .**

## §2. CHARACTERS

Let  $\rho : k[G] \rightarrow \operatorname{End}_k(E)$  be a representation. By the **character**  $\chi_\rho$  of the representation, we shall mean the  $k$ -valued function

$$\chi_\rho : k[G] \rightarrow k$$

such that  $\chi_\rho(\alpha) = \operatorname{tr} \rho(\alpha)$  for all  $\alpha \in k[G]$ . The trace here is the trace of an endomorphism, as defined in Chapter XIII, §3. If we select a basis for  $E$  over  $k$ , it is the trace of the matrix representing  $\rho(\alpha)$ , i.e., the sum of the diagonal elements. We have seen previously that the trace does not depend on the choice of the basis. We sometimes write  $\chi_E$  instead of  $\chi_\rho$ .

We also call  $E$  the **representation space** of  $\rho$ .

By the **trivial character** we shall mean the character of the representation of  $G$  on the  $k$ -space equal to  $k$  itself, such that  $\sigma x = x$  for all  $x \in k$ . It is the function taking the value 1 on all elements of  $G$ . We denote it by  $\chi_0$  or also by  $1_G$  if we need to specify the dependence on  $G$ .

We observe that characters are functions on  $G$ , and that the values of a character on elements of  $k[G]$  are determined by its values on  $G$  (the extension from  $G$  to  $k[G]$  being by  $k$ -linearity).

We say that two representations  $\rho, \varphi$  of  $G$  on spaces  $E, F$  are **isomorphic** if there is a  $G$ -isomorphism between  $E$  and  $F$ . We then see that if  $\rho, \varphi$  are isomorphic representations, then their characters are equal. (Put in another way, if  $E, F$  are  $G$ -spaces and are  $G$ -isomorphic, then  $\chi_E = \chi_F$ .) In everything that follows, we are interested only in isomorphism classes of representations.

If  $E, F$  are  $G$ -spaces, then their direct sum  $E \oplus F$  is also a  $G$ -space, the operation of  $G$  being componentwise. If  $x \oplus y \in E \oplus F$  with  $x \in E$  and  $y \in F$ , then  $\sigma(x \oplus y) = \sigma x \oplus \sigma y$ .

Similarly, the tensor product  $E \otimes_k F = E \otimes F$  is a  $G$ -space, the operation of  $G$  being given by  $\sigma(x \otimes y) = \sigma x \otimes \sigma y$ .

**Proposition 2.1.** *If  $E, F$  are  $G$ -spaces, then*

$$\chi_E + \chi_F = \chi_{E \oplus F} \quad \text{and} \quad \chi_E \chi_F = \chi_{E \otimes F}.$$

*If  $\chi^\vee$  denotes the character of the dual representation on  $E^\vee$ , then*

$$\begin{aligned} \chi^\vee(\sigma) &= \chi(\sigma^{-1}) \\ &= \overline{\chi(\sigma)} \text{ if } k = \mathbf{C}. \end{aligned}$$

*Proof.* The first relation holds because the matrix of an element  $\sigma$  in the representation  $E \oplus F$  decomposes into blocks corresponding to the representation in  $E$  and the representation in  $F$ . As to the second, if  $\{v_i\}$  is a basis of  $E$  and  $\{w_j\}$  is a basis of  $F$  over  $k$ , then we know that  $\{v_i \otimes w_j\}$  is a basis of  $E \otimes F$ . Let  $(a_{iv})$  be the matrix of  $\sigma$  with respect to our basis of  $E$ , and  $(b_{j\mu})$  its matrix with respect to our basis of  $F$ . Then

$$\begin{aligned} \sigma(v_i \otimes w_j) &= \sigma v_i \otimes \sigma w_j = \sum_v a_{iv} v_v \otimes \sum_\mu b_{j\mu} w_\mu \\ &= \sum_{v, \mu} a_{iv} b_{j\mu} v_v \otimes w_\mu. \end{aligned}$$

By definition, we find

$$\chi_{E \otimes F}(\sigma) = \sum_i \sum_j a_{ii} b_{jj} = \chi_E(\sigma) \chi_F(\sigma),$$

thereby proving the statement about tensor products. The statement for the character of the dual representation follows from the formula for the matrix  ${}^t M^{-1}$  given in §1. The value given as the complex conjugate in case  $k = \mathbf{C}$  will be proved later in Corollary 3.2.

So far, we have defined the notion of character associated with a representation. It is now natural to form linear combinations of such characters with more general coefficients than positive integers. Thus by a **character** of  $G$  we shall mean a function on  $G$  which can be written as a linear combination of characters of representations with arbitrary integer coefficients. The characters associated with representations will be called **effective characters**. Everything we have defined of course depends on the field  $k$ , and we shall add **over  $k$**  to our expressions if we need to specify the field  $k$ .

We observe that the characters form a ring in view of Proposition 2.1. For most of our work we do not need the multiplicative structure, only the additive one.

By a **simple** or **irreducible character** of  $G$  one means the character of a simple representation (i.e., the character associated with a simple  $k[G]$ -module).

Taking into account Theorem 1.2, and the results of the preceding chapter concerning the structure of simple and semisimple modules over a semisimple ring (Chapter XVII, §4) we obtain:

**Theorem 2.2.** *There are only a finite number of simple characters of  $G$  (over  $k$ ). The characters of representations of  $G$  are the linear combinations of the simple characters with integer coefficients  $\geq 0$ .*

We shall use the direct product decomposition of a semisimple ring. We have

$$k[G] = \prod_{i=1}^s R_i$$

where each  $R_i$  is simple, and we have a corresponding decomposition of the unit element of  $k[G]$ :

$$1 = e_1 + \cdots + e_s,$$

where  $e_i$  is the unit element of  $R_i$ , and  $e_i e_j = 0$  if  $i \neq j$ . Also,  $R_i R_j = 0$  if  $i \neq j$ . We note that  $s = s(k)$  depends on  $k$ .

If  $L_i$  denotes a typical simple module for  $R_i$  (say one of the simple left ideals), we let  $\chi_i$  be the character of the representation on  $L_i$ .

We observe that  $\chi_i(\alpha) = 0$  for all  $\alpha \in R_j$  if  $i \neq j$ . This is a fundamental relation of orthogonality, which is obvious, but from which all our other relations will follow.

**Theorem 2.3.** *Assume that  $k$  has characteristic 0. Then every effective character has a unique expression as a linear combination*

$$\chi = \sum_{i=1}^s n_i \chi_i, \quad n_i \in \mathbf{Z}, n_i \geq 0,$$

where  $\chi_1, \dots, \chi_s$  are the simple characters of  $G$  over  $k$ . Two representations are isomorphic if and only if their associated characters are equal.

*Proof.* Let  $E$  be the representation space of  $\chi$ . Then by Theorem 4.4 of Chapter XVII,

$$E \approx \bigoplus_{i=1}^s n_i L_i.$$

The sum is finite because we assume throughout that  $E$  is finite dimensional. Since  $e_i$  acts as a unit element on  $L_i$ , we find

$$\chi_i(e_i) = \dim_k L_i.$$

We have already seen that  $\chi_i(e_j) = 0$  if  $i \neq j$ . Hence

$$\chi(e_i) = n_i \dim_k L_i.$$

Since  $\dim_k L_i$  depends only on the structure of the group algebra, we have recovered the multiplicities  $n_1, \dots, n_s$ . Namely,  $n_i$  is the number of times that  $L_i$  occurs (up to an isomorphism) in the representation space of  $\chi$ , and is the value of  $\chi(e_i)$  divided by  $\dim_k L_i$  (we are in characteristic 0). This proves our theorem.

As a matter of definition, in Theorem 2.3 we call  $n_i$  the **multiplicity** of  $\chi_i$  in  $\chi$ . In both corollaries, we continue to assume that  $k$  has characteristic 0.

**Corollary 2.4.** *As functions of  $G$  into  $k$ , the simple characters*

$$\chi_1, \dots, \chi_s$$

*are linearly independent over  $k$ .*

*Proof.* Suppose that  $\sum a_i \chi_i = 0$  with  $a_i \in k$ . We apply this expression to  $e_j$  and get

$$0 = (\sum a_i \chi_i)(e_j) = a_j \dim_k L_j.$$

Hence  $a_j = 0$  for all  $j$ .

*In characteristic 0* we define the **dimension** of an effective character to be the dimension of the associated representation space.

**Corollary 2.5.** *The function  $\dim$  is a homomorphism of the monoid of effective characters into  $\mathbf{Z}$ .*

**Example.** Let  $G$  be a cyclic group of order equal to a prime number  $p$ . We form the group algebra  $\mathbf{Q}[G]$ . Let  $\sigma$  be a generator of  $G$ . Let

$$e_1 = \frac{1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1}}{p}, \quad e_2 = 1 - e_1.$$

Then  $\tau e_1 = e_1$  for any  $\tau \in G$  and consequently  $e_1^2 = e_1$ . It then follows that  $e_2^2 = e_2$  and  $e_1 e_2 = 0$ . The field  $\mathbf{Q}e_1$  is isomorphic to  $\mathbf{Q}$ . Let  $\omega = \sigma e_2$ . Then  $\omega^p = e_2$ . Let  $\mathbf{Q}_2 = \mathbf{Q}e_2$ . Since  $\omega \neq e_2$ , and satisfies the irreducible equation

$$X^{p-1} + \cdots + 1 = 0$$

over  $\mathbf{Q}_2$ , it follows that  $\mathbf{Q}_2(\omega)$  is isomorphic to the field obtained by adjoining a primitive  $p$ -th root of unity to the rationals. Consequently,  $\mathbf{Q}[G]$  admits the direct product decomposition

$$\mathbf{Q}[G] \approx \mathbf{Q} \times \mathbf{Q}(\zeta)$$

where  $\zeta$  is a primitive  $p$ -th root of unity.

As another example, let  $G$  be any finite group, and let

$$e_1 = \frac{1}{n} \sum_{\sigma \in G} \sigma.$$

Then for any  $\tau \in G$  we have  $\tau e_1 = e_1$ , and  $e_1^2 = e_1$ . If we let  $e'_1 = 1 - e_1$  then  $e'_1 = e'_1$ , and  $e'_1 e_1 = e_1 e'_1 = 0$ . Thus for any field  $k$  (whose characteristic does not divide the order of  $G$  according to conventions in force), we see that

$$k[G] = ke_1 \times k[G]e'_1$$

is a direct product decomposition. In particular, the representation of  $G$  on the group algebra  $k[G]$  itself contains a 1-dimensional representation on the component  $ke_1$ , whose character is the trivial character.

### §3. 1-DIMENSIONAL REPRESENTATIONS

By abuse of language, even in characteristic  $p > 0$ , we say that a **character is 1-dimensional** if it is a homomorphism  $G \rightarrow k^*$ .

Assume that  $E$  is a 1-dimensional vector space over  $k$ . Let

$$\rho : G \rightarrow \text{Aut}_k(E)$$

be a representation. Let  $\{v\}$  be a basis of  $E$  over  $k$ . Then for each  $\sigma \in G$ , we have

$$\sigma v = \chi(\sigma)v$$

for some element  $\chi(\sigma) \in k$ , and  $\chi(\sigma) \neq 0$  since  $\sigma$  induces an automorphism of  $E$ . Then for  $\tau \in G$ ,

$$\tau\sigma v = \chi(\sigma)\tau v = \chi(\sigma)\chi(\tau)v = \chi(\sigma\tau)v.$$

We see that  $\chi: G \rightarrow k^*$  is a homomorphism, and that our 1-dimensional character is the same type of thing that occurred in Artin's theorem in Galois theory.

Conversely, let  $\chi: G \rightarrow k^*$  be a homomorphism. Let  $E$  be a 1-dimensional  $k$ -space, with basis  $\{v\}$ , and define  $\sigma(av) = a\chi(\sigma)v$  for all  $a \in k$ . Then we see at once that this operation of  $G$  on  $E$  gives a representation of  $G$ , whose associated character is  $\chi$ .

Since  $G$  is finite, we note that

$$\chi(\sigma)^n = \chi(\sigma^n) = \chi(1) = 1.$$

Hence the values of 1-dimensional characters are  $n$ -th roots of unity. The 1-dimensional characters form a group under multiplication, and when  $G$  is a finite abelian group, we have determined its group of 1-dimensional characters in Chapter I, §9.

**Theorem 3.1.** *Let  $G$  be a finite abelian group, and assume that  $k$  is algebraically closed. Then every simple representation of  $G$  is 1-dimensional. The simple characters of  $G$  are the homomorphisms of  $G$  into  $k^*$ .*

*Proof.* The group ring  $k[G]$  is semisimple, commutative, and is a direct product of simple rings. Each simple ring is a ring of matrices over  $k$  (by Corollary 3.6 Chapter XVII), and can be commutative if and only if it is equal to  $k$ .

For every 1-dimensional character  $\chi$  of  $G$  we have

$$\chi(\sigma)^{-1} = \chi(\sigma^{-1}).$$

If  $k$  is the field of complex numbers, then

$$\overline{\chi(\sigma)} = \chi(\sigma)^{-1} = \chi(\sigma^{-1}).$$

**Corollary 3.2.** *Let  $k$  be algebraically closed. Let  $G$  be a finite group. For any character  $\chi$  and  $\sigma \in G$ , the value  $\chi(\sigma)$  is equal to a sum of roots of unity with integer coefficients (i.e. coefficients in  $\mathbf{Z}$  or  $\mathbf{Z}/p\mathbf{Z}$  depending on the characteristic of  $k$ ).*

*Proof.* Let  $H$  be the subgroup generated by  $\sigma$ . Then  $H$  is a cyclic subgroup. A representation of  $G$  having character  $\chi$  can be viewed as a representation for  $H$  by restriction, having the same character. Thus our assertion follows from Theorem 3.1.

---

## §4. THE SPACE OF CLASS FUNCTIONS

By a **class function** of  $G$  (over  $k$ , or with values in  $k$ ), we shall mean a function  $f: G \rightarrow k$  such that  $f(\sigma\tau\sigma^{-1}) = f(\tau)$  for all  $\sigma, \tau \in G$ . It is clear that characters are class functions, because for square matrices  $M, M'$  we have

$$\text{tr}(MM'M^{-1}) = \text{tr}(M').$$

Thus a class function may be viewed as a function on conjugacy classes.

We shall always extend the domain of definition of a class function to the group ring, by linearity. If

$$\alpha = \sum_{\sigma \in G} a_{\sigma} \sigma,$$

and  $f$  is a class function, we define

$$f(\alpha) = \sum_{\sigma \in G} a_{\sigma} f(\sigma).$$

Let  $\sigma_0 \in G$ . If  $\sigma \in G$ , we write  $\sigma \sim \sigma_0$  if  $\sigma$  is conjugate to  $\sigma_0$ , that is, if there exists an element  $\tau$  such that  $\sigma_0 = \tau\sigma\tau^{-1}$ . An element of the group ring of type

$$\gamma = \sum_{\sigma \sim \sigma_0} \sigma$$

will also be called a **conjugacy class**.

**Proposition 4.1.** *An element of  $k[G]$  commutes with every element of  $G$  if and only if it is a linear combination of conjugacy classes with coefficients in  $k$ .*

*Proof.* Let  $\alpha = \sum_{\sigma \in G} a_{\sigma} \sigma$  and assume  $\alpha\tau = \tau\alpha$  for all  $\tau \in G$ . Then

$$\sum_{\sigma \in G} a_{\sigma} \tau\sigma\tau^{-1} = \sum_{\sigma \in G} a_{\sigma} \sigma.$$

Hence  $a_{\sigma_0} = a_{\sigma}$  whenever  $\sigma$  is conjugate to  $\sigma_0$ , and this means that we can write

$$\alpha = \sum_{\gamma} a_{\gamma} \gamma$$

where the sum is taken over all conjugacy classes  $\gamma$ .

**Remark.** We note that the conjugacy classes in fact form a basis of the center of  $\mathbf{Z}[G]$  over  $\mathbf{Z}$ , and thus play a universal role in the theory of representations.

We observe that the conjugacy classes are linearly independent over  $k$ , and form a basis for the center of  $k[G]$  over  $k$ .

Assume for the rest of this section that  $k$  is algebraically closed. Then

$$k[G] = \prod_{i=1}^s R_i$$

is a direct product of simple rings, and each  $R_i$  is a matrix algebra over  $k$ . In a direct product, the center is obviously the product of the centers of each factor. Let us denote by  $k_i$  the image of  $k$  in  $R_i$ , in other words,

$$k_i = ke_i,$$

where  $e_i$  is the unit element of  $R_i$ . Then the center of  $k[G]$  is also equal to

$$\prod_{i=1}^s k_i$$

which is  $s$ -dimensional over  $k$ .

If  $L_i$  is a typical simple left ideal of  $R_i$ , then

$$R_i \approx \text{End}_k(L_i).$$

We let

$$d_i = \dim_k L_i.$$

Then

$$d_i^2 = \dim_k R_i \quad \text{and} \quad \sum_{i=1}^s d_i^2 = n.$$

We also have the direct sum decomposition

$$R_i \approx L_i^{(d_i)}$$

as a  $(G, k)$ -space.

The above notation will remain fixed from now on.

We can summarize some of our results as follows.

**Proposition 4.2.** *Let  $k$  be algebraically closed. Then the number of conjugacy classes of  $G$  is equal to the number of simple characters of  $G$ , both of these being equal to the number  $s$  above. The conjugacy classes  $\gamma_1, \dots, \gamma_s$  and the unit elements  $e_1, \dots, e_s$  form bases of the center of  $k[G]$ .*

The number of elements in  $\gamma_i$  will be denoted by  $h_i$ . The number of elements in a conjugacy class  $\gamma$  will be denoted by  $h_\gamma$ . We call it the **class number**. The center of the group algebra will be denoted by  $Z_k(G)$ .

We can view  $k[G]$  as a  $G$ -module. Its character will be called the **regular character**, and will be denoted by  $\chi_{\text{reg}}$  or  $r_G$  if we need to specify the dependence on  $G$ . The representation on  $k[G]$  is called the **regular representation**. From our direct sum decomposition of  $k[G]$  we get

$$\boxed{\chi_{\text{reg}} = \sum_{i=1}^s d_i \chi_i.}$$

We shall determine the values of the regular character.

**Proposition 4.3.** *Let  $\chi_{\text{reg}}$  be the regular character. Then*

$$\chi_{\text{reg}}(\sigma) = 0 \quad \text{if} \quad \sigma \in G, \sigma \neq 1$$

$$\chi_{\text{reg}}(1) = n.$$

*Proof.* Let  $1 = \sigma_1, \dots, \sigma_n$  be the elements of  $G$ . They form a basis of  $k[G]$  over  $k$ . The matrix of 1 is the unit  $n \times n$  matrix. Thus our second assertion follows. If  $\sigma \neq 1$ , then multiplication by  $\sigma$  permutes  $\sigma_1, \dots, \sigma_n$ , and it is immediately clear that all diagonal elements in the matrix representing  $\sigma$  are 0. This proves what we wanted.

We observe that we have two natural bases for the center  $Z_k(G)$  of the group ring. First, the conjugacy classes of elements of  $G$ . Second, the elements  $e_1, \dots, e_s$  (i.e. the unit elements of the rings  $R_i$ ). We wish to find the relation between these, in other words, we wish to find the coefficients of  $e_i$  when expressed in terms of the group elements. The next proposition does this. The values of these coefficients will be interpreted in the next section as scalar products. This will clarify their mysterious appearance.

**Proposition 4.4.** *Assume again that  $k$  is algebraically closed. Let*

$$e_i = \sum_{\tau \in G} a_{\tau} \tau, \quad a_{\tau} \in k.$$

*Then*

$$a_{\tau} = \frac{1}{n} \chi_{\text{reg}}(e_i \tau^{-1}) = \frac{d_i}{n} \chi_i(\tau^{-1}).$$

*Proof.* We have for all  $\tau \in G$ :

$$\chi_{\text{reg}}(e_i \tau^{-1}) = \chi_{\text{reg}}\left(\sum_{\sigma \in G} a_{\sigma} \sigma \tau^{-1}\right) = \sum_{\sigma \in G} a_{\sigma} \chi_{\text{reg}}(\sigma \tau^{-1}).$$

By Proposition 4.3, we find

$$\chi_{\text{reg}}(e_i \tau^{-1}) = na_{\tau}.$$

On the other hand,

$$\chi_{\text{reg}}(e_i \tau^{-1}) = \sum_{j=1}^s d_j \chi_j(e_i \tau^{-1}) = d_i \chi_i(e_i \tau^{-1}) = d_i \chi_i(\tau^{-1}).$$

Hence

$$d_i \chi_i(\tau^{-1}) = na_{\tau}$$

for all  $\tau \in G$ . This proves our proposition.

**Corollary 4.5.** *Each  $e_i$  can be expressed in terms of group elements with coefficients which lie in the field generated over the prime field by  $m$ -th roots of unity, if  $m$  is an exponent for  $G$ .*

**Corollary 4.6.** *The dimensions  $d_i$  are not divisible by the characteristic of  $k$ .*

*Proof.* Otherwise,  $e_i = 0$ , which is impossible.

**Corollary 4.7.** *The simple characters  $\chi_1, \dots, \chi_s$  are linearly independent over  $k$ .*

*Proof.* The proof in Corollary 2.4 applies, since we now know that the characteristic does not divide  $d_i$ .

**Corollary 4.8.** *Assume in addition that  $k$  has characteristic 0. Then  $d_i \mid n$  for each  $i$ .*

*Proof.* Multiplying our expression for  $e_i$  by  $n/d_i$ , and also by  $e_i$ , we find

$$\frac{n}{d_i} e_i = \sum_{\sigma \in G} \chi_i(\sigma^{-1}) \sigma e_i.$$

Let  $\zeta$  be a primitive  $m$ -th root of unity, and let  $M$  be the module over  $\mathbf{Z}$  generated by the finite number of elements  $\zeta^v \sigma e_i$  ( $v = 0, \dots, m-1$  and  $\sigma \in G$ ). Then from the preceding relation, we see at once that multiplication by  $n/d_i$  maps  $M$  into itself. By definition, we conclude that  $n/d_i$  is integral over  $\mathbf{Z}$ , and hence lies in  $\mathbf{Z}$ , as desired.

**Theorem 4.9.** *Let  $k$  be algebraically closed. Let  $Z_k(G)$  be the center of  $k[G]$ , and let  $X_k(G)$  be the  $k$ -space of class functions on  $G$ . Then  $Z_k(G)$  and  $X_k(G)$  are the dual spaces of each other, under the pairing*

$$(f, \alpha) \mapsto f(\alpha).$$

The simple characters and the unit elements  $e_1, \dots, e_s$  form orthogonal bases to each other. We have

$$\chi_i(e_j) = \delta_{ij} d_i.$$

*Proof.* The formula has been proved in the proof of Theorem 2.3. The two spaces involved here both have dimension  $s$ , and  $d_i \neq 0$  in  $k$ . Our proposition is then clear.

## §5. ORTHOGONALITY RELATIONS

*Throughout this section, we assume that  $k$  is algebraically closed.*

If  $R$  is a subring of  $k$ , we denote by  $X_R(G)$  the  $R$ -module generated over  $R$  by the characters of  $G$ . It is therefore the module of functions which are linear combinations of simple characters with coefficients in  $R$ . If  $R$  is the prime ring (i.e. the integers  $\mathbf{Z}$  or the integers mod  $p$  if  $k$  has characteristic  $p$ ), then we denote  $X_R(G)$  by  $X(G)$ .

We shall now define a bilinear map on  $X(G) \times X(G)$ . If  $f, g \in X(G)$ , we define

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma)g(\sigma^{-1}).$$

**Theorem 5.1.** *The symbol  $\langle f, g \rangle$  for  $f, g \in X(G)$  takes on values in the prime ring. The simple characters form an orthonormal basis for  $X(G)$ , in other words*

$$\langle \chi_i, \chi_j \rangle = \delta_{ij}.$$

*For each ring  $R \subset k$ , the symbol has a unique extension to an  $R$ -bilinear form  $X_R(G) \times X_R(G) \rightarrow R$ , given by the same formula as above.*

*Proof.* By Proposition 4.4, we find

$$\chi_j(e_i) = \frac{d_i}{n} \sum_{\sigma \in G} \chi_i(\sigma^{-1})\chi_j(\sigma).$$

If  $i \neq j$  we get 0 on the left-hand side, so that  $\chi_i$  and  $\chi_j$  are orthogonal. If  $i = j$  we get  $d_i$  on the left-hand side, and we know that  $d_i \neq 0$  in  $k$ , by Corollary 4.6. Hence  $\langle \chi_i, \chi_i \rangle = 1$ . Since every element of  $X(G)$  is a linear combination of simple characters with integer coefficients, it follows that the values of our bilinear map are in the prime ring. The extension statement is obvious, thereby proving our theorem.

Assume that  $k$  has characteristic 0. Let  $m$  be an exponent for  $G$ , and let  $R$  contain the  $m$ -th roots of unity. If  $R$  has an automorphism of order 2 such that its effect on a root of unity is  $\zeta \mapsto \zeta^{-1}$ , then we shall call such an automorphism a **conjugation**, and denote it by  $a \mapsto \bar{a}$ .

**Theorem 5.2.** *Let  $k$  have characteristic 0, and let  $R$  be a subring containing the  $m$ -th roots of unity, and having a conjugation. Then the bilinear form on  $X(G)$  has a unique extension to a hermitian form*

$$X_R(G) \times X_R(G) \rightarrow R,$$

given by the formula

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma) \overline{g(\sigma)}.$$

The simple characters constitute an orthonormal basis of  $X_R(G)$  with respect to this form.

*Proof.* The formula given in the statement of the theorem gives the same value as before for the symbol  $\langle f, g \rangle$  when  $f, g$  lie in  $X(G)$ . Thus the extension exists, and is obviously unique.

We return to the case when  $k$  has arbitrary characteristic.

Let  $Z(G)$  denote the additive group generated by the conjugacy classes  $\gamma_1, \dots, \gamma_s$  over the prime ring. It is of dimension  $s$ . We shall define a bilinear map on  $Z(G) \times Z(G)$ . If  $\alpha = \sum a_\sigma \sigma$  has coefficients in the prime ring, we denote by  $\alpha^-$  the element  $\sum a_\sigma \sigma^{-1}$ .

**Proposition 5.3.** *For  $\alpha, \beta \in Z(G)$ , we can define a symbol  $\langle \alpha, \beta \rangle$  by either one of the following expressions, which are equal:*

$$\langle \alpha, \beta \rangle = \frac{1}{n} \chi_{\text{reg}}(\alpha \beta^-) = \frac{1}{n} \sum_{v=1}^s \chi_v(\alpha) \chi_v(\beta^-).$$

*The values of the symbol lie in the prime ring.*

*Proof.* Each expression is linear in its first and second variable. Hence to prove their equality, it will suffice to prove that the two expressions are equal when we replace  $\alpha$  by  $e_i$  and  $\beta$  by an element  $\tau$  of  $G$ . But then, our equality is equivalent to

$$\chi_{\text{reg}}(e_i \tau^{-1}) = \sum_{v=1}^s \chi_v(e_i) \chi_v(\tau^{-1}).$$

Since  $\chi_v(e_i) = 0$  unless  $v = i$ , we see that the right-hand side of this last relation is equal to  $d_i \chi_i(\tau^{-1})$ . Our two expressions are equal in view of Proposition 4.4.

The fact that the values lie in the prime ring follows from Proposition 4.3: The values of the regular character on group elements are equal to 0 or  $n$ , and hence in characteristic 0, are integers divisible by  $n$ .

As with  $X_R(G)$ , we use the notation  $Z_R(G)$  to denote the  $R$ -module generated by  $\gamma_1, \dots, \gamma_s$  over an arbitrary subring  $R$  of  $k$ .

**Lemma 5.4.** *For each ring  $R$  contained in  $k$ , the pairing of Proposition 5.3 has a unique extension to a map*

$$Z_R(G) \times Z(G) \rightarrow R$$

which is  $R$ -linear in its first variable. If  $R$  contains the  $m$ -th roots of unity, where  $m$  is an exponent for  $G$ , and also contains  $1/n$ , then  $e_i \in Z_R(G)$  for all  $i$ . The class number  $h_i$  is not divisible by the characteristic of  $k$ , and we have

$$e_i = \sum_{v=1}^s \langle e_i, \gamma_v \rangle \frac{1}{h_v} \gamma_v.$$

*Proof.* We note that  $h_i$  is not divisible by the characteristic because it is the index of a subgroup of  $G$  (the isotropy group of an element in  $\gamma_i$  when  $G$  operates by conjugation), and hence  $h_i$  divides  $n$ . The extension of our pairing as stated is obvious, since  $\gamma_1, \dots, \gamma_s$  form a basis of  $Z(G)$  over the prime ring. The expression of  $e_i$  in terms of this basis is only a reinterpretation of Proposition 4.4 in terms of the present pairing.

Let  $E$  be a free module over a subring  $R$  of  $k$ , and assume that we have a bilinear symmetric (or hermitian) form on  $E$ . Let  $\{v_1, \dots, v_s\}$  be an orthogonal basis for this module. If

$$v = a_1 v_1 + \dots + a_s v_s$$

with  $a_i \in R$ , then we call  $a_1, \dots, a_s$  the **Fourier coefficients** of  $v$  with respect to our basis. In terms of the form, these coefficients are given by

$$a_i = \frac{\langle v, v_i \rangle}{\langle v_i, v_i \rangle}$$

provided  $\langle v_i, v_i \rangle \neq 0$ .

We shall see in the next theorem that the expression for  $e_i$  in terms of  $\gamma_1, \dots, \gamma_s$  is a Fourier expansion.

**Theorem 5.5.** *The conjugacy classes  $\gamma_1, \dots, \gamma_s$  constitute an orthogonal basis for  $Z(G)$ . We have  $\langle \gamma_i, \gamma_i \rangle = h_i$ . For each ring  $R$  contained in  $k$ , the bilinear map of Proposition 5.3 has a unique extension to a  $R$ -bilinear map*

$$Z_R(G) \times Z_R(G) \rightarrow R.$$

*Proof.* We use the lemma. By linearity, the formula in the lemma remains valid when we replace  $R$  by  $k$ , and when we replace  $e_i$  by any element of  $Z_k(G)$ , in particular when we replace  $e_i$  by  $\gamma_i$ . But  $\{\gamma_1, \dots, \gamma_s\}$  is a basis of  $Z_k(G)$ , over  $k$ . Hence we find that  $\langle \gamma_i, \gamma_i \rangle = h_i$  and  $\langle \gamma_i, \gamma_j \rangle = 0$  if  $i \neq j$ , as was to be shown.

**Corollary 5.6.** *If  $G$  is commutative, then*

$$\frac{1}{n} \sum_{v=1}^n \chi_v(\sigma) \chi_v(\tau^{-1}) = \begin{cases} 0 & \text{if } \sigma \text{ is not equal to } \tau \\ 1 & \text{if } \sigma \text{ is equal to } \tau. \end{cases}$$

*Proof.* When  $G$  is commutative, each conjugacy class has exactly one element, and the number of simple characters is equal to the order of the group.

We consider the case of characteristic 0 for our  $Z(G)$  just as we did for  $X(G)$ . Let  $k$  have characteristic 0, and  $R$  be a subring of  $k$  containing the  $m$ -th roots of unity, and having a conjugation. Let  $\alpha = \sum_{\sigma \in G} a_{\sigma} \sigma$  with  $a_{\sigma} \in R$ . We define

$$\bar{\alpha} = \sum_{\sigma \in G} \bar{a}_{\sigma} \sigma^{-1}.$$

**Theorem 5.7.** *Let  $k$  have characteristic 0, and let  $R$  be a subring of  $k$ , containing the  $m$ -th roots of unity, and having a conjugation. Then the pairing of Proposition 5.3 has a unique extension to a hermitian form*

$$Z_R(G) \times Z_R(G) \rightarrow R$$

given by the formulas

$$\langle \alpha, \beta \rangle = \frac{1}{n} \chi_{\text{reg}}(\alpha \bar{\beta}) = \frac{1}{n} \sum_{v=1}^s \chi_v(\alpha) \overline{\chi_v(\beta)}.$$

The conjugacy classes  $\gamma_1, \dots, \gamma_s$  form an orthogonal basis for  $Z_R(G)$ . If  $R$  contains  $1/n$ , then  $e_1, \dots, e_s$  lie in  $Z_R(G)$  and also form an orthogonal basis for  $Z_R(G)$ . We have  $\langle e_i, e_i \rangle = d_i^2/n$ .

*Proof.* The formula given in the statement of the theorem gives the same value as the symbol  $\langle \alpha, \beta \rangle$  of Proposition 5.3 when  $\alpha, \beta$  lie in  $Z(G)$ . Thus the extension exists, and is obviously unique. Using the second formula in Proposition 5.3, defining the scalar product, and recalling that  $\chi_v(e_i) = 0$  if  $v \neq i$ , we see that

$$\langle e_i, e_i \rangle = \frac{1}{n} \chi_i(e_i) \overline{\chi_i(e_i)},$$

whence our assertion follows.

We observe that the Fourier coefficients of  $e_i$  relative to the basis  $\gamma_1, \dots, \gamma_s$  are the same with respect to the bilinear form of Theorem 5.5, or the hermitian form of Theorem 5.7. This comes from the fact that  $\gamma_1, \dots, \gamma_s$  lie in  $Z(G)$ , and form a basis of  $Z(G)$  over the prime ring.

We shall now reprove and generalize the orthogonality relations by another method. Let  $E$  be a finite dimensional  $(G, k)$ -space, so we have a representation

$$G \rightarrow \text{Aut}_k(E).$$

After selecting a basis of  $E$ , we get a representation of  $G$  by  $d \times d$  matrices. If  $\{v_1, \dots, v_d\}$  is the basis, then we have the dual basis  $\{\lambda_1, \dots, \lambda_d\}$  such that  $\lambda_i(v_j) = \delta_{ij}$ . If an element  $\sigma$  of  $G$  is represented by a matrix  $(\rho_{ij}(\sigma))$ , then each coefficient  $\rho_{ij}(\sigma)$  is a function of  $\sigma$ , called the  **$ij$ -coefficient function**. We can also write

$$\rho_{ij}(\sigma) = \lambda_j(\sigma v_i).$$

But instead of indexing elements of a basis or the dual basis, we may just as well work with any functional  $\lambda$  on  $E$ , and any vector  $v$ . Then we get a function

$$\sigma \mapsto \lambda(\sigma v) = \rho_{\lambda, v}(\sigma),$$

which will also be called a **coefficient function**. In fact, one can always complete  $v = v_1$  to a basis such that  $\lambda = \lambda_1$  is the first element in the dual basis, but using the notation  $\rho_{\lambda, v}$  is in many respects more elegant.

We shall constantly use:

**Schur's Lemma.** *Let  $E, F$  be simple  $(G, k)$ -spaces, and let*

$$\varphi : E \rightarrow F$$

*be a homomorphism. Then either  $\varphi = 0$  or  $\varphi$  is an isomorphism.*

*Proof.* Indeed, the kernel of  $\varphi$  and the image of  $\varphi$  are subspaces, so the assertion is obvious.

We use the same formula as before to define a scalar product on the space of all  $k$ -valued functions on  $G$ , namely

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma)g(\sigma^{-1}).$$

We shall derive various orthogonality relations among coefficient functions.

**Theorem 5.8.** *Let  $E, F$  be simple  $(G, k)$ -spaces. Let  $\lambda$  be a  $k$ -linear functional on  $E$ , let  $x \in E$  and  $y \in F$ . If  $E, F$  are not isomorphic, then*

$$\sum_{\sigma \in G} \lambda(\sigma x)\sigma^{-1}y = 0.$$

If  $\mu$  is a functional on  $F$  then the coefficient functions  $\rho_{\lambda, x}$  and  $\rho_{\mu, y}$  are orthogonal, that is

$$\sum_{\sigma \in G} \lambda(\sigma x) \mu(\sigma^{-1} y) = 0.$$

*Proof.* The map  $x \mapsto \sum \lambda(\sigma x) \sigma^{-1} y$  is a  $G$ -homomorphism of  $E$  into  $F$ , so Schur's lemma concludes the proof of the first statement. The second comes by applying the functional  $\mu$ .

As a corollary, we see that if  $\chi, \psi$  are distinct irreducible characters of  $G$  over  $k$ , then

$$\langle \chi, \psi \rangle = 0,$$

that is the characters are orthogonal. Indeed, the character associated with a representation  $\rho$  is the sum of the diagonal coefficient functions,

$$\chi = \sum_{i=1}^d \rho_{ii},$$

where  $d$  is the dimension of the representation. Two distinct characters correspond to non-isomorphic representations, so we can apply Proposition 5.8.

**Lemma 5.9.** *Let  $E$  be a simple  $(G, k)$ -space. Then any  $G$ -endomorphism of  $E$  is equal to a scalar multiple of the identity.*

*Proof.* The algebra  $\text{End}_{G, k}(E)$  is a division algebra by Schur's lemma, and is finite dimensional over  $k$ . Since  $k$  is assumed algebraically closed, it must be equal to  $k$  because any element generates a commutative subfield over  $k$ . This proves the lemma.

**Lemma 5.10.** *Let  $E$  be a representation space for  $G$  of dimension  $d$ . Let  $\lambda$  be a functional on  $E$ , and let  $x \in E$ . Let  $\varphi_{\lambda, x} \in \text{End}_k(E)$  be the endomorphism such that*

$$\varphi_{\lambda, x}(y) = \lambda(y)x.$$

*Then  $\text{tr}(\varphi_{\lambda, x}) = \lambda(x)$ .*

*Proof.* If  $x = 0$  the statement is obvious. Let  $x \neq 0$ . If  $\lambda(x) \neq 0$  we pick a basis of  $E$  consisting of  $x$  and a basis of the kernel of  $\lambda$ . If  $\lambda(x) = 0$ , we pick a basis of  $E$  consisting of a basis for the kernel of  $\lambda$ , and one other element. In either case it is immediate from the corresponding matrix representing  $\varphi_{\lambda, x}$  that the trace is given by the formula as stated in the lemma.

**Theorem 5.11.** *Let  $\rho: G \rightarrow \text{Aut}_k(E)$  be a simple representation of  $G$ , of dimension  $d$ . Then the characteristic of  $k$  does not divide  $d$ . Let  $x, y \in E$ . Then for any functionals  $\lambda, \mu$  on  $E$ ,*

$$\sum_{\sigma \in G} \lambda(\sigma x) \mu(\sigma^{-1} y) = \frac{n}{d} \lambda(y) \mu(x).$$

*Proof.* It suffices to prove that

$$\sum_{\sigma \in G} \lambda(\sigma x) \sigma^{-1} y = \frac{n}{d} \lambda(y) x.$$

For fixed  $y$  the map

$$x \mapsto \sum_{\sigma \in G} \lambda(\sigma x) \sigma^{-1} y$$

is immediately verified to be a  $G$ -endomorphism of  $E$ , so is equal to  $cI$  for some  $c \in k$  by Lemma 5.9. In fact, it is equal to

$$\sum_{\sigma \in G} \rho(\sigma^{-1}) \circ \varphi_{\lambda, y} \circ \rho(\sigma).$$

The trace of this expression is equal to  $n \cdot \text{tr}(\varphi_{\lambda, y})$  by Lemma 5.10, and also to  $dc$ . Taking  $\lambda, y$  such that  $\lambda(y) = 1$  shows that the characteristic does not divide  $d$ , and then we can solve for  $c$  as stated in the theorem.

**Corollary 5.12.** *Let  $\chi$  be the character of the representation of  $G$  on the simple space  $E$ . Then*

$$\langle \chi, \chi \rangle = 1.$$

*Proof.* This follows immediately from the theorem, and the expression of  $\chi$  as

$$\chi = \rho_{11} + \cdots + \rho_{dd}.$$

We have now recovered the fact that the characters of simple representations are orthonormal. We may then recover the idempotents in the group ring, that is, if  $\chi_1, \dots, \chi_s$  are the simple characters, we may now *define*

$$e_i = \frac{d_i}{n} \sum_{\sigma \in G} \chi_i(\sigma) \sigma^{-1}.$$

Then the orthonormality of the characters yields the formulas:

**Corollary 5.13.**  $\chi_i(e_j) = \delta_{ij} d_i$  and  $\chi_{\text{reg}} = \sum_{i=1}^s d_i \chi_i$ .

*Proof.* The first formula is a direct application of the orthonormality of the characters. The second formula concerning the regular character is obtained by writing

$$\chi_{\text{reg}} = \sum_j m_j \chi_j$$

with unknown coefficients. We know the values  $\chi_{\text{reg}}(1) = n$  and  $\chi_{\text{reg}}(\sigma) = 0$  if  $\sigma \neq 1$ . Taking the scalar product of  $\chi_{\text{reg}}$  with  $\chi_i$  for  $i = 1, \dots, s$  immediately yields the desired values for the coefficients  $m_j$ .

Since a character is a class function, one sees directly that each  $e_i$  is a linear combination of conjugacy classes, and so is in the center of the group ring  $k[G]$ .

Now let  $E_i$  be a representation space of  $\chi_i$ , and let  $\rho_i$  be the representation of  $G$  or  $k[G]$  on  $E_i$ . For  $\alpha \in k[G]$  we let  $\rho_i(\alpha) : E_i \rightarrow E_i$  be the map such that  $\rho_i(\alpha)x = \alpha x$  for all  $x \in E_i$ .

**Proposition 5.14.** *We have*

$$\rho_i(e_i) = \text{id} \quad \text{and} \quad \rho_i(e_j) = 0 \quad \text{if } i \neq j.$$

*Proof.* The map  $x \mapsto e_i x$  is a  $G$ -homomorphism of  $E_i$  into itself since  $e_i$  is in the center of  $k[G]$ . Hence by Lemma 5.9 this homomorphism is a scalar multiple of the identity. Taking the trace and using the orthogonality relations between simple characters immediately gives the desired value of this scalar.

We now find that

$$\sum_{i=1}^s e_i = 1$$

because the group ring  $k[G]$  is a direct sum of simple spaces, possibly with multiplicities, and operates faithfully on itself.

The orthonormality relations also allow us to expand a function in a Fourier expression, relative to the characters if it is a class function, and relative to the coefficient functions in general. We state this in two theorems.

**Theorem 5.15.** *Let  $f$  be a class function on  $G$ . Then*

$$f = \sum_{i=1}^s \langle f, \chi_i \rangle \chi_i.$$

*Proof.* The number of conjugacy class is equal to the number of distinct characters, and these are linearly independent, so they form a basis for the class functions. The coefficients are given by the stated formula, as one sees by taking the scalar product of  $f$  with any character  $\chi_j$  and using the orthonormality.

**Theorem 5.16.** *Let  $\rho^{(i)}$  be a matrix representation of  $G$  on  $E_i$  relative to a choice of basis, and let  $\rho_{v,\mu}^{(i)}$  be the coefficient functions of this matrix,  $i = 1, \dots, s$  and  $v, \mu = 1, \dots, d_i$ . Then the functions  $\rho_{v,\mu}^{(i)}$  form an orthogonal basis for the space of all functions on  $G$ , and hence for any function  $f$  on  $G$  we have*

$$f = \sum_{i=1}^s \sum_{v,\mu} \frac{1}{d_i} \langle f, \rho_{v,\mu}^{(i)} \rangle \rho_{v,\mu}^{(i)}.$$

*Proof.* That the coefficient functions form an orthogonal basis follows from Theorems 5.8 and 5.11. The expression of  $f$  in terms of this basis is then merely the standard Fourier expansion relative to any scalar product. This concludes the proof.

Suppose now for concreteness that  $k = \mathbf{C}$  is the complex numbers. Recall that an **effective character**  $\chi$  is an element of  $X(G)$ , such that if

$$\chi = \sum_{i=1}^s m_i \chi_i$$

is a linear combination of the simple characters with integral coefficients, then we have  $m_i \geq 0$  for all  $i$ . In light of the orthonormality of the simple characters, we get for all elements  $\chi \in X(G)$  the relations

$$\|\chi\|^2 = \langle \chi, \chi \rangle = \sum_{i=1}^s m_i^2 \quad \text{and} \quad m_i = \langle \chi, \chi_i \rangle.$$

Hence we get (a) of the next theorem.

**Theorem 5.17.** (a) *Let  $\chi$  be an effective character in  $X(G)$ . Then  $\chi$  is simple over  $\mathbf{C}$  if and only if  $\|\chi\|^2 = 1$ , or alternatively,*

$$\sum_{\sigma \in G} |\chi(\sigma)|^2 = \#(G).$$

(b) *Let  $\chi, \psi$  be effective characters in  $X(G)$ , and let  $E, F$  be their representation spaces over  $\mathbf{C}$ . Then*

$$\langle \chi, \psi \rangle_G = \dim \text{Hom}_G(E, F).$$

*Proof.* The first part has been proved, and for (b), let  $\psi = \sum q_i \chi_i$ . Then by orthonormality, we get

$$\langle \chi, \psi \rangle_G = \sum m_i q_i.$$

But if  $E_i$  is the representation space of  $\chi_i$  over  $\mathbf{C}$ , then by Schur's lemma

$$\dim \text{Hom}_G(E_i, E_i) = 1 \text{ and } \dim \text{Hom}_G(E_i, E_j) = 0 \text{ for } i \neq j.$$

Hence  $\dim \text{Hom}_G(E, F) = \sum m_i q_i$ , thus proving (b).

**Corollary 5.18** *With the above notation and  $k = \mathbf{C}$  for simplicity, we have:*

- (a) *The multiplicity of  $1_G$  in  $E^\vee \otimes F$  is  $\dim_k \text{inv}_G(E^\vee \otimes F)$ .*
- (b) *The  $(G, k)$ -space  $E$  is simple if and only if  $1_G$  has multiplicity 1 in  $E^\vee \otimes E$ .*

*Proof.* Immediate from Theorem 5.17 and formula (3) of §1.

**Remark.** The criterion of Theorem 5.17(a) is useful in testing whether a representation is simple. In practice, representations are obtained by inducing from 1-dimensional characters, and such induced representations do have a tendency to be irreducible. We shall see a concrete case in §12.

---

## §6. INDUCED CHARACTERS

The notation is the same as in the preceding section. However, we don't need all the results proved there; all we need is the bilinear pairing on  $X(G)$ , and its extension to

$$X_R(G) \times X_R(G) \rightarrow R.$$

The symbol  $\langle \ , \ \rangle$  may be interpreted either as the bilinear extension, or the hermitian extension according to Theorem 5.2.

Let  $S$  be a subgroup of  $G$ . We have an  $R$ -linear map called the restriction

$$\text{res}_S^G : X_R(G) \rightarrow X_R(S)$$

which to each class function on  $G$  associates its restriction to  $S$ . It is a ring-homomorphism. We sometimes let  $f_S$  denote the restriction of  $f$  to  $S$ .

We shall define a map in the opposite direction,

$$\text{ind}_S^G : X_R(S) \rightarrow X_R(G),$$

which we call the **induction map**. If  $g \in X_R(S)$ , we extend  $g$  to  $g_S$  on  $G$  by letting  $g_S(\sigma) = 0$  if  $\sigma \notin S$ . Then we define the **induced function**

$$g^G(\sigma) = \text{ind}_S^G(g)(\sigma) = \frac{1}{(S : 1)} \sum_{\tau \in G} g_S(\tau\sigma\tau^{-1}).$$

Then  $\text{ind}_S^G(g)$  is a class function on  $G$ . It is clear that  $\text{ind}_S^G$  is  $R$ -linear.

Since we deal with two groups  $S$  and  $G$ , we shall denote the scalar product by  $\langle \ , \ \rangle_S$  and  $\langle \ , \ \rangle_G$  when it is taken with these respective groups. The next theorem shows among other things that the restriction and transfer are adjoint to each other with respect to our form.

**Theorem 6.1.** *Let  $S$  be a subgroup of  $G$ . Then the following rules hold:*

(i) **(Frobenius reciprocity)** *For  $f \in X_R(G)$ , and  $g \in X_R(S)$  we have*

$$\langle \text{ind}_S^G(g), f \rangle_G = \langle g, \text{Res}_S^G(f) \rangle_S.$$

(ii)  $\text{Ind}_S^G(g)f = \text{ind}_S^G(gf_S)$ .

(iii) *If  $T \subset S \subset G$  are subgroups of  $G$ , then*

$$\text{ind}_S^G \circ \text{ind}_T^S = \text{ind}_T^G.$$

(iv) *If  $\sigma \in G$  and  $g^\sigma$  is defined by  $g^\sigma(\tau^\sigma) = g(\tau)$ , where  $\tau^\sigma = \sigma^{-1}\tau\sigma$ , then*

$$\text{ind}_S^G(g) = \text{ind}_{S^\sigma}^G(g^\sigma).$$

(v) *If  $\psi$  is an effective character of  $S$  then  $\text{ind}_S^G(\psi)$  is effective.*

*Proof.* Let us first prove (ii). We must show that  $g^G f = (gf_S)^G$ . We have

$$(g^G f)(\tau) = \frac{1}{(S : 1)} \sum_{\sigma \in G} g_S(\sigma \tau \sigma^{-1}) f(\tau) = \frac{1}{(S : 1)} \sum_{\sigma \in G} g_S(\sigma \tau \sigma^{-1}) f(\sigma \tau \sigma^{-1}).$$

The last expression just obtained is equal to  $(gf_S)^G$ , thereby proving (ii). Let us sum over  $\tau$  in  $G$ . The only non-zero contributions in our double sum will come from those elements of  $S$  which can be expressed in the form  $\sigma \tau \sigma^{-1}$  with  $\sigma, \tau \in G$ . The number of pairs  $(\sigma, \tau)$  such that  $\sigma \tau \sigma^{-1}$  is equal to a fixed element of  $G$  is equal to  $n$  (because for every  $\lambda \in G$ ,  $(\sigma \lambda, \lambda^{-1} \tau \lambda)$  is another such pair, and the total number of pairs is  $n^2$ ). Hence our expression is equal to

$$(G : 1) \frac{1}{(S : 1)} \sum_{\lambda \in S} g(\lambda) f(\lambda).$$

Our first rule then follows from the definitions of the scalar products in  $G$  and  $S$  respectively.

Now let  $g = \psi$  be an effective character of  $S$ , and let  $f = \chi$  be a simple character of  $G$ . From (i) we find that the Fourier coefficients of  $g^G$  are integers  $\geq 0$  because  $\text{res}_S^G(\chi)$  is an effective character of  $S$ . Therefore the scalar product

$$\langle \psi, \text{res}_S^G(\chi) \rangle_S$$

is  $\geq 0$ . Hence  $\psi^G$  is an effective character of  $G$ , thereby proving (v).

In order to prove the transitivity property, it is convenient to use the following notation.

Let  $\{c\}$  denote the set of *right* cosets of  $S$  in  $G$ . For each right coset  $c$ , we select a fixed coset representative denoted by  $\bar{c}$ . Thus if  $\bar{c}_1, \dots, \bar{c}_r$  are these representatives, then

$$G = \bigcup_c c = \bigcup_c S\bar{c} = \bigcup_{i=1}^r S\bar{c}_i.$$

**Lemma 6.2.** *Let  $g$  be a class function on  $S$ . Then*

$$\text{ind}_S^G(g)(\xi) = \sum_{i=1}^r g_S(\bar{c}_i \xi \bar{c}_i^{-1}).$$

*Proof.* We can split the sum over all  $\sigma \in G$  in the definition of the induced function into a double sum

$$\sum_{\sigma \in G} = \sum_{\sigma \in S} \sum_{i=1}^r$$

and observe that each term  $g_S(\sigma\bar{c}\xi\bar{c}^{-1}\sigma^{-1})$  is equal to  $g_S(\bar{c}\xi\bar{c}^{-1})$  if  $\sigma \in S$ , because  $g$  is a class function. Hence the sum over  $\sigma \in S$  is enough to cancel the factor  $1/(S : 1)$  in front, to give the expression in the lemma.

If  $T \subset S \subset G$  are subgroups of  $G$ , and if

$$G = \bigcup S\bar{c}_i \quad \text{and} \quad S = \bigcup T\bar{d}_j$$

are decompositions into right cosets, then  $\{\bar{d}_j\bar{c}_i\}$  form a system of representatives for the right cosets of  $T$  in  $G$ . From this the transitivity property (iii) is obvious.

We shall leave (iv) as an exercise (trivial, using the lemma).

## §7. INDUCED REPRESENTATIONS

Let  $G$  be a group and  $S$  a subgroup of finite index. Let  $F$  be an  $S$ -module. We consider the category  $\mathcal{C}$  whose objects are  $S$ -homomorphisms  $\varphi : F \rightarrow E$  of  $F$  into a  $G$ -module  $E$ . (We note that a  $G$ -module  $E$  can be regarded as an  $S$ -module by restriction.) If  $\varphi' : F \rightarrow E'$  is another object in  $\mathcal{C}$ , we define a morphism  $\varphi' \rightarrow \varphi$  in  $\mathcal{C}$  to be a  $G$ -homomorphism  $\eta : E' \rightarrow E$  making the following diagram commutative:

$$\begin{array}{ccc} & E' & \\ \varphi' \nearrow & \downarrow \eta & \\ F & \xrightarrow{\varphi} & E \end{array}$$

A universal object in  $\mathcal{C}$  is determined up to a unique  $G$ -isomorphism. It will be denoted by

$$\text{ind}_S^G : F \rightarrow \text{ind}_S^G(F).$$

We shall prove below that a universal object always exists. If  $\varphi : F \rightarrow E$  is a universal object, we call  $E$  an **induced module**. It is uniquely determined, up to a unique  $G$ -isomorphism making a diagram commutative. For convenience, we shall select one induced module such that  $\varphi$  is an inclusion. We shall then call this particular module  $\text{ind}_S^G(F)$  the  **$G$ -module induced by  $F$** . In particular, given an  $S$ -homomorphism  $\varphi : F \rightarrow E$  into a  $G$ -module  $E$ , there is a unique  $G$ -homomorphism  $\varphi_* : \text{ind}_S^G(F) \rightarrow E$  making the following diagram commutative:

$$\begin{array}{ccc} & \text{ind}_S^G(F) & \\ \text{ind}_S^G \nearrow & \downarrow \varphi_* = \text{ind}_S^G(\varphi) & \\ F & \xrightarrow{\varphi} & E \end{array}$$

The association  $\varphi \mapsto \text{ind}_S^G(\varphi)$  then induces an isomorphism

$$\text{Hom}_G(\text{ind}_S^G(F), E) \approx \text{Hom}_S(F, \text{res}_S^G(E)),$$

for an  $S$ -module  $F$  and a  $G$ -module  $E$ . We shall see in a moment that  $\text{ind}_S^G$  is a functor from  $\text{Mod}(S)$  to  $\text{Mod}(G)$ , and the above formula may be described as saying that **induction is the adjoint functor of restriction**. One also calls this relation **Frobenius reciprocity for modules**, because Theorem 6.1(i) is a corollary.

Sometimes, if the reference to  $F$  as an  $S$ -module is clear, we shall omit the subscript  $S$ , and write simply

$$\text{ind}^G(F)$$

for the induced module.

Let  $f: F' \rightarrow F$  be an  $S$ -homomorphism. If

$$\varphi_S^G: F' \rightarrow \text{ind}_S^G(F')$$

is a  $G$ -module induced by  $F'$ , then there exists a unique  $G$ -homomorphism  $\text{ind}_S^G(F') \rightarrow \text{ind}_S^G(F)$  making the following diagram commutative:

$$\begin{array}{ccc} F' & \xrightarrow{\varphi_S^G} & \text{ind}_S^G(F') \\ f \downarrow & \searrow \text{dashed} & \downarrow \text{ind}_S^G(f) \\ F & \xrightarrow{\varphi_S^G} & \text{ind}_S^G(F) \end{array}$$

It is simply the  $G$ -homomorphism corresponding to the universal property for the  $S$ -homomorphism  $\varphi_G^S \circ f$ , represented by a dashed line in our diagram. *Thus  $\text{ind}_S^G$  is a functor, from the category of  $S$ -modules to the category of  $G$ -modules.*

From the universality and uniqueness of the induced module, we get some formal properties:

*$\text{ind}_S^G$  commutes with direct sums: If we have an  $S$ -direct sum  $F \oplus F'$ , then*

$$\text{ind}_S^G(F \oplus F') \approx \text{ind}_S^G(F) \oplus \text{ind}_S^G(F'),$$

*the direct sum on the right being a  $G$ -direct sum.*

*If  $f, g: F' \rightarrow F$  are  $S$ -homomorphisms, then*

$$\text{ind}_S^G(f + g) = \text{ind}_S^G(f) + \text{ind}_S^G(g).$$

*If  $T \subset S \subset G$  are subgroups of  $G$ , and  $F$  is a  $T$ -module, then*

$$\text{ind}_S^G \circ \text{ind}_T^S(F) \approx \text{ind}_T^G(F).$$

In all three cases, the equality between the left member and the right member of our equations follows at once by using the uniqueness of the universal object. We shall leave the verifications to the reader.

To prove the existence of the induced module, we let  $M_G^S(F)$  be the additive group of functions  $f: G \rightarrow F$  satisfying

$$\sigma f(\xi) = f(\sigma \xi)$$

for  $\sigma \in S$  and  $\xi \in G$ . We define an operation of  $G$  on  $M_G^S(F)$  by letting

$$(\sigma f)(\xi) = f(\xi \sigma)$$

for  $\sigma, \xi \in G$ . It is then clear that  $M_G^S(F)$  is a  $G$ -module.

**Proposition 7.1.** *Let  $\varphi: F \rightarrow M_G^S(F)$  be such that  $\varphi(x) = \varphi_x$  is the map*

$$\varphi_x(\tau) = \begin{cases} 0 & \text{if } \tau \notin S \\ \tau x & \text{if } \tau \in S. \end{cases}$$

*Then  $\varphi$  is an  $S$ -homomorphism,  $\varphi: F \rightarrow M_G^S(F)$  is universal, and  $\varphi$  is injective. The image of  $\varphi$  consists of those elements  $f \in M_G^S(F)$  such that  $f(\tau) = 0$  if  $\tau \notin S$ .*

*Proof.* Let  $\sigma \in S$  and  $x \in F$ . Let  $\tau \in G$ . Then

$$(\sigma \varphi_x)(\tau) = \varphi_x(\tau \sigma).$$

If  $\tau \in S$ , then this last expression is equal to  $\varphi_{\sigma x}(\tau)$ . If  $\tau \notin S$ , then  $\tau \sigma \notin S$ , and hence both  $\varphi_{\sigma x}(\tau)$  and  $\varphi_x(\tau \sigma)$  are equal to 0. Thus  $\varphi$  is an  $S$ -homomorphism, and it is immediately clear that  $\varphi$  is injective. Furthermore, if  $f \in M_G^S(F)$  is such that  $f(\tau) = 0$  if  $\tau \notin S$ , then from the definitions, we conclude that  $f = \varphi_x$  where  $x = f(1)$ .

There remains to prove that  $\varphi$  is universal. To do this, we shall analyze more closely the structure of  $M_G^S(F)$ .

**Proposition 7.2.** *Let  $G = \bigcup_{i=1}^r S\bar{c}_i$  be a decomposition of  $G$  into right cosets.*

*Let  $F_1$  be the additive group of functions in  $M_G^S(F)$  having value 0 at elements  $\xi \in G$ ,  $\xi \notin S$ . Then*

$$M_G^S(F) = \bigoplus_{i=1}^r \bar{c}_i^{-1} F_1,$$

*the direct sum being taken as an abelian group.*

*Proof.* For each  $f \in M_G^S(F)$ , let  $f_i$  be the function such that

$$f_i(\xi) = \begin{cases} 0 & \text{if } \xi \notin S\bar{c}_i \\ f(\xi) & \text{if } \xi \in S\bar{c}_i. \end{cases}$$

For all  $\sigma \in S$  we have  $f_i(\sigma \bar{c}_i) = (\bar{c}_i f_i)(\sigma)$ . It is immediately clear that  $\bar{c}_i f_i$  lies in  $F_1$ , and

$$f = \sum_{i=1}^r \bar{c}_i^{-1}(\bar{c}_i f_i).$$

Thus  $M_G^S(F)$  is the sum of the subgroups  $\bar{c}_i^{-1}F_1$ . It is clear that this sum is direct, as desired.

We note that  $\{\bar{c}_1^{-1}, \dots, \bar{c}_r^{-1}\}$  form a system of representatives for the *left* cosets of  $S$  in  $G$ . The operation of  $G$  on  $M_G^S(F)$  is defined by the preceding direct sum decomposition. We see that  $G$  permutes the factors transitively. The factor  $F_1$  is  $S$ -isomorphic to the original module  $F$ , as stated in Proposition 7.1.

Suppose that instead of considering arbitrary modules, we start with a commutative ring  $R$  and consider only  $R$ -modules  $E$  on which we have a representation of  $G$ , i.e. a homomorphism  $G \rightarrow \text{Aut}_R(E)$ , thus giving rise to what we call a  $(G, R)$ -module. Then it is clear that all our constructions and definitions can be applied in this context. Therefore if we have a representation of  $S$  on an  $R$ -module  $F$ , then we obtain an induced representation of  $G$  on  $\text{ind}_G^S(F)$ . Then we deal with the category  $\mathcal{C}$  of  $S$ -homomorphisms of an  $(S, R)$ -module into a  $(G, R)$ -module. To simplify the notation, we may write “ $G$ -module” to mean “ $(G, R)$ -module” when such a ring  $R$  enters as a ring of coefficients.

**Theorem 7.3.** *Let  $\{\lambda_1, \dots, \lambda_r\}$  be a system of left coset representatives of  $S$  in  $G$ . There exists a  $G$ -module  $E$  containing  $F$  as an  $S$ -submodule, such that*

$$E = \bigoplus_{i=1}^r \lambda_i F$$

*is a direct sum (as  $R$ -modules). Let  $\varphi : F \rightarrow E$  be the inclusion mapping. Then  $\varphi$  is universal in our category  $\mathcal{C}$ , i.e.  $E$  is an induced module.*

*Proof.* By the usual set-theoretic procedure of replacing  $F_1$  by  $F$  in  $M_G^S(F)$ , obtain a  $G$ -module  $E$  containing  $F$  as a  $S$ -submodule, and having the desired direct sum decomposition. Let  $\varphi' : F \rightarrow E'$  be an  $S$ -homomorphism into a  $G$ -module  $E'$ . We define

$$h : E \rightarrow E'$$

by the rule

$$h(\lambda_1 x_1 + \dots + \lambda_r x_r) = \lambda_1 \varphi'(x_1) + \dots + \lambda_r \varphi'(x_r)$$

for  $x_i \in F$ . This is well defined since our sum for  $E$  is direct. We must show that  $h$  is a  $G$ -homomorphism. Let  $\sigma \in G$ . Then

$$\sigma \lambda_i = \lambda_{\sigma(i)} \tau_{\sigma, i}$$

where  $\sigma(i)$  is some index depending on  $\sigma$  and  $i$ , and  $\tau_{\sigma, i}$  is an element of  $S$ , also

depending on  $\sigma, i$ . Then

$$h(\sigma \lambda_i x_i) = h(\lambda_{\sigma(i)} \tau_{\sigma, i} x_i) = \lambda_{\sigma(i)} \varphi'(\tau_{\sigma, i} x_i).$$

Since  $\varphi'$  is an  $S$ -homomorphism, we see that this expression is equal to

$$\lambda_{\sigma(i)} \tau_{\sigma, i} \varphi'(x_i) = \sigma h(\lambda_i x_i).$$

By linearity, we conclude that  $h$  is a  $G$ -homomorphism, as desired.

In the next proposition we return to the case when  $R$  is our field  $k$ .

**Proposition 7.4.** *Let  $\psi$  be the character of the representation of  $S$  on the  $k$ -space  $F$ . Let  $E$  be the space of an induced representation. Then the character  $\chi$  of  $E$  is equal to the induced character  $\psi^G$ , i.e. is given by the formula*

$$\chi(\xi) = \sum_c \psi_0(\bar{c} \xi \bar{c}^{-1}),$$

where the sum is taken over the right cosets  $c$  of  $S$  in  $G$ ,  $\bar{c}$  is a fixed coset representative for  $c$ , and  $\psi_0$  is the extension of  $\psi$  to  $G$  obtained by setting  $\psi_0(\sigma) = 0$  if  $\sigma \notin S$ .

*Proof.* Let  $\{w_1, \dots, w_m\}$  be a basis for  $F$  over  $k$ . We know that

$$E = \bigoplus \bar{c}^{-1} F.$$

Let  $\sigma$  be an element of  $G$ . The elements  $\{\bar{c} \sigma^{-1} w_j\}_{c, j}$  form a basis for  $E$  over  $k$ .

We observe that  $\bar{c} \sigma \bar{c} \sigma^{-1}$  is an element of  $S$  because

$$S \bar{c} \sigma = S c \sigma = S \bar{c} \sigma.$$

We have

$$\sigma(\bar{c} \sigma^{-1} w_j) = \bar{c}^{-1} (\bar{c} \sigma \bar{c} \sigma^{-1}) w_j.$$

Let

$$(\bar{c} \sigma \bar{c} \sigma^{-1})_{\mu j}$$

be the components of the matrix representing the effect of  $\bar{c} \sigma \bar{c} \sigma^{-1}$  on  $F$  with respect to the basis  $\{w_1, \dots, w_m\}$ . Then the action of  $\sigma$  on  $E$  is given by

$$\begin{aligned} \sigma(\bar{c} \sigma^{-1} w_j) &= \bar{c}^{-1} \sum_{\mu} (\bar{c} \sigma \bar{c} \sigma^{-1})_{\mu j} w_{\mu} \\ &= \sum_{\mu} (\bar{c} \sigma \bar{c} \sigma^{-1})_{\mu j} (\bar{c}^{-1} w_{\mu}). \end{aligned}$$

By definition,

$$\chi(\sigma) = \sum_{c \sigma = c} \sum_j (\bar{c} \sigma \bar{c} \sigma^{-1})_{jj}.$$

But  $c\sigma = c$  if and only if  $\bar{c}\sigma\bar{c}^{-1} \in S$ . Furthermore,

$$\psi(\bar{c}\sigma\bar{c}^{-1}) = \sum_j (\bar{c}\sigma\bar{c}^{-1})_{jj}.$$

Hence

$$\chi(\sigma) = \sum_c \psi_0(\bar{c}\sigma\bar{c}^{-1}),$$

as was to be shown.

**Remark.** Having given an explicit description of the representation space for an induced character, we have in some sense completed the more elementary part of the theory of induced characters. Readers interested in seeing an application can immediately read §12.

### Double cosets

Let  $G$  be a group and let  $S$  be a subgroup. To avoid superscripts we use the following notation. Let  $\gamma \in G$ . We write

$$[\gamma]S = \gamma S \gamma^{-1} \quad \text{and} \quad S[\gamma] = \gamma^{-1} S \gamma.$$

We shall suppose that  $S$  has finite index. We let  $H$  be a subgroup. A subset of  $G$  of the form  $H\gamma S$  is called a **double coset**. As with cosets, it is immediately verified that  $G$  is a disjoint union of double cosets. We let  $\{\gamma\}$  be a family of double coset representatives, so we have the disjoint union

$$G = \bigcup_{\gamma} H\gamma S.$$

For each  $\gamma$  we have a decomposition into ordinary cosets

$$H = \bigcup_{\tau_{\gamma}} \tau_{\gamma}(H \cap [\gamma]S),$$

where  $\{\tau_{\gamma}\}$  is a finite family of elements of  $H$ , depending on  $\gamma$ .

**Lemma 7.5.** *The elements  $\{\tau_{\gamma}\}$  form a family of left coset representatives for  $S$  in  $G$ ; that is, we have a disjoint union*

$$G = \bigcup_{\gamma, \tau_{\gamma}} \tau_{\gamma}\gamma S.$$

*Proof.* First we have by hypothesis

$$G = \bigcup_{\gamma} \bigcup_{\tau_{\gamma}} \tau_{\gamma}(H \cap [\gamma]S)\gamma S,$$

and so every element of  $G$  can be written in the form

$$\tau_{\gamma}\gamma s_1 \gamma^{-1} \gamma s_2 = \tau_{\gamma}\gamma s \quad \text{with} \quad s_1, s_2, s \in S.$$

On the other hand, the elements  $\tau_{\gamma}\gamma$  represent distinct cosets of  $S$ , because if  $\tau_{\gamma}\gamma S = \tau_{\gamma'}\gamma' S$ , then  $\gamma = \gamma'$ , since the elements  $\gamma$  represent distinct double cosets,

whence  $\tau_\gamma$  and  $\tau_{\gamma'}$  represent the same coset of  $\gamma S \gamma^{-1}$ , and therefore are equal. This proves the lemma.

Let  $F$  be an  $S$ -module. Given  $\gamma \in G$ , we denote by  $[\gamma]F$  the  $[\gamma]S$ -module such that for  $\gamma s \gamma^{-1} \in [\gamma]S$ , the operation is given by

$$\gamma s \gamma^{-1} \cdot [\gamma]x = [\gamma]sx.$$

This notation is compatible with the notation that if  $F$  is a submodule of a  $G$ -module  $E$ , then we may form  $\gamma F$  either according to the formal definition above, or according to the operation of  $G$ . The two are naturally isomorphic (essentially equal). We shall write

$$[\gamma] : F \rightarrow \gamma F \text{ or } [\gamma]F$$

for the above isomorphism from the  $S$ -module  $F$  to the  $[\gamma]S$ -module  $\gamma F$ . If  $S_1$  is a subgroup of  $S$ , then by restriction  $F$  is also an  $S_1$ -module, and we use  $[\gamma]$  also in this context, especially for the subgroup  $H \cap [\gamma]S$  which is contained in  $[\gamma]S$ .

**Theorem 7.6.** *Applied to the  $S$ -module  $F$ , we have an isomorphism of  $H$ -modules*

$$\text{res}_H^G \circ \text{ind}_S^G \approx \bigoplus_{\gamma} \text{ind}_{H \cap [\gamma]S}^H \circ \text{res}_{H \cap [\gamma]S}^{[\gamma]S} \circ [\gamma]$$

where the direct sum is taken over double coset representatives  $\gamma$ .

*Proof.* The induced module  $\text{ind}_S^G(F)$  is simply the direct sum

$$\text{ind}_S^G(F) = \bigoplus_{\gamma, \tau_\gamma} \tau_\gamma \gamma F$$

by Lemma 7.5, which gives us coset representatives of  $S$  in  $G$ , and Theorem 7.3. On the other hand, for each  $\gamma$ , the module

$$\bigoplus_{\tau_\gamma} \tau_\gamma \gamma F$$

is a representation module for the induced representation from  $H \cap [\gamma]S$  on  $\gamma F$  to  $H$ . Taking the direct sum over  $\gamma$ , we get the right-hand side of the expression in the theorem, and thus prove the theorem.

**Remark.** The formal relation of Theorem 7.6 is one which occurred in Artin's formalism of induced characters and  $L$ -functions; cf. the exercises and [La 70], Chapter XII, §3. For applications to the cohomology of groups, see [La 96]. The formalism also emerged in Mackey's work [Ma 51], [Ma 53], which we shall now consider more systematically. The rest of this section is due to Mackey. For more extensive results and applications, see Curtis-Reiner [CuR 81], especially Chapter 1. See also Exercises 15, 16, and 17.

To deal more systematically with conjugations, we make some general functorial remarks. Let  $E$  be a  $G$ -module. Possibly one may have a commutative ring  $R$  such that  $E$  is a  $(G, R)$ -module. We shall deal systematically with the functors

$\text{Hom}_G, E^\vee$ , and the tensor product. Let

$$\lambda : E \rightarrow \lambda E$$

by a  $R$ -isomorphism. Then interpreting elements of  $G$  as endomorphisms of  $E$  we obtain a group  $\lambda G \lambda^{-1}$  operating on  $\lambda E$ . We shall also write  $[\lambda]G$  instead of  $\lambda G \lambda^{-1}$ . Let  $E_1, E_2$  be  $(G, R)$ -modules. Let  $\lambda_1 : E_1 \rightarrow \lambda_1 E_1$  be  $R$ -isomorphisms. Then we have a natural  $R$ -isomorphism

$$(1) \quad \lambda_2 \text{Hom}_G(E_1, E_2) \lambda_1^{-1} = \text{Hom}_{\lambda_2 G \lambda_1^{-1}}(\lambda_1 E_1, \lambda_2 E_2),$$

and especially

$$[\lambda] \text{Hom}_G(E, E) = \text{Hom}_{[\lambda]G}(\lambda E, \lambda E).$$

As a special case of the general situation, let  $H, S$  be subgroups of  $G$ , and let  $F_1, F_2$  be  $(H, R)$ - and  $(S, R)$ -modules respectively, and let  $\sigma, \tau \in G$ . Suppose that  $\sigma^{-1}\tau$  lies in the double coset  $D = H\gamma S$ . Then we have an  $R$ -isomorphism

$$(2) \quad \text{Hom}_{[\sigma]H \cap [\tau]S}([\sigma]F_1, [\tau]F_2) \approx \text{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2).$$

This is immediate by conjugation, writing  $\tau = \sigma h \gamma s$  with  $h \in H, s \in S$ , conjugating first with  $[\sigma h]^{-1}$ , and then observing that for  $s \in S$ , and an  $S$ -module  $F$ , we have  $[s]S = S$ , and  $[s^{-1}]F$  is isomorphic to  $F$ . In light of (2), we see that the  $R$ -module on the left-hand side depends only on the double coset. Let  $D$  be a double coset. We shall use the notation

$$M_D(F_1, F_2) = \text{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2)$$

where  $\gamma$  represents the double coset  $D$ . With this notation we have:

**Theorem 7.7.** *Let  $H, S$  be subgroups of finite index in  $G$ . Let  $F_1, F_2$  be  $(H, R)$  and  $(S, R)$ -modules respectively. Then we have an isomorphism of  $R$ -modules*

$$\text{Hom}_G(\text{ind}_H^G(F_1), \text{ind}_S^G(F_2)) \approx \bigoplus_D M_D(F_1, F_2),$$

where the direct sum is taken over all double cosets  $H\gamma S = D$ .

*Proof.* We have the isomorphisms:

$$\begin{aligned} \text{Hom}_G(\text{ind}_H^G(F_1), \text{ind}_S^G(F_2)) &\approx \text{Hom}_H(F_1, \text{res}_H^G \circ \text{ind}_S^G(F_2)) \\ &\approx \bigoplus_{\gamma} \text{Hom}_H(F_1, \text{ind}_{H \cap [\gamma]S}^H \circ \text{res}_{H \cap [\gamma]S}^{[\gamma]S} \circ [\gamma]F_2) \\ &\approx \bigoplus_{\gamma} \text{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2) \end{aligned}$$

by applying the definition of the induced module in the first and third step, and applying Theorem 7.6 in the second step. Each term in the last expression is what we denoted by  $M_D(F_1, F_2)$  if  $\gamma$  is a representative for the double coset  $D$ . This proves the theorem.

**Corollary 7.8.** *Let  $R = k = \mathbf{C}$ . Let  $S, H$  be subgroups of the finite group  $G$ . Let  $D = H\gamma S$  range over the double cosets, with representatives  $\gamma$ . Let  $\chi$  be an effective character of  $H$  and  $\psi$  an effective character of  $S$ . Then*

$$\langle \text{ind}_H^G(\chi), \text{ind}_S^G(\psi) \rangle_G = \sum_{\gamma} \langle \chi, [\gamma]\psi \rangle_{H \cap [\gamma]S}.$$

*Proof.* Immediate from Theorem 5.17(b) and Theorem 7.7, taking dimensions on the left-hand side and on the right-hand side.

**Corollary 7.9. (Irreducibility of the induced character).** *Let  $S$  be a subgroup of the finite group  $G$ . Let  $R = k = \mathbf{C}$ . Let  $\psi$  be an effective character of  $S$ . Then  $\text{ind}_S^G(\psi)$  is irreducible if and only if  $\psi$  is irreducible and*

$$\langle \psi, [\gamma]\psi \rangle_{S \cap [\gamma]S} = 0$$

for all  $\gamma \in G$ ,  $\gamma \notin S$ .

*Proof.* Immediate from Corollary 7.8 and Theorem 5.17(a). It is of course trivial that if  $\psi$  is reducible, then so is the induced character.

Another way to phrase Corollary 7.9 is as follows. Let  $F, F'$  be representation spaces for  $S$  (over  $\mathbf{C}$ ). We call  $F, F'$  **disjoint** if no simple  $S$ -space occurs both in  $F$  and  $F'$ . Then Corollary 7.9 can be reformulated:

**Corollary 7.9'.** *Let  $S$  be a subgroup of the finite group  $G$ . Let  $F$  be an  $(S, k)$ -space (with  $k = \mathbf{C}$ ). Then  $\text{ind}_S^G(F)$  is simple if and only if  $F$  is simple and for all  $\gamma \in G$  and  $\gamma \notin S$ , the  $S \cap [\gamma]S$ -modules  $F$  and  $[\gamma]F$  are disjoint.*

Next we have the commutation of the dual and induced representations.

**Theorem 7.10.** *Let  $S$  be a subgroup of  $G$  and let  $F$  be a finite free  $R$ -module. Then there is a  $G$ -isomorphism*

$$\text{ind}_S^G(F^\vee) \approx (\text{ind}_S^G(F))^\vee.$$

*Proof.* Let  $G = \bigcup \lambda_i S$  be a left coset decomposition. Then, as in Theorem 7.3, we can express the representation space for  $\text{ind}_S^G(F)$  as

$$\text{ind}_S^G(F) = \bigoplus \lambda_i F.$$

We may select  $\lambda_1 = 1$  (unit element of  $G$ ). There is a unique  $R$ -homomorphism

$$f : F^\vee \rightarrow (\text{ind}_S^G(F))^\vee$$

such that for  $\varphi \in F^\vee$  and  $x \in F$  we have

$$f(\varphi)(\lambda_i x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \varphi(x) & \text{if } i = 1, \end{cases}$$

which is in fact an  $R$ -isomorphism of  $F^\vee$  on  $(\lambda_1 F)^\vee$ . We claim that it is an  $S$ -

homomorphism. This is a routine verification, which we write down. We have

$$f([\sigma]\phi)(\lambda_i x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \sigma(\phi(\sigma^{-1}x)) & \text{if } i = 1. \end{cases}$$

On the other hand, note that if  $\sigma \in S$  then  $\sigma^{-1}\lambda_1 \in S$  so  $\sigma^{-1}\lambda_1 x \in \lambda_1 F$  for  $x \in F$ ; but if  $\sigma \notin S$ , then  $\sigma^{-1}\lambda_i \notin S$  for  $i \neq 1$  so  $\sigma^{-1}\lambda_i x \notin \lambda_1 F$ . Hence

$$[\sigma](f(\phi))(\lambda_1 x) = \sigma f(\phi)(\sigma^{-1}\lambda_1 x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \sigma(\phi(\sigma^{-1}x)) & \text{if } i = 1. \end{cases}$$

This proves that  $f$  commutes with the action of  $S$ .

By the universal property of the induced module, it follows that there is a unique  $(G, R)$ -homomorphism

$$\text{ind}_S^G(f) : \text{ind}_S^G(F^\vee) \rightarrow (\text{ind}_S^G(F))^\vee,$$

which must be an isomorphism because  $f$  was an isomorphism on its image, the  $\lambda_1$ -component of the induced module. This concludes the proof of the theorem.

Theorems and definitions with Hom have analogues with the tensor product. We start with the analogue of the definition.

**Theorem 7.11.** *Let  $S$  be a subgroup of finite index in  $G$ . Let  $F$  be an  $S$ -module, and  $E$  a  $G$ -module (over the commutative ring  $R$ ). Then there is an isomorphism*

$$\text{ind}_S^G(\text{res}_S(E) \otimes F) \approx E \otimes \text{ind}_S^G(F).$$

*Proof.* The  $G$ -module  $\text{ind}_S^G(F)$  contains  $F$  as a summand, because it is the direct sum  $\bigoplus \lambda_i F$  with left coset representatives  $\lambda_i$  as in Theorem 7.3. Hence we have a natural  $S$ -isomorphism

$$f : \text{res}_S(E) \otimes F \xrightarrow{\sim} E \otimes \lambda_1 F \subset E \otimes \text{ind}_S^G(F).$$

taking the representative  $\lambda_1$  to be 1 (the unit element of  $G$ ). By the universal property of induction, there is a  $G$ -homomorphism

$$\text{ind}_S^G(f) : \text{ind}_S^G(\text{res}_S(E) \otimes F) \rightarrow E \otimes \text{ind}_S^G(F),$$

which is immediately verified to be an isomorphism, as desired. (Note that here it only needed to verify the bijectivity in this last step, which comes from the structure of direct sum as  $R$ -modules.)

Before going further, we make some remarks on functorialities. Suppose we have an isomorphism  $G \approx G'$ , a subgroup  $H$  of  $G$  corresponding to a subgroup  $H'$  of  $G'$  under the isomorphism, and an isomorphism  $F \approx F'$  from an  $H$ -module  $F$  to an  $H'$ -module  $F'$  commuting with the actions of  $H, H'$ . Then we get an isomorphism

$$\text{ind}_H^G(F) \approx \text{ind}_{H'}^{G'}(F').$$

In particular, we could take  $\sigma \in G$ , let  $G' = [\sigma]G = G$ ,  $H' = [\sigma]H$  and  $F' = [\sigma]F$ .

Next we deal with the analogue of Theorem 7.7. We keep the same notation as in that theorem and the discussion preceding it. With the two subgroups  $H$  and  $S$ , we may then form the tensor product

$$[\sigma]F_1 \otimes [\tau]F_2$$

with  $\sigma, \tau \in G$ . Suppose  $\sigma^{-1}\tau \in D$  for some double coset  $D = H\gamma S$ . Note that  $[\sigma]F_1 \otimes [\tau]F_2$  is a  $[\sigma]H \cap [\tau]S$ -module. By conjugation we have an isomorphism

$$(3) \quad \text{ind}_{[\sigma]H \cap [\tau]S}^G([\sigma]F_1 \otimes [\tau]F_2) \approx \text{ind}_{H \cap [\gamma]S}^G(F_1 \otimes [\gamma]F_2).$$

**Theorem 7.12.** *There is a  $G$ -isomorphism*

$$\text{ind}_H^G(F_1) \otimes \text{ind}_S^G(F_2) \approx \bigoplus_{\gamma} \text{ind}_{H \cap [\gamma]S}^G(F_1 \otimes [\gamma]F_2),$$

where the sum is taken over double coset representatives  $\gamma$ .

*Proof.* We have:

$$\begin{aligned} \text{ind}_H^G(F_1) \otimes \text{ind}_S^G(F_2) &\approx \text{ind}_H^G(F_1 \otimes \text{res}_H \text{ind}_S^G(F_2)) && \text{by Theorem 7.11} \\ &\approx \bigoplus_{\gamma} \text{ind}_H^G(F_1 \otimes \text{ind}_{H \cap [\gamma]S}^H \text{res}_{H \cap [\gamma]S}^{[\gamma]S}([\gamma]F_2)) && \text{by Theorem 7.6} \\ &\approx \bigoplus_{\gamma} \text{ind}_H^G \left( \text{ind}_{H \cap [\gamma]S}^H \left( \text{res}_{H \cap [\gamma]S}^H(F_1) \otimes \text{res}_{H \cap [\gamma]S}^{[\gamma]S}([\gamma]F_2) \right) \right) && \text{by Theorem 7.7} \\ &\approx \bigoplus_{\gamma} \text{ind}_{H \cap [\gamma]S}^G(F_1 \otimes [\gamma]F_2) && \text{by transitivity of induction} \end{aligned}$$

where we view  $F_1 \otimes [\gamma]F_2$  as an  $H \cap [\gamma]S$ -module in this last line. This proves the theorem.

**General comment.** This section has given a lot of relations for the induced representations. In light of the cohomology of groups, each formula may be viewed as giving an isomorphism of functors in dimension 0, and therefore gives rise to corresponding isomorphisms for the higher cohomology groups  $H^q$ . The reader may see this developed further than the exercises in [La 96].

## Bibliography

- [CuR 81] C. W. CURTIS and I. REINER, *Methods of Representation Theory*, John Wiley and Sons, 1981
- [La 96] S. LANG, *Topics in cohomology of groups*, Springer Lecture Notes 1996
- [La 70] S. LANG, *Algebraic Number Theory*, Addison-Wesley, 1970, reprinted by Springer Verlag, 1986
- [Ma 51] G. MACKEY, On induced representations of groups, *Amer. J. Math.* **73** (1951), pp. 576–592
- [Ma 53] G. MACKEY, Symmetric and anti-symmetric Kronecker squares of induced representations of finite groups, *Amer. J. Math.* **75** (1953), pp. 387–405

The next three sections, which are essentially independent of each other, give examples of induced representations. In each case, we show that certain representations are either induced from certain well-known types, or are linear combinations with integral coefficients of certain well-known types. The most striking feature is that we obtain all characters as linear combinations of induced characters arising from 1-dimensional characters. Thus the theory of characters is to a large extent reduced to the study of 1-dimensional, or abelian characters.

---

## §8. POSITIVE DECOMPOSITION OF THE REGULAR CHARACTER

Let  $G$  be a finite group and let  $k$  be the complex numbers. We let  $1_G$  be the trivial character, and  $r_G$  denote the regular character.

**Proposition 8.1.** *Let  $H$  be a subgroup of  $G$ , and let  $\psi$  be a character of  $H$ . Let  $\psi^G$  be the induced character. Then the multiplicity of  $1_H$  in  $\psi$  is the same as the multiplicity of  $1_G$  in  $\psi^G$ .*

*Proof.* By Theorem 6.1 (i), we have

$$\langle \psi, 1_H \rangle_H = \langle \psi^G, 1_G \rangle_G.$$

These scalar products are precisely the multiplicities in question.

**Proposition 8.2.** *The regular representation is the representation induced by the trivial character on the trivial subgroup of  $G$ .*

*Proof.* This follows at once from the definition of the induced character

$$\psi^G(\tau) = \sum_{\sigma \in G} \psi_H(\sigma \tau \sigma^{-1}),$$

taking  $\psi = 1$  on the trivial subgroup.

**Corollary 8.3.** *The multiplicity of  $1_G$  in the regular character  $r_G$  is equal to 1.*

We shall now investigate the character

$$u_G = r_G - 1_G.$$

**Theorem 8.4.** (Aramata). *The character  $nu_G$  is a linear combination with positive integer coefficients of characters induced by 1-dimensional characters of cyclic subgroups of  $G$ .*

The proof consists of two propositions, which give an explicit description of the induced characters. I am indebted to Serre for the exposition, derived from Brauer's.

If  $A$  is a cyclic group of order  $a$ , we define the function  $\theta_A$  on  $A$  by the conditions:

$$\theta_A(\sigma) = \begin{cases} a & \text{if } \sigma \text{ is a generator of } A \\ 0 & \text{otherwise.} \end{cases}$$

We let  $\lambda_A = \varphi(a)r_A - \theta_A$  (where  $\varphi$  is the Euler function), and  $\lambda_A = 0$  if  $a = 1$ .

The desired result is contained in the following two propositions.

**Proposition 8.5.** *Let  $G$  be a finite group of order  $n$ . Then*

$$nu_G = \sum \lambda_A^G,$$

*the sum being taken over all cyclic subgroups of  $G$ .*

*Proof.* Given two class functions  $\chi, \psi$  on  $G$ , we have the usual scalar product:

$$\langle \psi, \chi \rangle_G = \frac{1}{n} \sum_{\sigma \in G} \psi(\sigma) \overline{\chi(\sigma)}.$$

Let  $\psi$  be any class function on  $G$ . Then:

$$\begin{aligned} \langle \psi, nu_G \rangle &= \langle \psi, nr_G \rangle - \langle \psi, n1_G \rangle \\ &= n\psi(1) - \sum_{\sigma \in G} \psi(\sigma). \end{aligned}$$

On the other hand, using the fact that the induced character is the transpose of the restriction, we obtain

$$\begin{aligned} \sum_A \langle \psi, \lambda_A^G \rangle &= \sum_A \langle \psi | A, \lambda_A \rangle \\ &= \sum_A \langle \psi | A, \varphi(a)r_A - \theta_A \rangle \\ &= \sum_A \varphi(a)\psi(1) - \sum_A \frac{1}{a} \sum_{\sigma \in \text{gen } A} a\psi(\sigma) \\ &= n\psi(1) - \sum_{\sigma \in G} \psi(\sigma). \end{aligned}$$

Since the functions on the right and left of the equality sign in the statement of our proposition have the same scalar product with an arbitrary function, they are equal. This proves our proposition.

**Proposition 8.6.** *If  $A \neq \{1\}$ , the function  $\lambda_A$  is a linear combination of irreducible nontrivial characters of  $A$  with positive integral coefficients.*

*Proof.* If  $A$  is cyclic of prime order, then by Proposition 8.5, we know that  $\lambda_A = nu_A$ , and our assertion follows from the standard structure of the regular representation.

In order to prove the assertion in general, it suffices to prove that the Fourier coefficients of  $\lambda_A$  with respect to a character of degree 1 are integers  $\geq 0$ . Let  $\psi$  be a character of degree 1. We take the scalar product with respect to  $A$ , and obtain:

$$\begin{aligned}\langle \psi, \lambda_A \rangle &= \varphi(a)\psi(1) - \sum_{\sigma \text{ gen}} \psi(\sigma) \\ &= \varphi(a) - \sum_{\sigma \text{ gen}} \psi(\sigma) \\ &= \sum_{\sigma \text{ gen}} (1 - \psi(\sigma)).\end{aligned}$$

The sum  $\sum \psi(\sigma)$  taken over generators of  $A$  is an algebraic integer, and is in fact a rational number (for any number of elementary reasons), hence a rational integer. Furthermore, if  $\psi$  is non-trivial, all real parts of

$$1 - \psi(\sigma)$$

are  $> 0$  if  $\sigma \neq \text{id}$  and are 0 if  $\sigma = \text{id}$ . From the last two inequalities, we conclude that the sums must be equal to a positive integer. If  $\psi$  is the trivial character, then the sum is clearly 0. Our proposition is proved.

**Remark.** Theorem 8.4 and Proposition 8.6 arose in the context of zeta functions and  $L$ -functions, in Aramata's proof that the zeta function of a number field divides the zeta function of a finite extension [Ar 31], [Ar 33]. See also Brauer [Br 47a], [Br 47b]. These results were also used by Brauer in showing an asymptotic behavior in algebraic number theory, namely

$$\log(hR) \sim \log \mathbf{D}^{1/2} \text{ for } [k : \mathbf{Q}] / \log \mathbf{D} \rightarrow 0,$$

where  $h$  is the number of ideal classes in a number field  $k$ ,  $R$  is the regulator, and  $\mathbf{D}$  is the absolute value of the discriminant. For an exposition of this application, see [La 70], Chapter XVI.

## Bibliography

- [Ar 31] H. ARAMATA, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **7** (1931), pp. 334–336
- [Ar 33] H. ARAMATA, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **9** (1933), pp. 31–34
- [Br 47a] R. BRAUER, On the zeta functions of algebraic number fields, *Amer. J. Math.* **69** (1947), pp. 243–250
- [Br 47b] R. BRAUER, On Artin's L-series with general group characters, *Ann. Math.* **48** (1947), pp. 502–514
- [La 70] S. LANG, *Algebraic Number Theory*, Springer Verlag (reprinted from Addison-Wesley, 1970)

---

## §9. SUPERSOLVABLE GROUPS

Let  $G$  be a finite group. We shall say that  $G$  is **supersolvable** if there exists a sequence of subgroups

$$\{1\} \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$$

such that each  $G_i$  is normal in  $G$ , and  $G_{i+1}/G_i$  is cyclic of prime order.

From the theory of  $p$ -groups, we know that every  $p$ -group is super-solvable, and so is the direct product of a  $p$ -group with an abelian group.

**Proposition 9.1.** *Every subgroup and every factor group of a super-solvable group is supersolvable.*

*Proof.* Obvious, using the standard homomorphism theorems.

**Proposition 9.2.** *Let  $G$  be a non-abelian supersolvable group. Then there exists a normal abelian subgroup which contains the center properly.*

*Proof.* Let  $C$  be the center of  $G$ , and let  $\bar{G} = G/C$ . Let  $\bar{H}$  be a normal subgroup of prime order in  $\bar{G}$  and let  $H$  be its inverse image in  $G$  under the canonical map  $G \rightarrow G/C$ . If  $\sigma$  is a generator of  $\bar{H}$ , then an inverse image  $\sigma$  of  $\bar{\sigma}$ , together with  $C$ , generate  $H$ . Hence  $H$  is abelian, normal, and contains the center properly.

**Theorem 9.3.** (Blichfeldt). *Let  $G$  be a supersolvable group, let  $k$  be algebraically closed. Let  $E$  be a simple  $(G, k)$ -space. If  $\dim_k E > 1$ , then there exists a proper subgroup  $H$  of  $G$  and a simple  $H$ -space  $F$  such that  $E$  is induced by  $F$ .*

*Proof.* Since a simple representation of an abelian group is 1-dimensional, our hypothesis implies that  $G$  is not abelian.

We shall first give the proof of our theorem under the additional hypothesis that  $E$  is faithful. (This means that  $\sigma x = x$  for all  $x \in E$  implies  $\sigma = 1$ .) It will be easy to remove this restriction at the end.

**Lemma 9.4.** *Let  $G$  be a finite group, and assume  $k$  algebraically closed. Let  $E$  be a simple, faithful  $G$ -space over  $k$ . Assume that there exists a normal abelian subgroup  $H$  of  $G$  containing the center of  $G$  properly. Then there exists a proper subgroup  $H_1$  of  $G$  containing  $H$ , and a simple  $H_1$ -space  $F$  such that  $E$  is the induced module of  $F$  from  $H_1$  to  $G$ .*

*Proof.* We view  $E$  as an  $H$ -space. It is a direct sum of simple  $H$ -spaces, and since  $H$  is abelian, such simple  $H$ -space is 1-dimensional.

Let  $v \in E$  generate a 1-dimensional  $H$ -space. Let  $\psi$  be its character. If  $w \in E$  also generates a 1-dimensional  $H$ -space, with the same character  $\psi$ , then

for all  $a, b \in k$  and  $\tau \in H$  we have

$$\tau(av + bw) = \psi(\tau)(av + bw).$$

If we denote by  $F_\psi$  the subspace of  $E$  generated by all 1-dimensional  $H$ -subspaces having the character  $\psi$ , then we have an  $H$ -direct sum decomposition

$$E = \bigoplus_{\psi} F_\psi.$$

We contend that  $E \neq F_\psi$ . Otherwise, let  $v \in E$ ,  $v \neq 0$ , and  $\sigma \in G$ . Then  $\sigma^{-1}v$  is a 1-dimensional  $H$ -space by assumption, and has character  $\psi$ . Hence for  $\tau \in H$ ,

$$\tau(\sigma^{-1}v) = \psi(\tau)\sigma^{-1}v$$

$$(\sigma\tau\sigma^{-1})v = \sigma\psi(\tau)\sigma^{-1}v = \psi(\tau)v.$$

This shows that  $\sigma\tau\sigma^{-1}$  and  $\tau$  have the same effect on the element  $v$  of  $E$ . Since  $H$  is not contained in the center of  $G$ , there exist  $\tau \in H$  and  $\sigma \in G$  such that  $\sigma\tau\sigma^{-1} \neq \tau$ , and we have contradicted the assumption that  $E$  is faithful.

We shall prove that  $G$  permutes the spaces  $F_\psi$  transitively.

Let  $v \in F_\psi$ . For any  $\tau \in H$  and  $\sigma \in G$ , we have

$$\tau(\sigma v) = \sigma(\sigma^{-1}\tau\sigma)v = \sigma\psi(\sigma^{-1}\tau\sigma)v = \psi_\sigma(\tau)\sigma v,$$

where  $\psi_\sigma$  is the function on  $H$  given by  $\psi_\sigma(\tau) = \psi(\sigma^{-1}\tau\sigma)$ . This shows that  $\sigma$  maps  $F_\psi$  into  $F_{\psi_\sigma}$ . However, by symmetry, we see that  $\sigma^{-1}$  maps  $F_{\psi_\sigma}$  into  $F_\psi$ , and the two maps  $\sigma$ ,  $\sigma^{-1}$  give inverse mappings between  $F_{\psi_\sigma}$  and  $F_\psi$ . Thus  $G$  permutes the spaces  $\{F_\psi\}$ .

Let  $E' = GF_{\psi_0} = \sum \sigma F_{\psi_0}$  for some fixed  $\psi_0$ . Then  $E'$  is a  $G$ -subspace of  $E$ , and since  $E$  was assumed to be simple, it follows that  $E' = E$ . This proves that the spaces  $\{F_\psi\}$  are permuted transitively.

Let  $F = F_{\psi_1}$  for some fixed  $\psi_1$ . Then  $F$  is an  $H$ -subspace of  $E$ . Let  $H_1$  be the subgroup of all elements  $\tau \in G$  such that  $\tau F = F$ . Then  $H_1 \neq G$  since  $E \neq F_\psi$ . We contend that  $F$  is a simple  $H_1$ -subspace, and that  $E$  is the induced space of  $F$  from  $H_1$  to  $G$ .

To see this, let  $G = \bigcup H_1 \bar{c}$  be a decomposition of  $G$  in terms of right cosets of  $H_1$ . Then the elements  $\{\bar{c}^{-1}\}$  form a system of left coset representatives of  $H_1$ . Since

$$E = \sum_{\sigma \in G} \sigma F$$

it follows that

$$E = \sum_c \bar{c}^{-1} F.$$

We contend that this last sum is direct, and that  $F$  is a simple  $H_1$ -space.

Since  $G$  permutes the spaces  $\{F_\psi\}$ , we see by definition that  $H_1$  is the isotropy group of  $F$  for the operation of  $G$  on this set of spaces, and hence that the elements of the orbit are precisely  $\{\bar{c}^{-1}F\}$ , as  $c$  ranges over all the cosets. Thus the spaces  $\{\bar{c}^{-1}F\}$  are distinct, and we have a direct sum decomposition

$$E = \bigoplus_c \bar{c}^{-1}F.$$

If  $W$  is a proper  $H_1$ -subspace of  $F$ , then  $\bigoplus \bar{c}^{-1}W$  is a proper  $G$ -subspace of  $E$ , contradicting the hypothesis that  $E$  is simple. This proves our assertions.

We can now apply Theorem 7.3 to conclude that  $E$  is the induced module from  $F$ , thereby proving Theorem 9.3, in case  $E$  is assumed to be faithful.

Suppose now that  $E$  is not faithful. Let  $G_0$  be the normal subgroup of  $G$  which is the kernel of the representation  $G \rightarrow \text{Aut}_k(E)$ . Let  $\bar{G} = G/G_0$ . Then  $E$  gives a faithful representation of  $\bar{G}$ . As  $E$  is not 1-dimensional, then  $\bar{G}$  is not abelian and there exists a proper normal subgroup  $\bar{H}$  of  $\bar{G}$  and a simple  $\bar{H}$ -space  $F$  such that

$$E = \text{ind}_{\bar{H}}^{\bar{G}}(F).$$

Let  $H$  be the inverse image of  $\bar{H}$  in the natural map  $G \rightarrow \bar{G}$ . Then  $H \supset G_0$ , and  $F$  is a simple  $H$ -space. In the operation of  $\bar{G}$  as a permutation group of the  $k$ -subspaces  $\{\sigma F\}_{\sigma \in G}$ , we know that  $\bar{H}$  is the isotropy group of one component. Hence  $H$  is the isotropy group in  $G$  of this same operation, and hence applying Theorem 7.3 again, we conclude that  $E$  is induced by  $F$  in  $G$ , i.e.

$$E = \text{ind}_H^G(F),$$

thereby proving Theorem 9.3.

**Corollary 9.5.** *Let  $G$  be a product of a  $p$ -group and a cyclic group, and let  $k$  be algebraically closed. If  $E$  is a simple  $(G, k)$ -space and is not 1-dimensional, then  $E$  is induced by a 1-dimensional representation of some subgroup.*

*Proof.* We apply the theorem step by step using the transitivity of induced representations until we get a 1-dimensional representation of a subgroup.

## §10. BRAUER'S THEOREM

We let  $k = \mathbf{C}$  be the field of complex numbers. We let  $R$  be a subring of  $k$ . We shall deal with  $X_R(G)$ , i.e. the ring consisting of all linear combinations with coefficients in  $R$  of the simple characters of  $G$  over  $k$ . (It is a ring by Proposition 2.1.)

Let  $H = \{H_\alpha\}$  be a fixed family of subgroups of  $G$ , indexed by indices  $\{\alpha\}$ . We let  $V_R(G)$  be the additive subgroup of  $X_R(G)$  generated by all the functions which are induced by functions in  $X_R(H_\alpha)$  for some  $H_\alpha$  in our family. In other words,

$$V_R(G) = \sum_{\alpha} \text{ind}_{H_\alpha}^G(X_R(H_\alpha)).$$

We could also say that  $V_R(G)$  is the subgroup generated over  $R$  by all the characters induced from all the  $H_\alpha$ .

**Lemma 10.1.**  *$V_R(G)$  is an ideal in  $X_R(G)$ .*

*Proof.* This is immediate from Theorem 6.1.

For many applications, the family of subgroups will consist of “elementary” subgroups: Let  $p$  be a prime number. By a  **$p$ -elementary group** we shall mean the product of a  $p$ -group and a cyclic group (whose order may be assumed prime to  $p$ , since we can absorb the  $p$ -part of a cyclic factor into the  $p$ -group). An element  $\sigma \in G$  is said to be  **$p$ -regular** if its period is prime to  $p$ , and  **$p$ -singular** if its period is a power of  $p$ . Given  $x \in G$ , we can write in a unique way

$$x = \sigma\tau$$

where  $\sigma$  is  $p$ -singular,  $\tau$  is  $p$ -regular, and  $\sigma, \tau$  commute. Indeed, if  $p^r m$  is the period of  $x$ , with  $m$  prime to  $p$ , then  $1 = vp^r + \mu m$  whence  $x = (x^m)^\mu (x^{p^r})^v$  and we get our factorization. It is clearly unique, since the factors have to lie in the cyclic subgroup generated by  $x$ . We call the two factors the  **$p$ -singular** and  **$p$ -regular factors** of  $x$  respectively.

The above decomposition also shows:

**Proposition 10.2.** *Every subgroup and every factor group of a  $p$ -elementary group is  $p$ -elementary. If  $S$  is a subgroup of the  $p$ -elementary group  $P \times C$ , where  $P$  is a  $p$ -group, and  $C$  is cyclic, of order prime to  $p$ , then*

$$S = (S \cap P) \times (S \cap C).$$

*Proof.* Clear.

*Our purpose is to show, among other things, that if our family  $\{H_\alpha\}$  is such that every  $p$ -elementary subgroup of  $G$  is contained in some  $H_\alpha$ , then  $V_R(G) = X_R(G)$  for every ring  $R$ .* It would of course suffice to do it for  $R = \mathbf{Z}$ , but for our purposes, it is necessary to prove the result first using a bigger ring. The main result is contained in Theorems 10.11 and 10.13, due to Brauer. We shall give an exposition of Brauer-Tate (*Annals of Math.*, July 1955).

We let  $R$  be the ring  $\mathbf{Z}[\zeta]$  where  $\zeta$  is a primitive  $n$ -th root of unity. There exists a basis of  $R$  as a  $\mathbf{Z}$ -module, namely  $1, \zeta, \dots, \zeta^{N-1}$  for some integer  $N$ . This is a trivial fact, and we can take  $N$  to be the degree of the irreducible polynomial of  $\zeta$  over  $\mathbf{Q}$ . This irreducible polynomial has leading coefficient 1, and

has integer coefficients, so the fact that

$$1, \zeta, \dots, \zeta^{N-1}$$

form a basis of  $\mathbf{Z}[\zeta]$  follows from the Euclidean algorithm. We don't need to know anything more about this degree  $N$ .

We shall prove our assertion first for the above ring  $R$ . The rest then follows by using the following lemma.

**Lemma 10.3.** *If  $d \in \mathbf{Z}$  and the constant function  $d \cdot 1_G$  belongs to  $V_R$  then  $d \cdot 1_G$  belongs to  $V_{\mathbf{Z}}$ .*

*Proof.* We contend that  $1, \zeta, \dots, \zeta^{N-1}$  are linearly independent over  $X_{\mathbf{Z}}(G)$ . Indeed, a relation of linear dependence would yield

$$\sum_{v=1}^s \sum_{j=0}^{N-1} c_{vj} \chi_v \zeta^j = 0$$

with integers  $c_{vj}$  not all 0. But the simple characters are linearly independent over  $k$ . The above relation is a relation between these simple characters with coefficients in  $R$ , and we get a contradiction. We conclude therefore that

$$V_R = V_{\mathbf{Z}} \oplus V_{\mathbf{Z}} \zeta \oplus \dots \oplus V_{\mathbf{Z}} \zeta^{N-1}$$

is a direct sum (of abelian groups), and our lemma follows.

If we can succeed in proving that the constant function  $1_G$  lies in  $V_R(G)$ , then by the lemma, we conclude that it lies in  $V_{\mathbf{Z}}(G)$ , and since  $V_{\mathbf{Z}}(G)$  is an ideal, that  $X_{\mathbf{Z}}(G) = V_{\mathbf{Z}}(G)$ .

To prove our theorem, we need a sequence of lemmas.

Two elements  $x, x'$  of  $G$  are said to be  **$p$ -conjugate** if their  $p$ -regular factors are conjugate in the ordinary sense. It is clear that  $p$ -conjugacy is an equivalence relation, and an equivalence class will be called a  **$p$ -conjugacy class**, or simply a  **$p$ -class**.

**Lemma 10.4.** *Let  $f \in X_R(G)$ , and assume that  $f(\sigma) \in \mathbf{Z}$  for all  $\sigma \in G$ . Then  $f$  is constant mod  $p$  on every  $p$ -class.*

*Proof.* Let  $x = \sigma\tau$ , where  $\sigma$  is  $p$ -singular, and  $\tau$  is  $p$ -regular, and  $\sigma, \tau$  commute. It will suffice to prove that

$$f(x) \equiv f(\tau) \pmod{p}.$$

Let  $H$  be the cyclic subgroup generated by  $x$ . Then the restriction of  $f$  to  $H$  can be written

$$f_H = \sum a_j \psi_j$$

with  $a_j \in R$ , and  $\psi_j$  being the simple characters of  $H$ , hence homomorphisms of  $H$  into  $k^*$ . For some power  $p^r$  we have  $x^{p^r} = \tau^{p^r}$ , whence  $\psi_j(x)^{p^r} = \psi_j(\tau)^{p^r}$ , and hence

$$f(x)^{p^r} \equiv f(\tau)^{p^r} \pmod{pR}.$$

We now use the following lemma.

**Lemma 10.5.** *Let  $R = \mathbb{Z}[\zeta]$  be as before. If  $a \in \mathbb{Z}$  and  $a \in pR$  then  $a \in p\mathbb{Z}$ .*

*Proof.* This is immediate from the fact that  $R$  has a basis over  $\mathbb{Z}$  such that 1 is a basis element.

Applying Lemma 10.5, we conclude that  $f(x) \equiv f(\tau) \pmod{p}$ , because  $b^{p^r} \equiv b \pmod{p}$  for every integer  $b$ .

**Lemma 10.6.** *Let  $\tau$  be  $p$ -regular in  $G$ , and let  $T$  be the cyclic subgroup generated by  $\tau$ . Let  $C$  be the subgroup of  $G$  consisting of all elements commuting with  $\tau$ . Let  $P$  be a  $p$ -Sylow subgroup of  $C$ . Then there exists an element  $\psi \in X_R(T \times P)$  such that the induced function  $f = \psi^G$  has the following properties:*

- (i)  $f(\sigma) \in \mathbb{Z}$  for all  $\sigma \in G$ .
- (ii)  $f(\sigma) = 0$  if  $\sigma$  does not belong to the  $p$ -class of  $\tau$ .
- (iii)  $f(\tau) = (C : P) \not\equiv 0 \pmod{p}$ .

*Proof.* We note that the subgroup of  $G$  generated by  $T$  and  $P$  is a direct product  $T \times P$ . Let  $\psi_1, \dots, \psi_r$  be the simple characters of the cyclic group  $T$ , and assume that these are extended to  $T \times P$  by composition with the projection:

$$T \times P \rightarrow T \rightarrow k^*.$$

We denote the extensions again by  $\psi_1, \dots, \psi_r$ . Then we let

$$\psi = \sum_{v=1}^r \overline{\psi_v(\tau)} \psi_v.$$

The orthogonality relations for the simple characters of  $T$  show that

$$\psi(\tau y) = \psi(\tau) = (T : 1) \quad \text{for } y \in P$$

$$\psi(\sigma) = 0 \quad \text{if } \sigma \in TP, \quad \text{and} \quad \sigma \notin \tau P.$$

We contend that  $\psi^G$  satisfies our requirements.

First, it is clear that  $\psi$  lies in  $X_R(TP)$ .

We have for  $\sigma \in G$ :

$$\psi^G(\sigma) = \frac{1}{(TP : 1)} \sum_{x \in G} \psi_{TP}(x\sigma x^{-1}) = \frac{1}{(P : 1)} \mu(\sigma)$$

where  $\mu(\sigma)$  is the number of elements  $x \in G$  such that  $x\sigma x^{-1}$  lies in  $\tau P$ . The number  $\mu(\sigma)$  is divisible by  $(P : 1)$  because if an element  $x$  of  $G$  moves  $\sigma$  into  $\tau P$  by conjugation, so does every element of  $Px$ . Hence the values of  $\psi^G$  lie in  $\mathbf{Z}$ .

Furthermore,  $\mu(\sigma) \neq 0$  only if  $\sigma$  is  $p$ -conjugate to  $\tau$ , whence our condition (ii) follows.

Finally, we can have  $x\tau x^{-1} = \tau y$  with  $y \in P$  only if  $y = 1$  (because the period of  $\tau$  is prime to  $p$ ). Hence  $\mu(\tau) = (C : 1)$ , and our condition (iii) follows.

**Lemma 10.7.** *Assume that the family of subgroups  $\{H_\alpha\}$  covers  $G$  (i.e. every element of  $G$  lies in some  $H_\alpha$ ). If  $f$  is a class function on  $G$  taking its values in  $\mathbf{Z}$ , and such that all the values are divisible by  $n = (G : 1)$ , then  $f$  belongs to  $V_R(G)$ .*

*Proof.* Let  $\gamma$  be a conjugacy class, and let  $p$  be prime to  $n$ . Every element of  $G$  is  $p$ -regular, and all  $p$ -subgroups of  $G$  are trivial. Furthermore,  $p$ -conjugacy is the same as conjugacy. Applying Lemma 10.6, we find that there exists in  $V_R(G)$  a function taking the value 0 on elements  $\sigma \notin \gamma$ , and taking an integral value dividing  $n$  on elements of  $\gamma$ . Multiplying this function by some integer, we find that there exists a function in  $V_R(G)$  taking the value  $n$  for all elements of  $\gamma$ , and the value 0 otherwise. The lemma then follows immediately.

**Theorem 10.8.** (Artin). *Every character of  $G$  is a linear combination with rational coefficients of induced characters from cyclic subgroups.*

*Proof.* In Lemma 10.7, let  $\{H_\alpha\}$  be the family of cyclic subgroups of  $G$ . The constant function  $n.1_G$  belongs to  $V_R(G)$ . By Lemma 10.3, this function belongs to  $V_{\mathbf{Z}}(G)$ , and hence  $nX_{\mathbf{Z}}(G) \subset V_{\mathbf{Z}}(G)$ . Hence

$$X_{\mathbf{Z}}(G) \subset \frac{1}{n} V_{\mathbf{Z}}(G),$$

thereby proving the theorem.

**Lemma 10.9.** *Let  $p$  be a prime number, and assume that every  $p$ -elementary subgroup of  $G$  is contained in some  $H_\alpha$ . Then there exists a function  $f \in V_R(G)$  whose values are in  $\mathbf{Z}$ , and  $\equiv 1 \pmod{p^r}$ .*

*Proof.* We apply Lemma 10.6 again. For each  $p$ -class  $\gamma$ , we can find a function  $f_\gamma$  in  $V_R(G)$ , whose values are 0 on elements outside  $\gamma$ , and  $\not\equiv 0 \pmod{p}$  for elements of  $\gamma$ . Let  $f = \sum f_\gamma$ , the sum being taken over all  $p$ -classes. Then  $f(\sigma) \not\equiv 0 \pmod{p}$  for all  $\sigma \in G$ . Taking  $f^{(p-1)p^{r-1}}$  gives what we want.

**Lemma 10.10.** *Let  $p$  be a prime number and assume that every  $p$ -elementary subgroup of  $G$  is contained in some  $H_\alpha$ . Let  $n = n_0 p^r$  where  $n_0$  is prime to  $p$ . Then the constant function  $n_0 \cdot 1_G$  belongs to  $V_{\mathbf{Z}}(G)$ .*

*Proof.* By Lemma 10.3, it suffices to prove that  $n_0 \cdot 1_G$  belongs to  $V_R(G)$ . Let  $f$  be as in Lemma 10.9. Then

$$n_0 \cdot 1_G = n_0(1_G - f) + n_0 f.$$

Since  $n_0(1_G - f)$  has values divisible by  $n_0 p^r = n$ , it lies in  $V_R(G)$  by Lemma 10.7. On the other hand,  $n_0 f \in V_R(G)$  because  $f \in V_R(G)$ . This proves our lemma.

**Theorem 10.11.** (Brauer). *Assume that for every prime number  $p$ , every  $p$ -elementary subgroup of  $G$  is contained in some  $H_\alpha$ . Then  $X(G) = V_{\mathbf{Z}}(G)$ . Every character of  $G$  is a linear combination, with integer coefficients, of characters induced from subgroups  $H_\alpha$ .*

*Proof.* Immediate from Lemma 10.10, since we can find functions  $n_0 \cdot 1_G$  in  $V_{\mathbf{Z}}(G)$  with  $n_0$  relatively prime to any given prime number.

**Corollary 10.12.** *A class function  $f$  on  $G$  belongs to  $X(G)$  if and only if its restriction to  $H_\alpha$  belongs to  $X(H_\alpha)$  for each  $\alpha$ .*

*Proof.* Assume that the restriction of  $f$  to  $H_\alpha$  is a character on  $H_\alpha$  for each  $\alpha$ . By the theorem, we can write

$$1_G = \sum_{\alpha} c_{\alpha} \operatorname{ind}_{H_\alpha}^G(\psi_{\alpha})$$

where  $c_{\alpha} \in \mathbf{Z}$ , and  $\psi_{\alpha} \in X(H_\alpha)$ . Hence

$$f = \sum_{\alpha} c_{\alpha} \operatorname{ind}_{H_\alpha}^G(\psi_{\alpha} f_{H_\alpha}),$$

using Theorem 6.1. If  $f_{H_\alpha} \in X(H_\alpha)$ , we conclude that  $f$  belongs to  $X(G)$ . The converse is of course trivial.

**Theorem 10.13.** (Brauer). *Every character of  $G$  is a linear combination with integer coefficients of characters induced by 1-dimensional characters of subgroups.*

*Proof.* By Theorem 10.11, and the transitivity of induction, it suffices to prove that every character of a  $p$ -elementary group has the property stated in the theorem. But we have proved this in the preceding section, Corollary 9.5.

---

## §11. FIELD OF DEFINITION OF A REPRESENTATION

We go back to the general case of  $k$  having characteristic prime to  $\#G$ . Let  $E$  be a  $k$ -space and assume we have a representation of  $G$  on  $E$ . Let  $k'$  be an extension field of  $k$ . Then  $G$  operates on  $k' \otimes_k E$  by the rule

$$\sigma(a \otimes x) = a \otimes \sigma x$$

for  $a \in k'$  and  $x \in E$ . This is obtained from the bilinear map on the product  $k' \times E$  given by

$$(a, x) \mapsto a \otimes \sigma x.$$

We view  $E' = k' \otimes_k E$  as the extension of  $E$  by  $k'$ , and we obtain a representation of  $G$  on  $E'$ .

**Proposition 11.1.** *Let the notation be as above. Then the characters of the representations of  $G$  on  $E$  and on  $E'$  are equal.*

*Proof.* Let  $\{v_1, \dots, v_m\}$  be a basis of  $E$  over  $k$ . Then

$$\{1 \otimes v_1, \dots, 1 \otimes v_m\}$$

is a basis of  $E'$  over  $k'$ . Thus the matrices representing an element  $\sigma$  of  $G$  with respect to the two bases are equal, and consequently the traces are equal.

Conversely, let  $k'$  be a field and  $k$  a subfield. A representation of  $G$  on a  $k'$ -space  $E'$  is said to be **definable over  $k$**  if there exists a  $k$ -space  $E$  and a representation of  $G$  on  $E$  such that  $E'$  is  $G$ -isomorphic to  $k' \otimes_k E$ .

**Proposition 11.2.** *Let  $E, F$  be simple representation spaces for the finite group  $G$  over  $k$ . Let  $k'$  be an extension of  $k$ . Assume that  $E, F$  are not  $G$ -isomorphic. Then no  $k'$ -simple component of  $E_{k'}$  appears in the direct sum decomposition of  $F_{k'}$  into  $k'$ -simple subspaces.*

*Proof.* Consider the direct product decomposition

$$k[G] = \prod_{\mu=1}^{s(k)} R_\mu(k)$$

over  $k$ , into a direct product of simple rings. Without loss of generality, we may assume that  $E, F$  are simple left ideals of  $k[G]$ , and they will belong to distinct factors of this product by assumption. We now take the tensor product with  $k'$ , getting nothing else but  $k'[G]$ . Then we obtain a direct product decomposition over  $k'$ . Since  $R_v(k)R_\mu(k) = 0$  if  $v \neq \mu$ , this will actually be given by a direct

product decomposition of each factor  $R_\mu(k)$ :

$$k'[G] = \prod_{\mu=1}^{s(k)} \prod_{i=1}^{m(\mu)} R_{\mu i}(k').$$

Say  $E = L_v$  and  $F = L_\mu$  with  $v \neq \mu$ . Then  $R_\mu E = 0$ . Hence  $R_{\mu i} E_{k'} = 0$  for each  $i = 1, \dots, m(\mu)$ . This implies that no simple component of  $E_{k'}$  can be  $G$ -isomorphic to any one of the simple left ideals of  $R_{\mu i}$ , and proves what we wanted.

**Corollary 11.3.** *The simple characters  $\chi_1, \dots, \chi_{s(k)}$  of  $G$  over  $k$  are linearly independent over any extension  $k'$  of  $k$ .*

*Proof.* This follows at once from the proposition, together with the linear independence of the  $k'$ -simple characters over  $k'$ .

Propositions 11.1 and 11.2 are essentially general statements of an abstract nature. The next theorem uses Brauer's theorem in its proof.

**Theorem 11.4.** (Brauer). *Let  $G$  be a finite group of exponent  $m$ . Every representation of  $G$  over the complex numbers (or an algebraically closed field of characteristic 0) is definable over the field  $\mathbf{Q}(\zeta_m)$  where  $\zeta_m$  is a primitive  $m$ -th root of unity.*

*Proof.* Let  $\chi$  be the character of a representation of  $G$  over  $\mathbf{C}$ , i.e. an effective character. By Theorem 10.13, we can write

$$\chi = \sum_j c_j \text{ind}_{S_j}^G(\psi_j), \quad c_j \in \mathbf{Z},$$

the sum being taken over a finite number of subgroups  $S_j$ , and  $\psi_j$  being a 1-dimensional character of  $S_j$ . It is clear that each  $\psi_j$  is definable over  $\mathbf{Q}(\zeta_m)$ . Thus the induced character  $\psi_j^G$  is definable over  $\mathbf{Q}(\zeta_m)$ . Each  $\psi_j^G$  can be written

$$\psi_j^G = \sum_\mu d_{j\mu} \chi_\mu, \quad d_{j\mu} \in \mathbf{Z}$$

where  $\{\chi_\mu\}$  are the simple characters of  $G$  over  $\mathbf{Q}(\zeta_m)$ . Hence

$$\chi = \sum_\mu \left( \sum_j c_j d_{j\mu} \right) \chi_\mu.$$

The expression of  $\chi$  as a linear combination of the simple characters over  $k$  is unique, and hence the coefficient

$$\sum_j c_j d_{j\mu}$$

is  $\geq 0$ . This proves what we wanted.

---

## §12. EXAMPLE: $GL_2$ OVER A FINITE FIELD

Let  $F$  be a field. We view  $GL_2(F)$  as operating on the 2-dimensional vector space  $V = F^2$ . We let  $F^a$  be the algebraic closure as usual, and we let  $V^a = F^a \times F^a = F^a \otimes V$  (tensor product over  $F$ ). By **semisimple**, we always mean absolutely semisimple, i.e. semisimple over the algebraic closure  $F^a$ . An element  $\alpha \in GL_2(F)$  is called **semisimple** if  $V^a$  is semisimple over  $F^a[\alpha]$ . A subgroup is called **semisimple** if all its elements are semisimple.

Let  $K$  be a separable quadratic extension of  $F$ . Let  $\{\omega_1, \omega_2\}$  be a basis of  $K$ . Then we have the regular representation of  $K$  with respect to this basis, namely multiplication representing  $K^*$  as a subgroup of  $GL_2(F)$ . The elements of norm 1 correspond precisely to the elements of  $SL_2(F)$  in the image of  $K^*$ . A different choice of basis of  $K$  corresponds to conjugation of this image in  $GL_2(F)$ . Let  $C_K$  denote one of these images. Then  $C_K$  is called a **non-split Cartan subgroup**. The subalgebra

$$F[C_K] \subset \text{Mat}_2(F)$$

is isomorphic to  $K$  itself, and the units of the algebra are therefore the elements of  $C_K \approx K^*$ .

**Lemma 12.1.** *The subgroup  $C_K$  is a maximal commutative semisimple subgroup.*

*Proof.* If  $\alpha \in GL_2(F)$  commutes with all elements of  $C_K$  then  $\alpha$  must lie in  $F[C_K]$ , for otherwise  $\{1, \alpha\}$  would be linearly independent over  $F[C_K]$ , whence  $\text{Mat}_2(F)$  would be commutative, which is not the case. Since  $\alpha$  is invertible,  $\alpha$  is a unit in  $F[C_K]$ , so  $\alpha \in C_K$ , as was to be shown.

By the **split Cartan subgroup** we mean the group of diagonal matrices

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \text{ with } a, d \in F^*.$$

We denote the split Cartan by  $A$ , or  $A(F)$  if the reference to  $F$  is needed.

By a **Cartan subgroup** we mean a subgroup conjugate to the split Cartan or to one of the subgroups  $C_K$  as above.

**Lemma 12.2.** *Every maximal commutative semisimple subgroup of  $GL_2(F)$  is a Cartan subgroup, and conversely.*

*Proof.* It is clear that the split Cartan subgroup is maximal commutative semisimple. Suppose that  $H$  is a maximal commutative semisimple subgroup of  $GL_2(F)$ . If  $H$  is diagonalizable over  $F$ , then  $H$  is contained in a conjugate of the split Cartan. On the other hand, suppose  $H$  is not diagonalizable over  $F$ . It is diagonalizable over the separable closure of  $F$ , and the two eigenspaces of

dimension 1 give rise to two characters

$$\psi, \psi' : H \rightarrow F^*$$

of  $H$  in the multiplicative group of the separable closure. For each element  $\alpha \in H$  the values  $\psi(\alpha)$  and  $\psi'(\alpha)$  are the eigenvalues of  $\alpha$ , and for some element  $\alpha \in H$  these eigenvalues are distinct, otherwise  $H$  is diagonalizable over  $F$ . Hence the pair of elements  $\psi(\alpha), \psi'(\alpha)$  are conjugate over  $F$ . The image  $\psi(H)$  is cyclic, and if  $\psi(\alpha)$  generates this image, then we see that  $\psi(\alpha)$  generates a quadratic extension  $K$  of  $F$ . The map

$$\alpha \mapsto \psi(\alpha) \text{ with } \alpha \in H$$

extends to an  $F$ -linear mapping, also denoted by  $\psi$ , of the algebra  $F[H]$  into  $K$ . Since  $F[H]$  is semisimple, it follows that  $\psi : F[H] \rightarrow K$  is an isomorphism. Hence  $\psi$  maps  $H$  into  $K^*$ , and in fact maps  $H$  onto  $K^*$  because  $H$  was taken to be maximal. This proves the lemma.

In the above proof, the two characters  $\psi, \psi'$  are called the **(eigen)characters of the Cartan subgroup**. In the split case, if  $\alpha$  has diagonal elements,  $a, d$  then we get the two characters such that  $\psi(\alpha) = a$  and  $\psi'(\alpha) = d$ . In the split case, the values of the characters are in  $F$ . In the non-split case, these values are conjugate quadratic over  $F$ , and lie in  $K$ .

**Proposition 12.3.** *Let  $H$  be a Cartan subgroup of  $GL_2(F)$  (split or not). Then  $H$  is of index 2 in its normalizer  $N(H)$ .*

*Proof.* We may view  $GL_2(F)$  as operating on the 2-dimensional vector space  $V^a = F^a \oplus F^a$ , over the algebraic closure  $F^a$ . Whether  $H$  is split or not, the eigencharacters are distinct (because of the separability assumption in the non-split case), and an element of the normalizer must either fix or interchange the eigenspaces. If it fixes them, then it lies in  $H$  by the maximality of  $H$  in Lemma 12.2. If it interchanges them, then it does not lie in  $H$ , and generates a unique coset of  $N/H$ , so that  $H$  is of index 2 in  $N$ .

In the split case, a representative of  $N/A$  which interchanges the eigenspaces is given by

$$w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In the non-split case, let  $\sigma : K \rightarrow K$  be the non-trivial automorphism. Let  $\{\alpha, \sigma\alpha\}$  be a normal basis. With respect to this basis, the matrix of  $\sigma$  is precisely the matrix

$$w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Therefore again in this case we see that there exists a non-trivial element in the

normalizer of  $A$ . Note that it is immediate to verify the relation

$$M(\sigma)M(x)M(\sigma^{-1}) = M(\sigma x),$$

if  $M(x)$  is the matrix associated with an element  $x \in K$ .

Since the order of an element in the multiplicative group of a field is prime to the characteristic, we conclude:

*If  $F$  has characteristic  $p$ , then an element of finite order in  $GL_2(F)$  is semisimple if and only if its order is prime to  $p$ .*

## Conjugacy classes

We shall determine the conjugacy classes explicitly. We specialize the situation, and from now on we let:

$F$  = finite field with  $q$  elements;

$G = GL_2(F)$ ;

$Z$  = center of  $G$ ;

$A$  = diagonal subgroup of  $G$ ;

$C \approx K^* =$  a non-split Cartan subgroup of  $G$ .

Up to conjugacy there is only one non-split Cartan because over a finite field there is only one quadratic extension (in a given algebraic closure  $F^a$ ) (cf. Corollary 2.7 of Chapter XIV). Recall that

$$\#(G) = (q^2 - 1)(q^2 - q) = q(q + 1)(q - 1)^2.$$

This should have been worked out as an exercise before. Indeed,  $F \times F$  has  $q^2$  elements, and  $\#(G)$  is equal to the number of bases of  $F \times F$ . There are  $q^2 - 1$  choices for a first basis element, and then  $q^2 - q$  choices for a second (omitting  $(0, 0)$  the first time, and all chosen elements the second time). This gives the value for  $\#(G)$ .

There are two cases for the conjugacy classes of an element  $\alpha$ .

*Case 1.* The characteristic polynomial is reducible, so the eigenvalues lie in  $F$ . In this case, by the Jordan canonical form, such an element is conjugate to one of the matrices

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad \text{with } d \neq a.$$

These are called **central**, **unipotent**, or **rational not central** respectively.

*Case 2.* The characteristic polynomial is irreducible. Then  $\alpha$  is such that  $F[\alpha] \approx E$ , where  $E$  is the quadratic extension of  $F$  of degree 2. Then  $\{1, \alpha\}$  is a basis of  $F[\alpha]$  over  $F$ , and the matrix associated with  $\alpha$  under the representation by multiplication on  $F[\alpha]$  is

$$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix},$$

where  $a, b$  are the coefficients of the characteristic polynomial  $X^2 + ax + b$ .

We then have the following table.

**Table 12.4**

class	# of classes	# of elements in the class
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$q - 1$	1
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$q - 1$	$q^2 - 1$
$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ with $a \neq d$	$\frac{1}{2}(q - 1)(q - 2)$	$q^2 + q$
$\alpha \in C - F^*$	$\frac{1}{2}(q - 1)q$	$q^2 - q$

In each case one computes the number of elements in a given class as the index of the normalizer of the element (or centralizer of the element). Case 1 is trivial. Case 2 can be done by direct computation, since the centralizer is then seen to consist of the matrices

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}, x \in F,$$

with  $x \neq 0$ . The third and fourth cases can be done by using Proposition 12.3.

As for the number of classes of each type, the first and second cases correspond to distinct choices of  $a \in F^*$  so the number of classes is  $q - 1$  in each case. In the third case, the conjugacy class is determined by the eigenvalues. There are  $q - 1$  possible choices for  $a$ , and then  $q - 2$  possible choices for  $d$ . But the non-ordered pair of eigenvalues determines the conjugacy class, so one must divide  $(q - 1)(q - 2)$  by 2 to get the number of classes. Finally, in the case of an element in a non-split Cartan, we have already seen that if  $\sigma$  generates  $\text{Gal}(K/F)$ , then  $M(\sigma x)$  is conjugate to  $M(x)$  in  $GL_2(F)$ . But on the other hand, suppose  $x, x' \in K^*$  and  $M(x), M(x')$  are conjugate in  $GL_2(F)$  under a given regular representation of  $K^*$  on  $K$  with respect to a given basis. Then this conjugation induces an  $F$ -algebra isomorphism on  $F[C_K]$ , whence an automorphism of  $K$ , which is the identity, or the non-trivial automorphism  $\sigma$ . Consequently the number of conjugacy classes for elements of the fourth type is equal to

$$\frac{\#(K) - \#(F)}{2} = \frac{q^2 - q}{2},$$

which gives the value in the table.

### Borel subgroup and induced representations

We let:

$$U = \text{group of unipotent elements } \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix};$$

$$B = \text{Borel subgroup} = UA = AU.$$

Then  $\#(B) = q(q-1)^2 = (q-1)(q^2-q)$ . We shall construct representations of  $G$  by inducing characters from  $B$ , and eventually we shall construct all irreducible representations of  $G$  by combining the induced representations in a suitable way. We shall deal with four types of characters. Except in the first type, which is 1-dimensional and therefore obviously simple, we shall prove that the other types are simple by computing induced characters. In one case we need to subtract a one-dimensional character. In the other cases, the induced character will turn out to be simple. The procedure will be systematic. We shall give a table of values for each type. We verify in each case that for the character  $\chi$  which we want to prove simple we have

$$\sum_{\beta \in G} |\chi(\beta)|^2 = \#(G),$$

and then apply Theorem 5.17(a) to get the simplicity. Once we have done this for all four types, from the tables of values we see that they are distinct. Finally, the total number of distinct characters which we have exhibited will be equal to the number of conjugacy classes, whence we conclude that we have exhibited all simple characters.

We now carry out this program. I myself learned the simple characters of  $GL_2(F)$  from a one-page handout by Tate in a course at Harvard, giving the subsequent tables and the values of the characters on conjugacy classes. I filled out the proofs in the following pages.

#### First type

$\mu : F^* \rightarrow C^*$  denotes a homomorphism. Then we obtain the character

$$\mu \circ \det : G \rightarrow C^*,$$

which is 1-dimensional. Its values on representatives of the conjugacy classes are given in the following table.

Table 12.5(I)

$\chi$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, d \neq a$	$\alpha \in C - F^*$
$\mu \circ \det$	$\mu(a)^2$	$\mu(a)^2$	$\mu(ad)$	$\mu \circ \det(\alpha)$

The stated values are by definition. The last value can also be written

$$\mu(\det \alpha) = \mu(N_{K/F}(\alpha)),$$

viewing  $\alpha$  as an element of  $K^*$ , because the reader should know from field theory that the determinant gives the norm.

A character of  $G$  will be said to be of **first type** if it is equal to  $\mu \circ \det$  for some  $\mu$ . There are  $q - 1$  characters of first type, because  $\#(F^*) = q - 1$ .

### Second type

Observe that we have  $B/U = A$ . A character of  $A$  can therefore be viewed as a character on  $B$  via  $B/U$ . We let:

$\psi_\mu = \text{res}_A(\mu \circ \det)$ , and view  $\psi_\mu$  therefore as a character on  $B$ . Thus

$$\psi_\mu \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \mu(ad).$$

We obtain the induced character

$$\psi_\mu^G = \text{ind}_B^G(\psi_\mu).$$

Then  $\psi_\mu^G$  is not simple. It contains  $\mu \circ \det$ , as one sees by Frobenius reciprocity:

$$\langle \text{ind}_B^G \psi_\mu, \mu \circ \det \rangle_G = \langle \psi_\mu, \mu \circ \det \rangle_B = \frac{1}{\#(B)} \sum_{\beta \in B} |\mu \circ \det(\beta)|^2 = 1.$$

Characters  $\chi = \psi_\mu^G - \mu \circ \det$  will be called of **second type**.

The values on the representatives of conjugacy classes are as follows.

**Table 12.5(II)**

$\chi$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
$\psi_\mu^G - \mu \circ \det$	$q\mu(a)^2$	0	$\mu(ad)$	$-\mu \circ \det(\alpha)$

Actually, one computes the values of  $\psi_\mu^G$ , and one then subtracts the value of  $\theta \circ \det$ . For this case and the next two cases, we use the formula for the induced function:

$$\text{ind}_H^G(\varphi)(\alpha) = \frac{1}{\#(H)} \sum_{\beta \in G} \varphi_H(\beta \alpha \beta^{-1})$$

where  $\varphi_H$  is the function equal to  $\varphi$  on  $H$  and 0 outside  $H$ . An element of the center commutes with all  $\beta \in G$ , so for  $\varphi = \psi_\mu$  the value of the induced character

on such an element is

$$\frac{\#(G)}{\#(B)}\mu(a)^2 = (q + 1)\mu(a)^2,$$

which gives the stated value.

For an element  $u = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$ , the only elements  $\beta \in G$  such that  $\beta u \beta^{-1}$  lies in  $B$  are the elements of  $B$  (by direct verification). It is then immediate that

$$\text{ind}_B^G(\psi_\mu) \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \mu(a)^2,$$

which yields the stated value for the character  $\chi$ . Using Table 12.4, one finds at once that  $\sum |\chi(\beta)|^2 = \#(G)$ , and hence;

*A character  $\chi$  of second type is simple.*

The table of values also shows that there are  $q - 1$  characters of second type. The next two types deal especially with the Cartan subgroups.

### Third type

$\psi : A \rightarrow \mathbf{C}^*$  denotes a homomorphism.

As mentioned following Proposition 12.3, the representative  $w = w_A = w^{-1}$  for  $N(A)/A$  is such that

$$w \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} w = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix} = \alpha^w \quad \text{if } \alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

Thus conjugation by  $w$  is an automorphism of order 2 on  $A$ . Let  $[w]\psi$  be the conjugate character; that is,  $([w]\psi)(\alpha) = \psi(w\alpha w) = \psi(\alpha^w)$  for  $\alpha \in A$ . Then  $[w](\mu \circ \det) = \mu \circ \det$ . The characters  $\mu \circ \det$  on  $A$  are precisely those which are invariant under  $[w]$ . The others can be written in the form

$$\psi \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \psi_1(a)\psi_2(d),$$

with distinct characters  $\psi_1, \psi_2 : F^* \rightarrow \mathbf{C}^*$ . In light of the isomorphism  $B/U \approx A$ , we view  $\psi$  has a character on  $B$ . Then we form the induced character

$$\psi^G = \text{ind}_B^G(\psi) = \text{ind}_B^G([w]\psi).$$

With  $\psi$  such that  $[w]\psi \neq \psi$ , the characters  $\chi = \psi^G$  will be said to be of the **third type**. Here is their table of values.

**Table 12.5(III)**

$\chi$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, d \neq a$	$\alpha \in C - F^*$
$\psi^G$ $\psi \neq [w]\psi$	$(q + 1)\psi(a)$	$\psi(a)$	$\psi(\alpha) + \psi(\alpha^w)$	0

The first entry on central elements is immediate. For the second, we have already seen that if  $\beta \in G$  is such that conjugating

$$\beta \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \beta^{-1} \in B,$$

then  $\beta \in B$ , and so the formula

$$\psi^G(\alpha) = \frac{1}{\#(B)} \sum_{\beta \in G} \psi_B(\beta \alpha \beta^{-1})$$

immediately gives the value of  $\psi^G$  on unipotent elements. For an element of  $A$  with  $a \neq d$ , there is the additional possibility of the normalizer of  $A$  with the elements  $w$ , and the value in the table then drops out from the formula. For elements of the non-split Cartan group, there is no element of  $G$  which conjugates them to elements of  $B$ , so the value in the last column is 0.

We claim that a character  $\chi = \psi^G$  of third type is simple.

The proof again uses the test for simplicity, i.e. that  $\sum |\chi(\beta)|^2 = \#(G)$ . Observe that two elements  $\alpha, \alpha' \in A$  are in the same conjugacy class in  $G$  if and only if  $\alpha' = \alpha$  or  $\alpha' = [w]\alpha$ . This is verified by brute force. Therefore, writing the sum  $\sum |\psi^G(\beta)|^2$  for  $\beta$  in the various conjugacy classes, and using Table 12.4, we find:

$$\begin{aligned} \sum_{\beta \in G} |\psi^G(\beta)|^2 &= (q + 1)^2(q - 1) \\ &\quad + (q - 1)(q^2 - 1) + (q^2 + q) \sum_{\alpha \in (A - F^*)/w} |\psi(\alpha) + \psi(\alpha^w)|^2. \end{aligned}$$

The third term can be written

$$\begin{aligned} \frac{1}{2}(q^2 + q) \sum_{\alpha \in A - F^*} (\psi(\alpha) + \psi(\alpha^w))(\psi(\alpha^{-1}) + \psi(\alpha^{-w})) \\ = \frac{1}{2}(q^2 + q) \sum_{\alpha \in A - F^*} (1 + 1 + \psi(\alpha^{1-w}) + \psi(\alpha^{w-1})). \end{aligned}$$

We write the sum over  $\alpha \in A - F^*$  as a sum for  $\alpha \in A$  minus the sum for

$\alpha \in F^*$ . If  $\alpha \in F^*$  then  $\alpha^{1-w} = \alpha^{w-1} = 1$ . By assumption on  $\psi$ , the character  $\alpha \mapsto \psi(\alpha^{1-w})$  for  $\alpha \in A$

is non-trivial, and therefore the sum over  $\alpha \in A$  is equal to 0. Therefore, putting these remarks together, we find that the third term is equal to

$$\frac{1}{2}(q^2 + q)[2(q - 1)^2 - 2(q - 1) - 2(q - 1)] = q(q^2 - 1)(q - 3).$$

Hence finally

$$\begin{aligned} \sum_{\beta \in G} |\psi^G(\beta)|^2 &= (q + 1)(q^2 - 1) + (q - 1)(q^2 - 1) + q(q^2 - 1)(q - 3) \\ &= q(q - 1)(q^2 - 1) = \#(G), \end{aligned}$$

thus proving that  $\psi^G$  is simple.

Finally we observe that there are  $\frac{1}{2}(q - 1)(q - 2)$  characters of third type. This is the number of characters  $\psi$  such that  $[w]\psi \neq \psi$ , divided by 2 because each pair  $\psi$  and  $[w]\psi$  yields the same induced character  $\psi^G$ . The table of values shows that up to this coincidence, the induced characters are distinct.

#### Fourth type

$\theta : K^* \rightarrow \mathbf{C}^*$  denotes a homomorphism, which is viewed as a character on  $C = C_K$ .

By Proposition 12.3, there is an element  $w \in N(C)$  but  $w \notin C$ ,  $w = w^{-1}$ . Then

$$\alpha \mapsto w\alpha w = [w]\alpha$$

is an automorphism of  $C$ , but  $x \mapsto wxw$  is also a field automorphism of  $F[C] \approx K$  over  $F$ . Since  $[K : F] = 2$ , it follows that conjugation by  $w$  is the automorphism  $\alpha \mapsto \alpha^q$ . As a result we obtain the conjugate character  $[w]\theta$  such that

$$([w]\theta)(\alpha) = \theta([w]\alpha) = \theta(\alpha^w),$$

and we get the induced character

$$\theta^G = \text{ind}_C^G(\theta) = \text{ind}_C^G([w]\theta).$$

Let  $\mu : F^* \rightarrow \mathbf{C}^*$  denote a homomorphism as in the first type. Let:

$\lambda : F^+ \rightarrow \mathbf{C}^*$  be a *non-trivial* homomorphism.

$(\mu, \lambda) =$  the character on  $ZU$  such that

$$(\mu, \lambda) \left( \begin{pmatrix} a & ax \\ 0 & a \end{pmatrix} \right) = \mu(a)\lambda(x).$$

$$(\mu, \lambda)^G = \text{ind}_{ZU}^G(\mu, \lambda).$$

A routine computation of the same nature that we have had previously gives the following values for the induced characters  $\theta^G$  and  $(\mu, \lambda)^G$ .

$\chi$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}_{d \neq a}$	$\alpha \in C - F^*$
$\theta^G$	$(q^2 - q)\theta(a)$	0	0	$\theta(\alpha) + \theta(\alpha^w)$
$(\mu, \lambda)^G$	$(q^2 - 1)\mu(a)$	$-\mu(a)$	0	0

These are intermediate steps. Note that a direct computation using Frobenius reciprocity shows that  $\theta^G$  occurs in the character  $(\text{res } \theta, \lambda)^G$ , where the restriction  $\text{res } \theta$  is to the group  $F^*$ , so  $\text{res } \theta$  is one of our characters  $\mu$ . Thus we define:

$$\theta' = (\text{res } \theta, \lambda)^G - \theta^G = ([w]\theta)',$$

which is an effective character. A character  $\theta'$  is said to be of **fourth type** if  $\theta$  is such that  $\theta \neq [w]\theta$ . These are the characters we are looking for. Using the intermediate table of values, one then finds the table of values for those characters of fourth type.

**Table 12.5(IV)**

$\chi$	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}_{d \neq a}$	$\alpha \in C - F^*$
$\theta'$ $\theta \neq [w]\theta$	$(q - 1)\theta(a)$	$-\theta(a)$	0	$-\theta(\alpha) - \theta(\alpha^w)$

We claim that the characters  $\theta'$  of fourth type are simple.

To prove this, we evaluate

$$\begin{aligned} \sum_{\beta \in G} |\theta'(\beta)|^2 &= (q - 1)^2(q - 1) + (q - 1)(q^2 - 1) \\ &\quad + \frac{1}{2}(q^2 - q) \sum_{\alpha \in K^* - F^*} |\theta(\alpha) + \theta(\alpha^w)|^2. \end{aligned}$$

We use the same type of expansion as for characters of third type, and the final value does turn out to be  $\#(G)$ , thus proving that  $\theta'$  is simple.

The table also shows that there are  $\frac{1}{2}\#(C - F^*) = \frac{1}{2}(q^2 - q)$  distinct characters of fourth type. We thus come to the end result of our computations.

**Theorem 12.6.** *The irreducible characters of  $G = GL_2(F)$  are as follows.*

type		number of that type	dimension
I	$\mu \circ \det$	$q - 1$	1
II	$\psi_\mu^G - \mu \circ \det$	$q - 1$	$q$
III	$\psi^G$ from pairs $\psi \neq [w]\psi$	$\frac{1}{2}(q - 1)(q - 2)$	$q + 1$
IV	$\theta'$ from pairs $\theta \neq [w]\theta$	$\frac{1}{2}(q - 1)q$	$q - 1$

*Proof.* We have exhibited characters of four types. In each case it is immediate from our construction that we get the stated number of distinct characters of the given type. The dimensions as stated are immediately computed from the dimensions of induced characters as the index of the subgroup from which we induce, and on two occasions we have to subtract something which was needed to make the character of given type simple. The end result is the one given in the above table. The total number of listed characters is precisely equal to the number of classes in Table 12.4, and therefore we have found all the simple characters, thus proving the theorem.

---

## EXERCISES

1. **The group  $S_3$ .** Let  $S_3$  be the symmetric group on 3 elements,
  - Show that there are three conjugacy classes.
  - There are two characters of dimension 1, on  $S_3/A_3$ .
  - Let  $d_i$  ( $i = 1, 2, 3$ ) be the dimensions of the irreducible characters. Since  $\sum d_i^2 = 6$ , the third irreducible character has dimension 2. Show that the third representation can be realized by considering a cubic equation  $X^3 + aX + b = 0$ , whose Galois group is  $S_3$  over a field  $k$ . Let  $V$  be the  $k$ -vector space generated by the roots. Show that this space is 2-dimensional and gives the desired representation, which remains irreducible after tensoring with  $k^a$ .
  - Let  $G = S_3$ . Write down an idempotent for each one of the simple components of  $\mathbf{C}[G]$ . What is the multiplicity of each irreducible representation of  $G$  in the regular representation on  $\mathbf{C}[G]$ ?

2. **The groups  $S_4$  and  $A_4$ .** Let  $S_4$  be the symmetric group on 4 elements.

- (a) Show that there are 5 conjugacy classes.
- (b) Show that  $A_4$  has a unique subgroup of order 4, which is not cyclic, and which is normal in  $S_4$ . Show that the factor group is isomorphic to  $S_3$ , so the representations of Exercise 1 give rise to representations of  $S_4$ .
- (c) Using the relation  $\sum d_i^2 = \#(S_4) = 24$ , conclude that there are only two other irreducible characters of  $S_4$ , each of dimension 3.
- (d) Let  $X^4 + a_2X^2 + a_1X + a_0$  be an irreducible polynomial over a field  $k$ , with Galois group  $S_4$ . Show that the roots generate a 3-dimensional vector space  $V$  over  $k$ , and that the representation of  $S_4$  on this space is irreducible, so we obtain one of the two missing representations.
- (e) Let  $\rho$  be the representation of (d). Define  $\rho'$  by

$$\begin{aligned}\rho'(\sigma) &= \rho(\sigma) \text{ if } \sigma \text{ is even;} \\ \rho'(\sigma) &= -\rho(\sigma) \text{ if } \sigma \text{ is odd.}\end{aligned}$$

Show that  $\rho'$  is also irreducible, remains irreducible after tensoring with  $k^a$ , and is non-isomorphic to  $\rho$ . This concludes the description of all irreducible representations of  $S_4$ .

- (f) Show that the 3-dimensional irreducible representations of  $S_4$  provide an irreducible representation of  $A_4$ .
- (g) Show that all irreducible representations of  $A_4$  are given by the representations in (f) and three others which are one-dimensional.

3. **The quaternion group.** Let  $Q = \{\pm 1, \pm x, \pm y, \pm z\}$  be the quaternion group, with  $x^2 = y^2 = z^2 = -1$  and  $xy = -yx, xz = -zx, yz = -zy$ .

- (a) Show that  $Q$  has 5 conjugacy classes.  
Let  $A = \{\pm 1\}$ . Then  $Q/A$  is of type  $(2, 2)$ , and hence has 4 simple characters, which can be viewed as simple characters of  $Q$ .
- (b) Show that there is only one more simple character of  $Q$ , of dimension 2.  
Show that the corresponding representation can be given by a matrix representation such that

$$\rho(x) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \rho(y) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \rho(z) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

- (c) Let  $\mathbf{H}$  be the quaternion field, i.e. the algebra over  $\mathbf{R}$  having dimension 4, with basis  $\{1, x, y, z\}$  as in Exercise 3, and the corresponding relations as above. Show that  $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{H} \approx \text{Mat}_2(\mathbf{C})$  ( $2 \times 2$  complex matrices). Relate this to (b).

- 4. Let  $S$  be a normal subgroup of  $G$ . Let  $\psi$  be a simple character of  $S$  over  $\mathbf{C}$ . Show that  $\text{ind}_S^G(\psi)$  is simple if and only if  $\psi = [\sigma]\psi$  for all  $\sigma \in S$ .
- 5. Let  $G$  be a finite group and  $S$  a normal subgroup. Let  $\rho$  be an irreducible representation of  $G$  over  $\mathbf{C}$ . Prove that either the restriction of  $\rho$  to  $S$  has all its irreducible components  $S$ -isomorphic to each other, or there exists a proper subgroup  $H$  of  $G$  containing  $S$  and an irreducible representation  $\theta$  of  $H$  such that  $\rho \approx \text{ind}_H^G(\theta)$ .
- 6. **Dihedral group  $D_{2n}$ .** There is a group of order  $2n$  ( $n$  even integer  $\geq 2$ ) generated by two elements  $\sigma, \tau$  such that

$$\sigma^n = 1, \tau^2 = 1, \text{ and } \tau\sigma\tau = \sigma^{-1}.$$

It is called the **dihedral group**.

- (a) Show that there are four representations of dimension 1, obtained by the four possible values  $\pm 1$  for  $\sigma$  and  $\tau$ .
- (b) Let  $C_n$  be the cyclic subgroup of  $D_{2n}$  generated by  $\sigma$ . For each integer  $r = 0, \dots, n-1$  let  $\psi_r$  be the character of  $C_n$  such that

$$\psi_r(\sigma) = \zeta^r \quad (\zeta = \text{prim. } n\text{-th root of unity})$$

Let  $\chi_r$  be the induced character. Show that  $\chi_r = \chi_{n-r}$ .

- (c) Show that for  $0 < r < n/2$  the induced character  $\chi_r$  is simple, of dimension 2, and that one gets thereby  $\left(\frac{n}{2} - 1\right)$  distinct characters of dimension 2.
- (d) Prove that the simple characters of (a) and (c) give all simple characters of  $D_{2n}$ .

7. Let  $G$  be a finite group, semidirect product of  $A, H$  where  $A$  is commutative and normal. Let  $A^\wedge = \text{Hom}(A, \mathbf{C}^*)$  be the dual group. Let  $G$  operate by conjugation on characters, so that for  $\sigma \in G, a \in A$ , we have

$$[\sigma]\psi(a) = \psi(\sigma^{-1}a\sigma).$$

Let  $\psi_1, \dots, \psi_r$  be representatives of the orbits of  $H$  in  $A^\wedge$ , and let  $H_i (i = 1, \dots, r)$  be the isotropy group of  $\psi_i$ . Let  $G_i = AH_i$ .

- (a) For  $a \in A$  and  $h \in H_i$ , define  $\psi_i(ah) = \psi_i(a)$ . Show that  $\psi_i$  is thus extended to a character on  $G_i$ .
- Let  $\theta$  be a simple representation of  $H_i$  (on a vector space over  $\mathbf{C}$ ). From  $H_i = G_i/A$ , view  $\theta$  as a simple representation of  $G_i$ . Let

$$\rho_{i,\theta} = \text{ind}_{G_i}^G(\psi_i \otimes \theta).$$

- (b) Show that  $\rho_{i,\theta}$  is simple.
  - (c) Show that  $\rho_{i,\theta} \approx \rho_{i',\theta'}$  implies  $i = i'$  and  $\theta \approx \theta'$ .
  - (d) Show that every irreducible representation of  $G$  is isomorphic to some  $\rho_{i,\theta}$ .
8. Let  $G$  be a finite group operating on a finite set  $S$ . Let  $\mathbf{C}[S]$  be the vector space generated by  $S$  over  $\mathbf{C}$ . Let  $\psi$  be the character of the corresponding representation of  $G$  on  $\mathbf{C}[S]$ .
- (a) Let  $\sigma \in G$ . Show that  $\psi(\sigma) = \text{number of fixed points of } \sigma \text{ in } S$ .
  - (b) Show that  $\langle \psi, 1_G \rangle_G$  is the number of  $G$ -orbits in  $S$ .
9. Let  $A$  be a commutative subgroup of a finite group  $G$ . Show that every irreducible representation of  $G$  over  $\mathbf{C}$  has dimension  $\leq (G : A)$ .
10. Let  $\mathbf{F}$  be a finite field and let  $G = SL_2(\mathbf{F})$ . Let  $B$  be the subgroup of  $G$  consisting of all matrices

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL_2(\mathbf{F}), \text{ so } d = a^{-1}.$$

Let  $\mu : \mathbf{F}^* \rightarrow \mathbf{C}^*$  be a homomorphism and let  $\psi_\mu : B \rightarrow \mathbf{C}^*$  be the homomorphism such that  $\psi_\mu(\alpha) = \mu(a)$ . Show that the induced character  $\text{ind}_B^G(\psi_\mu)$  is simple if  $\mu^2 \neq 1$ .

11. Determine all simple characters of  $SL_2(\mathbf{F})$ , giving a table for the number of such characters, representatives for the conjugacy classes, as was done in the text for  $GL_2$ , over the complex numbers.
12. Observe that  $A_5 \approx SL_2(\mathbf{F}_4) \approx PSL_2(\mathbf{F}_5)$ . As a result, verify that there are 5 conjugacy classes, whose elements have orders 1, 2, 3, 5, 5 respectively, and write down explicitly the character table for  $A_5$  as was done in the text for  $GL_2$ .
13. Let  $G$  be a  $p$ -group and let  $G \rightarrow \text{Aut}(V)$  be a representation on a finite dimensional vector space over a field of characteristic  $p$ . Assume that the representation is irreducible. Show that the representation is trivial, i.e.  $G$  acts as the identity on  $V$ .
14. Let  $G$  be a finite group and let  $C$  be a conjugacy class. Prove that the following two conditions are equivalent. They define what it means for the class to be **rational**.
  - RAT 1.** For all characters  $\chi$  of  $G$ ,  $\chi(\sigma) \in \mathbf{Q}$  for  $\sigma \in C$ .
  - RAT 2.** For all  $\sigma \in C$ , and  $j$  prime to the order of  $\sigma$ , we have  $\sigma^j \in C$ .

15. Let  $G$  be a group and let  $H_1, H_2$  be subgroups of finite index. Let  $\rho_1, \rho_2$  be representations of  $H_1, H_2$  on  $R$ -modules  $F_1, F_2$  respectively. Let  $M_G(F_1, F_2)$  be the  $R$ -module of functions  $f: G \rightarrow \text{Hom}_R(F_1, F_2)$  such that

$$f(h_1 \sigma h_2) = \rho_2(h_2) f(\sigma) \rho_1(h_1)$$

for all  $\sigma \in G, h_i \in H_i$  ( $i = 1, 2$ ). Establish an  $R$ -module isomorphism

$$\text{Hom}_R(F_1^G, F_2^G) \xrightarrow{\sim} M_G(F_1, F_2).$$

By  $F_i^G$  we have abbreviated  $\text{ind}_{H_i}^G(F_i)$ .

16. (a) Let  $G_1, G_2$  be two finite groups with representations on  $\mathbf{C}$ -spaces  $E_1, E_2$ . Let  $E_1 \otimes E_2$  be the usual tensor product over  $\mathbf{C}$ , but now prove that there is an action of  $G_1 \times G_2$  on this tensor product such that

$$(\sigma_1, \sigma_2)(x \otimes y) = \sigma_1 x \otimes \sigma_2 y \text{ for } \sigma_1 \in G_1, \sigma_2 \in G_2.$$

This action is called the **tensor product** of the other two. If  $\rho_1, \rho_2$  are the representations of  $G_1, G_2$  on  $E_1, E_2$  respectively, then their tensor product is denoted by  $\rho_1 \otimes \rho_2$ . Prove: If  $\rho_1, \rho_2$  are irreducible then  $\rho_1 \otimes \rho_2$  is also irreducible. [Hint: Use Theorem 5.17.]

- (b) Let  $\chi_1, \chi_2$  be the characters of  $\rho_1, \rho_2$  respectively. Show that  $\chi_1 \otimes \chi_2$  is the character of the tensor product. By definition,

$$\chi_1 \otimes \chi_2(\sigma_1, \sigma_2) = \chi_1(\sigma_1) \chi_2(\sigma_2).$$

17. With the same notation as in Exercise 16, show that every irreducible representation of  $G_1 \times G_2$  over  $\mathbf{C}$  is isomorphic to a tensor product representation as in Exercise 16. [Hint: Prove that if a character is orthogonal to all the products  $\chi_1 \otimes \chi_2$  of Exercise 16(b) then the character is 0.]

### Tensor product representations

18. Let  $P$  be the non-commutative polynomial algebra over a field  $k$ , in  $n$  variables. Let  $x_1, \dots, x_r$  be distinct elements of  $P_1$  (i.e. linear expressions in the variables  $t_1, \dots, t_n$ )

and let  $a_1, \dots, a_r \in k$ . If

$$a_1 x_1^v + \dots + a_r x_r^v = 0$$

for all integers  $v = 1, \dots, r$  show that  $a_i = 0$  for  $i = 1, \dots, r$ . [Hint: Take the homomorphism on the commutative polynomial algebra and argue there.]

19. Let  $G$  be a finite set of endomorphisms of a finite-dimensional vector space  $E$  over the field  $k$ . For each  $\sigma \in G$ , let  $c_\sigma$  be an element of  $k$ . Show that if

$$\sum_{\sigma \in G} c_\sigma T^r(\sigma) = 0$$

for all integers  $r \geq 1$ , then  $c_\sigma = 0$  for all  $\sigma \in G$ . [Hint: Use the preceding exercise, and Proposition 7.2 of Chapter XVI.]

20. (Steinberg). Let  $G$  be a finite monoid, and  $k[G]$  the monoid algebra over a field  $k$ . Let  $G \rightarrow \text{End}_k(E)$  be a faithful representation (i.e. injective), so that we identify  $G$  with a multiplicative subset of  $\text{End}_k(E)$ . Show that  $T^r$  induces a representation of  $G$  on  $T^r(E)$ , whence a representation of  $k[G]$  on  $T^r(E)$  by linearity. If  $\alpha \in k[G]$  and if  $T^r(\alpha) = 0$  for all integers  $r \geq 1$ , show that  $\alpha = 0$ . [Hint: Apply the preceding exercise.]
21. (Burnside). Deduce from Exercise 20 the following theorem of Burnside: Let  $G$  be a finite group,  $k$  a field of characteristic prime to the order of  $G$ , and  $E$  a finite dimensional  $(G, k)$ -space such that the representation of  $G$  is faithful. Then every irreducible representation of  $G$  appears with multiplicity  $\geq 1$  in some tensor power  $T^r(E)$ .
22. Let  $X(G)$  be the character ring of a finite group  $G$ , generated over  $\mathbf{Z}$  by the simple characters over  $\mathbf{C}$ . Show that an element  $f \in X(G)$  is an effective irreducible character if and only if  $\langle f, f \rangle_G = 1$  and  $f(1) \geq 0$ .
23. In this exercise, we assume the next chapter on alternating products. Let  $\rho$  be an irreducible representation of  $G$  on a vector space  $E$  over  $\mathbf{C}$ . Then by functoriality we have the corresponding representations  $S^r(\rho)$  and  $\bigwedge^r(\rho)$  on the  $r$ -th symmetric power and  $r$ -th alternating power of  $E$  over  $\mathbf{C}$ . If  $\chi$  is the character of  $\rho$ , we let  $S^r(\chi)$  and  $\bigwedge^r(\chi)$  be the characters of  $S^r(\rho)$  and  $\bigwedge^r(\rho)$  respectively, on  $S^r(E)$  and  $\bigwedge^r(E)$ . Let  $t$  be a variable and let

$$\sigma_t(\chi) = \sum_{r=0}^{\infty} S^r(\chi) t^r, \quad \lambda_t(\chi) = \sum_{r=0}^{\infty} \bigwedge^r(\chi) t^r.$$

- (a) Comparing with Exercise 24 of Chapter XIV, prove that for  $x \in G$  we have

$$\sigma_t(\chi)(x) = \det(I - \rho(x)t)^{-1} \quad \text{and} \quad \lambda_t(\chi)(x) = \det(I + \rho(x)t).$$

- (b) For a function  $f$  on  $G$  define  $\Psi^n(f)$  by  $\Psi^n(f)(x) = f(x^n)$ . Show that

$$-\frac{d}{dt} \log \sigma_t(\chi) = \sum_{n=1}^{\infty} \Psi^n(\chi) t^n \quad \text{and} \quad -\frac{d}{dt} \log \lambda_{-t}(\chi) = \sum_{n=1}^{\infty} (-1)^{r-1} \Psi^r(\chi) t^n.$$

- (c) Show that

$$n S^n(\chi) = \sum_{r=1}^n \Psi^r(\chi) S^{n-r}(\chi) \quad \text{and} \quad n \bigwedge^n(\chi) = \sum_{r=1}^n (-1)^{r-1} \Psi^r(\chi) \bigwedge^{n-r}(\chi).$$

24. Let  $\chi$  be a simple character of  $G$ . Prove that  $\Psi^n(\chi)$  is also simple. (The characters are over  $\mathbb{C}$ .)
25. We now assume that you know §3 of Chapter XX.
- Prove that the Grothendieck ring defined there for  $\text{Mod}_{\mathbb{C}}(G)$  is naturally isomorphic to the character ring  $X(G)$ .
  - Relate the above formulas with Theorem 3.12 of Chapter XX.
  - Read Fulton-Lang's *Riemann-Roch Algebra*, Chapter I, especially §6, and show that  $X(G)$  is a  $\lambda$ -ring, with  $\Psi^n$  as the Adams operations.

*Note.* For further connections with homology and the cohomology of groups, see Chapter XX, §3, and the references given at the end of Chapter XX, §3.

26. The following formalism is the analogue of Artin's formalism of  $L$ -series in number theory. Cf. Artin's "Zur Theorie der  $L$ -Reihen mit allgemeinen Gruppencharakteren", Collected papers, and also S. Lang, " $L$ -series of a covering", *Proc. Nat. Acad. Sc. USA* (1956). For the Artin formalism in a context of analysis, see J. Jorgenson and S. Lang, "Artin formalism and heat kernels", *J. reine angew. Math.* **447** (1994) pp. 165–200.

We consider a category with objects  $\{U\}$ . As usual, we say that a finite group  $G$  operates on  $U$  if we are given a homomorphism  $\rho: G \rightarrow \text{Aut}(U)$ . We then say that  $U$  is a  $G$ -object, and also that  $\rho$  is a representation of  $G$  in  $U$ . We say that  $G$  operates trivially if  $\rho(G) = \text{id}$ . For simplicity, we omit the  $\rho$  from the notation. By a  $G$ -morphism  $f: U \rightarrow V$  between  $G$ -objects, one means a morphism such that  $f \circ \sigma = \sigma \circ f$  for all  $\sigma \in G$ .

We shall assume that for each  $G$ -object  $U$  there exists an object  $U/G$  on which  $G$  operates trivially, and a  $G$ -morphism  $\pi_{U,G}: U \rightarrow U/G$  having the following universal property: If  $f: U \rightarrow U'$  is a  $G$ -morphism, then there exists a unique morphism

$$f/G: U/G \rightarrow U'/G$$

making the following diagram commutative:

$$\begin{array}{ccc} U & \xrightarrow{f} & U' \\ \downarrow & & \downarrow \\ U/G & \xrightarrow{f/G} & U'/G \end{array}$$

In particular, if  $H$  is a normal subgroup of  $G$ , show that  $G/H$  operates in a natural way on  $U/H$ .

Let  $k$  be an algebraically closed field of characteristic 0. We assume given a functor  $E$  from our category to the category of finite dimensional  $k$ -spaces. If  $U$  is an object in our category, and  $f: U \rightarrow U'$  is a morphism, then we get a homomorphism

$$E(f) = f_*: E(U) \rightarrow E(U').$$

(The reader may keep in mind the special case when we deal with the category of reasonable topological spaces, and  $E$  is the homology functor in a given dimension.)

If  $G$  operates on  $U$ , then we get an operation of  $G$  on  $E(U)$  by functoriality.

Let  $U$  be a  $G$ -object, and  $F: U \rightarrow U$  a  $G$ -morphism. If  $P_F(t) = \prod (t - \alpha_i)$  is the characteristic polynomial of the linear map  $F_*: E(U) \rightarrow E(U)$ , we define

$$Z_F(t) = \prod (1 - \alpha_i t),$$

and call this the zeta function of  $F$ . If  $F$  is the identity, then  $Z_F(t) = (1 - t)^{B(U)}$  where we define  $B(U)$  to be  $\dim_k E(U)$ .

Let  $\chi$  be a simple character of  $G$ . Let  $d_\chi$  be the dimension of the simple representation of  $G$  belonging to  $\chi$ , and  $n = \text{ord}(G)$ . We define a linear map on  $E(U)$  by letting

$$e_\chi = \frac{d_\chi}{n} \sum_{\sigma \in G} \chi(\sigma^{-1}) \sigma_*.$$

Show that  $e_\chi^2 = e_\chi$ , and that for any positive integer  $\mu$  we have  $(e_\chi \circ F_*)^\mu = e_\chi \circ F_*^\mu$ . If  $P_\chi(t) = \prod (t - \beta_j(\chi))$  is the characteristic polynomial of  $e_\chi \circ F_*$ , define

$$L_F(t, \chi, U/G) = \prod (1 - \beta_j(\chi)t).$$

Show that the logarithmic derivative of this function is equal to

$$-\frac{1}{N} \sum_{\mu=1}^{\infty} \text{tr}(e_\chi \circ F_*^\mu) t^{\mu-1}.$$

Define  $L_F(t, \chi, U/G)$  for any character  $\chi$  by linearity. If we write  $V = U/G$  by abuse of notation, then we also write  $L_F(t, \chi, U/V)$ . Then for any  $\chi, \chi'$  we have by definition,

$$L_F(t, \chi + \chi', U/V) = L_F(t, \chi, U/V) L_F(t, \chi', U/V).$$

We make one additional assumption on the situation:

Assume that the characteristic polynomial of

$$\frac{1}{n} \sum_{\sigma \in G} \sigma_* \circ F_*$$

is equal to the characteristic polynomial of  $F/G$  on  $E(U/G)$ . Prove the following statement:

(a) If  $G = \{1\}$  then

$$L_F(t, 1, U/U) = Z_F(t).$$

(b) Let  $V = U/G$ . Then

$$L_F(t, 1, U/V) = Z_F(t).$$

(c) Let  $H$  be a subgroup of  $G$  and let  $\psi$  be a character of  $H$ . Let  $W = U/H$ , and let  $\psi^G$  be the induced character from  $H$  to  $G$ . Then

$$L_F(t, \psi, U/W) = L_F(t, \psi^G, U/V).$$

(d) Let  $H$  be normal in  $G$ . Then  $G/H$  operates on  $U/H = W$ . Let  $\psi$  be a character of  $G/H$ , and let  $\chi$  be the character of  $G$  obtained by composing  $\psi$  with the canonical map  $G \rightarrow G/H$ . Let  $\varphi = F/H$  be the morphism induced on

$$U/H = W.$$

Then

$$L_\varphi(t, \psi, W/V) = L_F(t, \chi, U/V).$$

(e) If  $V = U/G$  and  $B(V) = \dim_k E(V)$ , show that  $(1 - t)^{B(V)}$  divides  $(1 - t)^{B(U)}$ . Use the regular character to determine a factorization of  $(1 - t)^{B(U)}$ .

27. Do this exercise after you have read some of Chapter VII. The point is that for fields of characteristic not dividing the order of the group, the representations can be obtained by “reducing modulo a prime”. Let  $G$  be a finite group and let  $p$  be a prime not dividing the order of  $G$ . Let  $F$  be a finite extension of the rationals with ring of algebraic integers  $\mathfrak{o}_F$ . Suppose that  $F$  is sufficiently large so that all  $F$ -irreducible representations of  $G$  remain irreducible when tensored with  $\mathbf{Q}^a = F^a$ . Let  $\mathfrak{p}$  be a prime of  $\mathfrak{o}_F$  lying above  $p$ , and let  $\mathfrak{o}_{\mathfrak{p}}$  be the corresponding local ring.

- (a) Show that an irreducible  $(G, F)$ -space  $V$  can be obtained from a  $(G, \mathfrak{o}_{\mathfrak{p}})$ -module  $E$  free over  $\mathfrak{o}_{\mathfrak{p}}$ , by extending the base from  $\mathfrak{o}_{\mathfrak{p}}$  to  $F$ , i.e. by tensoring so that  $V = E \otimes F$  (tensor product over  $\mathfrak{o}_{\mathfrak{p}}$ ).
- (b) Show that the reduction mod  $\mathfrak{p}$  of  $E$  is an irreducible representation of  $G$  in characteristic  $p$ . In other words, let  $k = \mathfrak{o}/\mathfrak{p} = \mathfrak{o}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$  where  $\mathfrak{m}_{\mathfrak{p}}$  is the maximal ideal of  $\mathfrak{o}_{\mathfrak{p}}$ . Let  $E(\mathfrak{p}) = E \otimes k$  (tensor product over  $\mathfrak{o}_{\mathfrak{p}}$ ). Show that  $G$  operates on  $E(\mathfrak{p})$  in a natural way, and that this representation is irreducible. In fact, if  $\chi$  is the character of  $G$  on  $V$ , show that  $\chi$  is also the character on  $E$ , and that  $\chi \bmod \mathfrak{m}_{\mathfrak{p}}$  is the character on  $E(\mathfrak{p})$ .
- (c) Show that all irreducible characters of  $G$  in characteristic  $p$  are obtained as in (b).

---

# CHAPTER XIX

---

## The Alternating Product

The alternating product has applications throughout mathematics. In differential geometry, one takes the maximal alternating product of the tangent space to get a canonical line bundle over a manifold. Intermediate alternating products give rise to differential forms (sections of these products over the manifold). In this chapter, we give the algebraic background for these constructions.

For a reasonably self-contained treatment of the action of various groups of automorphisms of bilinear forms on tensor and alternating algebras, together with numerous classical examples, I refer to:

R. HOWE, Remarks on classical invariant theory, *Trans. AMS* **313** (1989),  
pp. 539–569

---

### §1 DEFINITION AND BASIC PROPERTIES

Consider the category of modules over a commutative ring  $R$ .

We recall that an  $r$ -multilinear map  $f: E^{(r)} \rightarrow F$  is said to be **alternating** if  $f(x_1, \dots, x_r) = 0$  whenever  $x_i = x_j$  for some  $i \neq j$ .

Let  $\mathfrak{a}_r$  be the submodule of the tensor product  $T^r(E)$  generated by all elements of type

$$x_1 \otimes \cdots \otimes x_r$$

where  $x_i = x_j$  for some  $i \neq j$ . We define

$$\bigwedge^r(E) = T^r(E)/\mathfrak{a}_r.$$

Then we have an  $r$ -multilinear map  $E^{(r)} \rightarrow \bigwedge^r(E)$  (called canonical) obtained

from the composition

$$E^{(r)} \rightarrow T^r(E) \rightarrow T^r(E)/\mathfrak{a}_r = \bigwedge^r(E).$$

It is clear that our map is alternating. Furthermore, it is universal with respect to  $r$ -multilinear alternating maps on  $E$ . In other words, if  $f: E^{(r)} \rightarrow F$  is such a map, there exists a unique linear map  $f_*: \bigwedge^r(E) \rightarrow F$  such that the following diagram is commutative:

$$\begin{array}{ccc} & & \bigwedge^r(E) \\ E^{(r)} & \nearrow & \downarrow f_* \\ & \searrow & \downarrow \\ & & F \end{array}$$

Our map  $f_*$  exists because we can first get an induced map  $T^r(E) \rightarrow F$  making the following diagram commutative:

$$\begin{array}{ccc} & & T^r(E) \\ E^{(r)} & \nearrow & \downarrow \\ & \searrow & \downarrow \\ & & F \end{array}$$

and this induced map vanishes on  $\mathfrak{a}_r$ , hence inducing our  $f_*$ .

The image of an element  $(x_1, \dots, x_r) \in E^{(r)}$  in the canonical map into  $\bigwedge^r(E)$  will be denoted by  $x_1 \wedge \dots \wedge x_r$ . It is also the image of  $x_1 \otimes \dots \otimes x_r$  in the factor homomorphism  $T^r(E) \rightarrow \bigwedge^r(E)$ .

In this way,  $\bigwedge^r$  becomes a functor, from modules to modules. Indeed, let  $u: E \rightarrow F$  be a homomorphism. Given elements  $x_1, \dots, x_r \in E$ , we can map

$$(x_1, \dots, x_r) \mapsto u(x_1) \wedge \dots \wedge u(x_r) \in \bigwedge^r(F).$$

This map is multilinear alternating, and therefore induces a homomorphism

$$\bigwedge^r(u): \bigwedge^r(E) \rightarrow \bigwedge^r(F).$$

The association  $u \mapsto \bigwedge^r(u)$  is obviously functorial.

**Example.** Open any book on differential geometry (complex or real) and you will see an application of this construction when  $E$  is the tangent space of a point on a manifold, or the dual of the tangent space. When taking the dual, the construction gives rise to differential forms.

We let  $\bigwedge(E)$  be the direct sum

$$\bigwedge(E) = \bigoplus_{r=0}^{\infty} \bigwedge^r(E).$$

We shall make  $\bigwedge(E)$  into a graded  $R$ -algebra and call it the **alternating algebra** of  $E$ , or also the **exterior algebra**, or the **Grassmann algebra**. We shall first discuss the general situation, with arbitrary graded rings.

Let  $G$  be an additive monoid again, and let  $A = \bigoplus_{r \in G} A_r$  be a  $G$ -graded  $R$ -algebra. Suppose given for each  $A_r$  a submodule  $\mathfrak{a}_r$ , and let  $\mathfrak{a} = \bigoplus_{r \in G} \mathfrak{a}_r$ . Assume that  $\mathfrak{a}$  is an ideal of  $A$ . Then  $\mathfrak{a}$  is called a **homogeneous ideal**, and we can define a graded structure on  $A/\mathfrak{a}$ . Indeed, the bilinear map

$$A_r \times A_s \rightarrow A_{r+s}$$

sends  $\mathfrak{a}_r \times A_s$  into  $\mathfrak{a}_{r+s}$  and similarly, sends  $A_r \times \mathfrak{a}_s$  into  $\mathfrak{a}_{r+s}$ . Thus using representatives in  $A_r, A_s$  respectively, we can define a bilinear map

$$A_r/\mathfrak{a}_r \times A_s/\mathfrak{a}_s \rightarrow A_{r+s}/\mathfrak{a}_{r+s},$$

and thus a bilinear map  $A/\mathfrak{a} \times A/\mathfrak{a} \rightarrow A/\mathfrak{a}$ , which obviously makes  $A/\mathfrak{a}$  into a graded  $R$ -algebra.

We apply this to  $T'(E)$  and the modules  $\mathfrak{a}_r$  defined previously. If

$$x_i = x_j \quad (i \neq j)$$

in a product  $x_1 \wedge \cdots \wedge x_r$ , then for any  $y_1, \dots, y_s \in E$  we see that

$$x_1 \wedge \cdots \wedge x_r \wedge y_1 \wedge \cdots \wedge y_s$$

lies in  $\mathfrak{a}_{r+s}$ , and similarly for the product on the left. Hence the direct sum  $\bigoplus \mathfrak{a}_r$  is an ideal of  $T(E)$ , and we can define an  $R$ -algebra structure on  $T(E)/\mathfrak{a}$ . The product on homogeneous elements is given by the formula

$$((x_1 \wedge \cdots \wedge x_r), (y_1 \wedge \cdots \wedge y_s)) \mapsto x_1 \wedge \cdots \wedge x_r \wedge y_1 \wedge \cdots \wedge y_s.$$

We use the symbol  $\wedge$  also to denote the product in  $\bigwedge(E)$ . This product is called the **alternating product** or **exterior product**. If  $x \in E$  and  $y \in E$ , then  $x \wedge y = -y \wedge x$ , as follows from the fact that  $(x + y) \wedge (x + y) = 0$ .

We observe that  $\bigwedge$  is a functor from the category of modules to the category of graded  $R$ -algebras. To each linear map  $f: E \rightarrow F$  we obtain a map

$$\bigwedge(f): \bigwedge(E) \rightarrow \bigwedge(F)$$

which is such that for  $x_1, \dots, x_r \in E$  we have

$$\bigwedge(f)(x_1 \wedge \cdots \wedge x_r) = f(x_1) \wedge \cdots \wedge f(x_r).$$

Furthermore,  $\bigwedge(f)$  is a homomorphism of graded  $R$ -algebras.

**Proposition 1.1.** *Let  $E$  be free of dimension  $n$  over  $R$ . If  $r > n$  then  $\bigwedge^r(E) = 0$ . Let  $\{v_1, \dots, v_n\}$  be a basis of  $E$  over  $R$ . If  $1 \leq r \leq n$ , then  $\bigwedge^r(E)$  is free over  $R$ , and the elements*

$$v_{i_1} \wedge \cdots \wedge v_{i_r}, \quad i_1 < \cdots < i_r$$

*form a basis of  $\bigwedge^r(E)$  over  $k$ . We have*

$$\dim_R \bigwedge^r(E) = \binom{n}{r}.$$

*Proof.* We shall first prove our assertion when  $r = n$ . Every element of  $E$  can be written in the form  $\sum a_i v_i$ , and hence using the formula  $x \wedge y = -y \wedge x$  we conclude that  $v_1 \wedge \cdots \wedge v_n$  generates  $\bigwedge^n(E)$ . On the other hand, we know from the theory of determinants that given  $a \in R$ , there exists a unique multi-linear alternating form  $f_a$  on  $E$  such that

$$f_a(v_1, \dots, v_n) = a.$$

Consequently, there exists a unique linear map

$$\bigwedge^n(E) \rightarrow R$$

taking the value  $a$  on  $v_1 \wedge \cdots \wedge v_n$ . From this it follows at once that  $v_1 \wedge \cdots \wedge v_n$  is a basis of  $\bigwedge^n(E)$  over  $R$ .

We now prove our statement for  $1 \leq r \leq n$ . Suppose that we have a relation

$$0 = \sum a_{(i)} v_{i_1} \wedge \cdots \wedge v_{i_r}$$

with  $i_1 < \cdots < i_r$  and  $a_{(i)} \in R$ . Select any  $r$ -tuple  $(j) = (j_1, \dots, j_r)$  such that  $j_1 < \cdots < j_r$ , and let  $j_{r+1}, \dots, j_n$  be those values of  $i$  which do not appear among  $(j_1, \dots, j_r)$ . Take the alternating product with  $v_{j_{r+1}} \wedge \cdots \wedge v_{j_n}$ . Then we shall have alternating products in the sum with repeated components in all the terms except the  $(j)$ -term, and thus we obtain

$$0 = a_{(j)} v_{j_1} \wedge \cdots \wedge v_{j_r} \wedge \cdots \wedge v_{j_n}.$$

Reshuffling  $v_{j_1} \wedge \cdots \wedge v_{j_n}$  into  $v_1 \wedge \cdots \wedge v_n$  simply changes the right-hand side by a sign. From what we proved at the beginning of this proof, it follows that  $a_{(j)} = 0$ . Hence we have proved our assertion for  $1 \leq r \leq n$ .

When  $r = 0$ , we deal with the empty product, and 1 is a basis for  $\bigwedge^0(E) = R$  over  $R$ . We leave the case  $r > n$  as a trivial exercise to the reader.

The assertion concerning the dimension is trivial, considering that there is a bijection between the set of basis elements, and the subsets of the set of integers  $(1, \dots, n)$ .

**Remark.** It is possible to give the first part of the proof, for  $\bigwedge^n(E)$ , without assuming known the existence of determinants. One must then show that  $\mathfrak{a}_n$  admits a 1-dimensional complementary submodule in  $T^n(E)$ . This can be done by simple means, which we leave as an exercise which the reader can look up in the more general situation of §4. When  $R$  is a field, this exercise is even more trivial, since one can verify at once that  $v_1 \otimes \cdots \otimes v_n$  does not lie in  $\mathfrak{a}_n$ . This alternative approach to the theorem then proves the existence of determinants.

**Proposition 1.2.** *Let*

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

*be an exact sequence of free  $R$ -modules of finite ranks  $r$ ,  $n$ , and  $s$  respectively. Then there is a natural isomorphism*

$$\varphi : \bigwedge^r E' \otimes \bigwedge^s E'' \rightarrow \bigwedge^n E.$$

*This isomorphism is the unique isomorphism having the following property. For elements  $v_1, \dots, v_r \in E'$  and  $w_1, \dots, w_s \in E''$ , let  $u_1, \dots, u_s$  be liftings of  $w_1, \dots, w_s$  in  $E$ . Then*

$$\varphi((v_1 \wedge \cdots \wedge v_r) \otimes (w_1 \wedge \cdots \wedge w_s)) = v_1 \wedge \cdots \wedge v_r \wedge u_1 \wedge \cdots \wedge u_s.$$

*Proof.* The proof proceeds in the usual two steps. First one shows the existence of a homomorphism  $\varphi$  having the desired effect. The value on the right of the above formula is independent of the choice of  $u_1, \dots, u_s$  lifting  $w_1, \dots, w_s$  by using the alternating property, so we obtain a homomorphism  $\varphi$ . Selecting in particular  $\{v_1, \dots, v_r\}$  and  $\{w_1, \dots, w_s\}$  to be bases of  $E'$  and  $E''$  respectively, one then sees that  $\varphi$  is both injective and surjective. We leave the details to the reader.

Given a free module  $E$  of rank  $n$ , we define its **determinant** to be

$$\det E = \bigwedge^{\max} E = \bigwedge^n E.$$

Then Proposition 1.2 may be reformulated by the isomorphism formula

$$\det(E') \otimes \det(E'') \approx \det(E).$$

If  $R = k$  is a field, then we may say that  $\det$  is an Euler-Poincaré map on the category of finite dimensional vector spaces over  $k$ .

**Example.** Let  $V$  be a finite dimensional vector space over  $\mathbf{R}$ . By a **volume** on  $V$  we mean a norm  $\| \cdot \|$  on  $\det V$ . Since  $V$  is finite dimensional, such a norm is equivalent to assigning a positive number  $c$  to a given basis of  $\det(V)$ . Such a basis can be expressed in the form  $e_1 \wedge \cdots \wedge e_n$ , where  $\{e_1, \dots, e_n\}$  is a basis of  $V$ . Then for  $a \in \mathbf{R}$  we have

$$\|ae_1 \wedge \cdots \wedge e_n\| = |a|c.$$

In analysis, given a volume as above, one then defines a Haar measure  $\mu$  on  $V$  by defining the measure of a set  $S$  to be

$$\mu(S) = \int_S \|e_1 \wedge \cdots \wedge e_n\| dx_1 \cdots dx_n,$$

where  $x_1, \dots, x_n$  are the coordinates on  $V$  with respect to the above basis. As an exercise, show that the expression on the right is the independent of the choice of basis.

Proposition 1.2 is a special case of the following more general situation. We consider again an exact sequence of free  $R$ -modules of finite rank as above. With respect to the submodule  $E'$  of  $E$ , we define

$$\bigwedge_i^n E = \text{submodule of } \bigwedge^n E \text{ generated by all elements}$$

$$x'_1 \wedge \cdots \wedge x'_i \wedge y_{i+1} \wedge \cdots \wedge y_n$$

with  $x'_1, \dots, x'_i \in E'$  viewed as submodule of  $E$ .

Then we have a filtration

$$\bigwedge_i^n E \supset \bigwedge_{i+1}^n E.$$

**Proposition 1.3.** *There is a natural isomorphism*

$$\bigwedge^i E' \otimes \bigwedge^{n-i} E'' \rightarrow \bigwedge_i^n E / \bigwedge_{i+1}^n E.$$

*Proof.* Let  $x''_1, \dots, x''_{n-i}$  be elements of  $E''$ , and lift them to elements  $y_1, \dots, y_{n-i}$  of  $E$ . We consider the map

$$(x'_1, \dots, x'_i, x''_1, \dots, x''_{n-i}) \mapsto x'_1 \wedge \cdots \wedge x'_i \wedge y_1 \wedge \cdots \wedge y_{n-i}$$

with the right-hand side taken mod  $\bigwedge_{i+1}^n E$ . Then it is immediate that this map factors through

$$\bigwedge^i E' \otimes \bigwedge^{n-i} E'' \rightarrow \bigwedge_i^n E / \bigwedge_{i+1}^n E,$$

and picking bases shows that one gets an isomorphism as desired.

In a similar vein, we have:

**Proposition 1.4.** *Let  $E = E' \oplus E''$  be a direct sum of finite free modules. Then for every positive integer  $n$ , we have a module isomorphism*

$$\bigwedge^n E \approx \bigoplus_{p+q=n} \bigwedge^p E' \otimes \bigwedge^q E''.$$

In terms of the alternating algebras, we have an isomorphism

$$\bigwedge E \approx \bigwedge E' \otimes_{su} \bigwedge E''.$$

where  $\otimes_{su}$  is the superproduct of graded algebras.

*Proof.* Each natural injection of  $E'$  and  $E''$  into  $E$  induces a natural map on the alternating algebras, and so gives the homomorphism

$$\bigwedge E' \otimes \bigwedge E'' \rightarrow \bigwedge E,$$

which is graded, i.e. for  $p = 0, \dots, n$  we have

$$\bigwedge^p E' \otimes \bigwedge^{n-p} E'' \rightarrow \bigwedge^n E.$$

To verify that this yields the desired isomorphism, one can argue by picking bases, which we leave to the reader. The anti-commutation rule of the alternating product immediately shows that the isomorphism is an algebra isomorphism for the super product  $\bigwedge E' \otimes_{su} \bigwedge E''$ .

We end this section with comments on duality. In Exercise 3, you will prove:

**Proposition 1.5.** *Let  $E$  be free of rank  $n$  over  $R$ . For each positive integer  $r$ , we have a natural isomorphism*

$$\bigwedge^r (E^\vee) \approx \bigwedge^r (E)^\vee.$$

The isomorphism is explicitly described in that exercise. A more precise property than “natural” would be that the isomorphism is functorial with respect to the category whose objects are finite free modules over  $R$ , and whose morphisms are isomorphisms.

**Examples.** Let  $L$  be a free module over  $R$  of rank 1. We have the dual module  $L^\vee = \text{Hom}_R(L, R)$ , which is also free of the same rank. For a positive integer  $m$ , we define

$$L^{\otimes -m} = (L^\vee)^{\otimes m} = L^\vee \otimes \cdots \otimes L^\vee \text{ (tensor product taken } m \text{ times).}$$

Thus we have defined the tensor product of a line with itself for negative integers. We define  $L^{\otimes 0} = R$ . You can easily verify that the rule

$$L^{\otimes p} \otimes L^{\otimes q} \approx L^{\otimes(p+q)}$$

holds for all integers  $p, q \in \mathbf{Z}$ , with a natural isomorphism. In particular, if  $q = -p$  then we get  $R$  itself on the right-hand side.

Now let  $\mathbf{E}$  be an exact sequence of free modules:

$$\mathbf{E} : 0 \rightarrow E_0 \rightarrow E_1 \rightarrow \cdots \rightarrow E_m \rightarrow 0.$$

We define the **determinant** of this exact sequence to be

$$\det(\mathbf{E}) = \bigotimes \det(E_i)^{\otimes(-1)^i}.$$

As an exercise, prove that  $\det(\mathbf{E})$  has a natural isomorphism with  $R$ , functorial with respect to isomorphisms of exact sequences.

**Examples.** Determinants of vector spaces or free modules occur in several branches of mathematics, e.g. complexes of partial differential operators, homology theories, the theory of determinant line bundles in algebraic geometry, etc. For instance, given a non-singular projective variety  $V$  over  $\mathbf{C}$ , one defines the **determinant of cohomology** of  $V$  to be

$$\det H(V) = \bigotimes \det H^i(V)^{\otimes(-1)^i},$$

where  $H^i(V)$  are the cohomology groups. Then  $\det H(V)$  is a one-dimensional vector space over  $\mathbf{C}$ , but there is no natural identification of this vector space with  $\mathbf{C}$ , because *a priori* there is no natural choice of a basis. For a notable application of the determinant of cohomology, following work of Faltings, see Deligne, *Le determinant de la cohomologie*, in Ribet, K. (ed.), *Current Trends in Arithmetical Algebraic Geometry*, Proc. Arcata 1985. (*Contemporary Math.* vol **67**, AMS (1985), pp. 93–178.)

## §2. FITTING IDEALS

Certain ideals generated by determinants are coming more and more into use, in several branches of algebra and algebraic geometry. Therefore I include this section which summarizes some of their properties. For a more extensive account, see Northcott's book *Finite Free Resolutions* which I have used, as well as the appendix of the paper by Mazur-Wiles: "Class Fields of abelian extensions of  $\mathbf{Q}$ ," which they wrote in a self-contained way. (*Invent. Math.* **76** (1984), pp. 179–330.)

Let  $R$  be a commutative ring. Let  $A$  be a  $p \times q$  matrix and  $B$  a  $q \times s$  matrix with coefficients in  $R$ . Let  $r \geq 0$  be an integer. We define the **determinant ideal**  $I_r(A)$  to be the ideal generated by all determinants of  $r \times r$  submatrices of  $A$ . This ideal may also be described as follows. Let  $S_r^p$  be the set of sequences

$$J = (j_1, \dots, j_r) \text{ with } 1 \leq j_1 < j_2 < \dots < j_r \leq p.$$

Let  $A = (a_{ij})$ . Let  $1 \leq r \leq \min(p, q)$ . Let  $K = (k_1, \dots, k_r)$  be another element of  $S_r^p$ . We define

$$A_{JK}^{(r)} = \begin{vmatrix} a_{j_1 k_1} & a_{j_1 k_2} & \cdots & a_{j_1 k_r} \\ a_{j_2 k_1} & a_{j_2 k_2} & \cdots & a_{j_2 k_r} \\ \vdots & \vdots & & \vdots \\ a_{j_r k_1} & a_{j_r k_2} & \cdots & a_{j_r k_r} \end{vmatrix}$$

where the vertical bars denote the determinant. With  $J, K$  ranging over  $S_r^p$  we may view  $A_{JK}^{(r)}$  as the  $JK$ -component of a matrix  $A^{(r)}$  which we call the  $r$ -th **exterior power** of  $A$ .

One may also describe the matrix as follows. Let  $\{e_1, \dots, e_p\}$  be a basis of  $R^p$  and  $\{u_1, \dots, u_q\}$  a basis of  $R^q$ . Then the elements

$$e_{j_1} \wedge \cdots \wedge e_{j_r} \quad (j_1 < j_2 < \cdots < j_r)$$

form a basis for  $\bigwedge^r R^p$  and similarly for a basis of  $\bigwedge^r R^q$ . We may view  $A$  as a linear map of  $R^p$  into  $R^q$ , and the matrix  $A^{(r)}$  is then the matrix representing the exterior power  $\bigwedge^r A$  viewed as a linear map of  $\bigwedge^r R^p$  into  $\bigwedge^r R^q$ . On the whole, this interpretation will not be especially useful for certain computations, but it does give a slightly more conceptual context for the exterior power. Just at the beginning, this interpretation allows for an immediate proof of Proposition 2.1.

For  $r = 0$  we define  $A^{(0)}$  to be the  $1 \times 1$  matrix whose single entry is the unit element of  $R$ . We also note that  $A^{(1)} = A$ .

**Proposition 2.1.** *Let  $A$  be a  $p \times q$  matrix and  $B$  a  $q \times s$  matrix. Then*

$$(AB)^{(r)} = A^{(r)}B^{(r)} \quad \text{for } r \geq 0.$$

If one uses the alternating products as mentioned above, the proof simply says that the matrix of the composite of linear maps with respect to fixed bases is the product of the matrices. If one does not use the alternating products, then one can prove the proposition by a direct computation which will be left to the reader.

We have formed a matrix whose entries are indexed by a finite set  $S_r^p$ . For any finite set  $S$  and doubly indexed family  $(c_{JK})$  with  $J, K \in S$  we may also define the **determinant** as

$$\det(c_{JK}) = \sum_{\sigma} \epsilon(\sigma) \left( \prod_{J \in S} c_{J, \sigma(J)} \right)$$

where  $\sigma$  ranges over all permutations of the set.

For  $r \geq 0$  we define the **determinant ideal**  $I_r(A)$  to be the ideal generated by all the components of  $A^{(r)}$ , or equivalently by all  $r \times r$  subdeterminants of  $A$ . We have by definition

$$A^{(0)} = R \quad \text{and} \quad A^{(1)} = \text{ideal generated by the components of } A.$$

Furthermore

$$I_r(A) = 0 \quad \text{for } r > \min(p, q)$$

and the inclusions

$$R = I_0(A) \supset I_1(A) \supset I_2(A) \supset \cdots$$

By Proposition 10.1, we also have

$$(1) \quad I_r(AB) \subset I_r(A) \cap I_r(B).$$

Therefore, if  $A = UBU'$  where  $U, U'$  are square matrices of determinant 1, then

$$(2) \quad I_r(A) = I_r(B).$$

Next, let  $E$  be an  $R$ -module. Let  $x_1, \dots, x_q$  be generators of  $E$ . Then we may form the matrix of relations  $(a_1, \dots, a_q) \in R^q$  such that

$$\sum_{i=1}^q a_i x_i = 0.$$

Suppose first we take only finitely many relations, thus giving rise to a  $p \times q$  matrix  $A$ . We form the determinant ideal  $I_r(A)$ . We let the **determinant ideals** of the family of generators be:

$$I_r(x_1, \dots, x_q) = I_r(x) = \text{ideal generated by } I_r(A) \text{ for all } A.$$

Thus we may in fact take the infinite matrix of relations, and say that  $I_r(x)$  is generated by the determinants of all  $r \times r$  submatrices. The inclusion relations of (1) show that

$$\begin{aligned} R &= I_0(x) \supset I_1(x) \supset I_2(x) \supset \dots \\ I_r(x) &= 0 \quad \text{if } r > q. \end{aligned}$$

Furthermore, it is easy to see that if we form a submatrix  $M$  of the matrix of all relations by taking only a family of relations which generate the ideal of all relations in  $R^q$ , then we have

$$I_r(M) = I_r(x).$$

We leave the verification to the reader. We can take  $M$  to be a finite matrix when  $E$  is finitely presented, which happens if  $R$  is Noetherian.

In terms of this representation of a module as a quotient of  $R^q$ , we get the following characterization.

**Proposition 2.2.** *Let  $R^q \rightarrow E \rightarrow 0$  be a representation of  $E$  as a quotient of  $R^q$ , and let  $x_1, \dots, x_q$  be the images of the unit vectors in  $R^q$ . Then  $I_r(x)$  is the ideal generated by all values*

$$\lambda(w_1, \dots, w_r)$$

where  $w_1, \dots, w_r \in \text{Ker}(R^q \rightarrow E)$  and  $\lambda \in L_a^r(R^q, R)$ .

*Proof.* This is immediate from the definition of the determinant ideal.

The above proposition can be useful to replace a matrix computation by a more conceptual argument with fewer indices. The reader can profitably translate some of the following matrix arguments in these more invariant terms.

We now change the numbering, and let the **Fitting ideals** be:

$$F_k(x) = I_{q-k}(x) \quad \text{for } 0 \leq k \leq q$$

$$F_k(x) = R \quad \text{when } k > q.$$

**Lemma 2.3.** *The Fitting ideal  $F_k(x)$  does not depend on the choice of generators  $(x)$ .*

*Proof.* Let  $y_1, \dots, y_s$  be elements of  $E$ . We shall prove that

$$I_r(x) = I_{r+s}(x, y).$$

The relations of  $(x, y)$  constitute a matrix of the form

$$W = \begin{pmatrix} a_{11} & \cdots & a_{1q} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{p1} & \cdots & a_{pq} & 0 & \cdots & 0 \\ b_{11} & \cdots & b_{1q} & 1 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & & \vdots \\ b_{s1} & \cdots & b_{sq} & 0 & \cdots & 1 \end{pmatrix}$$

By elementary column operations, we can change this to a matrix

$$\begin{pmatrix} A & 0 \\ 0 & 1_s \end{pmatrix}$$

and such operations do not change the determinant ideals by (2). Then we conclude that for all  $r \geq 0$  we have

$$I_r(A) = I_{r+s}(W) \subset I_{r+s}(x, y).$$

This proves that  $I_r(x) \subset I_{r+s}(x, y)$ .

Conversely, let  $C$  be a matrix of relations between the generators  $(x, y)$ . We also have a matrix of relations

$$Z = \begin{pmatrix} & & & C & & \\ b_{11} & \cdots & b_{1q} & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ b_{s1} & \cdots & b_{sq} & 0 & \cdots & 1 \end{pmatrix}$$

By elementary row operations, we can bring this matrix into the same shape

as  $B$  above, with some matrix of relations  $A'$  for  $(x)$ , namely

$$Z' = \begin{pmatrix} A' & 0 \\ B & 1_s \end{pmatrix}$$

Then

$$I_r(A') = I_{r+s}(Z') = I_{r+s}(Z) \supset I_{r+s}(C),$$

whence  $I_{r+s}(C) \subset I_r(x)$ . Taking all possible matrices of relations  $C$  shows that  $I_{r+s}(x, y) \subset I_r(x)$ , which combined with the previous inequality yields  $I_{r+s}(x, y) = I_r(x)$ .

Now given two families of generators  $(x)$  and  $(y)$ , we simply put them side by side  $(x, y)$  and use the new numbering for the  $F_k$  to conclude the proof of the lemma.

Now let  $E$  be a finitely generated  $R$ -module with presentation

$$0 \rightarrow K \rightarrow R^q \rightarrow E \rightarrow 0,$$

where the sequence is exact and  $K$  is defined as the kernel. Then  $K$  is generated by  $q$ -vectors, and can be viewed as an infinite matrix. The images of the unit vectors in  $R^q$  are generators  $(x_1, \dots, x_q)$ . We define the **Fitting ideal** of the module to be

$$F_k(E) = F_k(x).$$

Lemma 2.3 shows that the ideal is independent of the choice of presentation. The inclusion relations of a determinant ideal  $I_r(A)$  of a matrix now translate into reverse inclusion relations for the Fitting ideals, namely:

**Proposition 2.4.**

(i) *We have*

$$F_0(E) \subset F_1(E) \subset F_2(E) \subset \dots$$

(ii) *If  $E$  can be generated by  $q$  elements, then*

$$F_q(E) = R.$$

(iii) *If  $E$  is finitely presented then  $F_k(E)$  is finitely generated for all  $k$ .*

This last statement merely repeats the property that the determinant ideals of a matrix can be generated by the determinants associated with a finite submatrix if the row space of the matrix is finitely generated.

**Example.** Let  $E = R^q$  be the free module of dimension  $q$ . Then:

$$F_k(E) = \begin{cases} 0 & \text{if } 0 \leq k < q \\ R & \text{if } k \geq q. \end{cases}$$

This is immediate from the definitions and the fact that the only relation of a basis for  $E$  is the trivial one.

The Fitting ideal  $F_0(E)$  is called the **zero-th** or **initial Fitting ideal**. In some applications it is the only one which comes up, in which case it is called “**the** **Fitting ideal**  $F(E)$  of  $E$ . It is the ideal generated by all  $q \times q$  determinants in the matrix of relations of  $q$  generators of the module.

For any module  $E$  we let  $\text{ann}_R(E)$  be the annihilator of  $E$  in  $R$ , that is the set of elements  $a \in R$  such that  $aE = 0$ .

**Proposition 2.5.** *Suppose that  $E$  can be generated by  $q$  elements. Then*

$$(\text{ann}_R(E))^q \subset F(E) \subset \text{ann}_R(E).$$

*In particular, if  $E$  can be generated by one element, then*

$$F(E) = \text{ann}_R(E).$$

*Proof.* Let  $x_1, \dots, x_q$  be generators of  $E$ . Let  $a_1, \dots, a_q$  be elements of  $R$  annihilating  $E$ . Then the diagonal matrix whose diagonal components are  $a_1, \dots, a_q$  is a matrix of relations, so the definition of the Fitting ideal shows that the determinant of this matrix, which is the product  $a_1 \cdots a_q$  lies in  $I_q(E) \subset F_0(E)$ . This proves the inclusion

$$\text{ann}_R(E)^q \subset F(E).$$

Conversely, let  $A$  be a  $q \times q$  matrix of relations between  $x_1, \dots, x_q$ . Then  $\det(A)x_i = 0$  for all  $i$  so  $\det(A) \in \text{ann}_R(E)$ . Since  $F(E)$  is generated by such determinants, we get the reverse inclusion which proves the proposition.

**Corollary 2.6.** *Let  $E = R/\mathfrak{a}$  for some ideal  $\mathfrak{a}$ . Then  $F(E) = \mathfrak{a}$ .*

*Proof.* The module  $R/\mathfrak{a}$  can be generated by one element so the corollary is an immediate consequence of the proposition.

**Proposition 2.7.** *Let*

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

*be an exact sequence of finite  $R$ -modules. For integers  $m, n \geq 0$  we have*

$$F_m(E')F_n(E'') \subset F_{m+n}(E).$$

In particular for  $F = F_0$ ,

$$F(E')F(E'') \subset F(E).$$

*Proof.* We may assume  $E'$  is a submodule of  $E$ . We pick generators  $x_1, \dots, x_p$  of  $E'$  and elements  $y_1, \dots, y_q$  in  $E$  such that their images  $y_1'', \dots, y_q''$  in  $E''$  generate  $E''$ . Then  $(x, y)$  is a family of generators for  $E$ . Suppose first that  $m \leq p$  and  $n \leq q$ . Let  $A$  be a matrix of relations among  $y_1'', \dots, y_q''$  with  $q$  columns. If  $(a_1, \dots, a_q)$  is such a relation, then

$$a_1 y_1 + \dots + a_q y_q \in E'$$

so there exist elements  $b_1, \dots, b_p \in R$  such that

$$\sum a_i y_i + \sum b_j x_j = 0.$$

Thus we can find a matrix  $B$  with  $p$  columns and the same number of rows as  $A$  such that  $(B, A)$  is a matrix of relations of  $(x, y)$ . Let  $C$  be a matrix of relations of  $(x_1, \dots, x_p)$ . Then

$$\begin{pmatrix} B & A \\ C & 0 \end{pmatrix}$$

is a matrix of relations of  $(x, y)$ . If  $D''$  is a  $(q - n) \times (q - n)$  subdeterminant of  $A$  and  $D'$  is a  $(p - m) \times (p - m)$  subdeterminant of  $C$  then  $D''D'$  is a

$$(p + q - m - n) \times (p + q - m - n)$$

subdeterminant of the matrix

$$\begin{pmatrix} B & A \\ C & 0 \end{pmatrix}$$

and  $D''D' \in F_{m+n}(E)$ . Since  $F_m(E')$  is generated by determinants like  $D'$  and  $F_n(E'')$  is generated by determinants like  $D''$ , this proves the proposition in the present case.

If  $m > p$  and  $n > q$  then  $F_{m+n}(E) = F_m(E') = F_n(E'') = R$  so the proposition is trivial in this case.

Say  $m \leq p$  and  $n > q$ . Then  $F_n(E'') = R = F_q(E'')$  and hence

$$F_m(E')F_n(E'') = F_q(E'')F_m(E') \subset F_{p+n}(E) \subset F_{m+n}(E)$$

where the inclusion follows from the first case. A similar argument proves the remaining case with  $m > p$  and  $n \leq q$ . This concludes the proof.

**Proposition 2.8.** *Let  $E', E''$  be finite  $R$ -modules. For any integer  $n \geq 0$  we have*

$$F_n(E' \oplus E'') = \sum_{r+s=n} F_r(E')F_s(E'').$$

*Proof.* Let  $x_1, \dots, x_p$  generate  $E^i$  and  $y_1, \dots, y_q$  generate  $E''$ . Then  $(x, y)$  generate  $E' \oplus E''$ . By Proposition 2.6 we know the inclusion

$$\sum F_r(E')F_s(E'') \subset F_n(E' \oplus E''),$$

so we have to prove the converse. If  $n \geq p + q$  then we can take  $r \geq p$  and  $s \geq q$  in which case

$$F_r(E') = F_s(E'') = F_n(E) = R$$

and we are done. So we assume  $n < p + q$ . A relation between  $(x, y)$  in the direct sum splits into a relation for  $(x)$  and a relation for  $(y)$ . The matrix of relations for  $(x, y)$  is therefore of the form

$$C = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$$

where  $A'$  is the matrix of relations for  $(x)$  and  $A''$  the matrix of relations for  $(y)$ . Thus

$$F_n(E' \oplus E'') = \sum_C I_{p+q-n}(C)$$

where the sum is taken over all matrices  $C$  as above. Let  $D$  be a

$$(p + q - n) \times (p + q - n)$$

subdeterminant. Then  $D$  has the form

$$D = \begin{vmatrix} B' & 0 \\ 0 & B'' \end{vmatrix}$$

where  $B'$  is a  $k' \times (p - r)$  matrix, and  $B''$  is a  $k'' \times (q - s)$  matrix with some positive integers  $k', k'', r, s$  satisfying

$$k' + k'' = p + q - n \quad \text{and} \quad r + s = n.$$

Then  $D = 0$  unless  $k' = p - r$  and  $k'' = q - s$ . In that case

$$D = \det(B')\det(B'') \in F_r(E')F_s(E''),$$

which proves the reverse inclusion and concludes the proof of the proposition.

**Corollary 2.9.** *Let*

$$E = \bigoplus_{i=1}^s R/\mathfrak{a}_i$$

where  $\mathfrak{a}_i$  is an ideal. Then  $F(E) = \mathfrak{a}_1 \cdots \mathfrak{a}_s$ .

*Proof.* This is really a corollary of Proposition 2.8 and Corollary 2.6.

---

### §3. UNIVERSAL DERIVATIONS AND THE DE RHAM COMPLEX

In this section, all rings  $R$ ,  $A$ , etc. are assumed commutative.

Let  $A$  be an  $R$ -algebra and  $M$  an  $A$ -module. By a **derivation**  $D: A \rightarrow M$  (over  $R$ ) we mean an  $R$ -linear map satisfying the usual rules

$$D(ab) = aDb + bDa.$$

Note that  $D(1) = 2D(1)$  so  $D(1) = 0$ , whence  $D(R) = 0$ . Such derivations form an  $A$ -module  $\text{Der}_R(A, M)$  in a natural way, where  $aD$  is defined by  $(aD)(b) = aDb$ .

By a **universal derivation** for  $A$  over  $R$ , we mean an  $A$ -module  $\Omega$ , and a derivation

$$d: A \rightarrow \Omega$$

such that, given a derivation  $D: A \rightarrow M$  there exists a unique  $A$ -homomorphism  $f: \Omega \rightarrow M$  making the following diagram commutative:

$$\begin{array}{ccc} A & \xrightarrow{d} & \Omega \\ & \searrow D & \swarrow f \\ & M & \end{array}$$

It is immediate from the definition that a universal derivation  $(d, \Omega)$  is uniquely determined up to a unique isomorphism. By definition, we have a functorial isomorphism

$$\boxed{\text{Der}_R(A, M) \approx \text{Hom}_A(\Omega, M).}$$

We shall now prove the existence of a universal derivation.

The following general remark will be useful. Let

$$f_1, f_2: A \rightarrow B$$

be two homomorphisms of  $R$ -algebras, and let  $J$  be an ideal in  $B$  such that  $J^2 = 0$ . Assume that  $f_1 \equiv f_2 \pmod{J}$ ; this means that  $f_1(x) \equiv f_2(x) \pmod{J}$  for all  $x$  in  $A$ . Then

$$D = f_2 - f_1$$

is a derivation. This fact is immediately verified as follows:

$$\begin{aligned} f_2(ab) &= f_2(a)f_2(b) = [f_1(a) + D(a)][f_1(b) + D(b)] \\ &= f_1(ab) + f_1(b)D(a) + f_1(a)D(b). \end{aligned}$$

But the  $A$ -module structure of  $J$  is given via  $f_1$  or  $f_2$  (which amount to the same thing in light of our assumptions on  $f_1, f_2$ ), so the fact is proved.

Let the tensor product be taken over  $R$ .

Let  $\mathbf{m}_A: A \otimes A \rightarrow A$  be the multiplication homomorphism, such that  $\mathbf{m}_A(a \otimes b) = ab$ . Let  $J = \text{Ker } \mathbf{m}_A$ . We define the module of **differentials**

$$\Omega_{A/R} = J/J^2,$$

as an ideal in  $(A \otimes A)/J^2$ . The  $A$ -module structure will always be given via the embedding on the first factor:

$$A \rightarrow A \otimes A \quad \text{by} \quad a \mapsto a \otimes 1.$$

Note that we have a direct sum decomposition of  $A$ -modules

$$A \otimes A = (A \otimes 1) \oplus J,$$

and therefore

$$(A \otimes A)/J^2 = (A \otimes 1) \oplus J/J^2.$$

Let

$$d: A \rightarrow J/J^2 \text{ be the } R\text{-linear map } a \mapsto 1 \otimes a - a \otimes 1 \bmod J^2.$$

Taking  $f_1: a \mapsto a \otimes 1$  and  $f_2: a \mapsto 1 \otimes a$ , we see that  $d = f_2 - f_1$ . Hence  $d$  is a derivation when viewed as a map into  $J/J^2$ .

We note that  $J$  is generated by elements of the form

$$\sum x_i dy_i.$$

Indeed, if  $\sum x_i \otimes y_i \in J$ , then by definition  $\sum x_i y_i = 0$ , and hence

$$\sum x_i \otimes y_i = \sum x_i (1 \otimes y_i - y_i \otimes 1),$$

according to the  $A$ -module structure we have put on  $A \otimes A$  (operation of  $A$  on the left factor.)

**Theorem 3.1.** *The pair  $(J/J^2, d)$  is universal for derivations of  $A$ . This means: Given a derivation  $D: A \rightarrow M$  there exists a unique  $A$ -linear map  $f: J/J^2 \rightarrow M$  making the following diagram commutative.*

$$\begin{array}{ccc} A & \xrightarrow{d} & J/J^2 \\ & \searrow^D & \swarrow^f \\ & M & \end{array}$$

*Proof.* There is a unique  $R$ -bilinear map

$$f: A \otimes A \rightarrow M \quad \text{given by} \quad x \otimes y \mapsto xDy,$$

which is  $A$ -linear by our definition of the  $A$ -module structure on  $A \otimes A$ . Then by definition, the diagram is commutative on elements of  $A$ , when we take  $f$  restricted to  $J$ , because

$$f(1 \otimes y - y \otimes 1) = Dy.$$

Since  $J/J^2$  is generated by elements of the form  $x dy$ , the uniqueness of the map in the diagram of the theorem is clear. This proves the desired universal property.

We may write the result expressed in the theorem as a formula

$$\text{Der}_R(A, M) \approx \text{Hom}_A(J/J^2, M).$$

The reader will find exercises on derivations which give an alternative way of constructing the universal derivation, especially useful when dealing with finitely generated algebras, which are factors of polynomial rings.

I insert here without proofs some further fundamental constructions, important in differential and algebraic geometry. The proofs are easy, and provide nice exercises.

Let  $R \rightarrow A$  be an  $R$ -algebra of commutative rings. For  $i \geq 0$  define

$$\Omega_{A/R}^i = \bigwedge^i \Omega_{A/R}^1,$$

where  $\Omega_{A/R}^0 = A$ .

**Theorem 3.2.** *There exists a unique sequence of  $R$ -homomorphisms*

$$d_i: \Omega_{A/R}^i \rightarrow \Omega_{A/R}^{i+1}$$

*such that for  $\omega \in \Omega^i$  and  $\eta \in \Omega^j$  we have*

$$d(\omega \wedge \eta) = d\omega \wedge \eta + (-1)^i \omega \wedge d\eta.$$

*Furthermore  $d \circ d = 0$ .*

The proof will be left as an exercise.

Recall that a **complex** of modules is a sequence of homomorphisms

$$\dots \rightarrow E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \rightarrow$$

such that  $d^i \circ d^{i-1} = 0$ . One usually omits the superscript on the maps  $d$ . With this terminology, we see that the  $\Omega_{A/R}^i$  form a complex, called the **De Rham complex**.

**Theorem 3.3.** *Let  $k$  be a field of characteristic 0, and let  $A = k[X_1, \dots, X_n]$  be the polynomial ring in  $n$  variables. Then the De Rham complex*

$$0 \rightarrow k \rightarrow A \rightarrow \Omega_{A/k}^1 \rightarrow \dots \rightarrow \Omega_{A/k}^n \rightarrow 0$$

*is exact.*

Again the proof will be left as an exercise. *Hint:* Use induction and integrate formally.

Other results concerning connections will be found in the exercises below.

## §4. THE CLIFFORD ALGEBRA

Let  $k$  be a field. By an **algebra** throughout this section, we mean a  $k$ -algebra given by a ring homomorphism  $k \rightarrow A$  such that the image of  $k$  is in the center of  $A$ .

Let  $E$  be a finite dimensional vector space over the field  $k$ , and let  $g$  be a symmetric form on  $E$ . We would like to find a universal algebra over  $k$ , in which we can embed  $E$ , and such that the square in the algebra corresponds to the value of the quadratic form in  $E$ . More precisely, by a **Clifford algebra** for  $g$ , we shall mean a  $k$ -algebra  $C(g)$ , also denoted by  $C_g(E)$ , and a linear map  $\rho: E \rightarrow C(g)$  having the following property: If  $\psi: E \rightarrow L$  is a linear map of  $E$  into a  $k$ -algebra  $L$  such that

$$\psi(x)^2 = g(x, x) \cdot 1 \quad (1 = \text{unit element of } L)$$

for all  $x \in E$ , then there exists a unique algebra-homomorphism

$$C(\psi) = \psi_*: C(g) \rightarrow L$$

such that the following diagram is commutative:

$$\begin{array}{ccc} E & \xrightarrow{\rho} & C(g) \\ \psi \searrow & & \swarrow \psi_* \\ & L & \end{array}$$

By abstract nonsense, a Clifford algebra for  $g$  is uniquely determined, up to a unique isomorphism. Furthermore, it is clear that if  $(C(g), \rho)$  exists, then  $C(g)$  is generated by the image of  $\rho$ , i.e. by  $\rho(E)$ , as an algebra over  $k$ .

We shall write  $\rho = \rho_g$  if it is necessary to specify the reference to  $g$  explicitly.

We have trivially

$$\rho(x)^2 = g(x, x) \cdot 1$$

for all  $x \in E$ , and

$$\rho(x)\rho(y) + \rho(y)\rho(x) = 2g(x, y) \cdot 1$$

as one sees by replacing  $x$  by  $x + y$  in the preceding relation.

**Theorem 4.1.** *Let  $g$  be a symmetric bilinear form on a finite dimensional vector space  $E$  over  $k$ . Then the Clifford algebra  $(C(g), \rho)$  exists. The map  $\rho$  is injective, and  $C(g)$  has dimension  $2^n$  over  $k$ , if  $n = \dim E$ .*

*Proof.* Let  $T(E)$  be the tensor algebra as in Chapter XVI, §7. In that algebra, we let  $I_g$  be the two-sided ideal generated by all elements

$$x \otimes x - g(x, x) \cdot 1 \text{ for } x \in E.$$

We define  $C_g(E) = T(E)/I_g$ . Observe that  $E$  is naturally embedded in  $T(E)$  since

$$T(E) = k \oplus E \oplus (E \otimes E) \oplus \dots.$$

Then the natural embedding of  $E$  in  $TE$  followed by the canonical homomorphisms of  $T(E)$  onto  $C_g(E)$  defines our  $k$ -linear map  $\rho : E \rightarrow C_g(E)$ . It is immediate from the universal property of the tensor product that  $C_g(E)$  as just defined satisfies the universal property of a Clifford algebra, which therefore exists. The only problem is to prove that it has the stated dimension over  $k$ .

We first prove that the dimension is  $\leq 2^n$ . We give a proof only when the characteristic of  $k$  is  $\neq 2$  and leave characteristic 2 to the reader. Let  $\{v_1, \dots, v_n\}$  be an orthogonal basis of  $E$  as given by Theorem 3.1 of Chapter XV. Let  $e_i = \psi(v_i)$ , where  $\psi : E \rightarrow L$  is given as in the beginning of the section. Let  $c_i = g(v_i, v_i)$ . Then we have the relations

$$e_i^2 = c_i, \quad e_i e_j = -e_j e_i \text{ for all } i \neq j.$$

This immediately implies that the subalgebra of  $L$  generated by  $\psi(E)$  over  $k$  is generated as a vector space over  $k$  by all elements

$$e_1^{\nu_1} \cdots e_n^{\nu_n} \text{ with } \nu_i = 0 \text{ or } 1 \text{ for } i = 1, \dots, n.$$

Hence the dimension of this subalgebra is  $\leq 2^n$ . In particular,  $\dim C_g(E) \leq 2^n$  as desired.

There remains to show that there exists at least one  $\psi : E \rightarrow L$  such that  $L$  is generated by  $\psi(E)$  as an algebra over  $k$ , and has dimension  $2^n$ ; for in that case, the homomorphism  $\psi_* : C_g(E) \rightarrow L$  being surjective, it follows that  $\dim C_g(E) \geq 2^n$  and the theorem will be proved. We construct  $L$  in the following way. We first need some general notions.

Let  $M$  be a module over a commutative ring. Let  $i, j \in \mathbf{Z}/2\mathbf{Z}$ . Suppose  $M$  is a direct sum  $M = M_0 \oplus M_1$  where 0, 1 are viewed as the elements of  $\mathbf{Z}/2\mathbf{Z}$ . We then say that  $M$  is  **$\mathbf{Z}/2\mathbf{Z}$ -graded**. If  $M$  is an algebra over the ring, we say

it is a **Z/2Z-graded algebra** if  $M_i M_j \subset M_{i+j}$  for all  $i, j \in \mathbf{Z}/2\mathbf{Z}$ . We simply say **graded**, omitting the  $\mathbf{Z}/2\mathbf{Z}$  prefix when the reference to  $\mathbf{Z}/2\mathbf{Z}$  is fixed throughout a discussion, which will be the case in the rest of this section.

Let  $A, B$  be graded modules as above, with  $A = A_0 \oplus A_1$  and  $B = B_0 \oplus B_1$ . Then the tensor product  $A \otimes B$  has a direct sum decomposition

$$A \otimes B = \bigoplus_{i,j} A_i \otimes B_j.$$

We define a grading on  $A \otimes B$  by letting  $(A \otimes B)_0$  consist of the sum over indices  $i, j$  such that  $i + j = 0$  (in  $\mathbf{Z}/2\mathbf{Z}$ ), and  $(A \otimes B)_1$  consist of the sum over the indices  $i, j$  such that  $i + j = 1$ .

Suppose that  $A, B$  are graded algebras over the given commutative ring. There is a unique bilinear map of  $A \otimes B$  into itself such that

$$(a \otimes b)(a' \otimes b') = (-1)^{ij}aa' \otimes bb'$$

if  $a' \in A_i$  and  $b \in B_j$ . Just as in Chapter XVI, §6, one verifies associativity and the fact that this product gives rise to a graded algebra, whose product is called the **super tensor product**, or **super product**. As a matter of notation, when we take the super tensor product of  $A$  and  $B$ , we shall denote the resulting algebra by

$$A \otimes_{su} B$$

to distinguish it from the ordinary algebra  $A \otimes B$  of Chapter XVI, §6.

Next suppose that  $E$  has dimension 1 over  $k$ . Then the factor polynomial ring  $k[X]/(x^2 - c_1)$  is immediately verified to be the Clifford algebra in this case. We let  $t_1$  be the image of  $X$  in the factor ring, so  $C_g(E) = k[t_1]$  with  $t_1^2 = c_1$ . The vector space  $E$  is imbedded as  $kt_1$  in the direct sum  $k \oplus kt_1$ .

In general we now take the super tensor product inductively:

$$C_g(E) = k[t_1] \otimes_{su} k[t_2] \otimes_{su} \cdots \otimes_{su} k[t_n], \text{ with } k[t_i] = k[X]/(X^2 - c_i).$$

Its dimension is  $2^n$ . Then  $E$  is embedded in  $C_g(E)$  by the map

$$a_1 v_1 + \cdots + a_n v_n \mapsto a_1 t_1 \oplus \cdots \oplus a_n t_n.$$

The desired commutation rules among  $t_i, t_j$  are immediately verified from the definition of the super product, thus concluding the proof of the dimension of the Clifford algebra.

Note that the proof gives an explicit representation of the relations of the algebra, which also makes it easy to compute in the algebra. Note further that the alternating algebra of a free module is a special case, taking  $c_i = 0$  for all  $i$ . Taking the  $c_i$  to be algebraically independent shows that the alternating algebra is a specialization of the generic Clifford algebra, or that Clifford algebras are what one calls perturbations of the alternating algebra. Just as for the alternating algebra, we have immediately from the construction:

**Theorem 4.2.** *Let  $g, g'$  by symmetric forms on  $E, E'$  respectively. Then we*

have an algebra isomorphism

$$C(g \oplus g') \approx C(g) \otimes_{su} C(g').$$

**Examples.** Clifford algebras have had increasingly wide applications in physics, differential geometry, topology, group representations (finite groups and Lie groups), and number theory. First, in topology I refer to Adams [Ad 62] and [ABS 64] giving applications of the Clifford algebra to various problems in topology, notably a description of the way Clifford algebras over the reals are related to the existence of vector fields on spheres. The multiplication in the Clifford algebra gives rise to a multiplication on the sphere, whence to vector fields. [ABS 64] also gives a number of computations related to the Clifford algebra and its applications to topology and physics. For instance, let  $E = \mathbf{R}^n$  and let  $g$  be the negative of the standard dot product. Or more invariantly, take for  $E$  an  $n$ -dimensional vector space over  $\mathbf{R}$ , and let  $g$  be a *negative definite* symmetric form on  $E$ . Let  $C_n = C(g)$ .

The operation

$$v_1 \otimes \cdots \otimes v_r \mapsto v_r \otimes \cdots \otimes v_1 = (v_1 \otimes \cdots \otimes v_r)^* \text{ for } v_i \in E$$

induces an endomorphism of  $T^r(E)$  for  $r \geq 0$ . Since  $v \otimes v - g(v, v) \cdot 1$  (for  $v \in E$ ) is invariant under this operation, there is an induced endomorphism  $* : C_n \rightarrow C_n$ , which is actually an involution, that is  $x^{**} = x$  and  $(xy)^* = y^*x^*$  for  $x \in C_n$ . We let  $\text{Spin}(n)$  be the subgroup of units in  $C_n$  generated by the unit sphere in  $E$  (i.e. the set of elements such that  $g(v, v) = -1$ ), and lying in the even part of  $C_n$ . Equivalently,  $\text{Spin}(n)$  is the group of elements  $x$  such that  $xx^* = 1$ . The name dates back to Dirac who used this group in his study of electron spin. Topologists and others view that group as being the universal covering group of the special orthogonal group  $SO(n) = SU_n(\mathbf{R})$ .

An account of some of the results of [Ad 62] and [ABS 64] will also be found in [Hu 75], Chapter 11. Second I refer to two works encompassing two decades, concerning the heat kernel, Dirac operator, index theorem, and number theory, ranging from Atiyah, Bott and Patodi [ABP 73] to Faltings [Fa 91], see especially §4, entitled “The local index theorem for Dirac operators”. The vector space to which the general theory is applied is mostly the cotangent space at a point on a manifold. I recommend the book [BGV 92], Chapter 3.

Finally, I refer to Bröcker and Tom Dieck for applications of the Clifford algebra to representation theory, starting with their Chapter I, §6, [BtD 85].

## Bibliography

- [Ad 62] F. ADAMS, Vector Fields on Spheres, *Ann. Math.* **75** (1962) pp. 603–632
- [ABP 73] M. ATIYAH, R. BOTT, V. PATODI, On the heat equation and the index theorem, *Invent. Math.* **19** (1973) pp. 270–330; erratum **38** (1975) pp. 277–280

- [ABS 64] M. ATIYAH, R. BOTT, A. SHAPIRO, Clifford Modules, *Topology* **Vol. 3**, *Supp. 1* (1964) pp. 3–38
- [BGV 92] N. BERLINE, E. GETZLER, and M. VERGNE, *Heat Kernels and Dirac Operators*, Springer Verlag, 1992
- [BtD 85] T. BRÖCKER and T. TOM DIECK, *Representations of Compact Lie Groups*, Springer Verlag 1985
- [Fa 91] G. FALTINGS, *Lectures on the arithmetic Riemann-Roch theorem*, Annals of Math. Studies 1991
- [Hu 75] D. HUSEMOLLER, *Fibre Bundles*, Springer Verlag, Second Edition, 1975

## EXERCISES

1. Let  $E$  be a finite dimensional vector space over a field  $k$ . Let  $x_1, \dots, x_p$  be elements of  $E$  such that  $x_1 \wedge \dots \wedge x_p \neq 0$ , and similarly  $y_1 \wedge \dots \wedge y_p \neq 0$ . If  $c \in k$  and

$$x_1 \wedge \dots \wedge x_p = cy_1 \wedge \dots \wedge y_p$$

show that  $x_1, \dots, x_p$  and  $y_1, \dots, y_p$  generate the same subspace. Thus non-zero decomposable vectors in  $\bigwedge^p E$  up to non-zero scalar multiples correspond to  $p$ -dimensional subspaces of  $E$ .

2. Let  $E$  be a free module of dimension  $n$  over the commutative ring  $R$ . Let  $f: E \rightarrow E$  be a linear map. Let  $\alpha_r(f) = \text{tr } \bigwedge^r(f)$ , where  $\bigwedge^r(f)$  is the endomorphism of  $\bigwedge^r(E)$  into itself induced by  $f$ . We have

$$\alpha_0(f) = 1, \quad \alpha_1(f) = \text{tr}(f), \quad \alpha_n(f) = \det f,$$

and  $\alpha_r(f) = 0$  if  $r > n$ . Show that

$$\det(1 + f) = \sum_{r \geq 0} \alpha_r(f).$$

[Hint: As usual, prove the statement when  $f$  is represented by a matrix with variable coefficients over the integers.] Interpret the  $\alpha_r(f)$  in terms of the coefficients of the characteristic polynomial of  $f$ .

3. Let  $E$  be a finite dimensional free module over the commutative ring  $R$ . Let  $E^\vee$  be its dual module. For each integer  $r \geq 1$  show that  $\bigwedge^r E$  and  $\bigwedge^r E^\vee$  are dual modules to each other, under the bilinear map such that

$$(v_1 \wedge \dots \wedge v_r, v'_1 \wedge \dots \wedge v'_r) \mapsto \det (\langle v_i, v'_j \rangle)$$

where  $\langle v_i, v'_j \rangle$  is the value of  $v'_j$  on  $v_i$ , as usual, for  $v_i \in E$  and  $v'_j \in E^\vee$ .

4. Notation being as in the preceding exercise, let  $F$  be another  $R$ -module which is free, finite dimensional. Let  $f: E \rightarrow F$  be a linear map. Relative to the bilinear map of the preceding exercise, show that the transpose of  $\bigwedge^r f$  is  $\bigwedge^r(f)$ , i.e. is equal to the  $r$ -th alternating product of the transpose of  $f$ .

5. Let  $R$  be a commutative ring. If  $E$  is an  $R$ -module, denote by  $L_a^r(E)$  the module of

*r-multilinear alternating maps of  $E$  into  $R$  itself* (i.e. the  $r$ -multilinear alternating forms on  $E$ ). Let  $L_a^0(E) = R$ , and let

$$\Omega(E) = \bigoplus_{r=0}^{\infty} L_a^r(E).$$

Show that  $\Omega(E)$  is a graded  $R$ -algebra, the multiplication being defined as follows. If  $\omega \in L_a^r(E)$  and  $\psi \in L_a^s(E)$ , and  $v_1, \dots, v_{r+s}$  are elements of  $E$ , then

$$(\omega \wedge \psi)(v_1, \dots, v_{r+s}) = \sum \epsilon(\sigma) \omega(v_{\sigma 1}, \dots, v_{\sigma r}) \psi(v_{\sigma(r+1)}, \dots, v_{\sigma s}),$$

the sum being taken over all permutations  $\sigma$  of  $(1, \dots, r+s)$  such that  $\sigma 1 < \dots < \sigma r$  and  $\sigma(r+1) < \dots < \sigma s$ .

## Derivations

*In the following exercises on derivations, all rings are assumed commutative.* Among other things, the exercises give another proof of the existence of universal derivations.

Let  $R \rightarrow A$  be a  $R$ -algebra (of commutative rings, according to our convention). We denote the module of universal derivations of  $A$  over  $R$  by  $(d_{A/R}, \Omega_{A/R}^1)$ , but we do not assume that it necessarily exists. Sometimes we write  $d$  instead of  $d_{A/R}$  for simplicity if the reference to  $A/R$  is clear.

6. Let  $A = R[X_\alpha]$  be a polynomial ring in variables  $X_\alpha$ , where  $\alpha$  ranges over some indexing set, possibly infinite. Let  $\Omega$  be the free  $A$ -module on the symbols  $dX_\alpha$ , and let

$$d : A \rightarrow \Omega$$

be the mapping defined by

$$df(X) = \sum_{\alpha} \frac{\partial f}{\partial X_{\alpha}} dX_{\alpha}.$$

Show that the pair  $(d, \Omega)$  is a universal derivation  $(d_{A/R}, \Omega_{A/R}^1)$ .

7. Let  $A \rightarrow B$  be a homomorphism of  $R$ -algebras. Assume that the universal derivations for  $A/R$ ,  $B/R$ , and  $B/A$  exist. Show that one has a natural exact sequence:

$$B \otimes_A \Omega_{A/R}^1 \rightarrow \Omega_{B/R}^1 \rightarrow \Omega_{B/A}^1 \rightarrow 0.$$

[Hint: Consider the sequence

$$0 \rightarrow \text{Der}_A(B, M) \rightarrow \text{Der}_R(B, M) \rightarrow \text{Der}_R(A, M)$$

which you prove is exact. Use the fact that a sequence of  $B$ -modules

$$N' \rightarrow N \rightarrow N'' \rightarrow 0$$

is exact if and only if its Hom into  $M$  is exact for every  $B$ -module  $M$ . Apply this to the sequence of derivations.]

8. Let  $R \rightarrow A$  be an  $R$ -algebra, and let  $I$  be an ideal of  $A$ . Let  $B = A/I$ . Suppose that the universal derivation of  $A$  over  $R$  exists. Show that the universal derivation of  $B$  over  $R$

also exists, and that there is a natural exact sequence

$$I/I^2 \xrightarrow{d_{A/R}} B \otimes_A \Omega_{A/R}^1 \rightarrow \Omega_{B/R}^1 \rightarrow 0.$$

[Hint: Let  $M$  be a  $B$ -module. Show that the sequence

$$0 \rightarrow \text{Der}_R(B, M) \rightarrow \text{Der}_R(A, M) \rightarrow \text{Hom}_B(I/I^2, M)$$

is exact.]

9. Let  $R \rightarrow B$  be an  $R$ -algebra. Show that the universal derivation of  $B$  over  $R$  exists as follows. Represent  $B$  as a quotient of a polynomial ring, possibly in infinitely many variables. Apply Exercises 6 and 7.
10. Let  $R \rightarrow A$  be an  $R$ -algebra. Let  $S_0$  be a multiplicative subset of  $R$ , and  $S$  a multiplicative subset of  $A$  such that  $S_0$  maps into  $S$ . Show that the universal derivation of  $S^{-1}A$  over  $S_0^{-1}R$  is  $(d, S^{-1}\Omega_{A/R}^1)$ , where

$$d(a/s) = (sd_{A/R}(a) - ad_{A/R}(s))/s^2.$$

11. Let  $B$  be an  $R$ -algebra and  $M$  a  $B$ -module. On  $B \oplus M$  define a product

$$(b, x)(b', y) = (bb', by + b'x).$$

Show that  $B \oplus M$  is a  $B$ -algebra, if we identify an element  $b \in B$  with  $(b, 0)$ . For any  $R$ -algebra  $A$ , show that the algebra homomorphisms  $\text{Hom}_{\text{Alg}/R}(A, B \oplus M)$  consist of pairs  $(\varphi, D)$ , where  $\varphi: A \rightarrow B$  is an algebra homomorphism, and  $D: A \rightarrow M$  is a derivation for the  $A$ -module structure on  $M$  induced by  $\varphi$ .

12. Let  $A$  be an  $R$ -algebra. Let  $\varepsilon: A \rightarrow R$  be an algebra homomorphism, which we call an **augmentation**. Let  $M$  be an  $R$ -module. Define an  $A$ -module structure on  $M$  via  $\varepsilon$ , by

$$a \cdot x = \varepsilon(a)x \quad \text{for} \quad a \in A \quad \text{and} \quad x \in M.$$

Write  $M_\varepsilon$  to denote  $M$  with this new module structure. Let:

$$\text{Der}_\varepsilon(A, M) = A\text{-module of derivations for the } \varepsilon\text{-module structure on } M$$

$$I = \text{Ker } \varepsilon.$$

Then  $\text{Der}_\varepsilon(A, M)$  is an  $A/I$ -module. Note that there is an  $R$ -module direct sum decomposition  $A = R \oplus I$ . Show that there is a natural  $A$ -module isomorphism

$$\Omega_{A/R}/I\Omega_{A/R} \approx I/I^2$$

and an  $R$ -module isomorphism

$$\text{Der}_\varepsilon(A, M) \approx \text{Hom}_R(I/I^2, M).$$

In particular, let  $\eta: A \rightarrow I/I^2$  be the projection of  $A$  on  $I/I^2$  relative to the direct sum decomposition  $A = R \oplus I$ . Then  $\eta$  is the universal  $\varepsilon$ -derivation.

### Derivations and connections

13. Let  $R \rightarrow A$  be a homomorphism of commutative rings, so we view  $A$  as an  $R$ -algebra.

Let  $E$  be an  $A$ -module. A **connection** on  $E$  is a homomorphism of abelian groups

$$\nabla : E \rightarrow \Omega_{A/R}^1 \otimes_A E$$

such that for  $a \in A$  and  $x \in E$  we have

$$\nabla(ax) = a\nabla(x) + da \otimes x,$$

where the tensor product is taken over  $A$  unless otherwise specified. The kernel of  $\nabla$ , denoted by  $E_\nabla$ , is called the **submodule of horizontal elements**, or the **horizontal submodule** of  $(E, \nabla)$ .

(a) For any integer  $i \geq 1$ , define

$$\Omega_{A/R}^i = \bigwedge^i \Omega_{A/R}^1.$$

Show that  $\nabla$  can be extended to a homomorphism of  $R$ -modules

$$\nabla_i : \Omega_{A/R}^i \otimes E \rightarrow \Omega_{A/R}^{i+1} \otimes E$$

by

$$\nabla_i(\omega \otimes x) = d\omega \otimes x + (-1)^i \omega \wedge \nabla(x).$$

(b) Define the **curvature** of the connection to be the map

$$K = \nabla_1 \circ \nabla : E \rightarrow \Omega_{A/R}^2 \otimes_A E.$$

Show that  $K$  is an  $A$ -homomorphism. Show that

$$\nabla_{i+1} \circ \nabla_i(\omega \otimes x) = \omega \wedge K(x)$$

for  $\omega \in \Omega_{A/R}^i$  and  $x \in E$ .

(c) Let  $\text{Der}(A/R)$  denote the  $A$ -module of derivations of  $A$  into itself, over  $R$ . Let  $\nabla$  be a connection on  $E$ . Show that  $\nabla$  induces a unique  $A$ -linear map

$$\nabla : \text{Der}(A/R) \rightarrow \text{End}_R(E)$$

such that

$$\nabla(D)(ax) = D(a)x + a\nabla(D)(x).$$

(d) Prove the formula

$$[\nabla(D_1), \nabla(D_2)] - \nabla([D_1, D_2]) = (D_1 \wedge D_2)(K).$$

In this formula, the bracket is defined by  $[f, g] = f \circ g - g \circ f$  for two endomorphisms  $f, g$  of  $E$ . Furthermore, the right-hand side is the composed mapping

$$E \xrightarrow{K} \Omega_{A/R}^2 \otimes E \xrightarrow{D_1 \wedge D_2} A \otimes E \approx E.$$

14. (a) For any derivation  $D$  of a ring  $A$  into itself, prove **Leibniz's rule**:

$$D^n(xy) = \sum_{i=0}^n \binom{n}{i} D^i(x) D^{n-i}(y).$$

(b) Suppose  $A$  has characteristic  $p$ . Show that  $D^p$  is a derivation.

15. Let  $A/R$  be an algebra, and let  $E$  be an  $A$ -module with a connection  $\nabla$ . Assume that  $R$  has characteristic  $p$ . Define

$$\psi : \text{Der}(A/R) \rightarrow \text{End}_R(E)$$

by

$$\psi(D) = (\nabla(D))^p - \nabla(D^p).$$

Prove that  $\psi(D)$  is  $A$ -linear. [Hint: Use Leibniz's formula and the definition of a connection.] Thus the image of  $\psi$  is actually in  $\text{End}_A(E)$ .

### Some Clifford exercises

16. Let  $C_g(E)$  be the Clifford algebra as defined in §4. Define  $F_i(C_g) = (k + E)^i$ , viewing  $E$  as embedded in  $C_g$ . Define the similar object  $F_i(\bigwedge E)$  in the alternating algebra. Then  $F_{i+1} \supset F_i$  in both cases, and we define the  $i$ -th graded module  $\text{gr}_i = F_i/F_{i-1}$ . Show that there is a natural (functorial) isomorphism

$$\text{gr}_i(C_g(E)) \xrightarrow{\sim} \text{gr}_i(\bigwedge E).$$

17. Suppose that  $k = \mathbf{R}$ , so  $E$  is a real vector space, which we now assume of even dimension  $2m$ . We also assume that  $g$  is non-degenerate. We omit the index  $g$  since the symmetric form is now fixed, and we write  $C^+$ ,  $C^-$  for the spaces of degree 0 and 1 respectively in the  $\mathbf{Z}/2\mathbf{Z}$ -grading. For elements  $x, y$  in  $C^+$  or  $C^-$ , define their **supercommutator** to be

$$\{x, y\} = xy - (-1)^{(\deg x)(\deg y)} yx.$$

Show that  $F_{2m-1}$  is generated by supercommutators.

18. Still assuming  $g$  non-degenerate, let  $J$  be an automorphism of  $(E, g)$  (i.e.  $g(Jx, Jy) = g(x, y)$  for all  $x, y \in E$ ) such that  $J^2 = -\text{id}$ . Let  $E_{\mathbf{C}} = \mathbf{C} \otimes_{\mathbf{R}} E$  be the extension of scalars from  $\mathbf{R}$  to  $\mathbf{C}$ . Then  $E_{\mathbf{C}}$  has a direct sum decomposition

$$E_{\mathbf{C}} = E_{\mathbf{C}}^+ \oplus E_{\mathbf{C}}^-$$

into the eigenspaces of  $J$ , with eigenvalues 1 and  $-1$  respectively. (Proof?) There is a representation of  $E_{\mathbf{C}}$  on  $\bigwedge E_{\mathbf{C}}^+$ , i.e. a homomorphism  $E_{\mathbf{C}} \rightarrow \text{End}_{\mathbf{C}}(E_{\mathbf{C}}^+)$  whereby an element of  $E_{\mathbf{C}}^+$  operates by exterior multiplication, and an element of  $E_{\mathbf{C}}^-$  operates by inner multiplication, defined as follows.

For  $x' \in E_{\mathbf{C}}^-$  there is a unique  $\mathbf{C}$ -linear map having the effect

$$x'(x_1 \wedge \cdots \wedge x_r) = -2 \sum_{i=1}^r (-1)^{i-1} \langle x', x_i \rangle x_1 \wedge \cdots \wedge \hat{x}_i \wedge \cdots \wedge x_r.$$

Prove that under this operation, you get an isomorphism

$$C_g(E)_{\mathbf{C}} \rightarrow \text{End}_{\mathbf{C}}(\bigwedge E_{\mathbf{C}}^+).$$

[Hint: Count dimensions.]

19. Consider the Clifford algebra over  $\mathbf{R}$ . The standard notation is  $C_n$  if  $E = \mathbf{R}^n$  with the negative definite form, and  $C'_n$  if  $E = \mathbf{R}^n$  with the positive definite form. Thus  $\dim C_n = \dim C'_n = 2^n$ .

(a) Show that

$$\begin{aligned} C_1 &\approx \mathbf{C} & C_2 &\approx \mathbf{H} \text{ (the division ring of quaternions)} \\ C'_1 &\approx \mathbf{R} \times \mathbf{R} & C'_2 &\approx M_2(\mathbf{R}) \text{ (2} \times 2 \text{ matrices over } \mathbf{R}) \end{aligned}$$

20. Establish isomorphisms:

$$\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \approx \mathbf{C} \times \mathbf{C}; \quad \mathbf{C} \otimes_{\mathbf{R}} \mathbf{H} \approx M_2(\mathbf{C}); \quad \mathbf{H} \otimes_{\mathbf{R}} \mathbf{H} \approx M_4(\mathbf{R})$$

where  $M_d(F) = d \times d$  matrices over  $F$ . For the third one, with  $\mathbf{H} \otimes \mathbf{H}$ , define an isomorphism

$$f: \mathbf{H} \otimes_{\mathbf{R}} \mathbf{H} \rightarrow \text{Hom}_{\mathbf{R}}(\mathbf{H}, \mathbf{H}) \approx M_4(\mathbf{R})$$

by  $f(x \otimes y)(z) = xz\bar{y}$ , where if  $y = y_0 + y_1i + y_2j + y_3k$  then

$$\bar{y} = y_0 - y_1i - y_2j - y_3k.$$

21. (a) Establish isomorphisms

$$C_{n+2} \approx C'_n \otimes C_2 \quad \text{and} \quad C'_{n+2} \approx C_n \otimes C'_2.$$

[Hint: Let  $\{e_1, \dots, e_{n+2}\}$  be the orthonormalized basis with  $e_i^2 = -1$ . Then for the first isomorphism map  $e_i \mapsto e'_i \otimes e_1e_2$  for  $i = 1, \dots, n$  and map  $e_{n+1}, e_{n+2}$  on  $1 \otimes e_1$  and  $1 \otimes e_2$  respectively.]

(b) Prove that  $C_{n+8} \approx C_n \otimes M_{16}(\mathbf{R})$  (which is called the **periodicity property**).

(c) Conclude that  $C_n$  is a semi-simple algebra over  $\mathbf{R}$  for all  $n$ .

From (c) one can tabulate the simple modules over  $C_n$ . See [ABS 64], reproduced in Husemoller [Hu 75], Chapter 11, §6.

---

# Part Four

---

# HOMOLOGICAL ALGEBRA

---

In the forties and fifties (mostly in the works of Cartan, Eilenberg, MacLane, and Steenrod, see [CaE 57]), it was realized that there was a systematic way of developing certain relations of linear algebra, depending only on fairly general constructions which were mostly arrow-theoretic, and were affectionately called **abstract nonsense** by Steenrod. (For a more recent text, see [Ro 79].) The results formed a body of algebra, some of it involving homological algebra, which had arisen in topology, algebra, partial differential equations, and algebraic geometry. In topology, some of these constructions had been used in part to get homology and cohomology groups of topological spaces as in Eilenberg-Steenrod [ES 52]. In algebra, factor sets and 1-cocycles had arisen in the theory of group extensions, and, for instance, Hilbert's Theorem 90. More recently, homological algebra has entered in the cohomology of groups and the representation theory of groups. See for example Curtis-Reiner [CuR 81], and any book on the cohomology of groups, e.g. [La 96], [Se 64], and [Sh 72]. Note that [La 96] was written to provide background for class field theory in [ArT 68].

From an entirely different direction, Leray developed a theory of sheaves and spectral sequences motivated by partial differential equations. The basic theory of sheaves was treated in Godement's book on the subject [Go 58]. Fundamental insights were also given by Grothendieck in homological algebra [Gro 57], to be applied by Grothendieck in the theory of sheaves over schemes in the fifties and sixties. In Chapter XX, I have included whatever is necessary of homological algebra for Hartshorne's use in [Ha 77]. Both Chapters XX and XXI give an appropriate background for the homological algebra used in Griffiths-Harris [GrH 78], Chapter 5 (especially §3 and §4), and Gunning [Gu 90]. Chapter XX carries out the general theory of derived functors. The exercises and Chapter XXI may be viewed as providing examples and computations in specific concrete instances of more specialized interest.

The commutative algebra of Chapter X and the two chapters on homological algebra in this fourth part also provide an appropriate background for certain topics in algebraic geometry such as Serre's study of intersection theory [Se 65], Grothendieck duality, and Grothendieck's Riemann-Roch theorem in algebraic geometry. See for instance [SGA 6].

Finally I want to draw attention to the use of homological algebra in certain areas of partial differential equations, as in the papers of Atiyah-Bott-Patodi and Atiyah-Singer on complexes of elliptic operators. Readers can trace some of the literature from the bibliography given in [ABP 73].

The choice of material in this part was to a large extent motivated by all the above applications.

For this chapter, considering the number of references and cross-references given, the bibliography for the entire chapter is placed at the end of the chapter.

---

# CHAPTER XX

---

# General Homology Theory

To a large extent the present chapter is arrow-theoretic. There is a substantial body of linear algebra which can be formalized very systematically, and constitutes what Steenrod called abstract nonsense, but which provides a well-oiled machinery applicable to many domains. References will be given along the way.

Most of what we shall do applies to abelian categories, which were mentioned in Chapter III, end of §3. However, in first reading, I recommend that readers disregard any allusions to general abelian categories and assume that we are dealing with an abelian category of modules over a ring, or other specific abelian categories such as complexes of modules over a ring.

---

## §1. COMPLEXES

Let  $A$  be a ring. By an **open complex** of  $A$ -modules, one means a sequence of modules and homomorphisms  $\{(E^i, d^i)\}$ ,

$$\rightarrow E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \rightarrow$$

where  $i$  ranges over all integers and  $d_i$  maps  $E^i$  into  $E^{i+1}$ , and such that

$$d^i \circ d^{i-1} = 0$$

for all  $i$ .

One frequently considers a finite sequence of homomorphisms, say

$$E^1 \rightarrow \cdots \rightarrow E'$$

such that the composite of two successive ones is 0, and one can make this sequence into a complex by inserting 0 at each end:

$$\rightarrow 0 \rightarrow 0 \rightarrow E^1 \rightarrow \cdots \rightarrow E^r \rightarrow 0 \rightarrow 0 \rightarrow$$

Such a complex is called a **finite** or **bounded** complex.

**Remark.** Complexes can be indexed with a descending sequence of integers, namely,

$$\rightarrow E_{i+1} \xrightarrow{d_{i+1}} E_i \xrightarrow{d_i} E_{i-1} \rightarrow$$

When that notation is used systematically, then one uses upper indices for complexes which are indexed with an ascending sequence of integers:

$$\rightarrow E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \rightarrow$$

In this book, I shall deal mostly with ascending indices.

As stated in the introduction of this chapter, instead of modules over a ring, we could have taken objects in an arbitrary abelian category.

The homomorphisms  $d^i$  are often called **differentials**, because some of the first complexes which arose in practice were in analysis, with differential operators and differential forms. *Cf.* the examples below.

We denote a complex as above by  $(E, d)$ . If the complex is exact, it is often useful to insert the kernels and cokernels of the differentials in a diagram as follows, letting  $M_i = \text{Ker } d^i = \text{Im } d^{i-1}$ .

$$\begin{array}{ccccccc} & \longrightarrow & E^{i-2} & \longrightarrow & E^{i-1} & \longrightarrow & E^i & \longrightarrow & E^{i+1} & \longrightarrow \\ & & \searrow & \nearrow & \searrow & \nearrow & \searrow & \nearrow & \searrow & \nearrow \\ & & M^{i-1} & & M^i & & M^{i+1} & & \\ & & \nearrow & \searrow & \nearrow & \searrow & \nearrow & \searrow & \nearrow & \searrow \\ 0 & & 0 & & 0 & & 0 & & 0 & \end{array}$$

Thus by definition, we obtain a family of short exact sequences

$$0 \rightarrow M^i \rightarrow E^i \rightarrow M^{i+1} \rightarrow 0.$$

If the complex is not exact, then of course we have to insert both the image of  $d^{i-1}$  and the kernel of  $d^i$ . The factor

$$(\text{Ker } d^i)/(\text{Im } d^{i-1})$$

will be studied in the next section. It is called the **homology of the complex**, and measures the deviation from exactness.

Let  $M$  be a module. By a **resolution** of  $M$  we mean an exact sequence

$$\rightarrow E_n \rightarrow E_{n-1} \rightarrow \cdots \rightarrow E_0 \rightarrow M \rightarrow 0.$$

Thus a resolution is an exact complex whose furthest term on the right before 0 is  $M$ . The resolution is indexed as shown. We usually write  $E_M$  for the part of complex formed only of the  $E_i$ 's, thus:

$$E_M \text{ is: } \rightarrow E_n \rightarrow E_{n-1} \rightarrow \cdots \rightarrow E_0,$$

stopping at  $E_0$ . We then write  $E$  for the complex obtained by sticking 0 on the right:

$$E \text{ is: } \rightarrow E_n \rightarrow E_{n-1} \rightarrow \cdots \rightarrow E_0 \rightarrow 0.$$

If the objects  $E_i$  of the resolution are taken in some family, then the resolution is qualified in the same way as the family. For instance, if  $E_i$  is free for all  $i \geq 0$  then we say that the **resolution** is a **free resolution**. If  $E_i$  is projective for all  $i \geq 0$  then we say that the **resolution** is **projective**. And so forth. The same terminology is applied to the right, with a resolution

$$0 \rightarrow M \rightarrow E^0 \rightarrow E^1 \rightarrow \cdots \rightarrow E^{n-1} \rightarrow E^n \rightarrow,$$

also written

$$0 \rightarrow M \rightarrow E_M.$$

We then write  $E$  for the complex

$$0 \rightarrow E^0 \rightarrow E^1 \rightarrow E^2 \rightarrow \cdots.$$

See §5 for injective resolutions.

A resolution is said to be **finite** if  $E_i$  (or  $E^i$ ) = 0 for all but a finite number of indices  $i$ .

**Example.** Every module admits a free resolution (on the left). This is a simple application of the notion of free module. Indeed, let  $M$  be a module, and let  $\{x_j\}$  be a family of generators, with  $j$  in some indexing set  $J$ . For each  $j$  let  $Re_j$  be a free module over  $R$  with a basis consisting of one element  $e_j$ . Let

$$F = \bigoplus_{j \in J} Re_j$$

be their direct sum. There is a unique epimorphism

$$F \rightarrow M \rightarrow 0$$

sending  $e_j$  on  $x_j$ . Now we let  $M_1$  be the kernel, and again represent  $M_1$  as the quotient of a free module. Inductively, we can construct the desired free resolution.

**Example. The Standard Complex.** Let  $S$  be a set. For  $i = 0, 1, 2, \dots$  let  $E_i$  be the free module over  $\mathbf{Z}$  generated by  $(i + 1)$ -tuples  $(x_0, \dots, x_i)$  with  $x_0, \dots, x_i \in S$ . Thus such  $(i + 1)$ -tuples form a basis of  $E_i$  over  $\mathbf{Z}$ . There is a unique homomorphism

$$d_{i+1}: E_{i+1} \rightarrow E_i$$

such that

$$d_{i+1}(x_0, \dots, x_{i+1}) = \sum_{j=0}^{i+1} (-1)^j (x_0, \dots, \hat{x}_j, \dots, x_{i+1}),$$

where the symbol  $\hat{x}_j$  means that this term is to be omitted. For  $i = 0$ , we define  $d_0: E_0 \rightarrow \mathbf{Z}$  to be the unique homomorphism such that  $d_0(x_0) = 1$ . The map  $d_0$  is sometimes called the augmentation, and is also denoted by  $\varepsilon$ . Then we obtain a resolution of  $\mathbf{Z}$  by the complex

$$\rightarrow E_{i+1} \rightarrow E_i \rightarrow \dots \rightarrow E_0 \xrightarrow{\varepsilon} \mathbf{Z} \rightarrow 0.$$

The formalism of the above maps  $d_i$  is pervasive in mathematics. See Exercise 2 for the use of the standard complex in the cohomology theory of groups. For still another example of this same formalism, compare with the Koszul complex in Chapter XXI, §4.

Given a module  $M$ , one may form  $\text{Hom}(E_i, M)$  for each  $i$ , in which case one gets coboundary maps

$$\delta^i: \text{Hom}(E_i, M) \rightarrow \text{Hom}(E_{i+1}, M), \quad \delta(f) = f \circ d^{i+1},$$

obtained by composition of mappings. This procedure will be used to obtain derived functors in §6. In Exercises 2 through 6, you will see how this procedure is used to develop the cohomology theory of groups.

Instead of using homomorphisms, one may use a topological version with simplices, and continuous maps, in which case the standard complex gives rise to the singular homology theory of topological spaces. See [GreH 81], Chapter 9.

**Examples. Finite free resolutions.** In Chapter XXI, you will find other examples of complexes, especially finite free, constructed in various ways with different tools. This subsequent entire chapter may be viewed as providing examples for the current chapter.

**Examples with differential forms.** In Chapter XIX, §3, we gave the example of the de Rham complex in an algebraic setting. In the theory of differential manifolds, the de Rham complex has differential maps

$$d^i: \Omega^i \rightarrow \Omega^{i+1},$$

sending differential forms of degree  $i$  to those of degree  $i + 1$ , and allows for the computation of the homology of the manifold.

A similar situation occurs in complex differential geometry, when the maps  $d^i$  are given by the **Dolbeault**  $\bar{\partial}$ -operators

$$\bar{\partial}^i: \Omega^{p,i} \rightarrow \Omega^{p,i+1}$$

operating on forms of type  $(p, i)$ . Interested readers can look up for instance Gunning's book [Gu 90] mentioned in the introduction to Part IV, Volume I, E. The associated homology of this complex is called the **Dolbeault** or  **$\bar{\partial}$ -cohomology** of the complex manifold.

Let us return to the general algebraic aspects of complexes and resolutions.

It is an interesting problem to discuss which modules admit finite resolutions, and variations on this theme. Some conditions are discussed later in this chapter and in Chapter XXI. If a resolution

$$0 \rightarrow E_n \rightarrow E_{n-1} \rightarrow \cdots \rightarrow E_0 \rightarrow M \rightarrow 0$$

is such that  $E_m = 0$  for  $m > n$ , then we say that the resolution has **length**  $\leq n$  (sometimes we say it has **length**  $n$  by abuse of language).

A **closed complex** of  $A$ -modules is a sequence of modules and homomorphisms  $\{(E^i, d^i)\}$  where  $i$  ranges over the set of integers mod  $n$  for some  $n \geq 2$  and otherwise satisfying the same properties as above. Thus a closed complex looks like this:

$$E^1 \rightarrow E^2 \rightarrow \cdots \rightarrow E^n$$

$\curvearrowright$

We call  $n$  the **length** of the closed complex.

Without fear of confusion, one can omit the index  $i$  on  $d^i$  and write just  $d$ . We also write  $(E, d)$  for the complex  $\{(E^i, d^i)\}$ , or even more briefly, we write simply  $E$ .

Let  $(E, d)$  and  $(E', d')$  be complexes (both open or both closed). Let  $r$  be an integer. A **morphism** or **homomorphism** (of complexes)

$$f: (E', d') \rightarrow (E, d)$$

of **degree**  $r$  is a sequence

$$f_i: E'^i \rightarrow E^{i+r}$$

of homomorphisms such that for all  $i$  the following diagram is commutative:

$$\begin{array}{ccc} E'^{(i-1)} & \xrightarrow{f_{i-1}} & E^{i-1+r} \\ d' \downarrow & & \downarrow d \\ E'^i & \xrightarrow{f_i} & E^{i+r} \end{array}$$

Just as we write  $d$  instead of  $d^i$ , we shall also write  $f$  instead of  $f_i$ . If the complexes are closed, we define a morphism from one into the other only if they have the same length.

It is clear that complexes form a category. In fact they form an abelian category. Indeed, say we deal with complexes indexed by  $\mathbf{Z}$  for simplicity, and morphisms of degree 0. Say we have a morphism of complexes  $f: C \rightarrow C''$  or

putting the indices:

$$\begin{array}{ccccccc} & \longrightarrow & C_n & \longrightarrow & C_{n-1} & \longrightarrow & \\ & & \downarrow & & \downarrow & & \\ & \longrightarrow & C''_n & \longrightarrow & C''_{n-1} & \longrightarrow & \end{array}$$

We let  $C'_n = \text{Ker}(C_n \rightarrow C''_n)$ . Then the family  $(C'_n)$  forms a complex, which we define to be the kernel of  $f$ . We let the reader check the details that this and a similar definition for cokernel and finite direct sums make complexes of modules into an abelian category. At this point, readers should refer to Chapter III, §9, where kernels and cokernels are discussed in this context. The snake lemma of that chapter will now become central to the next section.

It will be useful to have another notion to deal with objects indexed by a monoid. Let  $G$  be a monoid, which we assume commutative and additive to fit the applications we have in mind here. Let  $\{M_i\}_{i \in G}$  be a family of modules indexed by  $G$ . The direct sum

$$M = \bigoplus_{i \in G} M_i$$

will be called the  **$G$ -graded module associated with the family  $\{M_i\}_{i \in G}$** . Let  $\{M_i\}_{i \in G}$  and  $\{M'_i\}_{i \in G}$  be families indexed by  $G$ , and let  $M, M'$  be their associated  $G$ -graded modules. Let  $r \in G$ . By a  **$G$ -graded morphism**  $f: M' \rightarrow M$  of degree  $r$  we shall mean a homomorphism such that  $f$  maps  $M'_i$  into  $M_{i+r}$  for each  $i \in G$  (identifying  $M_i$  with the corresponding submodule of the direct sum on the  $i$ -th component). Thus  $f$  is nothing else than a family of homomorphisms  $f_i: M'_i \rightarrow M_{i+r}$ .

If  $(E, d)$  is a complex we may view  $E$  as a  $G$ -graded module (taking the direct sum of the components of the complex), and we may view  $d$  as a  $G$ -graded morphism of degree 1, letting  $G$  be  $\mathbf{Z}$  or  $\mathbf{Z}/n\mathbf{Z}$ . The most common case we encounter is when  $G = \mathbf{Z}$ . Then we write the complex as

$$E = \bigoplus E_i, \quad \text{and} \quad d: E \rightarrow E$$

maps  $E$  into itself. The differential  $d$  is defined as  $d_i$  on each direct summand  $E_i$ , and has degree 1.

Conversely, if  $G$  is  $\mathbf{Z}$  or  $\mathbf{Z}/n\mathbf{Z}$ , one may view a  $G$ -graded module as a complex, by defining  $d$  to be the zero map.

For simplicity, we shall often omit the prefix “ $G$ -graded” in front of the word “morphism”, when dealing with  $G$ -graded morphisms.

---

## §2. HOMOLOGY SEQUENCE

Let  $(E, d)$  be a complex. We let

$$Z^i(E) = \text{Ker } d^i$$

and call  $Z^i(E)$  the module of  **$i$ -cycles**. We let

$$B^i(E) = \text{Im } d^{i-1}$$

and call  $B^i(E)$  the module of  **$i$ -boundaries**. We frequently write  $Z^i$  and  $B^i$  instead of  $Z^i(E)$  and  $B^i(E)$ , respectively. We let

$$H^i(E) = Z^i/B^i = \text{Ker } d^i/\text{Im } d^{i-1},$$

and call  $H^i(E)$  the  $i$ -th **homology group** of the complex. The graded module associated with the family  $\{H^i\}$  will be denoted by  $H(E)$ , and will be called the **homology** of  $E$ . One sometimes writes  $H^*(E)$  instead of  $H(E)$ .

If  $f: E' \rightarrow E$  is a morphism of complexes, say of degree 0, then we get an **induced canonical homomorphism**

$$H^i(f) : H^i(E') \rightarrow H^i(E)$$

on each homology group. Indeed, from the commutative diagram defining a morphism of complexes, one sees at once that  $f$  maps  $Z^i(E')$  into  $Z^i(E)$  and  $B^i(E')$  into  $B^i(E)$ , whence the induced homomorphism  $H^i(f)$ . Compare with the beginning remarks of Chapter III, §9. One often writes this induced homomorphism as  $f_*$  rather than  $H_i(f)$ , and if  $H(E)$  denotes the graded module of homology as above, then we write

$$H(f) = f_* : H(E') \rightarrow H(E).$$

We call  $H(f)$  the map **induced** by  $f$  on homology. If  $H^i(f)$  is an isomorphism for all  $i$ , then we say that  $f$  is a **homology isomorphism**.

Note that if  $f: E' \rightarrow E$  and  $g: E \rightarrow E''$  are morphisms of complexes, then it is immediately verified that

$$H(g) \circ H(f) = H(g \circ f) \quad \text{and} \quad H(\text{id}) = \text{id}.$$

Thus  $H$  is a functor from the category of complexes to the category of graded modules.

We shall consider short exact sequences of complexes with morphisms of degree 0:

$$0 \rightarrow E' \xrightarrow{f} E \xrightarrow{g} E'' \rightarrow 0,$$

which written out in full look like this:

$$\begin{array}{ccccccc}
 & \downarrow & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & E'^{(i-1)} & \longrightarrow & E^{i-1} & \longrightarrow & E''^{(i-1)} \longrightarrow 0 \\
 & \downarrow & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & E'^i & \xrightarrow{f} & E^i & \xrightarrow{g} & E''^i \longrightarrow 0 \\
 & \downarrow & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & E'^{(i+1)} & \xrightarrow{f} & E^{i+1} & \xrightarrow{g} & E''^{(i+1)} \longrightarrow 0 \\
 & \downarrow & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & E'^{(i+2)} & \longrightarrow & E^{i+2} & \longrightarrow & E''^{(i+2)} \longrightarrow 0 \\
 & \downarrow & \downarrow & & \downarrow & & \\
 & & & & & &
 \end{array}$$

One can define a morphism

$$\delta : H(E'') \rightarrow H(E')$$

of degree 1, in other words, a family of homomorphisms

$$\delta^i : H''^i \rightarrow H'^{i+1}$$

by the snake lemma.

**Theorem 2.1.** Let

$$0 \rightarrow E' \xrightarrow{f} E \xrightarrow{g} E'' \rightarrow 0$$

be an exact sequence of complexes with  $f, g$  of degree 0. Then the sequence

$$\begin{array}{ccc}
 H(E') & \xrightarrow{f_*} & H(E) \\
 \delta \swarrow & & \searrow g_* \\
 H(E'') & & 
 \end{array}$$

is exact.

This theorem is merely a special application of the snake lemma.

If one writes out in full the homology sequence in the theorem, then it looks like this:

$$\boxed{\rightarrow H'^i \rightarrow H^i \rightarrow H''^i \xrightarrow{\delta} H'^{(i+1)} \rightarrow H^{i+1} \rightarrow H''^{(i+1)} \xrightarrow{\delta} \rightarrow}$$

It is clear that our map  $\delta$  is functorial (in an obvious sense), and hence that our whole structure  $(H, \delta)$  is a functor from the category of short exact sequences of complexes into the category of complexes.

---

### §3. EULER CHARACTERISTIC AND THE GROTHENDIECK GROUP

This section may be viewed as a continuation of Chapter III, §8, on Euler-Poincaré maps. Consider complexes of  $A$ -modules, for simplicity.

Let  $E$  be a complex such that almost all homology groups  $H^i$  are equal to 0. Assume that  $E$  is an open complex. As in Chapter III, §8, let  $\varphi$  be an Euler-Poincaré mapping on the category of modules (i.e.  $A$ -modules). We define the **Euler-Poincaré characteristic**  $\chi_\varphi(E)$  (or more briefly the **Euler characteristic**) with respect to  $\varphi$ , to be

$$\chi_\varphi(E) = \sum (-1)^i \varphi(H^i)$$

provided  $\varphi(H^i)$  is defined for all  $H^i$ , in which case we say that  $\chi_\varphi$  is **defined** for the complex  $E$ .

If  $E$  is a closed complex, we select a definite order  $(E^1, \dots, E^n)$  for the integers mod  $n$  and define the Euler characteristic by the formula

$$\chi_\varphi(E) = \sum_{i=1}^n (-1)^i \varphi(H^i)$$

provided again all  $\varphi(H^i)$  are defined.

For an example, the reader may refer to Exercise 28 of Chapter I.

One may view  $H$  as a complex, defining  $d$  to be the zero map. In that case, we see that  $\chi_\varphi(H)$  is the alternating sum given above. More generally:

**Theorem 3.1.** *Let  $F$  be a complex, which is of even length if it is closed. Assume that  $\varphi(F^i)$  is defined for all  $i$ ,  $\varphi(F^i) = 0$  for almost all  $i$ , and  $H^i(F) = 0$  for almost all  $i$ . Then  $\chi_\varphi(F)$  is defined, and*

$$\chi_\varphi(F) = \sum_i (-1)^i \varphi(F^i).$$

*Proof.* Let  $Z^i$  and  $B^i$  be the groups of  $i$ -cycles and  $i$ -boundaries in  $F^i$  respectively. We have an exact sequence

$$0 \rightarrow Z^i \rightarrow F^i \rightarrow B^{i+1} \rightarrow 0.$$

Hence  $\chi_\varphi(F)$  is defined, and

$$\varphi(F^i) = \varphi(Z^i) + \varphi(B^{i+1}).$$

Taking the alternating sum, our conclusion follows at once.

A complex whose homology is trivial is called **acyclic**.

**Corollary 3.2.** *Let  $F$  be an acyclic complex, such that  $\varphi(F^i)$  is defined for all  $i$ , and equal to 0 for almost all  $i$ . If  $F$  is closed, we assume that  $F$  has even length. Then*

$$\chi_\varphi(F) = 0.$$

In many applications, an open complex  $F$  is such that  $F^i = 0$  for almost all  $i$ , and one can then treat this complex as a closed complex by defining an additional map going from a zero on the far right to a zero on the far left. Thus in this case, the study of such an open complex is reduced to the study of a closed complex.

**Theorem 3.3.** *Let*

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

*be an exact sequence of complexes, with morphisms of degree 0. If the complexes are closed, assume that their length is even. Let  $\varphi$  be an Euler-Poincaré mapping on the category of modules. If  $\chi_\varphi$  is defined for two of the above three complexes, then it is defined for the third, and we have*

$$\chi_\varphi(E) = \chi_\varphi(E') + \chi_\varphi(E'').$$

*Proof.* We have an exact homology sequence

$$\rightarrow H''^{(i-1)} \rightarrow H'^i \rightarrow H^i \rightarrow H''^i \rightarrow H'^{(i+1)} \rightarrow$$

This homology sequence is nothing but a complex whose homology is trivial. Furthermore, each homology group belonging say to  $E$  is between homology groups of  $E'$  and  $E''$ . Hence if  $\chi_\varphi$  is defined for  $E'$  and  $E''$  it is defined for  $E$ . Similarly for the other two possibilities. If our complexes are closed of even length  $n$ , then this homology sequence has even length  $3n$ . We can therefore apply the corollary of Theorem 3.1 to get what we want.

For certain applications, it is convenient to construct a universal Euler mapping. Let  $\mathfrak{Q}$  be the set of isomorphism classes of certain modules. If  $E$  is a module, let  $[E]$  denote its isomorphism class. We require that  $\mathfrak{Q}$  satisfy the **Euler-Poincaré condition**, i.e. if we have an exact sequence

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0,$$

then  $[E]$  is in  $\mathfrak{Q}$  if and only if  $[E']$  and  $[E'']$  are in  $\mathfrak{Q}$ . Furthermore, the zero module is in  $\mathfrak{Q}$ .

**Theorem 3.4.** *Assume that  $\mathfrak{Q}$  satisfies the Euler-Poincaré condition. Then there is a map*

$$\gamma: \mathfrak{Q} \rightarrow \mathbf{K}(\mathfrak{Q})$$

*of  $\mathfrak{Q}$  into an abelian group  $\mathbf{K}(\mathfrak{Q})$  having the universal property with respect to Euler-Poincaré maps defined on  $\mathfrak{Q}$ .*

To construct this, let  $F_{\text{ab}}(\mathfrak{Q})$  be the free abelian group generated by the set of such  $[E]$ . Let  $B$  be the subgroup generated by all elements of type

$$[E] - [E'] - [E''],$$

where

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

is an exact sequence whose members are in  $\mathfrak{Q}$ . We let  $\mathbf{K}(\mathfrak{Q})$  be the factor group  $F_{\text{ab}}(\mathfrak{Q})/B$ , and let  $\gamma: \mathfrak{Q} \rightarrow \mathbf{K}(\mathfrak{Q})$  be the natural map. It is clear that  $\gamma$  has the universal property.

We observe the similarity of construction with the Grothendieck group of a monoid. In fact, the present group is known as the **Euler-Grothendieck group** of  $\mathfrak{Q}$ , with Euler usually left out.

The reader should observe that the above arguments are valid in abelian categories, although we still used the word **module**. Just as with the elementary isomorphism theorems for groups, we have the analogue of the Jordan-Hölder theorem for modules. Of course in the case of modules, we don't have to worry about the normality of submodules.

We now go a little deeper into **K**-theory. Let  $\mathfrak{Q}$  be an abelian category. In first reading, one may wish to limit attention to an abelian category of modules over a ring. Let  $\mathfrak{C}$  be a family of objects in  $\mathfrak{Q}$ . We shall say that  $\mathfrak{C}$  is a **K-family** if it satisfies the following conditions.

**K 1.**  $\mathfrak{C}$  is closed under taking finite direct sums, and  $0$  is in  $\mathfrak{C}$ .

**K 2.** Given an object  $E$  in  $\mathfrak{Q}$  there exists an epimorphism

$$L \rightarrow E \rightarrow 0$$

with  $L$  in  $\mathfrak{C}$ .

**K 3.** Let  $E$  be an object admitting a finite resolution of length  $n$

$$0 \rightarrow L_n \rightarrow \cdots \rightarrow L_0 \rightarrow E \rightarrow 0$$

with  $L_i \in \mathfrak{C}$  for all  $i$ . If

$$0 \rightarrow N \rightarrow F_{n-1} \rightarrow \cdots \rightarrow F_0 \rightarrow E \rightarrow 0$$

is a resolution with  $N$  in  $\mathfrak{Q}$  and  $F_0, \dots, F_{n-1}$  in  $\mathfrak{C}$ , then  $N$  is also in  $\mathfrak{C}$ .

We note that it follows from these axioms that if  $F$  is in  $\mathcal{C}$  and  $F'$  is isomorphic to  $F$ , then  $F'$  is also in  $\mathcal{C}$ , as one sees by looking at the resolution

$$0 \rightarrow F' \rightarrow F \rightarrow 0 \rightarrow 0$$

and applying **K 3**. Furthermore, given an exact sequence

$$0 \rightarrow F' \rightarrow F \rightarrow F'' \rightarrow 0$$

with  $F$  and  $F''$  in  $\mathcal{C}$ , then  $F'$  is in  $\mathcal{C}$ , again by applying **K 3**.

**Example.** One may take for  $\mathfrak{Q}$  the category of modules over a commutative ring, and for  $\mathcal{C}$  the family of projective modules. Later we shall also consider Noetherian rings, in which case one may take finite modules, and finite projective modules instead. Condition **K 2** will be discussed in §8.

From now on we assume that  $\mathcal{C}$  is a **K**-family. For each object  $E$  in  $\mathfrak{Q}$ , we let  $[E]$  denote its isomorphism class. An object  $E$  of  $\mathfrak{Q}$  will be said to have **finite  $\mathcal{C}$ -dimension** if it admits a finite resolution with elements of  $\mathcal{C}$ . We let  $\mathfrak{Q}(\mathcal{C})$  be the family of objects in  $\mathfrak{Q}$  which are of finite  $\mathcal{C}$ -dimension. We may then form the

$$\mathbf{K}(\mathfrak{Q}(\mathcal{C})) = \mathbf{Z}[\mathfrak{Q}(\mathcal{C})]/R(\mathfrak{Q}(\mathcal{C}))$$

where  $R(\mathfrak{Q}(\mathcal{C}))$  is the group generated by all elements  $[E] - [E'] - [E'']$  arising from an exact sequence

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

in  $\mathfrak{Q}(\mathcal{C})$ . Similarly we define

$$\mathbf{K}(\mathcal{C}) = \mathbf{Z}[(\mathcal{C})]/R(\mathcal{C}),$$

where  $R(\mathcal{C})$  is the group of relations generated as above, but taking  $E'$ ,  $E$ ,  $E''$  in  $\mathcal{C}$  itself.

There are natural maps

$$\gamma_{a(e)} : \mathfrak{Q}(\mathcal{C}) \rightarrow \mathbf{K}(\mathfrak{Q}(\mathcal{C})) \quad \text{and} \quad \gamma_e : \mathcal{C} \rightarrow \mathbf{K}(\mathcal{C}),$$

which to each object associate its class in the corresponding Grothendieck group. There is also a natural homomorphism

$$\epsilon : \mathbf{K}(\mathcal{C}) \rightarrow \mathbf{K}(\mathfrak{Q}(\mathcal{C}))$$

since an exact sequence of objects of  $\mathcal{C}$  can also be viewed as an exact sequence of objects of  $\mathfrak{Q}(\mathcal{C})$ .

**Theorem 3.5.** *Let  $M \in \mathfrak{Q}(\mathcal{C})$  and suppose we have two resolutions*

$$L_M \rightarrow M \rightarrow 0 \quad \text{and} \quad L'_M \rightarrow M \rightarrow 0,$$

*by finite complexes  $L_M$  and  $L'_M$  in  $\mathcal{C}$ . Then*

$$\sum (-1)^i \gamma_e(L_i) = \sum (-1)^i \gamma_e(L'_i).$$

*Proof.* Take first the special case when there is an epimorphism  $L'_M \rightarrow L_M$ , with kernel  $E$  illustrated on the following commutative and exact diagram.

$$\begin{array}{ccccccc} 0 & \longrightarrow & E & \longrightarrow & L'_M & \longrightarrow & L_M & \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ & & M & \xrightarrow{\text{id}} & M & & & \\ & & \downarrow & & \downarrow & & & \\ & & 0 & & 0 & & & \end{array}$$

The kernel is a complex

$$0 \rightarrow E_n \rightarrow E_{n-1} \rightarrow \cdots \rightarrow E_0 \rightarrow 0$$

which is exact because we have the homology sequence

$$H_p(E) \rightarrow H_p(L') \rightarrow H_p(L) \rightarrow H_{p-1}(E)$$

For  $p \geq 1$  we have  $H_p(L) = H_p(L') = 0$  by definition, so  $H_p(E) = 0$  for  $p \geq 1$ . And for  $p = 0$  we consider the exact sequence

$$H_1(L) \rightarrow H_0(E) \rightarrow H_0(L') \rightarrow H_0(L)$$

Now we have  $H_1(L) = 0$ , and  $H_0(L') \rightarrow H_0(L)$  corresponds to the identity morphisms on  $M$  so is an isomorphism. It follows that  $H_0(E) = 0$  also.

By definition of  $\mathbf{K}$ -family, the objects  $E_p$  are in  $\mathcal{C}$ . Then taking the Euler characteristic in  $\mathbf{K}(\mathcal{C})$  we find

$$\chi(L') - \chi(L) = \chi(E) = 0$$

which proves our assertion in the special case.

The general case follows by showing that given two resolutions of  $M$  in  $\mathcal{C}$  we can always find a third one which tops both of them. The pattern of our construction will be given by a lemma.

**Lemma 3.6.** *Given two epimorphisms  $u: M \rightarrow N$  and  $v: M' \rightarrow N$  in  $\mathcal{Q}$ , there exist epimorphisms  $F \rightarrow M$  and  $F \rightarrow M'$  with  $F$  in  $\mathcal{C}$  making the following diagram commutative.*

$$\begin{array}{ccc} & F & \\ & \swarrow & \searrow \\ M & & M' \\ & \searrow & \swarrow \\ & N & \end{array}$$

*Proof.* Let  $E = M \times_N M'$ , that is  $E$  is the kernel of the morphism

$$M \times M' \rightarrow N$$

given by  $(x, y) \mapsto ux - vy$ . (Elements are not really used here, and we could write formally  $u - v$  instead.) There is some  $F$  in  $\mathcal{C}$  and an epimorphism  $F \rightarrow E \rightarrow 0$ . The composition of this epimorphism with the natural projections of  $E$  on each factor gives us what we want.

We construct a complex  $L''_M$  giving a resolution of  $M$  with a commutative and exact diagram:

$$\begin{array}{ccccccc} & & 0 & & & & \\ & & \uparrow & & & & \\ & & L_M & \longrightarrow & M & \longrightarrow & 0 \\ & & \uparrow & & \uparrow \text{id} & & \\ & & L''_M & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \text{id} & & \\ & & L_M & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow & & & & \\ & & 0 & & & & \end{array}$$

The construction is done inductively, so we put indices:

$$\begin{array}{ccccccc} & L_i & \longrightarrow & L_{i-1} & \longrightarrow & & \\ & \uparrow & & \uparrow & & & \\ & L''_i & \longrightarrow & L''_{i-1} & \longrightarrow & & \\ & \downarrow & & \downarrow & & & \\ & L'_i & \longrightarrow & L'_{i-1} & \longrightarrow & & \end{array}$$

Suppose that we have constructed up to  $L_{i-1}''$  with the desired epimorphisms on  $L_{i-1}$  and  $L_{i-1}'$ . We want to construct  $L_i''$ . Let  $B_i = \text{Ker}(L_{i-1} \rightarrow L_{i-2})$  and similarly for  $B_i'$  and  $B_i''$ . We obtain the commutative diagram:

$$\begin{array}{ccccccc}
 L_i & \longrightarrow & B_i & \longrightarrow & L_{i-1} & \longrightarrow & L_{i-2} \\
 \uparrow & & \uparrow & & \uparrow & & \uparrow \\
 B_i'' & \longrightarrow & L_{i-1}'' & \longrightarrow & L_{i-2}'' & & \\
 \downarrow & & \downarrow & & \downarrow & & \\
 L_i' & \longrightarrow & B_i' & \longrightarrow & L_{i-1}' & \longrightarrow & L_{i-2}' \\
 \end{array}$$

If  $B_i'' \rightarrow B_i$  or  $B_i'' \rightarrow B_i'$  are not epimorphisms, then we replace  $L_{i-1}''$  by

$$L_{i-1}'' \oplus L_i \oplus L_i'.$$

We let the boundary map to  $L_{i-2}''$  be 0 on the new summands, and similarly define the maps to  $L_{i-1}$  and  $L_{i-1}'$  to be 0 on  $L_i'$  and  $L_{i-1}'$  respectively.

Without loss of generality we may now assume that

$$B_i'' \rightarrow B_i \quad \text{and} \quad B_i'' \rightarrow B_i'$$

are epimorphisms. We then use the construction of the preceding lemma. We let

$$E_i = L_i \bigoplus_{B_i} B_i'' \quad \text{and} \quad E_i' = B_i'' \bigoplus_{B_i'} L_i'.$$

Then both  $E_i$  and  $E_i'$  have natural epimorphisms on  $B_i''$ . Then we let

$$N_i = E_i \bigoplus_{B_i''} E_i'$$

and we find an object  $L_i''$  in  $\mathcal{C}$  with an epimorphism  $L_i'' \rightarrow N_i$ . This gives us the inductive construction of  $L''$  up to the very end. To stop the process, we use **K 3** and take the kernel of the last constructed  $L_i''$  to conclude the proof.

**Theorem 3.7.** *The natural map*

$$\epsilon : \mathbf{K}(\mathcal{C}) \rightarrow \mathbf{K}(\mathbf{Q}(\mathcal{C}))$$

*is an isomorphism.*

*Proof.* The map is surjective because given a resolution

$$0 \rightarrow F_n \rightarrow \cdots \rightarrow F_0 \rightarrow M \rightarrow 0$$

with  $F_i \in \mathcal{C}$  for all  $i$ , the element

$$\sum (-1)^i \gamma_e(F_i)$$

maps on  $\gamma_{\alpha(\mathcal{C})}(M)$  under  $\epsilon$ . Conversely, Theorem 3.5 shows that the association

$$M \mapsto \sum (-1)^i \gamma_{\epsilon}(F_i)$$

is a well-defined mapping. Since for any  $L \in \mathcal{C}$  we have a short exact sequence  $0 \rightarrow L \rightarrow L \rightarrow 0$ , it follows that this mapping following  $\epsilon$  is the identity on  $\mathbf{K}(\mathcal{C})$ , so  $\epsilon$  is a monomorphism. Hence  $\epsilon$  is an isomorphism, as was to be shown.

It may be helpful to the reader actually to see the next lemma which makes the additivity of the inverse more explicit.

**Lemma 3.8.** *Given an exact sequence in  $\mathbf{Q}(\mathcal{C})$*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

*there exists a commutative and exact diagram*

$$\begin{array}{ccccccc} 0 & \longrightarrow & L_{M'} & \longrightarrow & L_M & \longrightarrow & L_{M''} & \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ & & 0 & & 0 & & 0 & \end{array}$$

*with finite resolutions  $L_{M'}, L_M, L_{M''}$  in  $\mathcal{C}$ .*

*Proof.* We first show that we can find  $L', L, L''$  in  $\mathcal{C}$  to fit an exact and commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L' & \longrightarrow & L & \longrightarrow & L'' & \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow & \\ & & 0 & & 0 & & 0 & \end{array}$$

We first select an epimorphism  $L'' \rightarrow M''$  with  $L'' \in \mathcal{C}$ . By Lemma 3.6 there exists  $L_1 \in \mathcal{C}$  and epimorphisms  $L_1 \rightarrow M, L_1 \rightarrow L''$  making the diagram commutative. Then let  $L_2 \rightarrow M'$  be an epimorphism with  $L_2 \in \mathcal{C}$ , and finally define  $L = L_1 \oplus L_2$ . Then we get morphisms  $L \rightarrow M$  and  $L \rightarrow L''$  in the obvious way. Let  $L'$  be the kernel of  $L \rightarrow L''$ . Then  $L_2 \subset L'$  so we get an epimorphism  $L' \rightarrow M'$ .

This now allows us to construct resolutions inductively until we hit the  $n$ -th step, where  $n$  is some integer such that  $M, M''$  admit resolutions of length  $n$  in  $\mathcal{C}$ . The last horizontal exact sequence that we obtain is

$$0 \rightarrow L'_n \rightarrow L_n \rightarrow L''_n \rightarrow 0$$

and  $L''_n$  can be chosen to be the kernel of  $L''_{n-1} \rightarrow L''_{n-2}$ . By **K 3** we know that  $L''_n$  lies in  $\mathcal{C}$ , and the sequence

$$0 \rightarrow L''_n \rightarrow L''_{n-1}$$

is exact. This implies that in the next inductive step, we can take  $L''_{n+1} = 0$ . Then

$$0 \rightarrow L'_{n+1} \rightarrow L_{n+1} \rightarrow 0 \rightarrow 0$$

is exact, and at the next step we just take the kernels of the vertical arrows to complete the desired finite resolutions in  $\mathcal{C}$ . This concludes the proof of the lemma.

**Remark.** The argument in the proof of Lemma 3.8 in fact shows:

*If*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

*is an exact sequence in  $\mathfrak{Q}$ , and if  $M, M''$  have finite  $\mathcal{C}$ -dimension, then so does  $M'$ .*

In the category of modules, one has a more precise statement:

**Theorem 3.9.** *Let  $\mathfrak{Q}$  be the category of modules over a ring. Let  $\mathfrak{P}$  be the family of projective modules. Given an exact sequence of modules*

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

*if any two of  $E', E, E''$  admit finite resolutions in  $\mathfrak{P}$  then the third does also.*

Proofs in a more subtle case will be given in Chapter XXI, Theorem 2.7.

Next we shall use the tensor product to investigate a ring structure on the Grothendieck group. We suppose for simplicity that we deal with an abelian category of modules over a commutative ring, denoted by  $\mathfrak{Q}$ , together with a **K**-family  $\mathcal{C}$  as above, but we now assume that  $\mathfrak{Q}$  is closed under the tensor product. The only properties we shall actually use for the next results are the following ones, denoted by **TG** (for “tensor” and “Grothendieck” respectively):

**TG 1.** There is a bifunctorial isomorphism giving commutativity

$$M \otimes N \approx N \otimes M$$

for all  $M, N$  in  $\mathfrak{Q}$ ; and similarly for distributivity over direct sums, and associativity.

**TG 2.** For all  $L$  in  $\mathcal{C}$  the functor  $M \mapsto L \otimes M$  is exact.

**TG 3.** If  $L, L'$  are in  $\mathcal{C}$  then  $L \otimes L'$  is in  $\mathcal{C}$ .

Then we may give  $\mathbf{K}(\mathcal{C})$  the structure of an algebra by defining

$$\text{cl}_{\mathcal{C}}(L) \text{ cl}_{\mathcal{C}}(L') = \text{cl}_{\mathcal{C}}(L \otimes L').$$

Condition **TG 1** implies that this algebra is commutative, and we call it the **Grothendieck algebra**. In practice, there is a unit element, but if we want one in the present axiomatization, we have to make it an explicit assumption:

**TG 4.** There is an object  $R$  in  $\mathcal{C}$  such that  $R \otimes M \approx M$  for all  $M$  in  $\mathcal{Q}$ .

Then  $\text{cl}_{\mathcal{C}}(R)$  is the unit element.

Similarly, condition **TG 2** shows that we can define a module structure on  $\mathbf{K}(\mathcal{Q})$  over  $\mathbf{K}(\mathcal{C})$  by the same formula

$$\text{cl}_{\mathcal{C}}(L) \text{ cl}_{\mathcal{Q}}(M) = \text{cl}_{\mathcal{Q}}(L \otimes M),$$

and similarly  $\mathbf{K}(\mathcal{Q}(\mathcal{C}))$  is a module over  $\mathbf{K}(\mathcal{C})$ , where we recall that  $\mathcal{Q}(\mathcal{C})$  is the family of objects in  $\mathcal{Q}$  which admit finite resolutions by objects in  $\mathcal{C}$ .

Since we know from Theorem 3.7 that  $\mathbf{K}(\mathcal{C}) \approx \mathbf{K}(\mathcal{Q}(\mathcal{C}))$ , we also have a ring structure on  $\mathbf{K}(\mathcal{Q}(\mathcal{C}))$  via this isomorphism. We then can make the product more explicit as follows.

**Proposition 3.10.** *Let  $M \in \mathcal{Q}(\mathcal{C})$  and let  $N \in \mathcal{Q}$ . Let*

$$0 \rightarrow L_n \rightarrow \cdots \rightarrow L_0 \rightarrow M \rightarrow 0$$

*be a finite resolution of  $M$  by objects in  $\mathcal{C}$ . Then*

$$\begin{aligned} \text{cl}_{\mathcal{C}}(M) \text{ cl}_{\mathcal{Q}}(N) &= \sum (-1)^i \text{ cl}_{\mathcal{Q}}(L_i \otimes N). \\ &= \sum (-1)^i \text{ cl}_{\mathcal{Q}}(H_i(K)) \end{aligned}$$

*where  $K$  is the complex*

$$0 \rightarrow L_n \otimes N \rightarrow \cdots \rightarrow L_0 \otimes N \rightarrow M \otimes N \rightarrow 0$$

*and  $H_i(K)$  is the  $i$ -th homology of this complex.*

*Proof.* The formulas are immediate consequences of the definitions, and of Theorem 3.1.

**Example.** Let  $\mathcal{Q}$  be the abelian category of modules over a commutative ring. Let  $\mathcal{C}$  be the family of projective modules. From §6 on derived functors the reader will know that the homology of the complex  $K$  in Proposition 3.10 is just  $\text{Tor}(M, N)$ . Therefore the formula in that proposition can also be written

$$\text{cl}_{\mathcal{C}}(M) \text{ cl}_{\mathcal{Q}}(N) = \sum (-1)^i \text{ cl}_{\mathcal{Q}}(\text{Tor}_i(M, N)).$$

**Example.** Let  $k$  be a field. Let  $G$  be a group. By a  **$(G, k)$ -module**, we shall mean a pair  $(E, \rho)$ , consisting of a  $k$ -space  $E$  and a homomorphism

$$\rho: G \rightarrow \text{Aut}_k(E).$$

Such a homomorphism is also called a **representation** of  $G$  in  $E$ . By abuse of language, we also say that the  $k$ -space  $E$  is a  $G$ -module. The group  $G$  operates on  $E$ , and we write  $\sigma x$  instead of  $\rho(\sigma)x$ . The field  $k$  will be kept fixed in what follows.

Let  $\text{Mod}_k(G)$  denote the category whose objects are  $(G, k)$ -modules. A morphism in  $\text{Mod}_k(G)$  is what we call a  **$G$ -homomorphism**, that is a  $k$ -linear map  $f: E \rightarrow F$  such that  $f(\sigma x) = \sigma f(x)$  for all  $\sigma \in G$ . The group of morphisms in  $\text{Mod}_k(G)$  is denoted by  $\text{Hom}_G$ .

If  $E$  is a  $G$ -module, and  $\sigma \in G$ , then we have by definition a  $k$ -automorphism  $\sigma: E \rightarrow E$ . Since  $T^r$  is a functor, we have an induced automorphism

$$T^r(\sigma): T^r(E) \rightarrow T^r(E)$$

for each  $r$ , and thus  $T^r(E)$  is also a  $G$ -module. Taking the direct sum, we see that  $T(E)$  is a  $G$ -module, and hence that  $T$  is a functor from the category of  $G$ -modules to the category of graded  $G$ -modules. Similarly for  $\bigwedge^r, S^r$ , and  $\bigwedge, S$ .

It is clear that the kernel of a  $G$ -homomorphism is a  $G$ -submodule, and that the factor module of a  $G$ -module by a  $G$ -submodule is again a  $G$ -module so the category of  $G$ -modules is an abelian category.

We can now apply the general considerations on the Grothendieck group which we write

$$\mathbf{K}(G) = \mathbf{K}(\text{Mod}_k(G))$$

for simplicity in the present case. We have the canonical map

$$\text{cl}: \text{Mod}_k(G) \rightarrow \mathbf{K}(G).$$

which to each  $G$ -module associates its class in  $\mathbf{K}(G)$ .

If  $E, F$  are  $G$ -modules, then their tensor product over  $k$ ,  $E \otimes F$ , is also a  $G$ -module. Here again, the operation of  $G$  on  $E \otimes F$  is given functorially. If  $\sigma \in G$ , there exists a unique  $k$ -linear map  $E \otimes F \rightarrow E \otimes F$  such that for  $x \in E$ ,  $y \in F$  we have  $x \otimes y \mapsto (\sigma x) \otimes (\sigma y)$ . The tensor product induces a law of composition on  $\text{Mod}_k(G)$  because the tensor products of  $G$ -isomorphic modules are  $G$ -isomorphic.

Furthermore all the conditions **TG 1** through **TG 4** are satisfied. Since  $k$  is a field, we find also that tensoring an exact sequence of  $G$ -modules over  $k$  with any  $G$ -module over  $k$  preserves the exactness, so **TG 2** is satisfied for all  $(G, k)$ -modules. Thus the Grothendieck group  $\mathbf{K}(G)$  is in fact the Grothendieck ring, or the Grothendieck algebra over  $k$ .

By Proposition 2.1 and Theorem 2.3 of Chapter XVIII, we also see:

*The Grothendieck ring of a finite group  $G$  consisting of isomorphism classes of finite dimensional  $(G, k)$ -spaces over a field  $k$  of characteristic 0 is naturally isomorphic to the character ring  $X_{\mathbf{Z}}(G)$ .*

We can axiomatize this a little more. We consider an abelian category of modules over a commutative ring  $R$ , which we denote by  $\mathfrak{Q}$  for simplicity. For two modules  $M, N$  in  $\mathfrak{Q}$  we let  $\text{Mor}(M, N)$  as usual be the morphisms in  $\mathfrak{Q}$ , but  $\text{Mor}(M, N)$  is an abelian subgroup of  $\text{Hom}_R(M, N)$ . For example, we could take  $\mathfrak{Q}$  to be the category of  $(G, k)$ -modules as in the example we have just discussed, in which case  $\text{Mor}(M, N) = \text{Hom}_G(M, N)$ .

We let  $\mathfrak{C}$  be the family of finite free modules in  $\mathfrak{Q}$ . *We assume that  $\mathfrak{C}$  satisfies TG 1, TG 2, TG 3, TG 4, and also that  $\mathfrak{C}$  is closed under taking alternating products, tensor products and symmetric products.* We let  $\mathbf{K} = \mathbf{K}(\mathfrak{C})$ . As we have seen,  $\mathbf{K}$  is itself a commutative ring. We abbreviate  $\text{cl}_e = \text{cl}$ .

We shall define non-linear maps

$$\lambda^i : \mathbf{K} \rightarrow \mathbf{K}$$

using the alternating product. If  $E$  is finite free, we let

$$\lambda^i(E) = \text{cl}(\bigwedge^i E).$$

Proposition 1.1 of Chapter XIX can now be formulated for the  $\mathbf{K}$ -ring as follows.

**Proposition 3.11.** *Let*

$$0 \rightarrow E' \rightarrow E \rightarrow E'' \rightarrow 0$$

*be an exact sequence of finite free modules in  $\mathfrak{Q}$ . Then for every integer  $n \geq 0$  we have*

$$\lambda^n(E) = \sum_{i=0}^n \lambda^i(E') \lambda^{n-i}(E'').$$

As a result of the proposition, we can define a map

$$\lambda_t : \mathbf{K} \rightarrow 1 + t\mathbf{K}[[t]]$$

of  $\mathbf{K}$  into the multiplicative group of formal power series with coefficients in  $\mathbf{K}$ , and with constant term 1, by letting

$$\lambda_t(x) = \sum_{i=0}^{\infty} \lambda^i(x) t^i.$$

Proposition 1.4 of Chapter XIX can be formulated by saying that:

*The map*

$$\lambda_t : \mathbf{K} \rightarrow 1 + t\mathbf{K}[[t]]$$

*is a homomorphism.*

We note that if  $L$  is free of rank 1, then

$$\lambda^0(L) = \text{ground ring};$$

$$\lambda^1(L) = \text{cl}(L);$$

$$\lambda^i(L) = 0 \quad \text{for } i > 1.$$

This can be summarized by writing

$$\lambda_t(L) = 1 + \text{cl}(L)t.$$

Next we can do a similar construction with the symmetric product instead of the alternating product. If  $E$  is a finite free module in  $\mathfrak{C}$  we let as usual:

$$S(E) = \text{symmetric algebra of } E;$$

$$S^i(E) = \text{homogeneous component of degree } i \text{ in } S(E).$$

We define

$$\sigma^i(E) = \text{cl}(S^i(E))$$

and the corresponding power series

$$\sigma_t(E) = \sum \sigma^i(E)t^i.$$

**Theorem 3.12.** *Let  $E$  be a finite free module in  $\mathfrak{C}$ , of rank  $r$ . Then for all integers  $n \geq 1$  we have*

$$\sum_{i=0}^r (-1)^i \lambda^i(E) \sigma^{n-i}(E) = 0,$$

where by definition  $\sigma^j(E) = 0$  for  $j < 0$ . Furthermore

$$\sigma_t(E) \lambda_{-t}(E) = 1,$$

so the power series  $\sigma_t(E)$  and  $\lambda_{-t}(E)$  are inverse to each other.

*Proof.* The first formula depends on the analogue for the symmetric product and the alternating product of the formula given in Proposition 1.1 of Chapter

XIX. It could be proved directly now, but the reader will find a proof as a special case of the theory of Koszul complexes in Chapter XXI, Corollary 4.14. The power series relation is essentially a reformulation of the first formula.

From the above formalism, it is possible to define other maps besides  $\lambda^i$  and  $\sigma^i$ .

**Example.** Assume that the group  $G$  is trivial, and just write  $\mathbf{K}$  for the Grothendieck ring instead of  $\mathbf{K}(1)$ . For  $x \in \mathbf{K}$  define

$$\psi_{-t}(x) = -t \frac{d}{dt} \log \lambda_t(x) = -t \lambda'_t(x)/\lambda_t(x).$$

Show that  $\psi_{-t}$  is an additive and multiplicative homomorphism. Show that

$$\psi_t(E) = 1 + \text{cl}(E)t + \text{cl}(E)^2t^2 + \dots$$

This kind of construction with the logarithmic derivative leads to the **Adams operations**  $\psi^i$  in topology and algebraic geometry. See Exercise 22 of Chapter XVIII.

**Remark.** If it happens in Theorem 3.12 that  $E$  admits a decomposition into 1-dimensional free modules in the  $\mathbf{K}$ -group, then the proof trivializes by using the fact that  $\lambda_t(L) = 1 + \text{cl}(L)t$  if  $L$  is 1-dimensional. But in the example of  $(G, k)$ -spaces when  $k$  is a field, this is in general not possible, and it is also not possible in other examples arising naturally in topology and algebraic geometry. However, by “changing the base,” one can sometimes achieve this simpler situation, but Theorem 3.12 is then used in establishing the basic properties. Cf. Grothendieck [SGA 6], mentioned in the introduction to Part IV, and other works mentioned in the bibliography at the end, namely [Ma 69], [At 61], [At 67], [Ba 68], [Bo 62]. The lectures by Atiyah and Bott emphasize the topological aspects as distinguished from the algebraic-geometric aspects. Grothendieck [Gr 68] actually shows how the formalism of Chern classes from algebraic geometry and topology also enters the theory of representations of linear groups. See also the exposition in [FuL 85], especially the formalism of Chapter I, §6. For special emphasis on applications to representation theory, see Bröcker-tom Dieck [BtD 85], especially Chapter II, §7, concerning compact Lie groups.

---

## §4. INJECTIVE MODULES

In Chapter III, §4, we defined projective modules, which have a natural relation to free modules. By reversing the arrows, we can define a module  $Q$  to be **injective** if it satisfies any one of the following conditions which are equivalent:

- I 1.** Given any module  $M$  and a submodule  $M'$ , and a homomorphism  $f: M' \rightarrow Q$ , there exists an extension of this homomorphism to  $M$ ,

that is there exists  $h : M' \rightarrow Q$  making the following diagram commutative:

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \downarrow f & & \swarrow h \\ & & Q & & \end{array}$$

**I 2.** The functor  $M \mapsto \text{Hom}_A(M, Q)$  is exact.

**I 3.** Every exact sequence  $0 \rightarrow Q \rightarrow M \rightarrow M'' \rightarrow 0$  splits.

We prove the equivalence. General considerations on homomorphisms as in Proposition 2.1, show that exactness of the homed sequence may fail only at one point, namely given

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0,$$

the question is whether

$$\text{Hom}_A(M, Q) \rightarrow \text{Hom}_A(M', Q) \rightarrow 0$$

is exact. But this is precisely the hypothesis as formulated in **I 1**, so **I 1** implies **I 2** is essentially a matter of linguistic reformulation, and in fact **I 1** is equivalent to **I 2**.

Assume **I 2** or **I 1**, which we know are equivalent. To get **I 3** is immediate, by applying **I 1** to the diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & Q & \longrightarrow & M \\ & & \downarrow \text{id} & & \swarrow h \\ & & Q & & \end{array}$$

To prove the converse, we need the notion of push-out (cf. Exercise 52 of Chapter I). Given an exact diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \downarrow & & \\ & & Q & & \end{array}$$

we form the push-out:

$$\begin{array}{ccccc} M' & \longrightarrow & M \\ \downarrow & & \downarrow \\ Q & \longrightarrow & N = Q \oplus_{M'} M. \end{array}$$

Since  $M' \rightarrow M$  is a monomorphism, it is immediately verified from the construction of the push-out that  $Q \rightarrow N$  is also a monomorphism. By **I 3**, the sequence

$$0 \rightarrow Q \rightarrow N$$

splits, and we can now compose the splitting map  $N \rightarrow Q$  with the push-out map  $M \rightarrow N$  to get the desired  $h: M \rightarrow Q$ , thus proving **I 1**.

We saw easily that every module is a homomorphic image of a free module. There is no equally direct construction for the dual fact:

**Theorem 4.1.** *Every module is a submodule of an injective module.*

The proof will be given by dualizing the situation, with some lemmas. We first look at the situation in the category of abelian groups. If  $M$  is an abelian group, let its dual group be  $M^\wedge = \text{Hom}(M, \mathbf{Q}/\mathbf{Z})$ . If  $F$  is a free abelian group, it is reasonable to expect, and in fact it is easily proved that its dual  $F^\wedge$  is an injective module, since injectivity is the dual notion of projectivity. Furthermore,  $M$  has a natural map into the double dual  $M^{\wedge\wedge}$ , which is shown to be a monomorphism. Now represent  $M^\wedge$  as a quotient of a free abelian group,

$$F \rightarrow M^\wedge \rightarrow 0.$$

Dualizing this sequence yields a monomorphism

$$0 \rightarrow M^{\wedge\wedge} \rightarrow F^\wedge,$$

and since  $M$  is embedded naturally as a subgroup of  $M^{\wedge\wedge}$ , we get the desired embedding of  $M$  as a subgroup of  $F^\wedge$ .

This proof also works in general, but there are details to be filled in. First we have to prove that the dual of a free module is injective, and second we have to be careful when passing from the category of abelian groups to the category of modules over an arbitrary ring. We now carry out the details.

We say that an abelian group  $T$  is **divisible** if for every integer  $m$ , the homomorphism

$$m_T: x \mapsto mx$$

is surjective.

**Lemma 4.2.** *If  $T$  is divisible, then  $T$  is injective in the category of abelian groups.*

*Proof.* Let  $M' \subset M$  be a subgroup of an abelian group, and let  $f: M' \rightarrow T$  be a homomorphism. Let  $x \in M$ . We want first to extend  $f$  to the module  $(M', x)$  generated by  $M'$  and  $x$ . If  $x$  is free over  $M'$ , then we select any value  $t \in T$ , and it is immediately verified that  $f$  extends to  $(M', x)$  by giving the value  $f(x) = t$ . Suppose that  $x$  is torsion with respect to  $M'$ , that is there is a positive integer  $m$  such that  $mx \in M'$ . Let  $d$  be the period of  $x \bmod M'$ , so

$dx \in M'$ , and  $d$  is the least positive integer such that  $dx \in M'$ . By hypothesis, there exists an element  $u \in T$  such that  $du = f(dx)$ . For any integer  $n$ , and  $z \in M'$  define

$$f(z + nx) = f(z) + nu.$$

By the definition of  $d$ , and the fact that  $\mathbf{Z}$  is principal, one sees that this value for  $f$  is independent of the representation of an element of  $(M', x)$  in the form  $z + nx$ , and then it follows at once that this extended definition of  $f$  is a homomorphism. Thus we have extended  $f$  to  $(M', x)$ .

The rest of the proof is merely an application of Zorn's lemma. We consider pairs  $(N, g)$  consisting of submodules of  $M$  containing  $M'$ , and an extension  $g$  of  $f$  to  $N$ . We say that  $(N, g) \leq (N_1, g_1)$  if  $N \subset N_1$  and the restriction of  $g_1$  to  $N$  is  $g$ . Then such pairs are inductively ordered. Let  $(N, g)$  be a maximal element. If  $N \neq M$  then there is some  $x \in M$ ,  $x \notin N$  and we can apply the first part of the proof to extend the homomorphism to  $(N, x)$ , which contradicts the maximality, and concludes the proof of the lemma.

**Example.** The abelian groups  $\mathbf{Q}/\mathbf{Z}$  and  $\mathbf{R}/\mathbf{Z}$  are divisible, and hence are injective in the category of abelian groups.

We can prove Theorem 4.1 in the category of abelian groups following the pattern described above. If  $F$  is a free abelian group, then the dual  $F^\wedge$  is a direct product of groups isomorphic to  $\mathbf{Q}/\mathbf{Z}$ , and is therefore injective in the category of abelian groups by Lemma 4.2. This concludes the proof.

Next we must make the necessary remarks to extend the system to modules. Let  $A$  be a ring and let  $T$  be an abelian group. We make  $\text{Hom}_{\mathbf{Z}}(A, T)$  into an  $A$ -module as follows. Let  $f: A \rightarrow T$  be an abelian group homomorphism. For  $a \in A$  we define the operation

$$(af)(b) = f(ba).$$

The rules for an operation are then immediately verified. Then for any  $A$ -module  $X$  we have a natural isomorphism of abelian groups:

$$\boxed{\text{Hom}_{\mathbf{Z}}(X, T) \xrightarrow{\sim} \text{Hom}_A(X, \text{Hom}_{\mathbf{Z}}(A, T)).}$$

Indeed, let  $\psi: X \rightarrow T$  be a  $\mathbf{Z}$ -homomorphism. We associate with  $\psi$  the homomorphism

$$f: X \rightarrow \text{Hom}_{\mathbf{Z}}(A, T)$$

such that

$$f(x)(a) = \psi(ax).$$

The definition of the  $A$ -module structure on  $\text{Hom}_{\mathbf{Z}}(A, T)$  shows that  $f$  is an  $A$ -homomorphism, so we get an arrow from  $\text{Hom}_{\mathbf{Z}}(X, T)$  to

$$\text{Hom}_A(X, \text{Hom}_{\mathbf{Z}}(A, T)).$$

Conversely, let  $f: X \rightarrow \text{Hom}_{\mathbf{Z}}(A, T)$  be an  $A$ -homomorphism. We define the corresponding  $\psi$  by

$$\psi(x) = f(x)(1).$$

It is then immediately verified that these maps are inverse to each other.

We shall apply this when  $T$  is any divisible group, although we think of  $T$  as being  $\mathbf{Q}/\mathbf{Z}$ , and we think of the homomorphisms into  $T$  as representing the dual group according to the pattern described previously.

**Lemma 4.3.** *If  $T$  is a divisible abelian group, then  $\text{Hom}_{\mathbf{Z}}(A, T)$  is injective in the category of  $A$ -modules.*

*Proof.* It suffices to prove that if  $0 \rightarrow X \rightarrow Y$  is exact in the category of  $A$ -modules, then the dual sequence obtained by taking  $A$ -homomorphisms into  $\text{Hom}_{\mathbf{Z}}(A, T)$  is exact, that is the top map in the following diagram is surjective.

$$\begin{array}{ccccccc} \text{Hom}_A(Y, \text{Hom}_{\mathbf{Z}}(A, T)) & \longrightarrow & \text{Hom}_A(X, \text{Hom}_{\mathbf{Z}}(A, T)) & \xrightarrow{?} & 0 \\ \uparrow \approx & & \uparrow \approx & & \\ \text{Hom}_{\mathbf{Z}}(Y, T) & \longrightarrow & \text{Hom}_{\mathbf{Z}}(X, T) & \longrightarrow & 0 \end{array}$$

But we have the isomorphisms described before the lemma, given by the vertical arrows of the diagram, which is commutative. The bottom map is surjective because  $T$  is an injective module in the category of abelian groups. Therefore the top map is surjective, thus proving the lemma.

Now we prove Theorem 4.1 for  $A$ -modules. Let  $M$  be an  $A$ -module. We can embed  $M$  in a divisible abelian group  $T$ ,

$$0 \rightarrow M \xrightarrow{f} T.$$

Then we get an  $A$ -homomorphism

$$M \rightarrow \text{Hom}_{\mathbf{Z}}(A, T)$$

by  $x \mapsto f_x$ , where  $f_x(a) = f(ax)$ . One verifies at once that  $x \mapsto f_x$  gives an embedding of  $M$  in  $\text{Hom}_{\mathbf{Z}}(A, T)$ , which is an injective module by Lemma 4.3. This concludes the proof of Theorem 4.1.

---

## §5. HOMOTOPIES OF MORPHISMS OF COMPLEXES

The purpose of this section is to describe a condition under which homomorphisms of complexes induce the same map on the homology and to show that this condition is satisfied in an important case, from which we derive applications in the next section.

The arguments are applicable to any abelian category. The reader may prefer to think of modules, but we use a language which applies to both, and is no more complicated than if we insisted on dealing only with modules.

Let  $E = \{(E^n, d^n)\}$  and  $E' = \{(E'^n, d'^n)\}$  be two complexes. Let

$$f, g : E \rightarrow E'$$

be two morphisms of complexes (of degree 0). We say that  $f$  is **homotopic to**  $g$  if there exists a sequence of homomorphisms

$$h_n : E^n \rightarrow E'^{(n-1)}$$

such that

$$f_n - g_n = d'^{(n-1)}h_n + h_{n+1}d^n.$$

**Lemma 5.1.** *If  $f, g$  are homotopic, then  $f, g$  induce the same homomorphism on the homology  $H(E)$ , that is*

$$H(f_n) = H(g_n) : H^n(E) \rightarrow H^n(E').$$

*Proof.* The lemma is immediate, because  $f_n - g_n$  vanishes on the cycles, which are the kernel of  $d^n$ , and the homotopy condition shows that the image of  $f_n - g_n$  is contained in the boundaries, that is, in the image of  $d'^{(n-1)}$ .

**Remark.** The terminology of homotopy is used because the notion and formalism first arose in the context of topology. Cf. [ES 52] and [GreH 81].

We apply Lemma 5.1 to injective objects. Note that as usual the definition of an injective module applies without change to define an injective object in any abelian category. Instead of a submodule in **I 1**, we use a subobject, or equivalently a monomorphism. The proofs of the equivalence of the three conditions defining an injective module depended only on arrow-theoretic juggling, and apply in the general case of abelian categories.

We say that an abelian category has **enough injectives** if given any object  $M$  there exists a monomorphism

$$0 \rightarrow M \rightarrow I$$

into an injective object. We proved in §4 that the category of modules over a ring has enough injectives. *We now assume that the abelian category we work with has enough injectives.*

By an **injective resolution** of an object  $M$  one means an exact sequence

$$0 \rightarrow M \rightarrow I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow \dots$$

such that each  $I_n$  ( $n \geq 0$ ) is injective. Given  $M$ , such a resolution exists. Indeed, the monomorphism

$$0 \rightarrow M \rightarrow I^0$$

exists by hypothesis. Let  $M^0$  be its image. Again by assumption, there exists a monomorphism

$$0 \rightarrow I^0/M^0 \rightarrow I^1,$$

and the corresponding homomorphism  $I^0 \rightarrow I^1$  has kernel  $M^0$ . So we have constructed the first step of the resolution, and the next steps proceed in the same fashion.

An injective resolution is of course not unique, but it has some uniqueness which we now formulate.

**Lemma 5.2.** *Consider two complexes:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & E^2 & \longrightarrow & \dots \\ & & \downarrow \varphi & & & & & & & & & \\ 0 & \longrightarrow & M' & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & \dots \end{array}$$

*Suppose that the top row is exact, and that each  $I^n$  ( $n \geq 0$ ) is injective. Let  $\varphi : M \rightarrow M'$  be a given homomorphism. Then there exists a morphism  $f$  of complexes such that  $f_{-1} = \varphi$ ; and any two such are homotopic.*

*Proof.* By definition of an injective, the homomorphism  $M \rightarrow I^0$  via  $M'$  extends to a homomorphism

$$f_0 : E^0 \rightarrow I^0,$$

which makes the first square commute:

$$\begin{array}{ccc} M & \longrightarrow & E_0 \\ \varphi \downarrow & & \downarrow f_0 \\ M' & \longrightarrow & I^0 \end{array}$$

Next we must construct  $f_1$ . We write the second square in the form

$$\begin{array}{ccccc} 0 & \longrightarrow & E^0/M & \longrightarrow & E^1 \\ & & \downarrow f_0 & & \\ & & I^0 & \longrightarrow & I^1 \end{array}$$

with the exact top row as shown. Again because  $I^1$  is injective, we can apply the same argument and find  $f_1$  to make the second square commute. And so on, thus constructing the morphism of complexes  $f$ .

Suppose  $f, g$  are two such morphisms. We define  $h_0 : E^0 \rightarrow M'$  to be 0. Then the condition for a homotopy is satisfied in the first instance, when

$$f_{-1} = g_{-1} = \varphi.$$

Next let  $d^{-1} : M \rightarrow E^0$  be the embedding of  $M$  in  $E^0$ . Since  $I^0$  is injective, we can extend

$$d^0 : E^0 / \text{Im } d^{-1} \rightarrow E_1$$

to a homomorphism  $h_1 : E^1 \rightarrow I^0$ . Then the homotopy condition is verified for  $f_0 - g_0$ . Since  $h_0 = 0$  we actually have in this case

$$f_0 - g_0 = h_1 d^0,$$

but this simplification is misleading for the inductive step which follows. We assume constructed the map  $h_{n+1}$ , and we wish to show the existence of  $h_{n+2}$  satisfying

$$f_{n+1} - g_{n+1} = d^n h_{n+1} + h_{n+2} d^{n+1}.$$

Since  $\text{Im } d^n = \text{Ker } d^{n+1}$ , we have a monomorphism  $E^{n+1} / \text{Im } d^n \rightarrow E^{n+2}$ . By the definition of an injective object, which in this case is  $I^{n+1}$ , it suffices to prove that

$$f_{n+1} - g_{n+1} - d^n h_{n+1} \text{ vanishes on the image of } d^n,$$

and to use the exact diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & E^{n+1} / \text{Im } d^n & \longrightarrow & E^{n+2} \\ & & \downarrow f_{n+1} - g_{n+1} & & \\ & & I^{n+1} & & \end{array}$$

to get the existence of  $h_{n+2} : E^{n+2} \rightarrow I^{n+1}$  extending  $f_{n+1} - g_{n+1}$ . But we have:

$$\begin{aligned} (f_{n+1} - g_{n+1} - d^n h_{n+1}) d^n \\ = (f_{n+1} - g_{n+1}) d^n - d^n h_{n+1} d^n \end{aligned}$$

$$\begin{aligned}
 &= (f_{n+1} - g_{n+1})d^n - d'^n(f_n - g_n - d'^{n-1}h_n) && \text{by induction} \\
 &= (f_{n+1} - g_{n+1})d^n - d'^n(f_n - g_n) && \text{because } d'd' = 0 \\
 &= 0 && \text{because } f, g \text{ are} \\
 &&& \text{homomorphisms of} \\
 &&& \text{complexes.}
 \end{aligned}$$

This concludes the proof of Lemma 5.2.

**Remark.** Dually, let  $P_{M'} \rightarrow M' \rightarrow 0$  be a complex with  $P^i$  projective for  $i \geq 0$ , and let  $E_M \rightarrow M \rightarrow 0$  be a resolution. Let  $\varphi: M' \rightarrow M$  be a homomorphism. Then  $\varphi$  extends to a homomorphism of complex  $P \rightarrow E$ . The proof is obtained by reversing arrows in Lemma 5.2. The books on homological algebra that I know of in fact carry out the projective case, and leave the injective case to the reader. However, one of my motivations is to do here what is needed, for instance in [Ha 77], Chapter III, on derived functors, as a preliminary to the cohomology of sheaves. For an example of projective resolutions using free modules, see Exercises 2–7, concerning the cohomology of groups.

---

## §6. DERIVED FUNCTORS

We continue to work in an abelian category. A covariant additive functor

$$F: \mathcal{C} \rightarrow \mathcal{B}$$

is said to be **left exact** if it transforms an exact sequence

$$0 \rightarrow M' \rightarrow M \rightarrow M''$$

into an exact sequence  $0 \rightarrow F(M') \rightarrow F(M) \rightarrow F(M'')$ . We remind the reader that  $F$  is called **additive** if the map

$$\text{Hom}(A', A) \rightarrow \text{Hom}(FA', FA)$$

is additive.

*We assume throughout that  $F$  is left exact unless otherwise specified, and additive. We continue to assume that our abelian category has enough injectives.*

Given an object  $M$ , let

$$0 \rightarrow M \rightarrow I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow$$

be an injective resolution, which we abbreviate by

$$0 \rightarrow M \rightarrow I_M,$$

where  $I_M$  is the complex  $I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow$ . We let  $I$  be the complex

$$0 \rightarrow I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow$$

We define the **right-derived functor**  $R^n F$  by

$$R^n F(M) = H^n(F(I)),$$

in other words, the  $n$ -th homology of the complex

$$0 \rightarrow F(I^0) \rightarrow F(I^1) \rightarrow F(I^2) \rightarrow$$

Directly from the definitions and the monomorphism  $M \rightarrow I_0$ , we see that there is an isomorphism

$$R^0 F(M) = F(M).$$

This isomorphism seems at first to depend on the injective resolution, and so do the functors  $R^n F(M)$  for other  $n$ . However, from Lemmas 5.1 and 5.2 we see that given two injective resolutions of  $M$ , there is a homomorphism between them, and that any two homomorphisms are homotopic. If we apply the functor  $F$  to these homomorphisms and to the homotopy, then we see that the homology of the complex  $F(I)$  is in fact determined up to a unique isomorphism. One therefore omits the resolution from the notation and from the language.

**Example 1.** Let  $R$  be a ring and let  $\mathfrak{Q} = \text{Mod}(R)$  be the category of  $R$ -modules. Fix a module  $A$ . The functor  $M \mapsto \text{Hom}(A, M)$  is left exact, i.e. given an exact sequence  $0 \rightarrow M' \rightarrow M \rightarrow M''$ , the sequence

$$0 \rightarrow \text{Hom}(A, M') \rightarrow \text{Hom}(A, M) \rightarrow \text{Hom}(A, M'')$$

is exact. Its right derived functors are denoted by  $\text{Ext}^n(A, M)$  for  $M$  variable. Similarly, for a fixed module  $B$ , the functor  $X \mapsto \text{Hom}(X, B)$  is right exact, and it gives rise to its **left derived functors**. For the explicit mirror image of the terminology, see the end of this section. In any case, we may consider  $A$  as variable. In §8 we shall go more deeply into this aspect of the formalism, by dealing with bifunctors. It will turn out that  $\text{Ext}^n(A, B)$  has a dual interpretation as a left derived functor of the first variable and right derived functor of the second variable. See Corollary 8.5.

In the exercises, you will prove that  $\text{Ext}^1(A, M)$  is in bijection with isomorphism classes of extensions, of  $M$  by  $A$ , that is, isomorphism classes of exact sequences

$$0 \rightarrow A \rightarrow E \rightarrow M \rightarrow 0.$$

The name  $\text{Ext}$  comes from this interpretation in dimension 1.

For the computation of  $\text{Ext}^i$  in certain important cases, see Chapter XXI, Theorems 4.6 and 4.11, which serve as examples for the general theory.

**Example 2.** Let  $R$  be commutative. The functor  $M \mapsto A \otimes M$  is right exact, in other words, the sequence

$$A \otimes M' \rightarrow A \otimes M \rightarrow A \otimes M'' \rightarrow 0$$

is exact. Its left derived functors are denoted by  $\text{Tor}_n(A, M)$  for  $M$  variable.

**Example 3.** Let  $G$  be a group and let  $R = \mathbf{Z}[G]$  be the group ring. Let  $\mathbf{G}$  be the category of  $G$ -modules, i.e.  $\mathbf{G} = \text{Mod}(R)$ , also denoted by  $\text{Mod}(G)$ . For a  $G$ -module  $A$ , let  $A^G$  be the submodule (abelian group) consisting of those elements  $v$  such that  $xv = v$  for all  $x \in G$ . Then  $A \mapsto A^G$  is a left exact functor from  $\text{Mod}(R)$  into the category of abelian groups. Its left derived functors give rise to the cohomology of groups. Some results from this special cohomology will be carried out in the exercises, as further examples of the general theory.

**Example 4.** Let  $X$  be a topological space (we assume the reader knows what this is). By a **sheaf**  $\mathbf{F}$  of abelian groups on  $X$ , we mean the data:

- (a) For every open set  $U$  of  $X$  there is given an abelian group  $\mathbf{F}(U)$ .
- (b) For every inclusion  $V \subset U$  of open sets there is given a homomorphism

$$\text{res}_V^U : \mathbf{F}(U) \rightarrow \mathbf{F}(V),$$

called the **restriction** from  $U$  to  $V$ , subject to the following conditions:

**SH 1.**  $\mathbf{F}(\text{empty set}) = 0$ .

**SH 2.**  $\text{res}_U^U$  is the identity  $\mathbf{F}(U) \rightarrow \mathbf{F}(U)$ .

**SH 3.** If  $W \subset V \subset U$  are open sets, then  $\text{res}_W^V \circ \text{res}_V^U = \text{res}_W^U$ .

**SH 4.** Let  $U$  be an open set and  $\{V_i\}$  be an open covering of  $U$ . Let  $s \in \mathbf{F}(U)$ . If the restriction of  $s$  to each  $V_i$  is 0, then  $s = 0$ .

**SH 5.** Let  $U$  be an open set and let  $\{V_i\}$  be an open covering of  $U$ . Suppose given  $s_i \in \mathbf{F}(V_i)$  for each  $i$ , such that given  $i, j$  the restrictions of  $s_i$  and  $s_j$  to  $V_i \cap V_j$  are equal. Then there exists a unique  $s \in \mathbf{F}(U)$  whose restriction to  $V_i$  is  $s_i$  for all  $i$ .

Elements of  $\mathbf{F}(U)$  are called **sections** of  $\mathbf{F}$  over  $U$ . Elements of  $\mathbf{F}(X)$  are called **global sections**. Just as for abelian groups, it is possible to define the notion of homomorphisms of sheaves, kernels, cokernels, and exact sequences. The association  $\mathbf{F} \mapsto \mathbf{F}(X)$  (global sections functor) is a functor from the category of sheaves of abelian groups to abelian groups, and this functor is left exact. Its right derived functors are the basis of cohomology theory in topology and algebraic geometry (among other fields of mathematics). The reader will find a self-contained brief definition of the basic properties in [Ha 77], Chapter II, §1, as well as a proof that these form an abelian category. For a more extensive treatment I recommend Gunning's [Gu 91], mentioned in the introduction to Part IV, notably Volume III, dealing with the cohomology of sheaves.

We now return to the general theory of derived functors. The general theory tells us that these derived functors do not depend on the resolution by projectives or injectives according to the variance. As we shall also see in §8, one can even use other special types of objects such as acyclic or exact (to be defined), which gives even more flexibility in the ways one has to compute homology. Through certain explicit resolutions, we obtain means of computing the derived functors

explicitly. For example, in Exercise 16, you will see that the cohomology of finite cyclic groups can be computed immediately by exhibiting a specific free resolution of  $\mathbf{Z}$  adapted to such groups. Chapter XXI will contain several other examples which show how to construct explicit finite resolutions, which allow the determination of derived functors in various contexts.

The next theorem summarizes the basic properties of derived functors.

**Theorem 6.1.** *Let  $\mathfrak{A}$  be an abelian category with enough injectives, and let  $F : \mathfrak{A} \rightarrow \mathfrak{B}$  be a covariant additive left exact functor to another abelian category  $\mathfrak{B}$ . Then:*

- (i) *For each  $n \geq 0$ ,  $R^n F$  as defined above is an additive functor from  $\mathfrak{A}$  to  $\mathfrak{B}$ . Furthermore, it is independent, up to a unique isomorphism of functors, of the choices of resolutions made.*
- (ii) *There is a natural isomorphism  $F \approx R^0 F$ .*
- (iii) *For each short exact sequence*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

*and for each  $n \geq 0$  there is a natural homomorphism*

$$\delta^n : R^n F(M'') \rightarrow R^{n+1} F(M)$$

*such that we obtain a long exact sequence:*

$$\rightarrow R^n F(M') \rightarrow R^n F(M) \rightarrow R^n F(M'') \xrightarrow{\delta^n} R^{n+1} F(M') \rightarrow \dots$$

- (iv) *Given a morphism of short exact sequences*

$$\begin{array}{ccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' \longrightarrow 0 \end{array}$$

*the  $\delta$ 's give a commutative diagram:*

$$\begin{array}{ccc} R^n F(M'') & \xrightarrow{\delta^n} & R^{n+1} F(M') \\ \downarrow & & \downarrow \\ R^n F(N'') & \xrightarrow{\delta^n} & R^{n+1} F(N') \end{array}$$

- (v) *For each injective object  $I$  of  $\mathfrak{A}$  and for each  $n > 0$  we have  $R^n F(I) = 0$ .*

Properties (i), (ii), (iii), and (iv) essentially say that  $R^n F$  is a delta-functor in a sense which will be expanded in the next section. The last property (v) will be discussed after we deal with the delta-functor part of the theorem.

We now describe how to construct the  $\delta$ -homomorphisms. Given a short exact sequence, we can find an injective resolution of  $M'$ ,  $M$ ,  $M''$  separately, but they don't necessarily fit in an exact sequence of complexes. So we must achieve this to apply the considerations of §1. Consider the diagram:

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & I'^0 & \longrightarrow & X & \longrightarrow & I''^0 \longrightarrow 0.
 \end{array}$$

We give monomorphisms  $M' \rightarrow I'^0$  and  $M'' \rightarrow I''^0$  into injectives, and we want to find  $X$  injective with a monomorphism  $M \rightarrow X$  such that the diagram is exact. We take  $X$  to be the direct sum

$$X = I'^0 \oplus I''^0.$$

Since  $I'^0$  is injective, the monomorphism  $M' \rightarrow I'^0$  can be extended to a homomorphism  $M \rightarrow I'^0$ . We take the homomorphism of  $M$  into  $I'^0 \oplus I''^0$  which comes from this extension on the first factor  $I'^0$ , and is the composite map

$$M \rightarrow M'' \rightarrow I''^0$$

on the second factor. Then  $M \rightarrow X$  is a monomorphism. Furthermore  $I'^0 \rightarrow X$  is the monomorphism on the first factor, and  $X \rightarrow I''^0$  is the projection on the second factor. So we have constructed the diagram we wanted, giving the beginning of the compatible resolutions.

Now we take the quotient homomorphism, defining the third row, to get an exact diagram:

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & I'^0 & \longrightarrow & I^0 & \longrightarrow & I''^0 \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & N' & \longrightarrow & N & \longrightarrow & N'' \longrightarrow 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
 \end{array}$$

where we let  $I^0 = X$ , and  $N', N, N''$  are the cokernels of the vertical maps by definition. The exactness of the  $N$ -sequence is left as an exercise to the reader. We then repeat the construction with the  $N$ -sequence, and by induction construct injective resolutions

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & I'_{M'} & \longrightarrow & I_M & \longrightarrow & I''_{M''} \longrightarrow 0
 \end{array}$$

of the  $M$ -sequence such that the diagram of the resolutions is exact.

We now apply the functor  $F$  to this diagram. We obtain a short sequence of complexes:

$$0 \rightarrow F(I') \rightarrow F(I) \rightarrow F(I'') \rightarrow 0,$$

which is exact because  $I = I' \oplus I''$  is a direct sum and  $F$  is left exact, so  $F$  commutes with direct sums. We are now in a position to apply the construction of §1 to get the coboundary operator in the homology sequence:

$$R^n F(M') \rightarrow R^n F(M) \rightarrow R^n F(M'') \xrightarrow{\delta^n} R^{n+1} F(M').$$

This is legitimate because the right derived functor is independent of the chosen resolutions.

So far, we have proved (i), (ii), and (iii). To prove (iv), that is the naturality of the delta homomorphisms, it is necessary to go through a three-dimensional commutative diagram. At this point, I feel it is best to leave this to the reader, since it is just more of the same routine.

Finally, the last property (v) is obvious, for if  $I$  is injective, then we can use the resolution

$$0 \rightarrow I \rightarrow I \rightarrow 0$$

to compute the derived functors, from which it is clear that  $R^n F = 0$  for  $n > 0$ .

This concludes the proof of Theorem 6.1.

In applications, it is useful to determine the derived functors by means of other resolutions besides injective ones (which are useful for theoretical purposes, but not for computational ones). Let again  $F$  be a left exact additive functor. An object  $X$  is called  **$F$ -acyclic** if  $R^n F(X) = 0$  for all  $n > 0$ .

**Theorem 6.2.** *Let*

$$0 \rightarrow M \rightarrow X^0 \rightarrow X^1 \rightarrow X^2 \rightarrow \cdots$$

*be a resolution of  $M$  by  $F$ -acyclics. Let*

$$0 \rightarrow M \rightarrow I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow \cdots$$

*be an injective resolution. Then there exists a morphism of complexes  $X_M \rightarrow I_M$  extending the identity on  $M$ , and this morphism induces an isomorphism*

$$H^n F(X) \approx H^n F(I) = R^n F(M) \quad \text{for all } n \geq 0.$$

*Proof.* The existence of the morphism of complexes extending the identity on  $M$  is merely Lemma 5.2. The usual proof of the theorem via spectral sequences can be formulated independently in the following manner, shown to me by David Benson. We need a lemma.

**Lemma 6.3.** *Let  $Y^i$  ( $i \geq 0$ ) be  $F$ -acyclic, and suppose the sequence*

$$0 \rightarrow Y^0 \rightarrow Y^1 \rightarrow Y^2 \rightarrow \cdots$$

*is exact. Then*

$$0 \rightarrow F(Y^0) \rightarrow F(Y^1) \rightarrow F(Y^2) \rightarrow \cdots$$

*is exact.*

*Proof.* Since  $F$  is left exact, we have an exact sequence

$$0 \rightarrow F(Y^0) \rightarrow F(Y^1) \rightarrow F(Y^2).$$

We want to show exactness at the next joint. We draw the cokernels:

$$\begin{array}{ccccccc}
 0 & \longrightarrow & Y^0 & \longrightarrow & Y^1 & \longrightarrow & Y^2 & \longrightarrow & Y^3 \\
 & & \searrow & \nearrow & \searrow & \nearrow & \searrow & \nearrow & \searrow \\
 & & & Z^1 & & Z^2 & & & \\
 & & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0
 \end{array}$$

So  $Z_1 = \text{Coker}(Y^0 \rightarrow Y^1)$ ;  $Z_2 = \text{Coker}(Y^1 \rightarrow Y^2)$ ; etc. Applying  $F$  we have an exact sequence

$$0 \rightarrow F(Y^0) \rightarrow F(Y^1) \rightarrow F(Z^1) \rightarrow R^1 F(Y^0) = 0.$$

So  $F(Z_1) = \text{Coker}(F(Y^0) \rightarrow F(Y^1))$ . We now consider the exact sequence

$$0 \rightarrow Z_1 \rightarrow Y_2 \rightarrow Y_3$$

giving the exact sequence

$$0 \rightarrow F(Z^1) \rightarrow F(Y^2) \rightarrow F(Y^3)$$

by the left-exactness of  $F$ , and proving what we wanted. But we can now continue by induction because  $Z_1$  is  $F$ -acyclic, by the exact sequence

$$0 \rightarrow R^n F(Y^1) \rightarrow R^n F(Z^1) \rightarrow R^{n+1} F(Y^0) = 0.$$

This concludes the proof of Lemma 6.3.

We return to the proof of Theorem 6.2. The injective resolution

$$0 \rightarrow M \rightarrow I_M$$

can be chosen such that the homomorphisms  $X_n \rightarrow I_n$  are monomorphisms for  $n \geq 0$ , because the derived functor is independent of the choice of injective resolution. Thus we may assume without loss of generality that we have an exact diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & M & \longrightarrow & X^0 & \longrightarrow & X^1 & \longrightarrow & X^2 & \longrightarrow & \cdots \\
 & & \downarrow \text{id} & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & M & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & I^2 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & Y^0 & \longrightarrow & Y^1 & \longrightarrow & Y^2 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
 \end{array}$$

defining  $Y^n$  as the appropriate cokernel of the vertical map.

Since  $X^n$  and  $I^n$  are acyclic, so is  $Y^n$  from the exact sequence

$$R^k F(I^n) \rightarrow R^k F(Y^n) \rightarrow R^{k+1} F(X^n).$$

Applying  $F$  we obtain a short exact sequence of complexes

$$0 \rightarrow F(X) \rightarrow F(I) \rightarrow F(Y) \rightarrow 0.$$

whence the corresponding homology sequence

$$H^{n-1}F(Y) \rightarrow H^nF(X) \rightarrow H^nF(I) \rightarrow H^nF(Y).$$

Both extremes are 0 by Lemma 6.3, so we get an isomorphism in the middle, which by definition is the isomorphism

$$H^nF(X) \approx R^nF(M),$$

thus proving the theorem.

### Left derived functors

We conclude this section by a summary of the properties of left derived functors.

We consider complexes going the other way,

$$\rightarrow X_n \rightarrow \cdots \rightarrow X_2 \rightarrow X_1 \rightarrow X_0 \rightarrow M \rightarrow 0$$

which we abbreviate by

$$X_M \rightarrow M \rightarrow 0.$$

We call such a complex a **resolution** of  $M$  if the sequence is exact. We call it a **projective resolution** if  $X_n$  is projective for all  $n \geq 0$ .

Given projective resolutions  $X_M$ ,  $Y_{M'}$  and a homomorphism

$$\varphi : M \rightarrow M'$$

there always exists a homomorphism  $X_M \rightarrow Y_{M'}$  extending  $\varphi$ , and any two such are homotopic.

In fact, one need only assume that  $X_M$  is a projective resolution, and that  $Y_{M'}$  is a resolution, not necessarily projective, for the proof to go through.

Let  $T$  be a covariant additive functor. Fix a projective resolution of an object  $M$ ,

$$P_M \rightarrow M \rightarrow 0.$$

We define the **left derived functor**  $L_n T$  by

$$L_n T(M) = H_n(T(P)),$$

where  $T(P)$  is the complex

$$\rightarrow T(P_n) \rightarrow \cdots \rightarrow T(P_2) \rightarrow T(P_1) \rightarrow T(P_0) \rightarrow 0.$$

The existence of homotopies shows that  $L_n T(M)$  is uniquely determined up to a unique isomorphism if one changes the projective resolution.

We define  $T$  to be **right exact** if an exact sequence

$$M' \rightarrow M \rightarrow M'' \rightarrow 0$$

yields an exact sequence

$$T(M') \rightarrow T(M) \rightarrow T(M'') \rightarrow 0.$$

If  $T$  is right exact, then we have immediately from the definitions

$$L_0 T(M) \approx M.$$

Theorems 6.1 and 6.2 then go over to this case with similar proofs. One has to replace “injectives” by “projectives” throughout, and in Theorem 6.1, the last condition states that for  $n > 0$ ,

$$L_n T(P) = 0 \quad \text{if } P \text{ is projective.}$$

Otherwise, it is just a question of reversing certain arrows in the proofs. For an example of such left derived functors, see Exercises 2–7 concerning the cohomology of groups.

## §7. DELTA-FUNCTORS

In this section, we axiomatize the properties stated in Theorem 6.1 following Grothendieck.

Let  $\mathfrak{A}, \mathfrak{B}$  be abelian categories. A (covariant)  **$\delta$ -functor** from  $\mathfrak{A}$  to  $\mathfrak{B}$  is a family of additive functors  $F = \{F_n\}_{n \geq 0}$ , and to each short exact sequence

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

an associated family of morphisms

$$\delta^n: F^n(M'') \rightarrow F^{n+1}(M')$$

with  $n \geq 0$ , satisfying the following conditions:

**DEL 1.** For each short exact sequence as above, there is a long exact sequence

$$\begin{aligned} 0 \rightarrow F^0(M') &\rightarrow F^0(M) \rightarrow F^0(M'') \rightarrow F^1(M') \rightarrow \dots \\ &\rightarrow F^n(M') \rightarrow F^n(M) \rightarrow F^n(M'') \rightarrow F^{n+1}(M') \rightarrow \end{aligned}$$

**DEL 2.** For each morphism of one short exact sequence as above into another  $0 \rightarrow N' \rightarrow N \rightarrow N'' \rightarrow 0$ , the  $\delta$ 's give a commutative diagram:

$$\begin{array}{ccc} F^n(M'') & \xrightarrow{\delta} & F^{n+1}(M') \\ \downarrow & & \downarrow \\ F^n(N'') & \xrightarrow{\delta} & F^{n+1}(N'). \end{array}$$

Before going any further, it is useful to give another definition. Many proofs in homology theory are given by induction from one index to the next. It turns out that the only relevant data for going up by one index is given in two successive dimensions, and that the other indices are irrelevant. Therefore we generalize the notion of  $\delta$ -functor as follows.

A  **$\delta$ -functor defined in degrees 0, 1** is a pair of functors  $(F^0, F^1)$  and to each short exact sequence

$$0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$$

an associated morphism

$$\delta : F^0(A'') \rightarrow F^1(A'')$$

satisfying the two conditions as before, but putting  $n = 0, n + 1 = 1$ , and forgetting about all other integers  $n$ . We could also use any two consecutive positive integers to index the  $\delta$ -functor, or any sequence of consecutive integers  $\geq 0$ . In practice, only the case of all integers  $\geq 0$  occurs, but for proofs, it is useful to have the flexibility provided by using only two indices, say 0, 1.

The  $\delta$ -functor  $F$  is said to be **universal**, if given any other  $\delta$ -functor  $G$  of  $\mathfrak{Q}$  into  $\mathfrak{G}$ , and given any morphism of functors

$$f_0 : F^0 \rightarrow G^0,$$

there exists a unique sequence of morphisms

$$f_n : F^n \rightarrow G^n$$

for all  $n \geq 0$ , which commute with the  $\delta^n$  for each short exact sequence.

By the definition of universality, a  $\delta$ -functor  $G$  such that  $G^0 = F^0$  is uniquely determined up to a unique isomorphism of functors. We shall give a condition for a functor to be universal.

An additive functor  $F$  of  $\mathfrak{Q}$  into  $\mathfrak{G}$  is called **erasable** if to each object  $A$  there exists a monomorphism  $u : A \rightarrow M$  for some  $M$  such that  $F(u) = 0$ . In practice, it even happens that  $F(M) = 0$ , but we don't need it in the axiomatization.

**Linguistic note.** Grothendieck originally called the notion “effaceable” in French. The dictionary translation is “erasable,” as I have used above. Apparently people who did not know French have used the French word in English, but there is no need for this, since the English word is equally meaningful and convenient.

We say the functor is erasable by **injectives** if in addition  $M$  can be taken to be injective.

**Example.** Of course, a right derived functor is erasable by injectives, and a left derived functor by projectives. However, there are many cases when one wants erasability by other types of objects. In Exercises 9 and 14, dealing with the cohomology of groups, you will see how one erases the cohomology functor with induced modules, or regular modules when  $G$  is finite. In the category of coherent sheaves in algebraic geometry, one erases the cohomology with locally free sheaves of finite rank.

**Theorem 7.1.** *Let  $F = \{F^n\}$  be a covariant  $\delta$ -functor from  $\mathfrak{Q}$  into  $\mathfrak{G}$ . If  $F^n$  is erasable for each  $n > 0$ , then  $F$  is universal.*

*Proof.* Given an object  $A$ , we erase it with a monomorphism  $u$ , and get a short exact sequence:

$$0 \rightarrow A \xrightarrow{\varphi} M \rightarrow X \rightarrow 0.$$

Let  $G$  be another  $\delta$ -functor with given  $f_0: F^0 \rightarrow G^0$ . We have an exact commutative diagram

$$\begin{array}{ccccccc} F^0(M) & \longrightarrow & F^0(X) & \xrightarrow{\delta'} & F^1(A) & \longrightarrow & 0 \\ f_0 \downarrow & & f_0 \downarrow & & \downarrow f_1? & & \\ G^0(M) & \longrightarrow & G^0(X) & \xrightarrow{\delta_G} & G^1(A) & & \end{array}$$

We get the 0 on the top right because of the erasability assumption that

$$F^1(\varphi) = 0.$$

We want to construct

$$f_1(A): F^1(A) \rightarrow G^1(A)$$

which makes the diagram commutative, is functorial in  $A$ , and also commutes with the  $\delta$ . Commutativity in the left square shows that  $\text{Ker } \delta_F$  is contained in the kernel of  $\delta_G \circ f_0$ . Hence there exists a unique homomorphism

$$f_1(A): F^1(A) \rightarrow G^1(A)$$

which makes the right square commutative. We are going to show that  $f_1(A)$  satisfies the desired conditions. The rest of the proof then proceeds by induction following the same pattern.

We first prove the functoriality in  $A$ .

Let  $u: A \rightarrow B$  be a morphism. We form the push-out  $P$  in the diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & M \\ u \downarrow & & \downarrow \\ B & \longrightarrow & P \end{array}$$

Since  $\varphi$  is a monomorphism, it follows that  $B \rightarrow P$  is a monomorphism also. Then we let  $P \rightarrow N$  be a monomorphism which erases  $F_1$ . This yields a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & M & \longrightarrow & X & \longrightarrow 0 \\ & & \downarrow u & & \downarrow v & & \downarrow w & \\ 0 & \longrightarrow & B & \longrightarrow & N & \longrightarrow & Y & \longrightarrow 0 \end{array}$$

where  $B \rightarrow N$  is the composite  $B \rightarrow P \rightarrow N$ , and  $Y$  is defined to be the cokernel of  $B \rightarrow N$ .

Functoriality in  $A$  means that the following diagram is commutative.

$$\begin{array}{ccc} F^1(A) & \xrightarrow{F^1(u)} & F^1(B) \\ \downarrow f_1(A) & & \downarrow f_1(B) \\ G^1(A) & \xrightarrow{F^1(u)} & G^1(B) \end{array}$$

This square is the right-hand side of the following cube:

$$\begin{array}{ccccc} & & \delta_F & & \\ & F^0(X) & \xrightarrow{\hspace{2cm}} & F^1(A) & \\ & \downarrow f_0(X) & \searrow F^0(w) & \downarrow & \searrow F^1(u) \\ & F^0(Y) & \xrightarrow{\hspace{2cm}} & F^1(B) & \\ & \downarrow & \downarrow \delta_F & \downarrow & \downarrow \\ & G^0(X) & \xrightarrow{\hspace{2cm}} & G^1(A) & \\ & \downarrow G^0(w) & \searrow \delta_G & \downarrow & \searrow G^1(u) \\ & G^0(Y) & \xrightarrow{\hspace{2cm}} & G^1(B) & \end{array}$$

All the faces of the cube are commutative except possibly the right-hand face. It is then a general fact that if the top maps here denoted by  $\delta_F$  are epimorphisms,

then the right-hand side is commutative also. This can be seen as follows. We start with  $f_1(B)F^1(u)\delta_F$ . We then use commutativity on the top of the cube, then the front face, then the left face, then the bottom, and finally the back face. This yields

$$f_1(B)F^1(u)\delta_F = G^1(u)f_1(A)\delta_F.$$

Since  $\delta_F$  is an epimorphism, we can cancel  $\delta_F$  to get what we want.

Second, we have to show that  $f_1$  commutes with  $\delta$ . Let

$$0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$$

be a short exact sequence. The same push-out argument as before shows that there exists an erasing monomorphism  $0 \rightarrow A' \rightarrow M$  and morphisms  $v, w$  making the following diagram commutative:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' \longrightarrow 0 \\ & & \downarrow \text{id} & & \downarrow v & & \downarrow w \\ 0 & \longrightarrow & A' & \longrightarrow & M & \longrightarrow & X \longrightarrow 0 \end{array}$$

Here  $X$  is defined as the appropriate cokernel of the bottom row. We now consider the following diagram:

$$\begin{array}{ccccc} & & F^0(A'') & & \\ & \swarrow & \downarrow f_0 & \searrow & \\ F^0(w) & & G^0(A'') & & \delta_F \\ \searrow & \downarrow \delta_F & \swarrow & \searrow & \\ F^0(X) & \xrightarrow{\delta_G} & F^1(A') & \xrightarrow{f_1(A')} & \\ \downarrow f_0 & \swarrow G^0(w) & \downarrow \delta_G & \searrow & \\ G^0(X) & \xrightarrow{\delta_G} & G^1(A') & & \end{array}$$

Our purpose is to prove that the right-hand face is commutative. The triangles on top and bottom are commutative by the definition of a  $\delta$ -functor. The

left-hand square is commutative by the hypothesis that  $f_0$  is a morphism of functors. The front square is commutative by the definition of  $f_1(A')$ . Therefore we find:

$$\begin{aligned} f_1(A')\delta_F &= f_1(A')\delta_F F^0(w) && \text{(top triangle)} \\ &= \delta_F f_0 F^0(w) && \text{(front square)} \\ &= \delta_F G^0(w)f_0 && \text{(left square)} \\ &= \delta_F f_0 && \text{(bottom triangle).} \end{aligned}$$

This concludes the proof of Theorem 7.1, since instead of the pair of indices  $(0, 1)$  we could have used  $(n, n + 1)$ .

**Remark.** The morphism  $f_1$  constructed in Theorem 7.1 depends functorially on  $f_0$  in the following sense. Suppose we have three delta functors  $F, G, H$  defined in degrees 0, 1. Suppose given morphisms

$$f_0 : F^0 \rightarrow G^0 \quad \text{and} \quad g_0 : G^0 \rightarrow H^0.$$

Suppose that the erasing monomorphisms erase both  $F$  and  $G$ . Then we can construct  $f_1$  and  $g_1$  by applying the theorem. On the other hand, the composite

$$g_0 f_0 = h_0 : F^0 \rightarrow H^0$$

is also a morphism of functors, and the theorem yields the existence of a morphism

$$h_1 : F^1 \rightarrow H^1$$

such that  $(h_0, h_1)$  is a  $\delta$ -morphism. By uniqueness, we therefore have

$$h_1 = g_1 f_1.$$

This is what we mean by the functorial dependence as mentioned above.

**Corollary 7.2.** *Assume that  $\mathfrak{Q}$  has enough injectives. Then for any left exact functor  $F : \mathfrak{Q} \rightarrow \mathfrak{G}$ , the derived functors  $R^n F$  with  $n \geq 0$  form a universal  $\delta$ -functor with  $F \approx R^0 F$ , which is erasable by injectives. Conversely, if  $G = \{G^n\}_{n \geq 0}$  is a universal  $\delta$ -functor, then  $G^0$  is left exact, and the  $G^n$  are isomorphic to  $R^n G^0$  for each  $n \geq 0$ .*

*Proof.* If  $F$  is a left exact functor, then the  $\{R^n F\}_{n \geq 0}$  form a  $\delta$ -functor by Theorem 6.1. Furthermore, for any object  $A$ , let  $u : A \rightarrow I$  be a monomorphism of  $A$  into an injective. Then  $R^n F(I) = 0$  for  $n > 0$  by Theorem 6.1(iv), so  $R^n F(u) = 0$ . Hence  $R^n F$  is erasable for all  $n > 0$ , and we can apply Theorem 7.1.

**Remark.** As usual, Theorem 7.1 applies to functors with different variance. Suppose  $\{F^n\}$  is a family of contravariant additive functors, with  $n$  ranging over

a sequence of consecutive integers, say for simplicity  $n \geq 0$ . We say that  $F$  is a **contravariant  $\delta$ -functor** if given an exact sequence

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

then there is an associated family of morphisms

$$\delta^n : F^n(M') \rightarrow F^{n+1}(M'')$$

satisfying **DEL 1** and **DEL 2** with  $M'$  interchanged with  $M''$  and  $N'$  interchanged with  $N''$ . We say that  $F$  is **coerasable** if to each object  $A$  there exists an epimorphism  $u : M \rightarrow A$  such that  $F(u) = 0$ . We say that  $F$  is **universal** if given any other  $\delta$ -functor  $G$  of  $\mathfrak{Q}$  into  $\mathfrak{G}$  and given a morphism of functors

$$f_0 : F^0 \rightarrow G^0$$

there exists a unique sequence of morphisms

$$f_n : F^n \rightarrow G^n$$

for all  $n \geq 0$  which commute with  $\delta$  for each short exact sequence.

**Theorem 7.1'.** *Let  $F = \{F^n\}$  ( $n$  ranging over a consecutive sequence of integers  $\geq 0$ ) be a contravariant  $\delta$ -functor from  $\mathfrak{Q}$  into  $\mathfrak{G}$ , and assume that  $F^n$  is coerasable for  $n \geq 1$ . Then  $F$  is universal.*

Examples of  $\delta$ -functors with the variances as in Theorems 7.1 and 7.1' will be given in the next section in connection with bifunctors.

### Dimension shifting

Let  $F = \{F^n\}$  be a contravariant delta functor with  $n \geq 0$ . Let  $\mathfrak{E}$  be a family of objects which erases  $F^n$  for all  $n \geq 1$ , that is  $F^n(E) = 0$  for  $n \geq 1$  and  $E \in \mathfrak{E}$ . Then such a family allows us to do what is called **dimension shifting** as follows. Given an exact sequence

$$0 \rightarrow Q \rightarrow E \rightarrow M \rightarrow 0$$

with  $E \in \mathfrak{E}$ , we get for  $n \geq 1$  an exact sequence

$$0 = F^n(E) \rightarrow F^n(Q) \rightarrow F^{n+1}(M) \rightarrow F^{n+1}(E) = 0,$$

and therefore an isomorphism

$$F^n(Q) \xrightarrow{\sim} F^{n+1}(M),$$

which exhibits a shift of dimensions by one. More generally:

**Proposition 7.3.** *Let*

$$0 \rightarrow Q \rightarrow E_{n-1} \rightarrow \cdots \rightarrow E_0 \rightarrow M \rightarrow 0$$

be an exact sequence, such that  $E_i \in \mathcal{E}$ . Then we have an isomorphism

$$F^p(Q) \approx F^{p+n}(M) \quad \text{for } p \geq 1.$$

*Proof.* Let  $Q = Q_n$ . Also without loss of generality, take  $p = 1$ . We may insert kernels and cokernels at each step as follows:

$$\begin{array}{ccccccc}
 & E_{n-1} & \longrightarrow & E_{n-2} & \longrightarrow & \cdots & \longrightarrow E_0 \\
 \nearrow & \downarrow & & \nearrow & \downarrow & & \nearrow \\
 Q_n & & Q_{n-1} & & Q_{n-2} & & Q_1 \\
 \nearrow & \downarrow & \nearrow & \downarrow & \nearrow & \downarrow & \nearrow \\
 0 & & 0 & & 0 & & 0 \cdots 0 \\
 & \nearrow & \downarrow & \nearrow & \downarrow & & \nearrow \\
 & & & & & M & \\
 & & & & & \downarrow & \\
 & & & & & & 0
 \end{array}$$

Then shifting dimension with respect to each short exact sequence, we find isomorphisms

$$F^1(Q_n) \approx F^2(Q_{n-1}) \approx \cdots \approx F^{n+1}(M).$$

This concludes the proof.

One says that  $M$  has  **$F$ -dimension**  $\leq d$  if  $F^n(M) = 0$  for  $n \geq d + 1$ . By dimension shifting, we see that if  $M$  has  $F$ -dimension  $\leq d$ , then  $Q$  has  $F$ -dimension  $\leq d - n$  in Proposition 7.3. In particular, if  $M$  has  $F$ -dimension  $n$ , then  $Q$  has  $F$ -dimension 0.

The reader should rewrite all this formalism by changing notation, using for  $F$  the standard functors arising from  $\text{Hom}$  in the first variable, on the category of modules over a ring, which has enough projectives to erase the left derived functors of

$$A \mapsto \text{Hom}(A, B),$$

for  $B$  fixed. We shall study this situation, suitably axiomatized, in the next section.

## §8. BIFUNCTORS

In an abelian category one often deals with  $\text{Hom}$ , which can be viewed as a functor in two variables; and also the tensor product, which is a functor in two variables, but their variance is different. In any case, these examples lead to the notion of **bifunctor**. This is an association

$$(A, B) \mapsto T(A, B)$$

where  $A, B$  are objects of abelian categories  $\mathfrak{Q}$  and  $\mathfrak{G}$  respectively, with values in some abelian category. This means that  $T$  is functorial in each variable, with the appropriate variance (there are four possibilities, with covariance and contravariance in all possible combinations); and if, say,  $T$  is covariant in all variables, we also require that for homomorphisms  $A' \rightarrow A$  and  $B' \rightarrow B$  there is a commutative diagram

$$\begin{array}{ccc} T(A', B') & \longrightarrow & T(A', B) \\ \downarrow & & \downarrow \\ T(A, B') & \longrightarrow & T(A, B). \end{array}$$

If the variances are shuffled, then the arrows in the diagram are to be reversed in the appropriate manner. Finally, we require that as a functor in each variable,  $T$  is additive.

Note that  $\text{Hom}$  is a bifunctor, contravariant in the first variable and covariant in the second. The tensor product is covariant in each variable.

The  $\text{Hom}$  functor is a bifunctor  $T$  satisfying the following properties:

**HOM 1.**  *$T$  is contravariant and left exact in the first variable.*

**HOM 2.**  *$T$  is covariant and left exact in the second variable.*

**HOM 3.** *For any injective object  $J$  the functor*

$$A \mapsto T(A, J)$$

*is exact.*

They are the only properties which will enter into consideration in this section. There is a possible fourth one which might come in other times:

**HOM 4.** *For any projective object  $Q$  the functor*

$$B \mapsto T(Q, B)$$

*is exact.*

But we shall deal *non-symmetrically*, and view  $T$  as a functor of the second variable, keeping the first one fixed, in order to get derived functors of the second variable. On the other hand, we shall also obtain a  $\delta$ -functor of the first variable by using the bifunctor, even though this  $\delta$ -functor is not a derived functor.

If  $\mathfrak{G}$  has enough injectives, then we may form the right derived functors with respect to the second variable

$$B \mapsto R^n T(A, B), \quad \text{also denoted by } R^n T_A(B),$$

fixing  $A$ , and viewing  $B$  as variable. If  $T = \text{Hom}$ , then this right derived functor is called **Ext**, so we have by definition

$$\text{Ext}^n(A, X) = R^n \text{Hom}(A, X).$$

We shall now give a criterion to compute the right derived functors in terms of the other (first) variable. We say that an object  $A$  is  **$T$ -exact** if the functor  $B \mapsto T(A, B)$  is exact. By a  **$T$ -exact resolution** of an object  $A$ , we mean a resolution

$$\rightarrow M_1 \rightarrow M_0 \rightarrow A \rightarrow 0$$

where  $M_n$  is  $T$ -exact for all  $n \geq 0$ .

**Examples.** Let  $\mathfrak{Q}$  and  $\mathfrak{G}$  be the categories of modules over a commutative ring. Let  $T = \text{Hom}$ . Then a  $T$ -exact object is by definition a projective module. Now let the **transpose** of  $T$  be given by

$${}^t T(A, B) = T(B, A).$$

Then a  ${}^t T$ -exact object is by definition an injective module.

If  $T$  is the tensor product, such that  $T(A, B) = A \otimes B$ , then a  $T$ -exact object is called **flat**.

**Remark.** In the category of modules over a ring, there are enough projectives and injectives. But there are other situations when this is not the case. Readers who want to see all this abstract nonsense in action may consult [GriH 78], [Ha 77], not to speak of [SGA 6] and Grothendieck's collected works. It may genuinely happen in practice that  $\mathfrak{G}$  has enough injectives but  $\mathfrak{Q}$  does not have enough projectives, so the situation is not all symmetric. Thus the functor  $A \mapsto R^n T(A, B)$  for fixed  $B$  is *not* a derived functor in the variable  $A$ . In the above references, we may take for  $\mathfrak{Q}$  the category of coherent sheaves on a variety, and for  $\mathfrak{G}$  the category of all sheaves. We let  $T = \text{Hom}$ . The locally free sheaves of finite rank are  $T$ -exact, and there are enough of them in  $\mathfrak{Q}$ . There are enough injectives in  $\mathfrak{G}$ . And so it goes. The balancing act between  $T$ -exacts on one side, and injectives on the other is inherent to the situation.

**Lemma 8.1.** *Let  $T$  be a bifunctor satisfying **HOM 1**, **HOM 2**. Let  $A \in \mathfrak{Q}$ , and let  $M_A \rightarrow A \rightarrow 0$ , that is*

$$\rightarrow M_1 \rightarrow M_0 \rightarrow A \rightarrow 0$$

*be a  $T$ -exact resolution of  $A$ . Let  $F^n(B) = H^n(T(M, B))$  for  $B \in \mathfrak{G}$ . Then  $F$  is a  $\delta$ -functor and  $F^0(B) = T(A, B)$ . If in addition  $T$  satisfies **HOM 3**, then  $F^n(J) = 0$  for  $J$  injective and  $n \geq 1$ .*

*Proof.* Given an exact sequence

$$0 \rightarrow B' \rightarrow B \rightarrow B'' \rightarrow 0$$

we get an exact sequence of complexes

$$0 \rightarrow T(M, B') \rightarrow T(M, B) \rightarrow T(M, B'') \rightarrow 0,$$

whence a cohomology sequence which makes  $T$  into a  $\delta$ -functor. For  $n = 0$  we get  $F^0(B) = T(A, B)$  because  $X \mapsto T(X, B)$  is contravariant and left exact for  $X \in \mathfrak{Q}$ . If  $B$  is injective, then  $F^n(B) = 0$  for  $n \geq 1$  by **HOM 3**, because  $X \mapsto T(X, B)$  is exact. This proves the lemma.

**Proposition 8.2.** *Let  $T$  be a bifunctor satisfying **HOM 1**, **HOM 2**, **HOM 3**. Assume that  $\mathfrak{G}$  has enough injectives. Let  $A \in \mathfrak{Q}$ . Let*

$$M_A \rightarrow A \rightarrow 0$$

*be a  $T$ -exact resolution of  $A$ . Then the two  $\delta$ -functors*

$$B \mapsto R^n T(A, B) \quad \text{and} \quad B \mapsto H^n(T(M, B))$$

*are isomorphic as universal  $\delta$ -functors vanishing on injectives, for  $n \geq 1$ , and such that*

$$R^0 T(A, B) = H^0(T(M), B) = T(A, B).$$

*Proof.* This comes merely from the universality of a  $\delta$ -functor erasable by injectives.

We now look at the functoriality in  $A$ .

**Lemma 8.3.** *Let  $T$  satisfy **HOM 1**, **HOM 2**, and **HOM 3**. Assume that  $\mathfrak{G}$  has enough injectives. Let*

$$0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$$

*be a short exact sequence. Then for fixed  $B$ , we have a long exact sequence*

$$\begin{aligned} 0 \rightarrow T(A'', B) &\rightarrow T(A, B) \rightarrow T(A', B) \rightarrow \\ &\rightarrow R^1 T(A'', B) \rightarrow R^1 T(A, B) \rightarrow R^1 T(A', B) \rightarrow \end{aligned}$$

*such that the association*

$$A \mapsto R^n T(A, B)$$

*is a  $\delta$ -functor.*

*Proof.* Let  $0 \rightarrow B \rightarrow I_B$  be an injective resolution of  $B$ . From the exactness of the functor  $A \mapsto T(A, J)$ , for  $J$  injective we get a short exact sequence of complexes

$$0 \rightarrow T(A'', I_B) \rightarrow T(A, I_B) \rightarrow T(A', I_B) \rightarrow 0.$$

Taking the associated long exact sequence of homology groups of these complexes yields the sequence of the proposition. (The functoriality is left to the readers.)

If  $T = \text{Hom}$ , then the exact sequence looks like

$$\begin{aligned} 0 \rightarrow \text{Hom}(A'', B) &\rightarrow \text{Hom}(A, B) \rightarrow \text{Hom}(A', B) \rightarrow \\ &\rightarrow \text{Ext}^1(A'', B) \rightarrow \text{Ext}^1(A, B) \rightarrow \text{Ext}^1(A', B) \rightarrow \end{aligned}$$

and so forth.

We shall say that  $\mathfrak{Q}$  has **enough  $T$ -exacts** if given an object  $A$  in  $\mathfrak{Q}$  there is a  $T$ -exact  $M$  and an epimorphism

$$M \rightarrow A \rightarrow 0.$$

**Proposition 8.4.** *Let  $T$  satisfy **HOM 1**, **HOM 2**, **HOM 3**. Assume that  $\mathfrak{Q}$  has enough injectives. Fix  $B \in \mathfrak{Q}$ . Then the association*

$$A \mapsto R^n T(A, B)$$

*is a contravariant  $\delta$ -functor on  $\mathfrak{Q}$  which vanishes on  $T$ -exacts, for  $n \geq 1$ . If  $\mathfrak{Q}$  has enough  $T$ -exacts, then this functor is universal, coerasable by  $T$ -exacts, with value*

$$R^0 T(A, B) = T(A, B).$$

*Proof.* By Lemma 8.3 we know that the association is a  $\delta$ -functor, and it vanishes on  $T$ -exacts by Lemma 8.1. The last statement is then merely an application of the universality of erasable  $\delta$ -functors.

**Corollary 8.5.** *Let  $\mathfrak{Q} = \mathfrak{G}$  be the category of modules over a ring. For fixed  $B$ , let  $\text{ext}^n(A, B)$  be the left derived functor of  $A \mapsto \text{Hom}(A, B)$ , obtained by means of projective resolutions of  $A$ . Then*

$$\text{ext}^n(A, B) = \text{Ext}^n(A, B).$$

*Proof.* Immediate from Proposition 8.4.

The following proposition characterizes  $T$ -exacts cohomologically.

**Proposition 8.6.** *Let  $T$  be a bifunctor satisfying **HOM 1**, **HOM 2**, **HOM 3**. Assume that  $\mathfrak{G}$  has enough injectives. Then the following conditions are equivalent:*

**TE 1.**  *$A$  is  $T$ -exact.*

**TE 2.** *For every  $B$  and every integer  $n \geq 1$ , we have  $R^n T(A, B) = 0$ .*

**TE 3.** *For every  $B$  we have  $R^1 T(A, B) = 0$ .*

*Proof.* Let

$$0 \rightarrow B \rightarrow I^0 \rightarrow I^1 \rightarrow$$

be an injective resolution of  $B$ . By definition,  $R^n T(A, B)$  is the  $n$ -th homology of the sequence

$$0 \rightarrow T(A, I^0) \rightarrow T(A, I^1) \rightarrow T(A, I^2) \rightarrow$$

If  $A$  is  $T$ -exact, then this sequence is exact for  $n \geq 1$ , so the homology is 0 and **TE 1** implies **TE 2**. Trivially, **TE 2** implies **TE 3**. Finally assume **TE 3**. Given an exact sequence

$$0 \rightarrow B' \rightarrow B \rightarrow B'' \rightarrow 0,$$

we have the homology sequence

$$0 \rightarrow T(A, B') \rightarrow T(A, B) \rightarrow T(A, B'') \rightarrow R^1 T(A, B') \rightarrow.$$

If  $R^1 T(A, B') = 0$ , then by definition  $A$  is  $T$ -exact, thus proving the proposition.

We shall say that an object  $A$  has  $T$ -**dimension**  $\leq d$  if

$$R^n T(A, B) = 0 \quad \text{for } n > d \text{ and all } B.$$

Then the proposition states in particular that  $A$  is  $T$ -exact if and only if  $A$  has  $T$ -dimension 0.

**Proposition 8.7.** *Let  $T$  satisfy **HOM 1**, **HOM 2**, **HOM 3**. Assume that  $\mathfrak{G}$  has enough injectives. Suppose that an object  $A$  admits a resolution*

$$0 \rightarrow E_d \rightarrow E_{d-1} \rightarrow \cdots \rightarrow E_0 \rightarrow A \rightarrow 0$$

where  $E_0, \dots, E_d$  are  $T$ -exact. Then  $A$  has  $T$ -dimension  $\leq d$ . Assume this is the case. Let

$$0 \rightarrow Q \rightarrow L_{d-1} \rightarrow \cdots \rightarrow L_0 \rightarrow A \rightarrow 0$$

be a resolution where  $L_0, \dots, L_{d-1}$  are  $T$ -exact. Then  $Q$  is  $T$ -exact also.

*Proof.* By dimension shifting we conclude that  $Q$  has  $T$ -dimension 0, whence  $Q$  is  $T$ -exact by Proposition 8.6.

Proposition 8.7, like others, is used in the context of modules over a ring. In that case, we can take  $T = \text{Hom}$ , and

$$R^n T(A, B) = \text{Ext}^n(A, B).$$

For  $A$  to have  $T$ -dimension  $\leq d$  means that

$$\text{Ext}^n(A, B) = 0 \quad \text{for } n > d \text{ and all } B.$$

Instead of  $T$ -exact, one can then read projective in the proposition.

Let us formulate the analogous result for a bifunctor that will apply to the tensor product. Consider the following properties.

**TEN 1.**  $T$  is covariant and right exact in the first variable.

**TEN 2.**  $T$  is covariant and right exact in the second variable.

**TEN 3.** For any projective object  $P$  the functor

$$A \mapsto T(A, P)$$

is exact.

As for  $\text{Hom}$ , there is a possible fourth property which will play no role in this section:

**TEN 4.** For any projective object  $Q$  the functor

$$B \mapsto T(Q, B)$$

is exact.

**Proposition 8.2'.** Let  $T$  be a bifunctor satisfying **TEN 1**, **TEN 2**, **TEN 3**. Assume that  $\mathfrak{Q}$  has enough projectives. Let  $A \in \mathfrak{Q}$ . Let

$$M_A \rightarrow A \rightarrow 0$$

be a  $T$ -exact resolution of  $A$ . Then the two  $\delta$ -functors

$$B \mapsto L_n T(A, B) \quad \text{and} \quad B \mapsto H_n(T(M, B))$$

are isomorphic as universal  $\delta$ -functors vanishing on projectives, and such that

$$L_0 T(A, B) = H_0(T(M), B) = T(A, B).$$

**Lemma 8.3'.** Assume that  $T$  satisfies **TEN 1**, **TEN 2**, **TEN 3**. Assume that  $\mathfrak{Q}$  has enough projectives. Let

$$0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$$

be a short exact sequence. Then for fixed  $B$ , we have a long exact sequence:

$$\begin{aligned} &\rightarrow L_1 T(A', B) \rightarrow L_1 T(A, B) \rightarrow L_1 T(A'', B) \rightarrow \\ &\rightarrow T(A', B) \rightarrow T(A, B) \rightarrow T(A'', B) \rightarrow 0 \end{aligned}$$

which makes the association  $A \mapsto L_n T(A, B)$  a  $\delta$ -functor.

**Proposition 8.4'.** Let  $T$  satisfy **TEN 1**, **TEN 2**, **TEN 3**. Assume that  $\mathfrak{G}$  has enough projectives. Fix  $B \in \mathfrak{G}$ . Then the association

$$A \mapsto L_n T(A, B)$$

is a contravariant  $\delta$ -functor on  $\mathfrak{G}$  which vanishes on  $T$ -exacts for  $n \geq 1$ . If  $\mathfrak{G}$  has enough  $T$ -exacts, then this functor is universal, coerasable by  $T$ -exacts, with the value

$$L_0 T(A, B) = T(A, B).$$

**Corollary 8.8.** If there is a bifunctorial isomorphism  $T(A, B) \approx T(B, A)$ , and if  $B$  is  $T$ -exact, then for all  $A$ ,  $L_n T(A, B) = 0$  for  $n \geq 1$ . In short,  $T$ -exact implies acyclic.

*Proof.* Let  $M_A = P_A$  be a projective resolution in Proposition 8.2'. By hypotheses,  $X \mapsto T(X, B)$  is exact so  $H_n(T(P, B)) = 0$  for  $n \geq 1$ ; so the corollary is a consequence of the proposition.

The above corollary is formulated so as to apply to the tensor product.

**Proposition 8.6'.** Let  $T$  be a bifunctor satisfying **TEN 1**, **TEN 2**, **TEN 3**. Assume that  $\mathfrak{G}$  has enough projectives. Then the following conditions are equivalent:

**TE 1.**  $A$  is  $T$ -exact.

**TE 2.** For every  $B$  and every integer  $n \geq 1$  we have  $L_n T(A, B) = 0$ .

**TE 3.** For every  $B$ , we have  $L_1 T(A, B) = 0$ .

*Proof.* We repeat the proof of 8.6 so the reader can see the arrows pointing in different ways.

Let

$$\rightarrow Q_1 \rightarrow Q_0 \rightarrow B \rightarrow 0$$

be a projective resolution of  $B$ . By definition,  $L_n T(A, B)$  is the  $n$ -th homology of the sequence

$$\rightarrow T(A, Q_1) \rightarrow T(A, Q_0) \rightarrow 0.$$

If  $A$  is  $T$ -exact, then this sequence is exact for  $n \geq 1$ , so the homology is 0, and **TE 1** implies **TE 2**. Trivially, **TE 2** implies **TE 3**. Finally, assume **TE 3**. Given an exact sequence

$$0 \rightarrow B' \rightarrow B \rightarrow B'' \rightarrow 0$$

we have the homology sequence

$$\rightarrow L_1 T(A, B'') \rightarrow T(A, B') \rightarrow T(A, B) \rightarrow T(A, B'') \rightarrow 0.$$

If  $L_1 T(A, B'')$  is 0, then by definition,  $A$  is  $T$ -exact, thus proving the proposition.

## §9. SPECTRAL SEQUENCES

This section is included for convenience of reference, and has two purposes: first, to draw attention to an algebraic gadget which has wide applications in topology, differential geometry, and algebraic geometry, see Griffiths-Harris, [GrH 78]; second, to show that the basic description of this gadget in the context in which it occurs most frequently can be done in just a few pages.

In the applications mentioned above, one deals with a filtered complex (which we shall define later), and a complex may be viewed as a graded object, with a differential  $d$  of degree 1. To simplify the notation at first, we shall deal with filtered objects and omit the grading index from the notation. This index is irrelevant for the construction of the spectral sequence, for which we follow Godement.

So let  $F$  be an object with a differential (i.e. endomorphism)  $d$  such that  $d^2 = 0$ . We assume that  $F$  is **filtered**, that is that we have a sequence

$$F = F^0 \supset F^1 \supset F^2 \supset \cdots \supset F^n \supset F^{n+1} = \{0\},$$

and that  $dF^p \subset F^p$ . This data is called a **filtered differential object**. (We assume that the filtration ends with 0 after a finite number of steps for convenience.)

One defines the **associated graded object**

$$\text{Gr } F = \bigoplus_{p \geq 0} \text{Gr}^p F \quad \text{where} \quad \text{Gr}^p F = F^p / F^{p+1}.$$

In fact,  $\text{Gr } F$  is a complex, with a differential of degree 0 induced by  $d$  itself, and we have the homology  $H(\text{Gr}^p F)$ .

The filtration  $\{F^p\}$  also induces a filtration on the homology  $H(F, d) = H(F)$ ; namely we let

$$H(F)^p = \text{image of } H(F^p) \text{ in } H(F).$$

Since  $d$  maps  $F^p$  into itself,  $H(F^p)$  is the homology of  $F^p$  with respect to the restriction of  $d$  to  $F^p$ , and it has a natural image in  $H(F)$  which yields this filtration. In particular, we then obtain a graded object associated with the filtered homology, namely

$$\text{Gr } H(F) = \bigoplus \text{Gr}^p H(F).$$

A **spectral sequence** is a sequence  $\{E_r, d_r\}$  ( $r \geq 0$ ) of graded objects

$$E_r = \bigoplus_{p \geq 0} E_r^p$$

together with homomorphisms (also called **differentials**) of degree  $r$ ,

$$d_r : E_r^p \rightarrow E_r^{p+r}$$

satisfying  $d_r^2 = 0$ , and such that the homology of  $E_r$  is  $E_{r+1}$ , that is

$$H(E_r) = E_{r+1}.$$

In practice, one usually has  $E_r = E_{r+1} = \dots$  for  $r \geq r_0$ . This limit object is called  $E_\infty$ , and one says that the spectral sequence **abuts** to  $E_\infty$ . Actually, to be perfectly strict, instead of equalities one should really be given isomorphisms, but for simplicity, we use equalities.

**Proposition 9.1.** *Let  $F$  be a filtered differential object. Then there exists a spectral sequence  $\{E_r\}$  with:*

$$E_0^p = F^p/F^{p+1}; \quad E_1^p = H(\text{Gr}^p F); \quad E_\infty^p = \text{Gr}^p H(F).$$

*Proof.* Define

$$Z_r^p = \{x \in F^p \text{ such that } dx \in F^{p+r}\}$$

$$E_r^p = Z_r^p / [dZ_{r-1}^{p-(r-1)} + Z_{r-1}^{p+1}].$$

The definition of  $E_r^p$  makes sense, since  $Z_r^p$  is immediately verified to contain  $dZ_{r-1}^{p-(r-1)} + Z_{r-1}^{p+1}$ . Furthermore,  $d$  maps  $Z_r^p$  into  $Z_r^{p+r}$ , and hence includes a homomorphism

$$d_r : E_r^p \rightarrow E_r^{p+r}.$$

We shall now compute the homology and show that it is what we want.

First, for the cycles: An element  $x \in Z_r^p$  represents a cycle of degree  $p$  in  $E_r$  if and only if  $dx \in dZ_{r+1}^{p+1} + Z_{r-1}^{p+r+1}$ , in other words

$$dx = dy + z, \quad \text{with } y \in Z_{r-1}^{p+1} \quad \text{and} \quad z \in Z_{r-1}^{p+r+1}.$$

Write  $x = y + u$ , so  $du = z$ . Then  $u \in F^p$  and  $du \in F^{p+r+1}$ , that is  $u \in Z_{r+1}^p$ . It follows that

$$p\text{-cycles of } E_r = (Z_{r+1}^p + Z_{r-1}^{p+1})/(dZ_{r-1}^{p-r+1} + Z_{r-1}^{p+1}).$$

On the other hand, the  $p$ -boundaries in  $E_r$  are represented by elements of  $dZ_r^{p-r}$ , which contains  $dZ_{r-1}^{p-r+1}$ . Hence

$$p\text{-boundaries of } E_r = (dZ_r^{p-r} + Z_{r-1}^{p+1})/(dZ_{r-1}^{p-r+1} + Z_{r-1}^{p+1}).$$

Therefore

$$\begin{aligned} H^p(E_r) &= (Z_{r+1}^p + Z_{r-1}^{p+1})/(dZ_r^{p-r} + Z_{r-1}^{p+1}) \\ &= Z_{r+1}^p / (Z_{r+1}^p \cap (dZ_r^{p-r} + Z_{r-1}^{p+1})). \end{aligned}$$

Since

$$Z_{r+1}^p \supset dZ_r^{p-r} \quad \text{and} \quad Z_{r+1}^p \cap Z_{r-1}^{p+1} = Z_r^{p+1},$$

it follows that

$$H^p(E_r) = Z_{r+1}^p / (dZ_r^{p-r} + Z_r^{p+1}) = E_{r+1}^p,$$

thus proving the property of a spectral sequence.

**Remarks.** It is sometimes useful in applications to note the relation

$$dZ_{r-1}^{p-(r-1)} + Z_{r-1}^{p+1} = Z_r^p \cap (dF^{p-r+1} + F^{p+1}).$$

The verification is immediate, but Griffiths-Harris use the expression on the right in defining the spectral sequence, whereas Godement uses the expression on the left as we have done above. Thus the spectral sequence may also be defined by

$$E_r^p = Z_r^p \mod (dF^{p-r+1} + F^{p+1}).$$

This is to be interpreted in the sense that  $Z \mod S$  means

$$(Z + S)/S \quad \text{or} \quad Z/(Z \cap S).$$

The term  $E_0^p$  is  $F^p/F^{p+1}$  immediately from the definitions, and by the general property already proved, we get  $E_1^p = H(F^p/F^{p+1})$ . As to  $E_\infty^p$ , for  $r$  large we have  $Z_r^p = Z^p = \text{cycles in } F^p$ , and

$$E_\infty^p = Z^p / (Z^{p+1} + (dF^0 \cap F^p))$$

which is independent of  $r$ , and is precisely  $\text{Gr}^p H(F)$ , namely the  $p$ -graded component of  $H(F)$ , thus proving the theorem.

The differential  $d_1$  can be specified as follows.

**Proposition 9.2.** *The homomorphism*

$$d_1 : E_1^p \rightarrow E_1^{p+1}$$

*is the coboundary operator arising from the exact sequence*

$$0 \rightarrow F^{p+1}/F^{p+2} \rightarrow F^p/F^{p+2} \rightarrow F^p/F^{p+1} \rightarrow 0$$

*viewing each term as a complex with differential induced by  $d$ .*

*Proof.* Indeed, the coboundary

$$\delta : E_1^p = H(F^p/F^{p+1}) \rightarrow H(F^{p+1}/F^{p+2}) = E_1^{p+1}$$

is defined on a representative cycle  $z$  by  $dz$ , which is the same way that we defined  $d_1$ .

In most applications, the filtered differential object is itself graded, because it arises from the following situation. Let  $K$  be a complex,  $K = (K^p, d)$  with  $p \geq 0$  and  $d$  of degree 1. By a **filtration**  $FK$ , also called a **filtered complex**, we mean a decreasing sequence of subcomplexes

$$K = F^0 K \supset F^1 K \supset F^2 K \supset \cdots \supset F^n K \supset F^{n+1} K = \{0\}.$$

Observe that a short exact sequence of complexes

$$0 \rightarrow K' \rightarrow K \rightarrow K'' \rightarrow 0$$

gives rise to a filtration  $K \supset K' \supset \{0\}$ , viewing  $K'$  as a subcomplex.

To each filtered complex  $FK$  we associate the complex

$$\text{Gr } FK = \text{Gr } K = \bigoplus_{p \geq 0} \text{Gr}^p K,$$

where

$$\text{Gr}^p K = F^p K / F^{p+1} K,$$

and the differential is the obvious one. The filtration  $F^p K$  on  $K$  also induces a filtration  $F^p H(K)$  on the cohomology, by

$$F^p H^q(K) = F^p Z^q / F^p B^q.$$

The associated graded homology is

$$\text{Gr } H(K) = \bigoplus_{p, q} \text{Gr}^p H^q(K),$$

where

$$\text{Gr}^p H^q(K) = F^p H^q(K) / F^{p+1} H^q(K).$$

A **spectral sequence** is a sequence  $\{E_r, d_r\}$  ( $r \geq 0$ ) of bigraded objects

$$E_r = \bigoplus_{p, q \geq 0} E_r^{p, q}$$

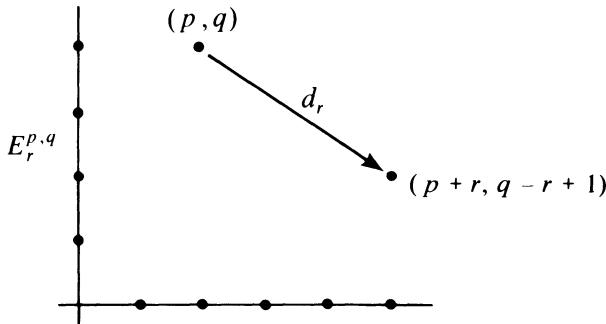
together with homomorphisms (called **differentials**)

$$d_r : E_r^{p, q} \rightarrow E_r^{p+r, q-r+1} \quad \text{satisfying} \quad d_r^2 = 0,$$

and such that the homology of  $E_r$  is  $E_{r+1}$ , that is

$$H(E_r) = E_{r+1}.$$

A spectral sequence is usually represented by the following picture:



In practice, one usually has  $E_r = E_{r+1} = \dots$  for  $r \geq r_0$ . This limit object is called  $E_\infty$ , and one says that the spectral sequence **abuts** to  $E_\infty$ .

**Proposition 9.3.** *Let  $FK$  be a filtered complex. Then there exists a spectral sequence  $\{E_r\}$  with:*

$$E_0^{p, q} = F^p K^{p+q} / F^{p+1} K^{p+q};$$

$$E_1^{p, q} = H^{p+q}(\text{Gr}^p K);$$

$$E_\infty^{p, q} = \text{Gr}^p (H^{p+q}(K)).$$

The last relation is usually written

$$E_r \Rightarrow H(K),$$

and we say that the spectral sequence **abuts** to  $H(K)$ .

The statement of Proposition 9.3 is merely a special case of Proposition 9.1, taking into account the extra graduation.

One of the main examples is the spectral sequence associated with a double complex

$$K = \bigoplus_{p, q \geq 0} K^{p, q}$$

which is a bigraded object, together with differentials

$$d' : K^{p, q} \rightarrow K^{p+1, q} \quad \text{and} \quad d'' : K^{p, q} \rightarrow K^{p, q+1}$$

satisfying

$$d'^2 = d''^2 = 0 \quad \text{and} \quad d'd'' + d''d' = 0.$$

We denote the double complex by  $(K, d', d'')$ . The associated single complex  $(\text{Tot}(K), D)$  (Tot for **total complex**), abbreviated  $K^*$ , is defined by

$$K^n = \bigoplus_{p+q=n} K^{p, q} \quad \text{and} \quad D = d' + d''.$$

There are two filtrations on  $(K^*, D)$  given by

$$\begin{aligned} {}'F^p K^n &= \bigoplus_{\substack{p'+q=n \\ p' \geq p}} K^{p', q} \\ {}''F^q K^n &= \bigoplus_{\substack{p+q'=n \\ q' \geq q}} K^{p, q'}. \end{aligned}$$

There are two spectral sequences  $\{{}'E_r\}$  and  $\{{}''E_r\}$ , both abutting to  $H(\text{Tot}(K))$ . For applications, see [GrH 78], Chapter 3, §5; and also, for instance, [FuL 85], Chapter V. There are many situations when dealing with a double complex directly is a useful substitute for using spectral sequences, which are derived from double complexes anyhow.

We shall now derive the existence of a spectral sequence in one of the most important cases, the **Grothendieck spectral sequence** associated with the composite of two functors. *We assume that our abelian category has enough injectives.*

Let  $C = \bigoplus C^p$  be a complex, and suppose  $C^p = 0$  if  $p < 0$  for simplicity. We define **injective resolution** of  $C$  to be a resolution

$$0 \rightarrow C \rightarrow I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow \dots$$

written briefly

$$0 \rightarrow C \rightarrow I_C$$

such that each  $I^j$  is a complex,  $I^j = \bigoplus I^{j, p}$ , with differentials

$$d^{j, p} : I^{j, p} \rightarrow I^{j, p+1}$$

and such that  $I^{j,p}$  is an injective object. Then in particular, for each  $p$  we get an injective resolution of  $C^p$ , namely:

$$0 \rightarrow C^p \rightarrow I^{0,p} \rightarrow I^{1,p} \rightarrow \dots$$

We let:

$$Z^{j,p} = \text{Ker } d^{j,p} = \text{cycles in degree } p$$

$$B^{j,p} = \text{Im } d^{j,p-1} = \text{boundaries in degree } p$$

$$H^{j,p} = Z^{j,p}/B^{j,p} = \text{homology in degree } p.$$

We then get complexes

$$0 \rightarrow Z^p(C) \rightarrow Z^{0,p} \rightarrow Z^{1,p} \rightarrow$$

$$0 \rightarrow B^p(C) \rightarrow B^{0,p} \rightarrow B^{1,p} \rightarrow$$

$$0 \rightarrow H^p(C) \rightarrow H^{0,p} \rightarrow H^{1,p} \rightarrow$$

We say that the resolution  $0 \rightarrow C \rightarrow I_C$  is **fully injective** if these three complexes are injective resolutions of  $Z^p(C)$ ,  $B^p(C)$  and  $H^p(C)$  respectively.

**Lemma 9.4.** *Let*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

*be a short exact sequence. Let*

$$0 \rightarrow M' \rightarrow I_{M'} \quad \text{and} \quad 0 \rightarrow M'' \rightarrow I_{M''}$$

*be injective resolutions of  $M'$  and  $M''$ . Then there exists an injective resolution*

$$0 \rightarrow M \rightarrow I_M$$

*of  $M$  and morphisms which make the following diagram exact and commutative:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & I_{M'} & \longrightarrow & I_M & \longrightarrow & I_{M''} \longrightarrow 0 \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' \longrightarrow 0 \\ & & \uparrow & & \uparrow & & \uparrow \\ & & 0 & & 0 & & 0 \end{array}$$

*Proof.* The proof is the same as at the beginning of the proof of Theorem 6.1.

**Lemma 9.5.** *Given a complex  $C$  there exists a fully injective resolution of  $C$ .*

*Proof.* We insert the kernels and cokernels in  $C$ , giving rise to the short exact sequences with boundaries  $B^p$  and cycles  $Z^p$ :

$$\begin{aligned} 0 \rightarrow B^p \rightarrow Z^p \rightarrow H^p \rightarrow 0 \\ 0 \rightarrow Z^{p-1} \rightarrow C^{p-1} \rightarrow B^p \rightarrow 0. \end{aligned}$$

We proceed inductively. We start with an injective resolution of

$$0 \rightarrow Z^{p-1} \rightarrow C^{p-1} \rightarrow B^p \rightarrow 0$$

using Lemma 9.4. Next let

$$0 \rightarrow H^p \rightarrow I_{H^p}$$

be an injective resolution of  $H^p$ . By Lemma 9.4 there exists an injective resolution

$$0 \rightarrow Z^p \rightarrow I_{Z^p}$$

which fits in the middle of the injective resolutions we already have for  $B^p$  and  $H^p$ . This establishes the inductive step, and concludes the proof.

Given a left exact functor  $G$  on an abelian category with enough injectives, we say that an object  $X$  is  **$G$ -acyclic** if  $R^pG(X) = 0$  for  $p \geq 1$ . Of course,

$$R^0G(X) = G(X).$$

**Theorem 9.6. (Grothendieck spectral sequence).** *Let*

$$T: \mathfrak{Q} \rightarrow \mathfrak{Q} \quad \text{and} \quad G: \mathfrak{Q} \rightarrow \mathfrak{C}$$

*be covariant left exact functors such that if  $I$  is injective in  $\mathfrak{Q}$ , then  $T(I)$  is  $G$ -acyclic. Then for each  $A$  in  $\mathfrak{Q}$  there is a spectral sequence  $\{E_r(A)\}$ , such that*

$$E_2^{p,q}(A) = R^pG(R^qT(A))$$

*and  $E_r^{p,q}$  abuts (with respect to  $p$ ) to  $R^{p+q}(GT)(A)$ , where  $q$  is the grading index.*

*Proof.* Let  $A$  be an object of  $\mathfrak{Q}$ , and let  $0 \rightarrow A \rightarrow C_A$  be an injective resolution. We apply  $T$  to get a complex

$$TC: 0 \rightarrow TC^0 \rightarrow TC^1 \rightarrow TC^2 \rightarrow$$

By Lemma 9.5 there exists a fully injective resolution

$$0 \rightarrow TC \rightarrow I_{TC}$$

which has the 2-dimensional representation:

$$\begin{array}{ccccccc}
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 \longrightarrow I^{0,1} \longrightarrow I^{1,1} \longrightarrow I^{2,1} \longrightarrow & & & & \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 \longrightarrow I^{0,0} \longrightarrow I^{1,0} \longrightarrow I^{2,0} \longrightarrow & & & & \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 \longrightarrow TC^0 \longrightarrow TC^1 \longrightarrow TC^2 \longrightarrow & & & & \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Then  $GI$  is a double complex. Let  $\text{Tot}(GI)$  be the associated single complex. We now consider each of the two possible spectral sequences in succession, which we denote by  ${}^1E_r^{p,q}$  and  ${}^2E_r^{p,q}$ .

The first one is the easiest. For fixed  $p$ , we have an injective resolution

$$0 \rightarrow TC^p \rightarrow I_{TC}^p$$

where we write  $I_{TC}^p$  instead of  $I_{TC^p}$ . This is the  $p$ -th column in the diagram. By definition of derived functors,  $GI^p$  is a complex whose homology is  $R^qG$ , in other words, taking homology with respect to  $d''$  we have

$${}^0H^{p,q}(GI) = H^q(GI^p) = (R^qG)(TC^p).$$

By hypothesis,  $C^p$  injective implies that  $(R^qG)(TC^p) = 0$  for  $q > 0$ . Since  $G$  is left exact, we have  $R^0G(TC^p) = TC^p$ . Hence we get

$${}^0H^{p,q}(GI) = \begin{cases} GT(C^p) & \text{if } q = 0 \\ 0 & \text{if } q > 0. \end{cases}$$

Hence the non-zero terms are on the  $p$ -axis, which looks like

$$0 \rightarrow GT(C^0) \rightarrow GT(C^1) \rightarrow GT(C^2) \rightarrow$$

Taking  ${}^1H^p$  we get

$${}^1E_2^{p,q}(A) = \begin{cases} R^p(GT)(A) & \text{if } q = 0 \\ 0 & \text{if } q > 0. \end{cases}$$

This yields

$$H^n(\text{Tot}(GI)) \approx R^n(GT)(A).$$

The second one will use the full strength of Lemma 9.5, which had not been used in the first part of the proof, so it is now important that the resolution  $I_{TC}$  is fully injective. We therefore have injective resolutions

$$\begin{aligned} 0 \rightarrow Z^p(TC) &\rightarrow {}^1Z^{0,p} \rightarrow {}^1Z^{1,p} \rightarrow {}^1Z^{2,p} \rightarrow \\ 0 \rightarrow B^p(TC) &\rightarrow {}^1B^{0,p} \rightarrow {}^1B^{1,p} \rightarrow {}^1B^{2,p} \rightarrow \\ 0 \rightarrow H^p(TC) &\rightarrow {}^1H^{0,p} \rightarrow {}^1H^{1,p} \rightarrow {}^1H^{2,p} \rightarrow \end{aligned}$$

and the exact sequences

$$\begin{aligned} 0 \rightarrow {}^1Z^{q,p} &\rightarrow I^{q,p} \rightarrow {}^1B^{q+1,p} \rightarrow 0 \\ 0 \rightarrow {}^1B^{q,p} &\rightarrow {}^1Z^{q,p} \rightarrow {}^1H^{q,p} \rightarrow 0 \end{aligned}$$

split because of the injectivity of the terms. We denote by  $I^{(p)}$  the  $p$ -th row of the double complex  $I = \{I^{q,p}\}$ . Then we find:

$$\begin{aligned} {}^1H^{q,p}(GI) &= H^q(GI^{(p)}) = G^1Z^{q,p}/G^1B^{q,p} && \text{by the first split sequence} \\ &= G'{}^1H^{q,p}(I) && \text{by the second split sequence} \end{aligned}$$

because applying the functor  $G$  to a split exact sequence yields a split exact sequence.

Then

$${}^2E_2^{p,q} = {}^2H^p({}^1H^{q,p}(GI)) = H^p(G^1H^{q,p}(I)).$$

By the full injectivity of the resolutions, the complex  ${}^1H^{q,p}(I)$  with  $p \geq 0$  is an injective resolution of

$$H^q(TC) = (R^qT)(A).$$

Furthermore, we have

$$H^p(G'{}^1H^{q,p}) = R^pG(R^qT(A)),$$

since a derived functor is the homology of an injective resolution. This proves that  $(R^pG)R^qT(A)$  abuts to  $R^n(GT)(A)$ , and concludes the proof of the theorem.

Just to see the spectral sequence at work, we give one application relating it to the Euler characteristic discussed in §3.

Let  $\mathfrak{Q}$  have enough injectives, and let

$$T : \mathfrak{Q} \rightarrow \mathfrak{G}$$

be a covariant left exact functor. Let  $\mathfrak{F}_a$  be a family of objects in  $\mathfrak{Q}$  giving rise to a **K**-group. More precisely, in a short exact sequence in  $\mathfrak{Q}$ , if two of the objects lie in  $\mathfrak{F}_a$ , then so does the third. We also assume that the objects of  $\mathfrak{F}_a$  have **finite RT-dimension**, which means by definition that if  $A \in \mathfrak{F}_a$  then  $R^iT(A) = 0$

for all  $i$  sufficiently large. We could take  $\mathfrak{F}_a$  in fact to be the family of all objects in  $\mathfrak{Q}$  which have finite  $RT$ -dimension.

We define the **Euler characteristic associated with  $T$**  on  $\mathbf{K}(\mathfrak{F}_a)$  to be

$$\chi_T(A) = \sum_{i=0}^{\infty} (-1)^i \text{cl}(R^i T(A)).$$

The  $\text{cl}$  denotes the class in the  $\mathbf{K}$ -group  $K(\mathfrak{F}_a)$  associated with some family  $\mathfrak{F}_a$  of objects in  $\mathfrak{Q}$ , and such that  $R^i T(A) \in \mathfrak{F}_a$  for all  $A \in \mathfrak{F}_a$ . This is the minimum required for the formula to make sense.

**Lemma 9.7.** *The map  $\chi_T$  extends to a homomorphism*

$$\mathbf{K}(\mathfrak{F}_a) \rightarrow \mathbf{K}(\mathfrak{F}_a).$$

*Proof.* Let

$$0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$$

be an exact sequence in  $\mathfrak{F}$ . Then we have the cohomology sequence

$$\rightarrow R^i T(A') \rightarrow R^i T(A) \rightarrow R^i T(A'') \rightarrow R^{i+1} T(A') \rightarrow$$

in which all but a finite number of terms are 0. Taking the alternating sum in the  $\mathbf{K}$ -group shows that  $\chi_T$  is an Euler–Poincaré map, and concludes the proof.

Note that we have merely repeated something from §3, in a jazzed up context. In the next theorem, we have another functor

$$G : \mathfrak{G} \rightarrow \mathfrak{C},$$

and we also have a family  $\mathfrak{F}_e$  giving rise to a  $\mathbf{K}$ -group  $\mathbf{K}(\mathfrak{F}_e)$ . We suppose that we can perform the above procedure at each step, and also need some condition so that we can apply the spectral sequence. So, precisely, we assume:

**CHAR 1.** For all  $i$ ,  $R^i T$  maps  $\mathfrak{F}_a$  into  $\mathfrak{F}_a$ ,  $R^i G$  maps  $\mathfrak{F}_a$  into  $\mathfrak{F}_e$ , and  $R^i(GT)$  maps  $\mathfrak{F}_a$  into  $\mathfrak{F}_e$ .

**CHAR 2.** Each subobject of an element of  $\mathfrak{F}_a$  lies in  $\mathfrak{F}_a$  and has finite  $RT$ - and  $R(GT)$ -dimension; each subobject of an element of  $\mathfrak{F}_a$  lies in  $\mathfrak{F}_a$  and has finite  $RG$ -dimension.

**Theorem 9.8.** *Assume that  $T : \mathfrak{Q} \rightarrow \mathfrak{G}$  and  $G : \mathfrak{G} \rightarrow \mathfrak{C}$  satisfy the conditions*

**CHAR 1** *and* **CHAR 2**. *Also assume that  $T$  maps injectives to  $G$ -acyclics. Then*

$$\chi_G \circ \chi_T = \chi_{GT}.$$

*Proof.* By Theorem 9.6, the Grothendieck spectral sequence of the composite functor implies the existence of a filtration

$$\cdots \subset F^p R^n(GT)(A) \subset F^{p+1} R^n(GT)(A) \subset \cdots$$

of  $R^n(GT)(A)$ , such that

$$F^{p+1}/F^p \approx E_\infty^{p, n-p}.$$

Then

$$\begin{aligned} \chi_{GT}(A) &= \sum_{n=0}^{\infty} (-1)^n \operatorname{cl}(R^n(GT)(A)) \\ &= \sum_{n=0}^{\infty} (-1)^n \sum_{p=0}^{\infty} \operatorname{cl}(E_\infty^{p, n-p}) \\ &= \sum_{n=0}^{\infty} (-1)^n \operatorname{cl}(E_\infty^n). \end{aligned}$$

On the other hand,

$$\chi_T(A) = \sum_{q=0}^{\infty} (-1)^q \operatorname{cl}(R^q T(A))$$

and so

$$\begin{aligned} \chi_G \circ \chi_T(A) &= \sum_{q=0}^{\infty} (-1)^q \chi_G(R^q T(A)) \\ &= \sum_{q=0}^{\infty} (-1)^q \sum_{p=0}^{\infty} (-1)^p \operatorname{cl}(R^p G(R^q T(A))) \\ &= \sum_{n=0}^{\infty} (-1)^n \sum_{p=0}^n \operatorname{cl}(R^p G(R^{n-p} T(A))) \\ &= \sum_{n=0}^{\infty} (-1)^n \operatorname{cl}(E_2^n). \end{aligned}$$

Since  $E_{r+1}$  is the homology of  $E_r$ , we get

$$\sum_{n=0}^{\infty} (-1)^n \operatorname{cl}(E_2^n) = \sum_{n=0}^{\infty} (-1)^n \operatorname{cl}(E_3^n) = \cdots = \sum_{n=0}^{\infty} (-1)^n \operatorname{cl}(E_\infty^n).$$

This concludes the proof of the theorem.

---

**EXERCISES**

1. Prove that the example of the standard complex given in §1 is actually a complex, and is exact, so it gives a resolution of  $\mathbf{Z}$ . [Hint: To show that the sequence of the standard complex is exact, choose an element  $z \in S$  and define  $h : E^i \rightarrow E^{i+1}$  by letting

$$h(x_0, \dots, x_i) = (z, x_0, \dots, x_i).$$

Prove that  $dh + hd = \text{id}$ , and that  $dd = 0$ . Exactness follows at once.]

**Cohomology of groups**

2. Let  $G$  be a group. Use  $G$  as the set  $S$  in the standard complex. Define an action of  $G$  on the standard complex  $E$  by letting

$$x(x_0, \dots, x_i) = (xx_0, \dots, xx_i).$$

Prove that each  $E_i$  is a free module over the group ring  $\mathbf{Z}[G]$ . Thus if we let  $R = \mathbf{Z}[G]$  be the group ring, and consider the category  $\text{Mod}(G)$  of  $G$ -modules, then the standard complex gives a free resolution of  $\mathbf{Z}$  in this category.

3. The standard complex  $E$  was written in homogeneous form, so the boundary maps have a certain symmetry. There is another complex which exhibits useful features as follows. Let  $F^i$  be the free  $\mathbf{Z}[G]$ -module having for basis  $i$ -tuples (rather than  $(i+1)$ -tuples)  $(x_1, \dots, x_i)$ . For  $i = 0$  we take  $F_0 = \mathbf{Z}[G]$  itself. Define the boundary operator by the formula

$$\begin{aligned} d(x_1, \dots, x_i) = & x_1(x_2, \dots, x_i) + \sum_{j=1}^{i-1} (-1)^j (x_1, \dots, x_j x_{j+1}, \dots, x_i) \\ & + (-1)^{i+1} (x_1, \dots, x_i). \end{aligned}$$

Show that  $E \approx F$  (as complexes of  $G$ -modules) via the association

$$(x_1, \dots, x_i) \mapsto (1, x_1, x_1 x_2, \dots, x_1 x_2 \cdots x_i),$$

and that the operator  $d$  given for  $F$  corresponds to the operator  $d$  given for  $E$  under this isomorphism.

4. If  $A$  is a  $G$ -module, let  $A^G$  be the submodule consisting of all elements  $v \in A$  such that  $xv = v$  for all  $x \in G$ . Thus  $A^G$  has trivial  $G$ -action. (This notation is convenient, but is *not* the same as for the induced module of Chapter XVIII.)

- (a) Show that if  $H^q(G, A)$  denotes the  $q$ -th homology of the complex  $\text{Hom}_G(E, A)$ , then  $H^0(G, A) = A^G$ . Thus the left derived functors of  $A \mapsto A^G$  are the homology groups of the complex  $\text{Hom}_G(E, A)$ , or for that matter, of the complex  $\text{Hom}(F, A)$ , where  $F$  is as in Exercise 3.
- (b) Show that the group of 1-cycles  $Z^1(G, A)$  consists of those functions  $f : G \rightarrow A$  satisfying

$$f(x) + xf(y) = f(xy) \text{ for all } x, y \in G.$$

Show that the subgroup of coboundaries  $B^1(G, A)$  consists of those functions  $f$  for which there exists an element  $a \in A$  such that  $f(x) = xa - a$ . The factor group is then  $H^1(G, A)$ . See Chapter VI, §10 for the determination of a special case.

- (c) Show that the group of 2-cocycles  $Z^2(G, A)$  consists of those functions  $f: G \rightarrow A$  satisfying

$$xf(y, z) - f(xy, z) + f(x, yz) - f(x, y) = 0.$$

Such 2-cocycles are also called **factor sets**, and they can be used to describe isomorphism classes of group extensions, as follows.

5. **Group extensions.** Let  $W$  be a group and  $A$  a normal subgroup, written multiplicatively. Let  $G = W/A$  be the factor group. Let  $F: G \rightarrow W$  be a choice of coset representatives. Define

$$f(x, y) = F(x)F(y)F(xy)^{-1}.$$

- (a) Prove that  $f$  is  $A$ -valued, and that  $f: G \times G \rightarrow A$  is a 2-cocycle.  
 (b) Given a group  $G$  and an abelian group  $A$ , we view an extension  $W$  as an exact sequence

$$1 \rightarrow A \rightarrow W \rightarrow G \rightarrow 1.$$

Show that if two such extensions are isomorphic then the 2-cocycles associated to these extensions as in (a) define the same class in  $H^1(G, A)$ .

- (c) Prove that the map which we obtained above from isomorphism classes of group extensions to  $H^2(G, A)$  is a bijection.

6. **Morphisms of the cohomology functor.** Let  $\lambda: G' \rightarrow G$  be a group homomorphism. Then  $\lambda$  gives rise to an exact functor

$$\Phi_\lambda: \text{Mod}(G) \rightarrow \text{Mod}(G'),$$

because every  $G$ -module can be viewed as a  $G'$ -module by defining the operation of  $\sigma' \in G'$  to be  $\sigma'a = \lambda(\sigma')a$ . Thus we obtain a cohomology functor  $H^{G'} \circ \Phi_\lambda$ .

Let  $G'$  be a subgroup of  $G$ . In dimension 0, we have a morphism of functors

$$\lambda^*: H_G^0 \rightarrow H_{G'}^0 \circ \Phi_\lambda \text{ given by the inclusion } A^G \hookrightarrow A^{G'} = \Phi_\lambda(A)^{G'}.$$

- (a) Show that there is a unique morphism of  $\delta$ -functors

$$\lambda^*: H_G \rightarrow H_{G'} \circ \Phi_\lambda$$

which has the above effect on  $H_G^0$ . We have the following important special cases.

**Restriction.** Let  $H$  be a subgroup of  $G$ . Let  $A$  be a  $G$ -module. A function from  $G$  into  $A$  restricts to a function from  $H$  into  $A$ . In this way, we get a natural homomorphism called the **restriction**

$$\text{res}: H^q(G, A) \rightarrow H^q(H, A).$$

**Inflation.** Suppose that  $H$  is normal in  $G$ . Let  $A^H$  be the subgroup of  $A$  consisting of those elements fixed by  $H$ . Then it is immediately verified that  $A^H$  is stable under  $G$ , and so is a  $G/H$ -module. The inclusion  $A^H \hookrightarrow A$  induces a homomorphism

$$H_G^q(u) = u_q: H^q(G, A^H) \rightarrow H^q(A).$$

Define the **inflation**

$$\text{inf}_{G/H}^H: H^q(G/H, A^H) \rightarrow H^q(G, A)$$

as the composite of the functorial morphism  $H^q(G/H, A^H) \rightarrow H^q(G, A^H)$  followed by the induced homomorphism  $u_q = H_G^q(u)$  as above.

In dimension 0, the inflation gives the identity  $(A^H)^{G/H} = A^G$ .

- (b) Show that the inflation can be expressed on the standard cochain complex by the natural map which to a function of  $G/H$  in  $A^H$  associates a function of  $G$  into  $A^H \subset A$ .
- (c) Prove that the following sequence is exact.

$$0 \rightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A).$$

- (d) Describe how one gets an operation of  $G$  on the cohomology functor  $H_G$  “by conjugation” and functoriality.
- (e) In (c), show that the image of restriction on the right actually lies in  $H^1(H, A)^G$  (the fixed subgroup under  $G$ ).

**Remark.** There is an analogous result for higher cohomology groups, whose proof needs a spectral sequence of Hochschild-Serre. See [La 96], Chapter VI, §2, Theorem 2. It is actually this version for  $H^2$  which is applied to  $H^2(G, K^*)$ , when  $K$  is a Galois extension, and is used in class field theory [ArT 67].

7. Let  $G$  be a group,  $B$  an abelian group and  $M_G(B) = M(G, B)$  the set of mappings from  $G$  into  $B$ . For  $x \in G$  and  $f \in M(G, B)$  define  $([x]f)(y) = f(yx)$ .

- (a) Show that  $B \mapsto M_G(B)$  is a covariant, additive, exact functor from  $\text{Mod}(\mathbf{Z})$  (category of abelian groups) into  $\text{Mod}(G)$ .
- (b) Let  $G'$  be a subgroup of  $G$  and  $G = \bigcup_{x_j} G'$  a coset decomposition. For  $f \in M(G, B)$  let  $f_j$  be the function in  $M(G', B)$  such that  $f_j(y) = f(x_j y)$ . Show that the map

$$f \mapsto \prod_j f_j$$

is a  $G'$ -isomorphism from  $M(G, B)$  to  $\prod_j M(G', B)$ .

8. For each  $G$ -module  $A \in \text{Mod}(G)$ , define  $\varepsilon_A: A \rightarrow M(G, A)$  by the condition  $\varepsilon_A(a) =$  the function  $f_a$  such that  $f_a(\sigma) = \sigma a$  for  $\sigma \in G$ . Show that  $a \mapsto f_a$  is a  $G$ -module embedding, and that the exact sequence

$$0 \rightarrow A \xrightarrow{\varepsilon_A} M(G, A) \rightarrow X_A = \text{coker } \varepsilon_A \rightarrow 0$$

splits over  $\mathbf{Z}$ . (In fact, the map  $f \mapsto f(e)$  splits the left side arrow.)

9. Let  $B \in \text{Mod}(\mathbf{Z})$ . Let  $H^q$  be the left derived functor of  $A \mapsto A^G$ .

- (a) Show that  $H^q(G, M_G(B)) = 0$  for all  $q > 0$ . [Hint: use a contracting homotopy

$$s: C^r(G, M_G(B)) \rightarrow C^{r-1}(G, M_G(B)) \quad \text{by} \quad (sf)_{x_2, \dots, x_r}(x) = f_{x, x_2, \dots, x_r}(1).$$

Show that  $f = sdf + dsf$ .] Thus  $M_G$  erases the cohomology functor.

- (b) Also show that for all subgroups  $G'$  of  $G$  one has  $H^q(G', M_G(B)) = 0$  for  $q > 0$ .

10. Let  $G$  be a group and  $S$  a subgroup. Show that the bifunctors

$$(A, B) \mapsto \text{Hom}_G(A, M_G^S(B)) \text{ and } (A, B) \mapsto \text{Hom}_S(A, B)$$

on  $\text{Mod}(G) \times \text{Mod}(S)$  with value in  $\text{Mod}(\mathbf{Z})$  are isomorphic. The isomorphism is given by the maps

$$\varphi \mapsto (a \mapsto g_a), \text{ for } \varphi \in \text{Hom}_S(A, B), \text{ where } g_a(\sigma) = \varphi(\sigma a), g_a \in M_G^S(B).$$

The inverse mapping is given by

$$f \mapsto f(1) \text{ with } f \in \text{Hom}_G(A, M_G^S(B)).$$

Recall that  $M_G^S(B)$  was defined in Chapter XVIII, §7 for the induced representation. Basically you should already know the above isomorphism.

11. Let  $G$  be a group and  $S$  a subgroup. Show that the map

$$H^q(G, M_G^S(B)) \rightarrow H^q(S, B) \text{ for } B \in \text{Mod}(S),$$

obtained by composing the restriction  $\text{res}_G^S$  with the  $S$ -homomorphism  $f \mapsto f(1)$ , is an isomorphism for  $q > 0$ . [Hint: Use the uniqueness theorem for cohomology functors.]

12. Let  $G$  be a group. Let  $\varepsilon : \mathbf{Z}[G] \rightarrow \mathbf{Z}$  be the homomorphism such that  $\varepsilon(\sum n(x)x) = \sum n(x)$ . Let  $I_G$  be its kernel. Prove that  $I_G$  is an ideal of  $\mathbf{Z}[G]$  and that there is an isomorphism of functors (on the category of groups)

$$G/G^c \approx I_G/I_G^2, \quad \text{by} \quad xG^c \mapsto (x - 1) + I_G^2.$$

13. Let  $A \in \text{Mod}(G)$  and  $\alpha \in H^1(G, A)$ . Let  $\{a(x)\}_{x \in G}$  be a standard 1-cocycle representing  $\alpha$ . Show that there exists a  $G$ -homomorphism  $f : I_G \rightarrow A$  such that  $f(x - 1) = a(x)$ , so  $f \in (\text{Hom}(I_G, A))^G$ . Show that the sequence

$$0 \rightarrow A = \text{Hom}(\mathbf{Z}, A) \rightarrow \text{Hom}(\mathbf{Z}[G], A) \rightarrow \text{Hom}(I_G, A) \rightarrow 0$$

is exact, and that if  $\delta$  is the coboundary for the cohomology sequence, then  $\delta(f) = -\alpha$ .

## Finite groups

We now turn to the case of *finite* groups  $G$ . For such groups and a  $G$ -module  $A$  we have the **trace**

$$T_G : A \rightarrow A \quad \text{defined by} \quad T_G(a) = \sum_{\sigma \in G} \sigma a.$$

We define a module  $A$  to be  **$G$ -regular** if there exists a  $\mathbf{Z}$ -endomorphism  $u : A \rightarrow A$  such that  $\text{id}_A = T_G(u)$ . Recall that the operation of  $G$  on  $\text{End}(A)$  is given by

$$[\sigma]f(a) = \sigma f(\sigma^{-1}a) \text{ for } \sigma \in G.$$

14. (a) Show that a projective object in  $\text{Mod}(G)$  is  $G$ -regular.  
 (b) Let  $R$  be a commutative ring and let  $A$  be in  $\text{Mod}_R(G)$  (the category of  $(G, R)$ -modules). Show that  $A$  is  $R[G]$ -projective if and only if  $A$  is  $R$ -projective and  $R[G]$ -regular, meaning that  $\text{id}_A = T_G(u)$  for some  $R$ -homomorphism  $u : A \rightarrow A$ .
15. Consider the exact sequences:

$$(1) \quad 0 \rightarrow I_G \rightarrow \mathbf{Z}[G] \xrightarrow{\varepsilon} \mathbf{Z} \rightarrow 0$$

$$(2) \quad 0 \rightarrow \mathbf{Z} \xrightarrow{\varepsilon'} \mathbf{Z}[G] \rightarrow J_G \rightarrow 0$$

where the first one defines  $I_G$ , and the second is defined by the embedding

$$\varepsilon' : \mathbf{Z} \rightarrow \mathbf{Z}[G] \text{ such that } \varepsilon'(n) = n(\sum \sigma),$$

i.e. on the “diagonal”. The cokernel of  $\varepsilon'$  is  $J_G$  by definition.

- (a) Prove that both sequences (1) and (2) split in  $\text{Mod}(G)$ .

- (b) Define  $M'_G(A) = \mathbf{Z}[G] \otimes A$  (tensor product over  $\mathbf{Z}$ ) for  $A \in \text{Mod}(G)$ . Show that  $M'_G(A)$  is  $G$ -regular, and that one gets exact sequences  $(1_A)$  and  $(2_A)$  by tensoring  $(1)$  and  $(2)$  with  $A$ . As a result one gets an embedding

$$\varepsilon'_A = \varepsilon' \otimes \text{id} : A = \mathbf{Z} \otimes A \rightarrow \mathbf{Z}[G] \otimes A.$$

16. **Cyclic groups.** Let  $G$  be a finite cyclic group of order  $n$ . Let  $\sigma$  be a generator of  $G$ . Let  $K^i = \mathbf{Z}[G]$  for  $i > 0$ . Let  $\varepsilon : K^0 \rightarrow \mathbf{Z}$  be the augmentation as before. For  $i$  odd  $\geq 1$ , let  $d^i : K^i \rightarrow K^{i-1}$  be multiplication by  $1 - \sigma$ . For  $i$  even  $\geq 2$ , let  $d^i$  be multiplication by  $1 + \sigma + \dots + \sigma^{n-1}$ . Prove that  $K$  is a resolution of  $\mathbf{Z}$ . Conclude that:

For  $i$  odd:  $H^i(G, A) = A^G / T_G A$  where  $T_G : a \mapsto (1 + \sigma + \dots + \sigma^{n-1})a$ ;

For  $i$  even  $\geq 2$ :  $H^i(G, A) = A_T / (1 - \sigma)A$ , where  $A_T$  is the kernel of  $T_G$  in  $A$ .

17. Let  $G$  be a finite group. Show that there exists a  $\delta$ -functor  $\mathbf{H}$  from  $\text{Mod}(G)$  to  $\text{Mod}(\mathbf{Z})$  such that:

- (1)  $\mathbf{H}^0$  is (isomorphic to) the functor  $A \mapsto A^G / T_G A$ .
- (2)  $\mathbf{H}^q(A) = 0$  if  $A$  is injective and  $q > 0$ , and  $\mathbf{H}^q(A) = 0$  if  $A$  is projective and  $q$  is arbitrary.
- (3)  $\mathbf{H}$  is erased by  $G$ -regular modules. In particular,  $\mathbf{H}$  is erased by  $M_G$ .

The  $\delta$ -functor of Exercise 17 is called the **special cohomology functor**. It differs from the other one only in dimension 0.

18. Let  $\mathbf{H} = \mathbf{H}_G$  be the special cohomology functor for a finite group  $G$ . Show that:

$$\mathbf{H}^0(I_G) = 0; \mathbf{H}^0(\mathbf{Z}) \approx \mathbf{H}^1(I) \approx \mathbf{Z}/n\mathbf{Z} \text{ where } n = \#(G);$$

$$\mathbf{H}^0(Q/\mathbf{Z}) = \mathbf{H}^1(\mathbf{Z}) = \mathbf{H}^2(I) = 0$$

$$\mathbf{H}^1(Q/\mathbf{Z}) \approx \mathbf{H}^2(\mathbf{Z}) \approx \mathbf{H}^3(I) \approx G^\wedge = \text{Hom}(G, \mathbf{Q}/\mathbf{Z}) \text{ by definition.}$$

## Injectives

19. (a) Show that if an abelian group  $T$  is injective in the category of abelian groups, then it is divisible.
- (b) Let  $A$  be a principal entire ring. Define the notion of divisibility by elements of  $A$  for modules in a manner analogous to that for abelian groups. Show that an  $A$ -module is injective if and only if it is  $A$ -divisible. [The proof for  $\mathbf{Z}$  should work in exactly the same way.]
20. Let  $S$  be a multiplicative subset of the commutative Noetherian ring  $A$ . If  $I$  is an injective  $A$ -module, show that  $S^{-1}I$  is an injective  $S^{-1}A$ -module.
21. (a) Show that a direct sum of projective modules is projective.  
(b) Show that a direct product of injective modules is injective.
22. Show that a factor module, direct summand, direct product, and direct sum of divisible modules are divisible.
23. Let  $Q$  be a module over a commutative ring  $A$ . Assume that for every left ideal  $J$  of  $A$ , every homomorphism  $\varphi : J \rightarrow Q$  can be extended to a homomorphism of  $A$  into  $Q$ . Show that  $Q$  is injective. [Hint: Given  $M' \subset M$  and  $f : M' \rightarrow Q$ , let  $x_0 \in M$  and  $x_0 \notin M'$ . Let  $J$  be the left ideal of elements  $a \in A$  such that  $ax_0 \in M'$ . Let  $\varphi(a) = f(ax_0)$  and extend  $\varphi$  to  $A$ , as can be done by hypothesis. Then show that

one can extend  $f$  to  $M$  by the formula

$$f(x' + bx_0) = f(x') + \varphi(b),$$

for  $x' \in M$  and  $b \in A$ . Then use Zorn's lemma. This is the same pattern of proof as the proof of Lemma 4.2.]

24. Let

$$0 \rightarrow I_1 \rightarrow I_2 \rightarrow I_3 \rightarrow 0$$

be an exact sequence of modules. Assume that  $I_1, I_2$  are injective.

- (a) Show that the sequence splits.
- (b) Show that  $I_3$  is injective.
- (c) If  $I$  is injective and  $I = M \oplus N$ , show that  $M$  is injective.

25. (Do this exercise after you have read about Noetherian rings.) Let  $A$  be a Noetherian commutative ring, and let  $Q$  be an injective  $A$ -module. Let  $\mathfrak{a}$  be an ideal of  $A$ , and let  $Q^{(\mathfrak{a})}$  be the subset of elements  $x \in Q$  such that  $\mathfrak{a}^n x = 0$  for some  $n$ , depending on  $x$ . Show that  $Q^{(\mathfrak{a})}$  is injective. [Hint: Use Exercise 23.]

26. Let  $A$  be a commutative ring. Let  $E$  be an  $A$ -module, and let  $E^\wedge = \text{Hom}_{\mathbf{Z}}(E, \mathbf{Q}/\mathbf{Z})$  be the dual module. Prove the following statements.

- (a) A sequence

$$0 \rightarrow N \rightarrow M \rightarrow E \rightarrow 0$$

is exact if and only if the dual sequence

$$0 \rightarrow E^\wedge \rightarrow M^\wedge \rightarrow N^\wedge \rightarrow 0$$

is exact.

- (b) Let  $F$  be flat and  $I$  injective in the category of  $A$ -modules. Show that  $\text{Hom}_A(F, I)$  is injective.
- (c)  $E$  is flat if and only if  $E^\wedge$  is injective.

27. **Extensions of modules.** Let  $M, N$  be modules over a ring. By an **extension** of  $M$  by  $N$  we mean an exact sequence

$$(*) \quad 0 \rightarrow N \rightarrow E \rightarrow M \rightarrow 0.$$

We shall now define a map from such extensions to  $\text{Ext}^1(M, N)$ . Let  $P$  be projective, with a surjective homomorphism onto  $M$ , so we get an exact sequence

$$(**) \quad 0 \rightarrow K \xrightarrow{w} P \xrightarrow{p} M \rightarrow 0$$

where  $K$  is defined to be the kernel. Since  $P$  is projective, there exists a homomorphism  $u: P \rightarrow E$ , and depending on  $u$  a unique homomorphism  $v: K \rightarrow N$  making the diagram commutative:

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \longrightarrow & P & \longrightarrow & M & \longrightarrow 0 \\ & & \downarrow v & & \downarrow u & & \downarrow \text{id} & \\ 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M & \longrightarrow 0 \end{array}$$

On the other hand, we have the exact sequence

$$(***) \quad 0 \rightarrow \text{Hom}(M, N) \rightarrow \text{Hom}(P, N) \rightarrow \text{Hom}(K, N) \rightarrow \text{Ext}^1(M, N) \rightarrow 0,$$

with the last term on the right being equal to 0 because  $\text{Ext}^1(P, N) = 0$ . To the extension (\*) we associate the image of  $v$  in  $\text{Ext}^1(M, N)$ .

Prove that this association is a bijection between isomorphism classes of extensions (i.e. isomorphism classes of exact sequences as in (\*)), and  $\text{Ext}^1(M, N)$ . [Hint: Construct an inverse as follows. Given an element  $e$  of  $\text{Ext}^1(M, N)$ , using an exact sequence (\*\*), there is some element  $v \in \text{Hom}(K, N)$  which maps on  $e$  in (\*\*\*)]. Let  $E$  be the push-out of  $v$  and  $w$ . In other words, let  $J$  be the submodule of  $N \oplus P$  consisting of all elements  $(v(x), -w(x))$  with  $x \in K$ , and let  $E = (N \oplus P)/J$ . Show that the map  $y \mapsto (y, 0) \bmod J$  gives an injection of  $N$  into  $E$ . Show that the map  $N \oplus P \rightarrow M$  vanishes on  $J$ , and so gives a surjective homomorphism  $E \rightarrow M \rightarrow 0$ . Thus we obtain an exact sequence (\*); that is, an extension of  $M$  by  $N$ . Thus to each element of  $\text{Ext}^1(M, N)$  we have associated an isomorphism class of extensions of  $M$  by  $N$ . Show that the maps we have defined are inverse to each other between isomorphism classes of extensions and elements of  $\text{Ext}^1(M, N)$ .]

28. Let  $R$  be a principal entire ring. Let  $a \in R$ . For every  $R$ -module  $N$ , prove:
- $\text{Ext}^1(R/aR, N) = N/aN$ .
  - For  $b \in R$  we have  $\text{Ext}^1(R/aR, R/bR) = R/(a, b)$ , where  $(a, b)$  is the g.c.d of  $a$  and  $b$ , assuming  $ab \neq 0$ .

### Tensor product of complexes.

29. Let  $K = \bigoplus K_p$  and  $L = \bigoplus L_q$  be two complexes indexed by the integers, and with boundary maps lower indices by 1. Define  $K \otimes L$  to be the direct sum of the modules  $(K \otimes L)_n$ , where

$$(K \otimes L)_n = \bigoplus_{p+q=n} K_p \otimes L_q.$$

Show that there exist unique homomorphisms

$$d = d_n : (K \otimes L)_n \rightarrow (K \otimes L)_{n-1}$$

such that

$$d(x \otimes y) = d(x) \otimes y + (-1)^p x \otimes d(y).$$

Show that  $K \otimes L$  with these homomorphisms is a complex, that is  $d \circ d = 0$ .

30. Let  $K, L$  be double complexes. We write  $K_{i \cdot}$  and  $L_{i \cdot}$  for the ordinary column complexes of  $K$  and  $L$  respectively. Let  $\varphi: K \rightarrow L$  be a homomorphism of double complexes. Assume that each homomorphism

$$\varphi_i: K_{i \cdot} \rightarrow L_{i \cdot}$$

is a homology isomorphism.

- Prove that  $\text{Tot}(\varphi): \text{Tot}(K) \rightarrow \text{Tot}(L)$  is a homology isomorphism. (If you want to see this worked out, cf. [FuL 85], Chapter V, Lemma 5.4.)
- Prove Theorem 9.8 using (a) instead of spectral sequences.

## Bibliography

- [ArT 68] E. ARTIN and J. TATE, *Class Field Theory*, Benjamin, 1968; Addison-Wesley, 1991
- [At 61] M. ATIYAH, Characters and cohomology of finite groups, *Pub. IHES* **9** (1961), pp. 5–26
- [At 67] M. ATIYAH, *K-theory*, Benjamin, 1967; reprinted Addison-Wesley, 1991
- [ABP 73] M. ATIYAH, R. BOTT, and R. PATODI, On the heat equation and the index theorem, *Invent. Math.* **19** (1973), pp. 279–330
- [Ba 68] H. BASS, *Algebraic K-theory*, Benjamin, 1968
- [Bo 69] R. BOTT, *Lectures on K(X)*, Benjamin, 1969
- [BtD 85] T. BROCKER and T. TOM DIECK, *Representations of Compact Lie Groups*, Springer Verlag, 1985
- [CaE 57] H. CARTAN and S. EILENBERG, *Homological Algebra*, Princeton University Press, 1957
- [CuR 81] C. CURTIS and I. REINER, *Methods of Representation Theory*, John Wiley & Sons, 1981
- [ES 52] S. EILENBERG and N. STEENROD, *Foundations of Algebraic Topology*, Princeton University Press, 1952
- [FuL 85] W. FULTON and S. LANG, *Riemann-Roch algebra*, Springer Verlag, 1985
- [Go 58] R. GODEMENT, *Théorie des faisceaux*, Hermann Paris, 1958
- [GreH 81] M. GREENBERG and J. HARRER, *Algebraic Topology: A First Course*, Benjamin-Addison-Wesley, 1981
- [GriH 78] P. GRIFFITHS and J. HARRIS, *Principles of algebraic geometry*, Wiley Interscience 1978
- [Gro 57] A. GROTHENDIECK, Sur quelques points d'algèbre homologique, *Tohoku Math. J.* **9** (1957) pp. 119–221
- [Gro 68] A. GROTHENDIECK, *Classes de Chern et représentations linéaires des groupes discrets*, Dix exposés sur la cohomologie étale des schémas, North-Holland, Amsterdam, 1968
- [Gu 91] R. GUNNING, *Introduction to holomorphic functions of several variables*, Vol. III Wadsworth & Brooks/Cole, 1990
- [Ha 77] R. HARTSHORNE, *Algebraic Geometry*, Springer Verlag, 1977
- [HiS 70] P. J. HILTON and U. STAMMBACH, *A Course in Homological Algebra*, Graduate Texts in Mathematics, Springer Verlag, 1970.
- [La 96] S. LANG, *Topics in cohomology of groups*, Springer Lecture Notes, 1996
- [Man 69] J. MANIN, *Lectures on the K-functor in Algebraic Geometry*, *Russian Math Surveys* **24**(5) (1969) pp. 1–89
- [Mat 70] H. MATSUMURA, *Commutative Algebra*, Second Edition, Benjamin-Cummings, 1981
- [No 68] D. NORTHCOTT, *Lessons on Rings, Modules and Multiplicities*, Cambridge University Press, 1968
- [No 76] D. NORTHCOTT, *Finite Free Resolutions*, Cambridge University Press, 1976
- [Ro 79] J. ROTMAN, *Introduction to Homological Algebra*, Academic Press, 1979
- [Se 64] J.-P. SERRE, *Cohomologie Galoisiennne*, Springer Lecture Notes **5**, 1964

- [Se 65] J.-P. SERRE, *Algèbre locale, multiplicités*, Springer Lecture Notes **11** (1965)  
Third Edition 1975
- [SGA 6] P. BERTHELOT, A. GROTHENDIECK, L. ILLUSIE et al. *Théorie des intersections  
et théorème de Riemann-Roch*, Springer Lecture Notes 146, 1970
- [Sh 72] S. SHATZ, *Profinite groups, arithmetic and geometry*, Ann. of Math Studies,  
Princeton University Press 1972

---

# CHAPTER XXI

---

## Finite Free Resolutions

This chapter puts together specific computations of complexes and homology. Partly these provide examples for the general theory of Chapter XX, and partly they provide concrete results which have occupied algebraists for a century. They have one aspect in common: the computation of homology is done by means of a finite free resolution, i.e. a finite complex whose modules are finite free.

The first section shows a general technique (the mapping cylinder) whereby the homology arising from some complex can be computed by using another complex which is finite free. One application of such complexes has already been given in Chapter X, putting together Proposition 4.5 followed by Exercises 10–15 of that chapter.

Then we go to major theorems, going from Hilbert's Syzygy theorem, from a century ago, to Serre's theorem about finite free resolutions of modules over polynomial rings, and the Quillen-Suslin theorem. We also include a discussion of certain finite free resolutions obtained from the Koszul complex. These apply, among other things, to the Grothendieck Riemann-Roch theorem of algebraic geometry.

Bibliographical references refer to the list given at the end of Chapter XX.

---

### §1. SPECIAL COMPLEXES

As in the preceding chapter, we work with the category of modules over a ring, but the reader will notice that the arguments hold quite generally in an abelian category.

In some applications one determines homology from a complex which is not suitable for other types of construction, like changing the base ring. In this section, we give a general procedure which constructs another complex with

better properties than the first one, while giving the same homology. For an application to Noetherian modules, see Exercises 12–15 of Chapter X.

Let  $f: K \rightarrow C$  be a morphism of complexes. We say that  $f$  is a **homology isomorphism** if the natural map

$$H(f): H(K) \rightarrow H(C)$$

is an isomorphism. The definition is valid in an abelian category, but the reader may think of modules over a ring, or abelian groups even. A family  $\mathfrak{F}$  of objects will be called **sufficient** if given an object  $E$  there exists an element  $F$  in  $\mathfrak{F}$  and an epimorphism

$$F \rightarrow E \rightarrow 0,$$

and if  $\mathfrak{F}$  is closed under taking finite direct sums. For instance, we may use for  $\mathfrak{F}$  the family of free modules. However, in important applications, we shall deal with finitely generated modules, in which case  $\mathfrak{F}$  might be taken as the family of finite free modules. These are in fact the applications I have in mind, which resulted in having axiomatized the situation.

**Proposition 1.1.** *Let  $C$  be a complex such that  $H^p(C) \neq 0$  only for  $0 \leq p \leq n$ . Let  $\mathfrak{F}$  be a sufficient family of projectives. There exists a complex*

$$0 \rightarrow K^0 \rightarrow K^1 \rightarrow \cdots \rightarrow K^n \rightarrow 0$$

such that:

$$K^p \neq 0 \quad \text{only for } 0 \leq p \leq n;$$

$$K^p \text{ is in } \mathfrak{F} \text{ for all } p \geq 1;$$

and there exists a homomorphism of complexes

$$f: K \rightarrow C$$

which is a homology isomorphism.

*Proof.* We define  $f_m$  by descending induction on  $m$ :

$$\begin{array}{ccccccc} \longrightarrow & K^m & \longrightarrow & K^{m+1} & \xrightarrow{\delta_K^{m+1}} & K^{m+2} & \longrightarrow \\ & \downarrow f_m & & \downarrow f_{m+1} & & \downarrow f_{m+2} & \\ \longrightarrow & C^m & \longrightarrow & C^{m+1} & \xrightarrow{\delta_C^{m+1}} & C^{m+2} & \longrightarrow \end{array}$$

We suppose that we have defined a morphism of complexes with  $p \geq m + 1$  such that  $H^p(f)$  is an isomorphism for  $p \geq m + 2$ , and

$$f_{m+1}: Z^{m+1}(K) \rightarrow H^{m+1}(C)$$

is an epimorphism, where  $Z$  denotes the cycles, that is  $\text{Ker } \delta$ . We wish to construct  $K^m$  and  $f_m$ , thus propagating to the left. First let  $m \geq 0$ . Let  $B^{m+1}$  be the kernel of

$$\text{Ker } \delta_K^{m+1} \rightarrow H^{m+1}(C).$$

Let  $K'$  be in  $\mathfrak{F}$  with an epimorphism

$$\delta' : K' \rightarrow B^{m+1}.$$

Let  $K'' \rightarrow H^m(C)$  be an epimorphism with  $K''$  in  $\mathfrak{F}$ , and let

$$f'' : K'' \rightarrow Z^m(C)$$

be any lifting, which exists since  $K''$  is projective. Let

$$K^m = K' \oplus K''$$

and define  $\delta^m : K^m \rightarrow K^{m+1}$  to be  $\delta'$  on  $K'$  and 0 on  $K''$ . Then

$$f_{m+1} \circ \delta'(K') \subset \delta_C(C_m),$$

and hence there exists  $f' : K' \rightarrow C^m$  such that

$$\delta_C \circ f' = f_{m+1} \circ \delta'.$$

We now define  $f_m : K^m \rightarrow C^m$  to be  $f'$  on  $K'$  and  $f''$  on  $K''$ . Then we have defined a morphism of complexes truncated down to  $m$  as desired.

Finally, if  $m = -1$ , we have constructed down to  $K^0$ ,  $\delta^0$ , and  $f_0$  with

$$K^0 \xrightarrow{f_0} H^0(C) \rightarrow 0$$

exact. The last square looks like this, defining  $K^{-1} = 0$ .

$$\begin{array}{ccccccc} 0 & \longrightarrow & K' \oplus K'' & \xrightarrow{\delta_0 = \delta'} & \delta' K' \subset K^1 & & \\ & & \downarrow f' & \swarrow f'' & & & \\ 0 & \longrightarrow & C^0 & \longrightarrow & C^1 & & \end{array}$$

We replace  $K^0$  by  $K^0 / (\text{Ker } \delta^0 \cap \text{Ker } f_0)$ . Then  $H^0(f)$  becomes an isomorphism, thus proving the proposition.

We want to say something more about  $K^0$ . For this purpose, we define a new concept. Let  $\mathfrak{F}$  be a family of objects in the given abelian category (think of modules in first reading). We shall say that  $\mathfrak{F}$  is **complete** if it is sufficient, and for any exact sequence

$$0 \rightarrow F' \rightarrow F \rightarrow F'' \rightarrow 0$$

with  $F''$  and  $F$  in  $\mathfrak{F}$  then  $F'$  is also in  $\mathfrak{F}$ .

**Example.** In Chapter XVI, Theorem 3.4 we proved that the family of finite flat modules in the category of finite modules over a Noetherian ring is complete. Similarly, the family of flat modules in the category of modules over a ring is complete. We cannot get away with just projectives or free modules, because in the statement of the proposition,  $K^0$  is not necessarily free but we want to include it in the family as having especially nice properties. In practice, the family consists of the flat modules, or finite flat modules. Cf. Chapter X, Theorem 4.4, and Chapter XVI, Theorem 3.8.

**Proposition 1.2.** *Let  $f: K \rightarrow C$  be a morphism of complexes, such that  $K^p, H^p(C)$  are  $\neq 0$  only for  $p = 1, \dots, n$ . Let  $\mathfrak{F}$  be a complete family, and assume that  $K^p, C^p$  are in  $\mathfrak{F}$  for all  $p$ , except possibly for  $K^0$ . If  $f$  is a homology isomorphism, then  $K^0$  is also in  $\mathfrak{F}$ .*

Before giving the proof, we define a new complex called the **mapping cylinder** of an arbitrary morphism of complexes  $f$  by letting

$$M^p = K^p \oplus C^{p-1}$$

and defining  $\delta_M: M^p \rightarrow M^{p+1}$  by

$$\delta_M(x, y) = (\delta x, fx - \delta y).$$

It is trivially verified that  $M$  is then a complex, i.e.  $\delta \circ \delta = 0$ . If  $C'$  is the complex obtained from  $C$  by shifting degrees by one (and making a sign change in  $\delta_C$ ), so  $C'^p = C^{p-1}$ , then we get an exact sequence of complexes

$$0 \rightarrow C' \rightarrow M \rightarrow K \rightarrow 0$$

and hence the **mapping cylinder exact cohomology sequence**

$$\begin{array}{ccccccc} H^p(K) & \longrightarrow & H^{p+1}(C') & \longrightarrow & H^{p+1}(M) & \longrightarrow & H^{p+1}(K) \longrightarrow H^{p+2}(C') \\ & & \parallel & & & & \parallel \\ & & H^p(C) & & & & H^{p+1}(C) \end{array}$$

and one sees from the definitions that the cohomology maps

$$H^p(K) \rightarrow H^{p+1}(C') \approx H^p(C)$$

are the ones induced by  $f: K \rightarrow C$ .

We now return to the assumptions of Proposition 1.2, so that these maps are isomorphisms. We conclude that  $H(M) = 0$ . This implies that the sequence

$$0 \rightarrow K^0 \rightarrow M^1 \rightarrow M^2 \rightarrow \dots \rightarrow M^{n+1} \rightarrow 0$$

is exact. Now each  $M^p$  is in  $\mathfrak{F}$  by assumption. Inserting the kernels and cokernels at each step and using induction together with the definition of a complete family, we conclude that  $K^0$  is in  $\mathfrak{F}$ , as was to be shown.

In the next proposition, we have axiomatized the situation so that it is applicable to the tensor product, discussed later, and to the case when the family  $\mathfrak{F}$  consists of flat modules, as defined in Chapter XVI. No knowledge of this chapter is needed here, however, since the axiomatization uses just the general language of functors and exactness.

Let  $\mathfrak{F}$  be a complete family again, and let  $T$  be a covariant additive functor on the given category. We say that  $\mathfrak{F}$  is **exact for  $T$**  if given an exact sequence

$$0 \rightarrow F' \rightarrow F \rightarrow F'' \rightarrow 0$$

in  $\mathfrak{F}$ , then

$$0 \rightarrow T(F') \rightarrow T(F) \rightarrow T(F'') \rightarrow 0$$

is exact.

**Proposition 1.3.** *Let  $\mathfrak{F}$  be a complete family which is exact for  $T$ . Let  $f : K \rightarrow C$  be a morphism of complexes, such that  $K^p$  and  $C^p$  are in  $\mathfrak{F}$  for all  $p$ , and  $K^p, H^p(C)$  are zero for all but a finite number of  $p$ . Assume that  $f$  is a homology isomorphism. Then*

$$T(f) : T(K) \rightarrow T(C)$$

*is a homology isomorphism.*

*Proof.* Construct the mapping cylinder  $M$  for  $f$ . As in the proof of Proposition 1.2, we get  $H(M) = 0$  so  $M$  is exact. We then start inductively from the right with zeros. We let  $Z^p$  be the cycles in  $M^p$  and use the short exact sequences

$$0 \rightarrow Z^p \rightarrow M^p \rightarrow Z^{p+1} \rightarrow 0$$

together with the definition of a complete family to conclude that  $Z^p$  is in  $\mathfrak{F}$  for all  $p$ . Hence the short sequences obtained by applying  $T$  are exact. But  $T(M)$  is the mapping cylinder of the morphism

$$T(f) : T(K) \rightarrow T(C),$$

which is therefore an isomorphism, as one sees from the homology sequence of the mapping cylinder. This concludes the proof.

---

## §2. FINITE FREE RESOLUTIONS

The first part of this section develops the notion of resolutions for a case somewhat more subtle than projective resolutions, and gives a good example for the considerations of Chapter XX. Northcott in [No 76] pointed out that minor adjustments of standard proofs also applied to the non-Noetherian rings, only occasionally slightly less tractable than the Noetherian ones.

Let  $A$  be a ring. A module  $E$  is called **stably free** if there exists a finite free module  $F$  such that  $E \oplus F$  is finite free, and thus isomorphic to  $A^{(n)}$  for some positive integer  $n$ . In particular,  $E$  is projective and finitely generated.

We say that a module  $M$  has a **finite free resolution** if there exists a resolution

$$0 \rightarrow E_n \rightarrow \cdots \rightarrow E_0 \rightarrow M \rightarrow 0$$

such that each  $E_i$  is finite free.

**Theorem 2.1.** *Let  $M$  be a projective module. Then  $M$  is stably free if and only if  $M$  admits a finite free resolution.*

*Proof.* If  $M$  is stably free then it is trivial that  $M$  has a finite free resolution. Conversely assume the existence of the resolution with the above notation. We prove that  $M$  is stably free by induction on  $n$ . The assertion is obvious if  $n = 0$ . Assume  $n \geq 1$ . Insert the kernels and cokernels at each step, in the manner of dimension shifting. Say

$$M_1 = \text{Ker}(E_0 \rightarrow P),$$

giving rise to the exact sequence

$$0 \rightarrow M_1 \rightarrow E_0 \rightarrow M \rightarrow 0.$$

Since  $M$  is projective, this sequence splits, and  $E_0 \approx M \oplus M_1$ . But  $M_1$  has a finite free resolution of length smaller than the resolution of  $M$ , so there exists a finite free module  $F$  such that  $M_1 \oplus F$  is free. Since  $E_0 \oplus F$  is also free, this concludes the proof of the theorem.

A resolution

$$0 \rightarrow E_n \rightarrow \cdots \rightarrow E_0 \rightarrow M \rightarrow 0$$

is called **stably free** if all the modules  $E_i$  ( $i = 0, \dots, n$ ) are stably free.

**Proposition 2.2.** *Let  $M$  be an  $A$ -module. Then  $M$  has a finite free resolution of length  $n \geq 1$  if and only if  $M$  has a stably free resolution of length  $n$ .*

*Proof.* One direction is trivial, so we suppose given a stably free resolution with the above notation. Let  $0 \leq i < n$  be some integer, and let  $F_i, F_{i+1}$  be finite free such that  $E_i \oplus F_i$  and  $E_{i+1} \oplus F_{i+1}$  are free. Let  $F = F_i \oplus F_{i+1}$ . Then we can form an exact sequence

$$0 \rightarrow E_n \rightarrow \cdots \rightarrow E_{i+1} \oplus F \rightarrow E_i \oplus F \rightarrow \cdots \rightarrow E_0 \rightarrow M \rightarrow 0$$

in the obvious manner. In this way, we have changed two consecutive modules in the resolution to make them free. Proceeding by induction, we can then make  $E_0, E_1$  free, then  $E_1, E_2$  free, and so on to conclude the proof of the proposition.

The next lemma is designed to facilitate dimension shifting.

We say that two modules  $M_1, M_2$  are **stably isomorphic** if there exist finite free modules  $F_1, F_2$  such that  $M_1 \oplus F_1 \approx M_2 \oplus F_2$ .

**Lemma 2.3.** *Let  $M_1$  be stably isomorphic to  $M_2$ . Let*

$$0 \rightarrow N_1 \rightarrow E_1 \rightarrow M_1 \rightarrow 0$$

$$0 \rightarrow N_2 \rightarrow E_2 \rightarrow M_2 \rightarrow 0$$

*be exact sequences, where  $M_1$  is stably isomorphic to  $M_2$ , and  $E_1, E_2$  are stably free. Then  $N_1$  is stably isomorphic to  $N_2$ .*

*Proof.* By definition, there is an isomorphism  $M_1 \oplus F_1 \approx M_2 \oplus F_2$ . We have exact sequences

$$0 \rightarrow N_1 \rightarrow E_1 \oplus F_1 \rightarrow M_1 \oplus F_1 \rightarrow 0$$

$$0 \rightarrow N_2 \rightarrow E_2 \oplus F_2 \rightarrow M_2 \oplus F_2 \rightarrow 0$$

By Schanuel's lemma (see below) we conclude that

$$N_1 \oplus E_2 \oplus F_2 \approx N_2 \oplus E_1 \oplus F_1.$$

Since  $E_1, E_2, F_1, F_2$  are stably free, we can add finite free modules to each side so that the summands of  $N_1$  and  $N_2$  become free, and by adding 1-dimensional free modules if necessary, we can preserve the isomorphism, which proves that  $N_1$  is stably isomorphic to  $N_2$ .

We still have to take care of **Schanuel's lemma**:

**Lemma 2.4.** *Let*

$$0 \rightarrow K \rightarrow P \rightarrow M \rightarrow 0$$

$$0 \rightarrow K' \rightarrow P' \rightarrow M \rightarrow 0$$

*be exact sequences where  $P, P'$  are projective. Then there is an isomorphism*

$$K \oplus P' \approx K' \oplus P.$$

*Proof.* Since  $P$  is projective, there exists a homomorphism  $P \rightarrow P'$  making the right square in the following diagram commute.

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \xrightarrow{i} & P & \longrightarrow & M \longrightarrow 0 \\ & & \downarrow u & & \downarrow w & & \downarrow \text{id} \\ 0 & \longrightarrow & K' & \xrightarrow{j} & P' & \longrightarrow & M \longrightarrow 0 \end{array}$$

Then one can find a homomorphism  $K \rightarrow K'$  which makes the left square commute. Then we get an exact sequence

$$0 \rightarrow K \rightarrow P \oplus K' \rightarrow P' \rightarrow 0$$

by  $x \mapsto (ix, ux)$  for  $x \in K$  and  $(y, z) \mapsto wy - jz$ . We leave the verification of exactness to the reader. Since  $P'$  is projective, the sequence splits thus proving Schanuel's lemma. This also concludes the proof of Lemma 2.3.

The minimal length of a stably free resolution of a module is called its **stably free dimension**. To construct a stably free resolution of a finite module, we proceed inductively. The preceding lemmas allow us to carry out the induction, and also to stop the construction if a module is of finite stably free dimension.

**Theorem 2.5.** *Let  $M$  be a module which admits a stably free resolution of length  $n$*

$$0 \rightarrow E_n \rightarrow \cdots \rightarrow E_0 \rightarrow M \rightarrow 0.$$

Let

$$F_m \rightarrow \cdots \rightarrow F_0 \rightarrow M \rightarrow 0$$

be an exact sequence with  $F_i$  stably free for  $i = 0, \dots, m$ .

(i) If  $m < n - 1$  then there exists a stably free  $F_{m+1}$  such that the exact sequence can be continued exactly to

$$F_{m+1} \rightarrow \cdots \rightarrow F_0 \rightarrow M \rightarrow 0.$$

(ii) If  $m = n - 1$ , let  $F_n = \text{Ker}(F_{n-1} \rightarrow F_{n-2})$ . Then  $F_n$  is stably free and thus

$$0 \rightarrow F_n \rightarrow F_{n-1} \rightarrow \cdots \rightarrow F_0 \rightarrow M \rightarrow 0$$

is a stably free resolution.

**Remark.** If  $A$  is Noetherian then of course (i) is trivial, and we can even pick  $F_{m+1}$  to be finite free.

*Proof.* Insert the kernels and cokernels in each sequence, say

$$K_m = \text{Ker}(E_m \rightarrow E_{m-1}) \quad \text{if } m \neq 0$$

$$K_0 = \text{Ker}(E_0 \rightarrow M),$$

and define  $K'_m$  similarly. By Lemma 2.3,  $K_m$  is stably isomorphic to  $K'_m$ , say

$$K_m \oplus F \approx K'_m \oplus F'$$

with  $F, F'$  finite free.

If  $m < n - 1$ , then  $K_m$  is a homomorphic image of  $E_{m+1}$ ; so both  $K_m \oplus F$  and  $K'_m \oplus F'$  are homomorphic images of  $E_{m+1} \oplus F$ . Therefore  $K'_m$  is a homomorphic image of  $E_{m+1} \oplus F$  which is stably free. We let  $F_{m+1} = E_{m+1} \oplus F$  to conclude the proof in this case.

If  $m = n - 1$ , then we can take  $K_n = E_n$ . Hence  $K_m \oplus F$  is stably free, and so is  $K'_m \oplus F'$  by the isomorphism in the first part of the proof. It follows trivially that  $K'_m$  is stably free, and by definition,  $K'_m = F_{m+1}$  in this case. This concludes the proof of the theorem.

**Corollary 2.6.** *If  $0 \rightarrow M_1 \rightarrow E \rightarrow M \rightarrow 0$  is exact,  $M$  has stably free dimension  $\leq n$ , and  $E$  is stably free, then  $M_1$  has stably free dimension  $\leq n - 1$ .*

**Theorem 2.7.** *Let*

$$0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$$

*be an exact sequence. If any two of these modules have a finite free resolution, then so does the third.*

*Proof.* Assume  $M'$  and  $M$  have finite free resolutions. Since  $M$  is finite, it follows that  $M''$  is also finite. By essentially the same construction as Chapter XX, Lemma 3.8, we can construct an exact and commutative diagram where  $E', E, E''$  are stably free:

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 & \longrightarrow & M'_1 & \longrightarrow & M_1 & \longrightarrow & M''_1 & \longrightarrow 0 \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
 0 & \longrightarrow & E' & \longrightarrow & E & \longrightarrow & E'' & \longrightarrow 0 \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow 0 \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
 & 0 & & 0 & & 0 &
 \end{array}$$

We then argue by induction on the stably free dimension of  $M$ . We see that  $M_1$  has stably free dimension  $\leq n - 1$  (actually  $n - 1$ , but we don't care), and  $M'_1$  has finite stably free dimension. By induction we are reduced to the case when  $M$  has stably free dimension 0, which means that  $M$  is stably free. Since by assumption there is a finite free resolution of  $M'$ , it follows that  $M''$  also has a finite free resolution, thus concluding the proof of the first assertion.

Next assume that  $M', M''$  have finite free resolutions. Then  $M$  is finite. If both  $M'$  and  $M''$  have stably free dimension 0, then  $M', M''$  are projective and  $M \approx M' \oplus M''$  is also stably free and we are done. We now argue by induction on the maximum of their stably free dimension  $n$ , and we assume  $n \geq 1$ . We can construct an exact and commutative diagram as in the previous case with  $E', E, E''$  finite free (we leave the details to the reader). But the maximum of the stably free dimensions of  $M'_1$  and  $M''_1$  is at most  $n - 1$ , and so by induction it follows that  $M_1$  has finite stably free dimension. This concludes the proof of the second case.

Observe that the third statement has been proved in Chapter XX, Lemma 3.8 when  $A$  is Noetherian, taking for  $\mathfrak{Q}$  the abelian category of finite modules, and for  $\mathfrak{C}$  the family of stably free modules. Mitchell Stokes pointed out to me that the statement is valid in general without Noetherian assumption, and can be proved as follows. We assume that  $M, M''$  have finite free resolutions. We first show that  $M'$  is finitely generated. Indeed, suppose first that  $M$  is finite free. We have two exact sequences

$$\begin{aligned} 0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0 \\ 0 \rightarrow K'' \rightarrow F'' \rightarrow M'' \rightarrow 0 \end{aligned}$$

where  $F''$  is finite free, and  $K''$  is finitely generated because of the assumption that  $M''$  has a finite free resolution. That  $M'$  is finitely generated follows from Schanuel's lemma. If  $M$  is not free, one can reduce the finite generation of  $M'$  to the case when  $M$  is free by a pull-back, which we leave to the reader.

Now suppose that the stably free dimension of  $M''$  is positive. We use the same exact commutative diagram as in the previous cases, with  $E', E, E''$  finite free. The stably free dimension of  $M'_1$  is one less than that of  $M''$ , and we are done by induction. This concludes the proof of Theorem 2.7.

This also concludes our general discussion of finite free resolutions. For more information cf. Northcott's book on the subject.

We now come to the second part of this section, which provides an application to polynomial rings.

**Theorem 2.8.** *Let  $R$  be a commutative Noetherian ring. Let  $x$  be a variable. If every finite  $R$ -module has a finite free resolution, then every finite  $R[x]$ -module has a finite free resolution.*

In other words, in the category of finite  $R$ -modules, if every object is of finite stably free dimension, then the same property applies to the category of finite  $R[x]$ -modules. Before proving the theorem, we state the application we have in mind.

**Theorem 2.9. (Serre).** *If  $k$  is a field and  $x_1, \dots, x_r$  independent variables, then every finite projective module over  $k[x_1, \dots, x_r]$  is stably free, or equivalently admits a finite free resolution.*

*Proof.* By induction and Theorem 2.8 we conclude that every finite module over  $k[x_1, \dots, x_r]$  is of finite stably free dimension. (We are using Theorem 2.1.) This concludes the proof.

The rest of this section is devoted to the proof of Theorem 2.8.

Let  $M$  be a finite  $R[x]$ -module. By Chapter X, Corollary 2.8,  $M$  has a finite filtration

$$M = M_0 \supset M_1 \supset \dots \supset M_n = 0$$

such that each factor  $M_i/M_{i+1}$  is isomorphic to  $R[x]/P_i$  for some prime  $P_i$ . In light of Theorem 2.7, it suffices to prove the theorem in case  $M = R[x]/P$  where  $P$  is prime, which we now assume. In light of the exact sequence

$$0 \rightarrow P \rightarrow R[x] \rightarrow R[x]/P \rightarrow 0.$$

and Theorem 2.7, we note that  $M$  has a finite free resolution if and only if  $P$  does.

Let  $\mathfrak{p} = P \cap R$ . Then  $\mathfrak{p}$  is prime in  $R$ . Suppose there is some  $M = R[x]/P$  which does not admit a finite free resolution. Among all such  $M$  we select one for which the intersection  $\mathfrak{p}$  is maximal in the family of prime ideals obtained as above. This is possible in light of one of the basic properties characterizing Noetherian rings.

Let  $R_0 = R/\mathfrak{p}$  so  $R_0$  is entire. Let  $P_0 = P/\mathfrak{p}R[x]$ . Then we may view  $M$  as an  $R_0[x]$ -module, equal to  $R_0/P_0$ . Let  $f_1, \dots, f_n$  be a finite set of generators for  $P_0$ , and let  $f$  be a polynomial of minimal degree in  $P_0$ . Let  $K_0$  be the quotient field of  $R_0$ . By the Euclidean algorithm, we can write

$$f_i = q_i f + r_i \quad \text{for } i = 1, \dots, n$$

with  $q_i, r_i \in K_0[x]$  and  $\deg r_i < \deg f$ . Let  $d_0$  be a common denominator for the coefficients of all  $q_i, r_i$ . Then  $d_0 \neq 0$  and

$$d_0 f_i = q'_i f + r'_i$$

where  $q'_i = d_0 q_i$  and  $r'_i = d_0 r_i$  lie in  $R_0[x]$ . Since  $\deg f$  is minimal in  $P_0$  it follows that  $r'_i = 0$  for all  $i$ , so

$$d_0 P_0 \subset R_0[x]f = (f).$$

Let  $N_0 = P_0/(f)$ , so  $N_0$  is a module over  $R_0[x]$ , and we can also view  $N_0$  as a module over  $R[x]$ . When so viewed, we denote  $N_0$  by  $N$ . Let  $d \in R$  be any element reducing to  $d_0 \bmod \mathfrak{p}$ . Then  $d \notin \mathfrak{p}$  since  $d_0 \neq 0$ . The module  $N_0$  has a finite filtration such that each factor module of the filtration is isomorphic to some  $R_0[x]/Q_0$  where  $Q_0$  is an associated prime of  $N_0$ . Let  $Q$  be the inverse image of  $Q_0$  in  $R[x]$ . These prime ideals  $Q$  are precisely the associated primes of  $N$  in  $R[x]$ . Since  $d_0$  kills  $N_0$  it follows that  $d$  kills  $N$  and therefore  $d$  lies in every associated prime of  $N$ . By the maximality property in the selection of  $P$ ,

it follows that every one of the factor modules in the filtration of  $N$  has a finite free resolution, and by Theorem 2.7 it follows that  $N$  itself has a finite free resolution.

Now we view  $R_0[x]$  as an  $R[x]$ -module, via the canonical homomorphism

$$R[x] \rightarrow R_0[x] = R[x]/\mathfrak{p}R[x].$$

By assumption,  $\mathfrak{p}$  has a finite free resolution as  $R$ -module, say

$$0 \rightarrow E_n \rightarrow \cdots \rightarrow E_0 \rightarrow \mathfrak{p} \rightarrow 0.$$

Then we may simply form the modules  $E_i[x]$  in the obvious sense to obtain a finite free resolution of  $\mathfrak{p}[x] = \mathfrak{p}R[x]$ . From the exact sequence

$$0 \rightarrow \mathfrak{p}R[x] \rightarrow R[x] \rightarrow R_0[x] \rightarrow 0$$

we conclude that  $R_0[x]$  has a finite free resolution as  $R[x]$ -module.

Since  $R_0$  is entire, it follows that the principal ideal  $(f)$  in  $R_0[x]$  is  $R[x]$ -isomorphic to  $R_0[x]$ , and therefore has a finite free resolution as  $R[x]$ -module. Theorem 2.7 applied to the exact sequence of  $R[x]$ -modules

$$0 \rightarrow (f) \rightarrow P_0 \rightarrow N \rightarrow 0$$

shows that  $P_0$  has a finite free resolution; and further applied to the exact sequence

$$0 \rightarrow \mathfrak{p}R[x] \rightarrow P \rightarrow P_0 \rightarrow 0$$

shows that  $P$  has a finite free resolution, thereby concluding the proof of Theorem 2.8.

### §3. UNIMODULAR POLYNOMIAL VECTORS

Let  $A$  be a commutative ring. Let  $(f_1, \dots, f_n)$  be elements of  $A$  generating the unit ideal. We call such elements **unimodular**. We shall say that they have the **unimodular extension property** if there exists a matrix in  $GL_n(A)$  with first column  $'(f_1, \dots, f_n)$ . If  $A$  is a principal entire ring, then it is a trivial exercise to prove that this is always the case. Serre originally asked the question whether it is true for a polynomial ring  $k[x_1, \dots, x_r]$  over a field  $k$ . The problem was solved by Quillen and Suslin. We give here a simplification of Suslin's proof by Vaserstein, also using a previous result of Horrocks. The method is by induction on the number of variables, in some fashion.

We shall write  $f = '(f_1, \dots, f_n)$  for the column vector. We first remark that  $f$  has the unimodular extension property if and only if the vector obtained by a permutation of its components has this property. Similarly, we can make

the usual row operations, adding a multiple  $gf_i$  to  $f_j$  ( $j \neq i$ ), and  $f$  has the unimodular extension property if and only if any one of its transforms by row operations has the unimodular extension property.

We first prove the theorem in a context which allows the induction.

**Theorem 3.1.** (Horrocks). *Let  $(\mathfrak{o}, \mathfrak{m})$  be a local ring and let  $A = \mathfrak{o}[x]$  be the polynomial ring in one variable over  $\mathfrak{o}$ . Let  $f$  be a unimodular vector in  $A^{(n)}$  such that some component has leading coefficient 1. Then  $f$  has the unimodular extension property.*

*Proof.* (Suslin). If  $n = 1$  or  $2$  then the theorem is obvious even without assuming that  $\mathfrak{o}$  is local. So we assume  $n \geq 3$  and do an induction of the smallest degree  $d$  of a component of  $f$  with leading coefficient 1. First we note that by the Euclidean algorithm and row operations, we may assume that  $f_1$  has leading coefficient 1, degree  $d$ , and that  $\deg f_i < d$  for  $j \neq 1$ . Since  $f$  is unimodular, a relation  $\sum g_i f_i = 1$  shows that not all coefficients of  $f_2, \dots, f_n$  can lie in the maximal ideal  $\mathfrak{m}$ . Without loss of generality, we may assume that some coefficient of  $f_2$  does not lie in  $\mathfrak{m}$  and so is a unit since  $\mathfrak{o}$  is local. Write

$$\begin{aligned} f_1(x) &= x^d + a_{d-1}x^{d-1} + \cdots + a_0 \quad \text{with } a_i \in \mathfrak{o}, \\ f_2(x) &= \qquad b_s x^s + \cdots + b_0 \quad \text{with } b_i \in \mathfrak{o}, s \leq d-1, \end{aligned}$$

so that some  $b_i$  is a unit. Let  $\mathfrak{a}$  be the ideal generated by all leading coefficients of polynomials  $g_1 f_1 + g_2 f_2$  of degree  $\leq d-1$ . Then  $\mathfrak{a}$  contains all the coefficients  $b_i$ ,  $i = 0, \dots, s$ . One sees this by descending induction, starting with  $b_s$  which is obvious, and then using a linear combination

$$x^{d-s} f_2(x) - b_s f_1(x).$$

Therefore  $\mathfrak{a}$  is the unit ideal, and there exists a polynomial  $g_1 f_1 + g_2 f_2$  of degree  $\leq d-1$  and leading coefficient 1. By row operations, we may now get a polynomial of degree  $\leq d-1$  and leading coefficient 1 as some component in the  $i$ -th place for some  $i \neq 1, 2$ . Thus ultimately, by induction, we may assume that  $d = 0$  in which case the theorem is obvious. This concludes the proof.

Over any commutative ring  $A$ , for two column vectors  $f, g$  we write  $f \sim g$  over  $A$  to mean that there exists  $M \in GL_n(A)$  such that

$$f = Mg,$$

and we say that  $f$  is **equivalent to  $g$  over  $A$** . Horrocks' theorem states that a unimodular vector  $f$  with one component having leading coefficient 1 is  $\mathfrak{o}[x]$ -equivalent to the first unit vector  $e^1$ . We are interested in getting a similar descent over non-local rings. We can write  $f = f(x)$ , and there is a natural “constant” vector  $f(0)$  formed with the constant coefficients. As a corollary of Horrocks' theorem, we get:

**Corollary 3.2.** *Let  $\mathfrak{o}$  be a local ring. Let  $f$  be a unimodular vector in  $\mathfrak{o}[x]^{(n)}$  such that some component has leading coefficient 1. Then  $f \sim f(0)$  over  $\mathfrak{o}[x]$ .*

*Proof.* Note that  $f(0) \in \mathfrak{o}^{(n)}$  has one component which is a unit. It suffices to prove that over any commutative ring  $R$  any element  $c \in R^{(n)}$  such that some component is a unit is equivalent over  $R$  to  $e^1$ , and this is obvious.

**Lemma 3.3.** *Let  $R$  be an entire ring, and let  $S$  be a multiplicative subset. Let  $x, y$  be independent variables. If  $f(x) \sim f(0)$  over  $S^{-1}R[x]$ , then there exists  $c \in S$  such that  $f(x + cy) \sim f(x)$  over  $R[x, y]$ .*

*Proof.* Let  $M \in GL_n(S^{-1}R[x])$  be such that  $f(x) = M(x)f(0)$ . Then  $M(x)^{-1}f(x) = f(0)$  is constant, and thus invariant under translation  $x \mapsto x + y$ . Let

$$G(x, y) = M(x)M(x + y)^{-1}.$$

Then  $G(x, y)f(x + y) = f(x)$ . We have  $G(x, 0) = I$  whence

$$G(x, y) = I + yH(x, y)$$

with  $H(x, y) \in S^{-1}R[x, y]$ . There exists  $c \in S$  such that  $cH$  has coefficients in  $R$ . Then  $G(x, cy)$  has coefficients in  $R$ . Since  $\det M(x)$  is constant in  $S^{-1}R$ , it follows that  $\det M(x + cy)$  is equal to this same constant and therefore that  $\det G(x, cy) = 1$ . This proves the lemma.

**Theorem 3.4.** *Let  $R$  be an entire ring, and let  $f$  be a unimodular vector in  $R[x]^{(n)}$ , such that one component has leading coefficient 1. Then  $f(x) \sim f(0)$  over  $R[x]$ .*

*Proof.* Let  $J$  be the set of elements  $c \in R$  such that  $f(x + cy)$  is equivalent to  $f(x)$  over  $R[x, y]$ . Then  $J$  is an ideal, for if  $c \in J$  and  $a \in R$  then replacing  $y$  by  $ay$  in the definition of equivalence shows that  $f(x + cay)$  is equivalent to  $f(x)$  over  $R[x, ay]$ , so over  $R[x, y]$ . Equally easily, one sees that if  $c, c' \in J$  then  $c + c' \in J$ . Now let  $\mathfrak{p}$  be a prime ideal of  $R$ . By Corollary 3.2 we know that  $f(x)$  is equivalent to  $f(0)$  over  $R_{\mathfrak{p}}[x]$ , and by Lemma 3.3 it follows that there exists  $c \in R$  and  $c \notin \mathfrak{p}$  such that  $f(x + cy)$  is equivalent to  $f(x)$  over  $R[x, y]$ . Hence  $J$  is not contained in  $\mathfrak{p}$ , and so  $J$  is unit ideal in  $R$ , so there exists an invertible matrix  $M(x, y)$  over  $R[x, y]$  such that

$$f(x + y) = M(x, y)f(x).$$

Since the homomorphic image of an invertible matrix is invertible, we substitute 0 for  $x$  in this last relation to conclude the proof of the theorem.

**Theorem 3.5. (Quillen-Suslin).** *Let  $k$  be a field and let  $f$  be a unimodular vector in  $k[x_1, \dots, x_r]^{(n)}$ . Then  $f$  has the unimodular extension property.*

*Proof.* By induction on  $r$ . If  $r = 1$  then  $k[x_1]$  is a principal ring and the theorem is left to the reader. Assume the theorem for  $r - 1$  variables with  $r \geq 2$ , and put

$$R = k[x_1, \dots, x_{r-1}].$$

We view  $f$  as a vector of polynomials in the last variable  $x_r$ , and want to apply Theorem 3.4. We can do so if some component of  $f$  has leading coefficient 1 in the variable  $x_r$ . We reduce the theorem to this case as follows. The proof of the Noether Normalization Theorem (Chapter VIII, Theorem 2.1) shows that if we let

$$y_r = x_r$$

$$y_i = x_i - x_r^{m_i}$$

then the polynomial vector

$$f(x_1, \dots, x_r) = g(y_1, \dots, y_r)$$

has one component with  $y_r$ -leading coefficient equal to 1. Hence there exists a matrix  $N(y) = M(x)$  invertible over  $R[x_r] = R[y_r]$  such that

$$g(y_1, \dots, y_r) = N(y_1, \dots, y_r)g(y_1, \dots, y_{r-1}, 0),$$

and  $g(y_1, \dots, y_{r-1}, 0)$  is unimodular in  $k[y_1, \dots, y_{r-1}]^{(n)}$ . We can therefore conclude the proof by induction.

We now give other formulations of the theorem. First we recall that a module  $E$  over a commutative ring  $A$  is called **stably free** if there exists a finite free module  $F$  such that  $E \oplus F$  is finite free.

We shall say that a commutative ring  $A$  has the **unimodular column extension property** if every unimodular vector  $f \in A^{(n)}$  has the unimodular extension property, for all positive integers  $n$ .

**Theorem 3.6.** *Let  $A$  be a commutative ring which has the unimodular column extension property. Then every stably free module over  $A$  is free.*

*Proof.* Let  $E$  be stably free. We use induction on the rank of the free modules  $F$  such that  $E \oplus F$  is free. By induction, it suffices to prove that if  $E \oplus A$  is free then  $E$  is free. Let  $E \oplus A = A^{(n)}$  and let

$$p : A^{(n)} \rightarrow A$$

be the projection. Let  $u^1$  be a basis of  $A$  over itself. Viewing  $A$  as a direct summand in  $E \oplus A = A^{(n)}$  we write

$$u^1 = {}^t(a_{11}, \dots, a_{n1}) \quad \text{with} \quad a_{i1} \in A.$$

Then  $u^1$  is unimodular, and by assumption  $u^1$  is the first column of a matrix  $M = (a_{ij})$  whose determinant is a unit in  $A$ . Let

$$u^j = M e^j \quad \text{for } j = 1, \dots, n,$$

where  $e^j$  is the  $j$ -th unit column vector of  $A^{(n)}$ . Note that  $u^1$  is the first column of  $M$ . By elementary column operations, we may change  $M$  so that  $u^j \in E$  for  $j = 2, \dots, n$ . Indeed, if  $pe^j = cu^1$  for  $j \geq 2$  we need only replace  $e^j$  by  $e^j - ce^1$ . Without loss of generality we may therefore assume that  $u^2, \dots, u^n$  lie in  $E$ . Since  $M$  is invertible over  $A$ , it follows that  $M$  induces an automorphism of  $A^{(n)}$  as  $A$ -module with itself by

$$X \mapsto MX.$$

It follows immediately from the construction and the fact that  $A^{(n)} = E \oplus A$  that  $M$  maps the free module with basis  $\{e^2, \dots, e^n\}$  onto  $E$ . This concludes the proof.

If we now feed Serre's Theorem 2.9 into the present machinery consisting of the Quillen-Suslin theorem and Theorem 3.6, we obtain the alternative version of the Quillen-Suslin theorem:

**Theorem 3.7.** *Let  $k$  be a field. Then every finite projective module over the polynomial ring  $k[x_1, \dots, x_r]$  is free.*

## §4. THE KOSZUL COMPLEX

In this section, we describe a finite complex built out of the alternating product of a free module. This gives an application of the alternating product, and also gives a fundamental construction used in algebraic geometry, both abstract and complex, as the reader can verify by looking at Griffiths-Harris [GrH 78], Chapter V, §3; Grothendieck's [SGA 6]; Hartshorne [Ha 77], Chapter III, §7; and Fulton-Lang [FuL 85], Chapter IV, §2.

We know from Chapter XX that a free resolution of a module allows us to compute certain homology or cohomology groups of a functor. We apply this now to  $\text{Hom}$  and also to the tensor product. Thus we also get examples of explicit computations of homology, illustrating Chapter XX, by means of the Koszul complex. We shall also obtain a classical application by deriving the so-called Hilbert Syzygy theorem.

Let  $A$  be a ring (always assumed commutative) and  $M$  a module. A sequence of elements  $x_1, \dots, x_r$  in  $A$  is called  **$M$ -regular** if  $M/(x_1, \dots, x_r)M \neq 0$ , if  $x_1$

is not divisor of zero in  $M$ , and for  $i \geq 2$ ,  $x_i$  is not divisor of 0 in

$$M/(x_1, \dots, x_{i-1})M.$$

It is called **regular** when  $M = A$ .

**Proposition 4.1.** *Let  $I = (x_1, \dots, x_r)$  be generated by a regular sequence in  $A$ . Then  $I/I^2$  is free of dimension  $r$  over  $A/I$ .*

*Proof.* Let  $\bar{x}_i$  be the class of  $x_i \bmod I^2$ . It suffices to prove that  $\bar{x}_1, \dots, \bar{x}_r$  are linearly independent. We do this by induction on  $r$ . For  $r = 1$ , if  $\bar{a}\bar{x} = 0$ , then  $ax = bx^2$  for some  $b \in A$ , so  $x(a - bx) = 0$ . Since  $x$  is not zero divisor in  $A$ , we have  $a = bx$  so  $\bar{a} = 0$ .

Now suppose the proposition true for the regular sequence  $x_1, \dots, x_{r-1}$ . Suppose

$$\sum_{i=1}^r \bar{a}_i \bar{x}_i = 0 \quad \text{in } I/I^2.$$

We may assume that  $\sum a_i x_i = 0$  in  $A$ ; otherwise  $\sum a_i x_i = \sum y_i x_i$  with  $y_i \in I$  and we can replace  $a_i$  by  $a_i - y_i$  without changing  $\bar{a}_i$ .

Since  $x_r$  is not zero divisor in  $A/(x_1, \dots, x_{r-1})$  there exist  $b_i \in A$  such that

$$a_r x_r + \sum_{i=1}^{r-1} a_i x_i = 0 \Rightarrow a_r = \sum_{i=1}^{r-1} b_i x_i \Rightarrow \sum_{i=1}^{r-1} (a_i + b_i x_r) x_i = 0.$$

By induction,

$$a_j + b_j x_r \in \sum_{i=1}^{r-1} Ax_i \quad (j = 1, \dots, r-1)$$

so  $a_j \in I$  for all  $j$ , so  $\bar{a}_j = 0$  for all  $j$ , thus proving the proposition.

Let  $K, L$  be complexes, which we write as direct sums

$$K = \bigoplus K_p \quad \text{and} \quad L = \bigoplus L_q$$

with  $p, q \in \mathbf{Z}$ . Usually,  $K_p = L_q = 0$  for  $p, q < 0$ . Then the **tensor product**  $K \otimes L$  is the complex such that

$$(K \otimes L)_n = \bigoplus_{p+q=n} K_p \otimes L_q;$$

and for  $u \in K_p, v \in L_q$  the differential is defined by

$$d(u \otimes v) = du \otimes v + (-1)^p u \otimes dv.$$

(Carry out the detailed verification, which is routine, that this gives a complex.)

Let  $A$  be a commutative ring and  $x \in A$ . We define the complex  $K(x)$  to have  $K_0(x) = A$ ,  $K_1(x) = Ae_1$ , where  $e_1$  is a symbol,  $Ae_1$  is the free module of rank 1 with basis  $\{e_1\}$ , and the boundary map is defined by  $de_1 = x$ , so the complex can be represented by the sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ae_1 & \xrightarrow{d} & A & \longrightarrow & 0 \\ & & \parallel & & \parallel & & \\ 0 & \longrightarrow & K_1(x) & \longrightarrow & K_0(x) & \longrightarrow & 0 \end{array}$$

More generally, for elements  $x_1, \dots, x_r \in A$  we define the **Koszul complex**  $K(x) = K(x_1, \dots, x_r)$  as follows. We put:

$$K_0(x) = A;$$

$$K_1(x) = \text{free module } E \text{ with basis } \{e_1, \dots, e_r\};$$

$$K_p(x) = \text{free module } \bigwedge^p E \text{ with basis } \{e_{i_1} \wedge \dots \wedge e_{i_p}\}, i_1 < \dots < i_p;$$

$$K_r(x) = \text{free module } \bigwedge^r E \text{ of rank 1 with basis } e_1 \wedge \dots \wedge e_r.$$

We define the **boundary maps** by  $de_i = x_i$  and in general

$$d : K_p(x) \rightarrow K_{p-1}(x)$$

by

$$d(e_{i_1} \wedge \dots \wedge e_{i_p}) = \sum_{j=1}^p (-1)^{j-1} x_{i_j} e_{i_1} \wedge \dots \wedge \hat{e}_{i_j} \wedge \dots \wedge e_{i_p}.$$

A direct verification shows that  $d^2 = 0$ , so we have a complex

$$0 \rightarrow K_r(x) \rightarrow \dots \rightarrow K_1(x) \rightarrow K_0(x) \rightarrow A \rightarrow 0$$

The next lemma shows the extent to which the complex is independent of the ideal  $I = (x_1, \dots, x_r)$  generated by  $(x)$ . Let

$$I = (x_1, \dots, x_r) \supset I' = (y_1, \dots, y_r)$$

be two ideals of  $A$ . We have a natural ring homomorphism

$$\text{can} : A/I' \rightarrow A/I.$$

Let  $\{e'_1, \dots, e'_r\}$  be a basis for  $K_1(y)$ , and let

$$y_i = \sum c_{ij} x_j \quad \text{with} \quad c_{ij} \in A.$$

We define  $f_1 : K_1(y) \rightarrow K_1(x)$  by

$$f_1 e'_i = \sum c_{ij} e_j$$

and

$$f_p = f_1 \wedge \cdots \wedge f_1, \quad \text{product taken } p \text{ times.}$$

Let  $D = \det(c_{ij})$  be the determinant. Then for  $p = r$  we get that

$$f_r : K_r(y) \rightarrow K_r(x) \text{ is multiplication by } D.$$

**Lemma 4.2.** *Notation as above, the homomorphisms  $f_p$  define a morphism of Koszul complexes:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & K_r(y) & \longrightarrow & \cdots & \longrightarrow & K_1(y) & \longrightarrow & A & \longrightarrow & A/I' & \longrightarrow 0 \\ & & \downarrow f_r = D & & & & \downarrow f_1 & & \downarrow \text{id} & & \downarrow \text{can} & \\ 0 & \longrightarrow & K_r(x) & \longrightarrow & \cdots & \longrightarrow & K_1(x) & \longrightarrow & A & \longrightarrow & A/I & \longrightarrow 0 \end{array}$$

and define an isomorphism if  $D$  is a unit in  $A$ , for instance if  $(y)$  is a permutation of  $(x)$ .

*Proof.* By definition

$$f(e'_{i_1} \wedge \cdots \wedge e'_{i_p}) = \left( \sum_{j=1}^r c_{i_1 j} e_j \right) \wedge \cdots \wedge \left( \sum_{j=1}^r c_{i_p j} e_j \right).$$

Then

$$\begin{aligned} & fd(e'_{i_1} \wedge \cdots \wedge e'_{i_p}) \\ &= f \left( \sum_k (-1)^{k-1} y_{i_k} e'_{i_1} \wedge \cdots \wedge \widehat{e'_{i_k}} \wedge \cdots \wedge e'_{i_p} \right) \\ &= \sum_k (-1)^{k-1} y_{i_k} \left( \sum_{j=1}^r c_{i_1 j} e_j \right) \wedge \cdots \wedge \widehat{\left( \sum_{j=1}^r c_{i_k j} e_j \right)} \wedge \cdots \wedge \left( \sum_{j=1}^r c_{i_p j} e_j \right) \\ &= \sum (-1)^{k-1} \left( \sum_{j=1}^r c_{i_1 j} e_j \right) \wedge \cdots \wedge \underbrace{\left( \sum_{j=1}^r c_{i_k j} x_j e_j \right)}_{\text{omitted}} \wedge \cdots \wedge \left( \sum_{j=1}^r c_{i_p j} e_j \right) \\ &= df(e'_{i_1} \wedge \cdots \wedge e'_{i_p}) \end{aligned}$$

using  $y_{i_k} = \sum c_{i_k j} x_j$ . This concludes the proof that the  $f_p$  define a homomorphism of complexes.

In particular, if  $(x)$  and  $(y)$  generate the same ideal, and the determinant  $D$  is a unit (i.e. the linear transformation going from  $(x)$  to  $(y)$  is invertible over the ring), then the two Koszul complexes are isomorphic.

The next lemma gives us a useful way of making inductions later.

**Proposition 4.3.** *There is a natural isomorphism*

$$K(x_1, \dots, x_r) \approx K(x_1) \otimes \cdots \otimes K(x_r).$$

*Proof.* The proof will be left as an exercise.

Let  $I = (x_1, \dots, x_r)$  be the ideal generated by  $x_1, \dots, x_r$ . Then directly from the definitions we see that the 0-th homology of the Koszul complex is simply  $A/IA$ .

More generally, let  $M$  be an  $A$ -module. Define the **Koszul complex of  $M$**  by

$$K(x; M) = K(x_1, \dots, x_r; M) = K(x_1, \dots, x_r) \otimes_A M$$

Then this complex looks like

$$0 \rightarrow K_r(x) \otimes M \rightarrow \cdots \rightarrow K_2(x) \otimes_A M \rightarrow M^{(r)} \rightarrow M \rightarrow 0.$$

We sometimes abbreviate  $H_p(x; M)$  for  $H_p K(x; M)$ . The first and last homology groups are then obtained directly from the definition of boundary. We get

$$H_0(K(x; M)) \approx M/IM;$$

$$H_r(K(x; M)) = \{v \in M \text{ such that } x_i v = 0 \text{ for all } i = 1, \dots, r\}.$$

In light of Proposition 4.3, we study generally what happens to a tensor product of any complex with  $K(x)$ , when  $x$  consists of a single element. Let  $y \in A$  and let  $C$  be an arbitrary complex of  $A$ -modules. We have an exact sequence of complexes

$$(1) \quad 0 \rightarrow C \rightarrow C \otimes K(y) \rightarrow (C \otimes K(y))/C \rightarrow 0$$

made explicit as follows.

$$\begin{array}{ccccccc}
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \longrightarrow & C_{n+1} \longrightarrow & (C_{n+1} \otimes A) \oplus (C_n \otimes K_1(y)) \longrightarrow & C_n \otimes K_1(y) \longrightarrow & 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \longrightarrow & C_n \longrightarrow & (C_n \otimes A) \oplus (C_{n-1} \otimes K_1(y)) \longrightarrow & C_{n-1} \otimes K_1(y) \longrightarrow & 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 0 \longrightarrow & C_{n-1} \longrightarrow & (C_{n-1} \otimes A) \oplus (C_{n-2} \otimes K_1(y)) \longrightarrow & C_{n-2} \otimes K_1(y) \longrightarrow & 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & & & & & & 
 \end{array}$$

$d_n \otimes \text{id}$        $d_{n-1} \otimes \text{id}$

We note that  $C \otimes K_1(y)$  is just  $C$  with a dimension shift by one unit, in other words

$$(2) \quad (C \otimes K_1(y))_{n+1} = C_n \otimes K_1(y).$$

In particular,

$$(3) \quad H_{n+1}(C \otimes K(y)/C) \approx H_n(C).$$

Associated with an exact sequence of complexes, we have the homology sequence, which in this case yields the long exact sequence

$$\begin{aligned} \longrightarrow H_{n+1}(C) \longrightarrow H_{n+1}(C \otimes K_1(y)) \\ \longrightarrow H_{n+1}(C \otimes K(y)/C) \xrightarrow{\delta} H_n(C) \\ \Downarrow \\ H_n(C) \end{aligned}$$

which we write stacked up according to the index:

$$(4) \quad \begin{aligned} \rightarrow H_{p+1}(C) \rightarrow H_{p+1}(C) \rightarrow H_{p+1}(C \otimes K(y)) \rightarrow \\ \rightarrow H_p(C) \rightarrow H_p(C) \rightarrow H_p(C \otimes K(y)) \rightarrow \end{aligned}$$

ending in lowest dimension with

$$(5) \quad \rightarrow H_1(C) \rightarrow H_1(C \otimes K(y)) \rightarrow H_0(C) \rightarrow H_0(C).$$

Furthermore, a direct application of the definition of the boundary map and the tensor product of complexes yields:

*The boundary map on  $H_p(C)$  ( $p \geq 0$ ) is induced by multiplication by  $(-1)^p y$ :*

$$(6) \quad \delta = (-1)^p m(y) : H_p(C) \rightarrow H_{p-1}(C).$$

Indeed, write

$$(C \otimes K(y))_p = (C_p \otimes A) \oplus (C_{p-1} \otimes K_1(y)) \approx C_p \oplus C_{p-1}.$$

Let  $(v, w) \in C_p \oplus C_{p-1}$  with  $v \in C_p$  and  $w \in C_{p-1}$ . Then directly from the definitions,

$$(7) \quad d(v, w) = (dv + (-1)^{p-1} yw, dw).$$

To see (6), one merely follows up the definitions of the boundary, taking an element  $w \in C_p \approx C_p \otimes K_1(y)$ , lifting back to  $(0, w)$ , applying  $d$ , and lifting back to  $C_p$ . If we start with a cycle, i.e.  $dw = 0$ , then the map is well defined on the homology class, with values in the homology.

**Lemma 4.4.** *Let  $y \in A$  and let  $C$  be a complex as above. Then  $m(y)$  annihilates  $H_p(C \otimes K(y))$  for all  $p \geq 0$ .*

*Proof.* If  $(v, w)$  is a cycle, i.e.  $d(v, w) = 0$ , then from (7) we get at once that  $(yv, yw) = d(0, (-1)^p v)$ , which proves the lemma.

In the applications we have in mind, we let  $y = x_r$  and

$$C = K(x_1, \dots, x_{r-1}; M) = K(x_1, \dots, x_{r-1}) \otimes M.$$

Then we obtain:

**Theorem 4.5.(a)** *There is an exact sequence with maps as above:*

$$\begin{aligned} \rightarrow H_p K(x_1, \dots, x_{r-1}; M) &\rightarrow H_p K(x_1, \dots, x_{r-1}; M) \rightarrow H_p K(x_1, \dots, x_r; M) \\ \cdots \rightarrow H_1(x_1, \dots, x_r; M) &\rightarrow H_0(x_1, \dots, x_{r-1}; M) \xrightarrow{m(x_r)} H_0(x_1, \dots, x_{r-1}; M). \end{aligned}$$

(b) *Every element of  $I = (x_1, \dots, x_r)$  annihilates  $H_p(x; M)$  for  $p \geq 0$ .*

(c) *If  $I = A$ , then  $H_p(x; M) = 0$  for all  $p \geq 0$ .*

*Proof.* This is immediate from Proposition 4.3 and Lemma 4.4.

We define the **augmented Koszul complex** to be

$$0 \rightarrow K_r(x; M) \rightarrow \cdots \rightarrow K_1(x; M) = M^{(r)} \rightarrow M \rightarrow M/IM \rightarrow 0.$$

**Theorem 4.6.** *Let  $M$  be an  $A$ -module.*

- (a) *Let  $x_1, \dots, x_r$  be a regular sequence for  $M$ . Then  $H_p(x; M) = 0$  for  $p > 0$ . (Of course,  $H_0 K(x; M) = M/IM$ .) In other words, the augmented Koszul complex is exact.*
- (b) *Conversely, suppose  $A$  is local, and  $x_1, \dots, x_r$  lie in the maximal ideal of  $A$ . Suppose  $M$  is finite over  $A$ , and also assume that  $H_1 K(x; M) = 0$ . Then  $(x_1, \dots, x_r)$  is  $M$ -regular.*

*Proof.* We prove (a) by induction on  $r$ . If  $r = 1$  then  $H_1(x; M) = 0$  directly from the definition. Suppose  $r > 1$ . We use the exact sequence of Theorem 4.5(a). If  $p > 1$  then  $H_p(x; M)$  is between two homology groups which are 0, so  $H_p(x; M) = 0$ . If  $p = 1$ , we use the very end of the exact sequence of Theorem 4.5(a), noting that  $m(x_r)$  is injective, so by induction we find  $H_1(x; M) = 0$  also, thus proving (a).

As to (b), by Lemma 4.4 and the hypothesis, we get an exact sequence

$$H_1(x_1, \dots, x_{r-1}; M) \xrightarrow{m(x_r)} H_1(x_1, \dots, x_{r-1}; M) \rightarrow H_1(x; M) = 0,$$

so  $m(x_r)$  is surjective. By Nakayama's lemma, it follows that

$$H_1(x_1, \dots, x_{r-1}; M) = 0.$$

By induction  $(x_1, \dots, x_{r-1})$  is an  $M$ -regular sequence. Looking again at the tail end of the exact sequence as in (a) shows that  $x_r$  is  $M/(x_1, \dots, x_{r-1})M$ -regular, whence proving (b) and the theorem.

We note that (b), which uses only the triviality of  $H_1$  (and not all  $H_p$ ) is due to Northcott [No 68], 8.5, Theorem 8. By (a), it follows that  $H_p = 0$  for  $p > 0$ .

An important special case of Theorem 4.6(a) is when  $M = A$ , in which case we restate the theorem in the form:

*Let  $x_1, \dots, x_r$  be a regular sequence in  $A$ . Then  $K(x_1, \dots, x_r)$  is a free resolution of  $A/I$ :*

$$0 \rightarrow K_r(x) \rightarrow \cdots \rightarrow K_1(x) \rightarrow A \rightarrow A/I \rightarrow 0.$$

*In particular,  $A/I$  has Tor-dimension  $\leq r$ .*

For the Hom functor, we have:

**Theorem 4.7.** *Let  $x_1, \dots, x_r$  be a regular sequence in  $A$ . Then there is an isomorphism*

$$\varphi_{x, M} : H^r(\text{Hom}(K(x), M)) \rightarrow M/IM$$

*to be described below.*

*Proof.* The module  $K_r(x)$  is 1-dimensional, with basis  $e_1 \wedge \cdots \wedge e_r$ . Depending on this basis, we have an isomorphism

$$\text{Hom}(K_r(x), M) \approx M,$$

whereby a homomorphism is determined by its value at the basis element in  $M$ . Then directly from the definition of the boundary map  $d_r$  in the Koszul complex, which is

$$d_r : e_1 \wedge \cdots \wedge e_r \mapsto \sum_{j=1}^r (-1)^{j-1} x_j e_1 \wedge \cdots \wedge \hat{e}_j \wedge \cdots \wedge e_r$$

we see that

$$\begin{aligned} H^r(\text{Hom}(K_r(x), M)) &\approx \text{Hom}(K_r(x), M)/d_r^{-1} \text{Hom}(K_{r-1}(x), M) \\ &\approx M/IM. \end{aligned}$$

This proves the theorem.

The reader who has read Chapter XX knows that the  $i$ -th homology group of  $\text{Hom}(K(x), M)$  is called  $\text{Ext}^i(A/I, M)$ , determined up to a unique isomorphism by the complex, since two resolutions of  $A/I$  differ by a morphism of complexes, and two such morphisms differ by a homotopy which induces a homology isomorphism. Thus Theorem 4.7 gives an isomorphism

$$\varphi_{x, M} : \text{Ext}^r(A/I, M) \rightarrow M/IM.$$

In fact, we shall obtain morphisms of the Koszul complex from changing the sequence. We go back to the hypothesis of Lemma 4.2.

**Lemma 4.8.** *If  $I = (x) = (y)$  where  $(x), (y)$  are two regular sequences, then we have a commutative diagram*

$$\begin{array}{ccc} & & M/IM \\ & \nearrow \varphi_{x, M} & \downarrow D = \det(c_{ij}) \\ \mathrm{Ext}^r(A/I, M) & & M/IM \\ & \searrow \varphi_{y, M} & \end{array}$$

where all the maps are isomorphisms of  $A/I$ -modules.

The fact that we are dealing with  $A/I$ -modules is immediate since multiplication by an element of  $A$  commutes with all homomorphisms in sight, and  $I$  annihilates  $A/I$ .

By Proposition 4.1, we know that  $I/I^2$  is a free module of rank  $r$  over  $A/I$ . Hence

$$\bigwedge^r(I/I^2)$$

is a free module of rank 1, with basis  $\bar{x}_1 \wedge \cdots \wedge \bar{x}_r$  (where the bar denotes residue class mod  $I^2$ ). Taking the dual of this exterior product, we see that under a change of basis, it transforms according to the inverse of the determinant mod  $I^2$ . This allows us to get a canonical isomorphism as in the next theorem.

**Theorem 4.9.** *Let  $x_1, \dots, x_r$  be a regular sequence in  $A$ , and let  $I = (x)$ . Let  $M$  be an  $A$ -module. Let*

$$\psi_{x, M} : M/IM \rightarrow (M/IM) \otimes \bigwedge^r(I/I^2)^{\mathrm{dual}}$$

*be the embedding determined by the basis  $(\bar{x}_1 \wedge \cdots \wedge \bar{x}_r)^{\mathrm{dual}}$  of  $\bigwedge^r(I/I^2)^{\mathrm{dual}}$ . Then the composite isomorphism*

$$\mathrm{Ext}^r(A/I, M) \xrightarrow{\varphi_{x, M}} M/IM \xrightarrow{\psi_{x, M}} (M/IM) \otimes \bigwedge^r(I/I^2)^{\mathrm{dual}}$$

*is a functorial isomorphism, independent of the choice of regular generators for  $I$ .*

We also have the analogue of Theorem 4.5 in intermediate dimensions.

**Theorem 4.10.** *Let  $x_1, \dots, x_r$  be an  $M$ -regular sequence in  $A$ . Let  $I = (x)$ . Then*

$$\mathrm{Ext}^i(A/I, M) = 0 \quad \text{for } i < r.$$

*Proof.* For the proof, we assume that the reader is acquainted with the exact homology sequence. Assume by induction that  $\mathrm{Ext}^i(A/I, M) = 0$  for

$i < r - 1$ . Then we have the exact sequence

$$0 = \text{Ext}^{i-1}(A/I, M/x_1 M) \rightarrow \text{Ext}^i(A/I, M) \xrightarrow{x_1} \text{Ext}^i(A/I, M)$$

for  $i < r$ . But  $x_1 \in I$  so multiplication by  $x_1$  induces 0 on the homology groups, which gives  $\text{Ext}^i(A/I, M) = 0$  as desired.

Let  $L_N \rightarrow N \rightarrow 0$  be a free resolution of a module  $N$ . By definition,

$$\text{Tor}_i^A(N, M) = i\text{-th homology of the complex } L \otimes M.$$

This is independent of the choice of  $L_N$  up to a unique isomorphism. We now want to do for  $\text{Tor}$  what we have just done for  $\text{Ext}$ .

**Theorem 4.11.** *Let  $I = (x_1, \dots, x_r)$  be an ideal of  $A$  generated by a regular sequence of length  $r$ .*

(i) *There is a natural isomorphism*

$$\text{Tor}_i^A(A/I, A/I) \approx \bigwedge_{A/I}^i(I/I^2), \quad \text{for } i \geq 0.$$

(ii) *Let  $L$  be a free  $A/I$ -module, extended naturally to an  $A$ -module. Then*

$$\text{Tor}_i^A(L, A/I) \approx L \otimes \bigwedge_{A/I}^i(I/I^2), \quad \text{for } i \geq 0.$$

These isomorphisms will follow from the next considerations.

First we use again that the residue classes  $\bar{x}_1, \dots, \bar{x}_r \bmod I^2$  form a basis of  $I/I^2$  over  $A/I$ . Therefore we have a unique isomorphism of complexes

$$\varphi_x : K(x) \otimes A/I \rightarrow \bigwedge(I/I^2) = \bigoplus \bigwedge^i(I/I^2)$$

with zero differentials on the right-hand side, such that

$$e_{i_1} \wedge \cdots \wedge e_{i_p} \mapsto \bar{x}_{i_1} \wedge \cdots \wedge \bar{x}_{i_p}.$$

**Lemma 4.12.** *Let  $I = (x) \supset I' = (y)$  be two ideals generated by regular sequences of length  $r$ . Let  $f : K(y) \rightarrow K(x)$  be the morphism of Koszul complexes defined in Lemma 4.2. Then the following diagram is commutative:*

$$\begin{array}{ccc} K(y) \otimes A/I' & \xrightarrow{\varphi_y} & \bigwedge_{A/I'}(I'/I'^2) \\ f \otimes \text{can} \downarrow & & \downarrow \text{canonical hom} \\ K(x) \otimes A/I & \xrightarrow{\varphi_x} & \bigwedge_{A/I}(I/I^2) \end{array}$$

*Proof.* We have

$$\begin{aligned}
 & \varphi_x \circ (f \otimes \text{can})(e'_{i_1} \wedge \cdots \wedge e'_{i_p} \otimes 1) \\
 &= \sum_{j=2}^r c_{i_1 j} \bar{x}_j \wedge \cdots \wedge \sum_{j=1}^r c_{i_p j} \bar{x}_j \\
 &= \bar{y}_{i_1} \wedge \cdots \wedge \bar{y}_{i_p} = \text{can}(\varphi_y(e'_{i_1} \wedge \cdots \wedge e'_{i_p})).
 \end{aligned}$$

This proves the lemma.

In particular, if  $I' = I$  then we have the commutative diagram

$$\begin{array}{ccc}
 K(y) & & \\
 \downarrow f \otimes d & \nearrow \varphi_y & \\
 K(x) & \nearrow \varphi_x & \bigwedge (I/I^2)
 \end{array}$$

which shows that the identification of  $\text{Tor}_i(A/I, A/I)$  with  $\bigwedge^i(I/I^2)$  via the choices of bases is compatible under one isomorphism of the Koszul complexes, which provide a resolution of  $A/I$ . Since any other homomorphism of Koszul complexes is homotopic to this one, it follows that this identification does not depend on the choices made and proves the first part of Theorem 4.11.

The second part follows at once, because we have

$$\begin{aligned}
 \text{Tor}_i^A(A/I, L) &= H_i(K(x) \otimes L) = H_i((K(x) \otimes_A A/I) \otimes_{A/I} L) \\
 &= \bigwedge_{A/I}^i(I/I^2) \otimes L.
 \end{aligned}$$

This concludes the proof of Theorem 4.11.

**Example.** Let  $k$  be a field and let  $A = k[x_1, \dots, x_r]$  be the polynomial ring in  $r$  variables. Let  $I = (x_1, \dots, x_r)$  be the ideal generated by the variables. Then  $A/I = k$ , and therefore Theorem 4.11 yields for  $i \geq 0$ :

$$\begin{aligned}
 \text{Tor}_i^A(k, k) &\approx \bigwedge_k^i(I/I^2) \\
 \text{Tor}_i^A(L, k) &\approx L \otimes \bigwedge_k^i(I/I^2)
 \end{aligned}$$

Note that in the present case, we can think of  $I/I^2$  as the vector space over  $k$  with basis  $\bar{x}_1, \dots, \bar{x}_r$ . Then  $A$  can be viewed as the symmetric algebra  $SE$ , where  $E$  is this vector space. We can give a specific example of the Koszul complex in this context as in the next theorem, given for a free module.

**Theorem 4.13.** *Let  $E$  be a finite free module of rank  $r$  over the ring  $R$ . For each  $p = 1, \dots, r$  there is a unique homomorphism*

$$d_p: \bigwedge^p E \otimes SE \rightarrow \bigwedge^{p-1} E \otimes SE$$

*such that*

$$d_i((x_1 \wedge \dots \wedge x_p) \otimes y)$$

$$= \sum_{i=1}^p (-1)^{i-1} (x_1 \wedge \dots \wedge \hat{x}_i \wedge \dots \wedge x_p) \otimes (x_i \otimes y)$$

*where  $x_i \in E$  and  $y \in SE$ . This gives the resolution*

$$0 \rightarrow \bigwedge^r E \otimes SE \rightarrow \bigwedge^{r-1} E \otimes SE \rightarrow \dots \rightarrow \bigwedge^0 E \otimes SE \rightarrow R \rightarrow 0$$

*Proof.* The above definitions are merely examples of the Koszul complex for the symmetric algebra  $SE$  with respect to the regular sequence consisting of some basis of  $E$ .

Since  $d_p$  maps  $\bigwedge^p E \otimes S^q E$  into  $\bigwedge^{p-1} E \otimes S^{q+1} E$ , we can decompose this complex into a direct sum corresponding to a given graded component, and hence:

**Corollary 4.14.** *For each integer  $n \geq 1$ , we have an exact sequence*

$$0 \rightarrow \bigwedge^r E \otimes S^{n-r} E \rightarrow \dots \rightarrow \bigwedge^1 E \otimes S^{n-1} E \rightarrow S^n E \rightarrow 0$$

*where  $S^j E = 0$  for  $j < 0$ .*

Finally, we give an application to a classical theorem of Hilbert. The polynomial ring  $A = k[x_1, \dots, x_r]$  is naturally graded, by the degrees of the homogeneous components. *We shall consider graded modules, where the grading is in dimensions  $\geq 0$ , and we assume that homomorphisms are graded of degree 0.*

So suppose  $M$  is a graded module (and thus  $M_i = 0$  for  $i < 0$ ) and  $M$  is finite over  $A$ . Then we can find a graded surjective homomorphism

$$L_0 \rightarrow M \rightarrow 0$$

where  $L_0$  is finite free. Indeed, let  $w_1, \dots, w_n$  be homogeneous generators of  $M$ . Let  $e_1, \dots, e_n$  be basis elements for a free module  $L_0$  over  $A$ . We give  $L_0$  the grading such that if  $a \in A$  is homogeneous of degree  $d$  then  $ae_i$  is homogeneous of degree

$$\deg ae_i = \deg a + \deg w_i.$$

Then the homomorphism of  $L_0$  onto  $M$  sending  $e_i \mapsto w_i$  is graded as desired.

The kernel  $M_1$  is a graded submodule of  $L_0$ . Repeating the process, we can find a surjective homomorphism

$$L_1 \rightarrow M_1 \rightarrow 0.$$

We continue in this way to obtain a graded resolution of  $M$ . We want this resolution to stop, and the possibility of its stopping is given by the next theorem.

**Theorem 4.15. (Hilbert Syzygy Theorem).** *Let  $k$  be a field and*

$$A = k[x_1, \dots, x_r]$$

*the polynomial ring in  $r$  variables. Let  $M$  be a graded module over  $A$ , and let*

$$0 \rightarrow K \rightarrow L_{r-1} \rightarrow \dots \rightarrow L_0 \rightarrow M \rightarrow 0$$

*be an exact sequence of graded homomorphisms of graded modules, such that  $L_0, \dots, L_{r-1}$  are free. Then  $K$  is free. If  $M$  is in addition finite over  $A$  and  $L_0, \dots, L_{r-1}$  are finite free, then  $K$  is finite free.*

*Proof.* From the Koszul complex we know that  $\text{Tor}_i(M, k) = 0$  for  $i > r$  and all  $M$ . By dimension shifting, it follows that

$$\text{Tor}_i(K, k) = 0 \quad \text{for } i > 0.$$

The theorem is then a consequence of the next result.

**Theorem 4.16.** *Let  $F$  be a graded finite module over  $A = k[x_1, \dots, x_r]$ . If  $\text{Tor}_1(F, k) = 0$  then  $F$  is free.*

*Proof.* The method is essentially to do a Nakayama type argument in the case of the non-local ring  $A$ . First note that

$$F \otimes k = F/IF$$

where  $I = (x_1, \dots, x_r)$ . Thus  $F \otimes k$  is naturally an  $A/I = k$ -module. Let  $v_1, \dots, v_n$  be homogeneous elements of  $F$  whose residue classes mod  $IF$  form a basis of  $F/IF$  over  $k$ . Let  $L$  be a free module with basis  $e_1, \dots, e_n$ . Let

$$L \rightarrow F$$

be the graded homomorphism sending  $e_i \mapsto v_i$  for  $i = 1, \dots, n$ . It suffices to prove that this is an isomorphism. Let  $C$  be the cokernel, so we have the exact sequence

$$L \rightarrow F \rightarrow C \rightarrow 0.$$

Tensoring with  $k$  yields the exact sequence

$$L \otimes k \rightarrow F \otimes k \rightarrow C \otimes k \rightarrow 0.$$

Since by construction the map  $L \otimes k \rightarrow F \otimes k$  is surjective, it follows that  $C \otimes k = 0$ . But  $C$  is graded, so the next lemma shows that  $C = 0$ .

**Lemma 4.17.** *Let  $N$  be a graded module over  $A = k[x_1, \dots, x_r]$ . Let  $I = (x_1, \dots, x_r)$ . If  $N/IN = 0$  then  $N = 0$ .*

*Proof.* This is immediate by using the grading, looking at elements of  $N$  of smallest degree if they exist, and using the fact that elements of  $I$  have degree  $> 0$ .

We now get an exact sequence of graded modules

$$0 \rightarrow E \rightarrow L \rightarrow F \rightarrow 0$$

and we must show that  $E = 0$ . But the exact homology sequence and our assumption yields

$$0 = \text{Tor}_1(F, k) \rightarrow E \otimes k \rightarrow L \otimes k \rightarrow F \otimes k \rightarrow 0.$$

By construction  $L \otimes k \rightarrow F \otimes k$  is an isomorphism, and hence  $E \otimes k = 0$ . Lemma 4.17 now shows that  $E = 0$ . This concludes the proof of the syzygy theorem.

**Remark.** The only place in the proof where we used that  $k$  is a field is in the proof of Theorem 4.16 when we picked homogeneous elements  $v_1, \dots, v_n$  in  $M$  whose residue classes mod  $IM$  form a basis of  $M/IM$  over  $A/IA$ . Hilbert's theorem can be generalized by making the appropriate hypothesis which allows us to carry out this step, as follows.

**Theorem 4.18.** *Let  $R$  be a commutative local ring and let  $A = R[x_1, \dots, x_r]$  be the polynomial ring in  $r$  variables. Let  $M$  be a graded finite module over  $A$ , projective over  $R$ . Let*

$$0 \rightarrow K \rightarrow L_{r-1} \rightarrow \dots \rightarrow L_0 \rightarrow M \rightarrow 0$$

*be an exact sequence of graded homomorphisms of graded modules such that  $L_0, \dots, L_{r-1}$  are finite free. Then  $K$  is finite free.*

*Proof.* Replace  $k$  by  $R$  everywhere in the proof of the Hilbert syzygy theorem. We use the fact that a finite projective module over a local ring is free. Not a word needs to be changed in the above proof with the following exception. We note that the projectivity propagates to the kernels and cokernels in the given resolution. Thus  $F$  in the statement of Theorem 4.16 may be assumed projective, and each graded component is projective. Then  $F/IF$  is projective over  $A/IA = R$ , and so is each graded component. Since a finite projective module over a local ring is free, and one gets the freeness by lifting a basis from the residue class field, we may pick  $v_1, \dots, v_n$  homogeneous exactly as we did in the proof of Theorem 4.16. This concludes the proof.

---

**EXERCISES**

For exercises 1 through 4 on the Koszul complex, see [No 68], Chapter 8.

1. Let  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  be an exact sequence of  $A$ -modules. Show that tensoring with the Koszul complex  $K(x)$  one gets an exact sequence of complexes, and therefore an exact homology sequence

$$\begin{aligned} 0 &\rightarrow H_r K(x; M') \rightarrow H_r K(x; M) \rightarrow H_r K(x; M'') \rightarrow \cdots \\ \cdots &\rightarrow H_p K(x; M') \rightarrow H_p K(x; M) \rightarrow H_p K(x; M'') \rightarrow \cdots \\ \cdots &\rightarrow H_0 K(x; M') \rightarrow H_0 K(x; M) \rightarrow H_0 K(x; M'') \rightarrow 0 \end{aligned}$$

2. (a) Show that there is a unique homomorphism of complexes

$$f: K(x; M) \rightarrow K(x_1, \dots, x_{r-1}; M)$$

such that for  $v \in M$ :

$$f_p(e_{i_1} \wedge \cdots \wedge e_{i_p} \otimes v) = \begin{cases} e_{i_1} \wedge \cdots \wedge e_{i_p} \otimes x_r v & \text{if } i_p = r \\ e_{i_1} \wedge \cdots \wedge e_{i_p} \otimes v & \text{if } i_p < r. \end{cases}$$

- (b) Show that  $f$  is injective if  $x_r$  is not a divisor of zero in  $M$ .  
 (c) For a complex  $C$ , denote by  $C(-1)$  the complex shifted by one place to the left, so  $C(-1)_n = C_{n-1}$  for all  $n$ . Let  $\bar{M} = M/x_r M$ . Show that there is a unique homomorphism of complexes

$$g: K(x_1, \dots, x_{r-1}, 1; M) \rightarrow K(x_1, \dots, x_{r-1}; \bar{M})(-1)$$

such that for  $v \in M$ :

$$g_p(e_{i_1} \wedge \cdots \wedge e_{i_p} \otimes v) = \begin{cases} e_{i_1} \wedge \cdots \wedge e_{i_{p-1}} \otimes v & \text{if } i_p = r \\ 0 & \text{if } i_p < r. \end{cases}$$

- (d) If  $x_r$  is not a divisor of 0 in  $M$ , show that the following sequence is exact:

$$0 \rightarrow K(x; M) \xrightarrow{f} K(x_1, \dots, x_{r-1}, 1; M) \xrightarrow{g} K(x_1, \dots, x_{r-1}; \bar{M})(-1) \rightarrow 0.$$

Using Theorem 4.5(c), conclude that for all  $p \geq 0$ , there is an isomorphism

$$H_p K(x; M) \xrightarrow{\sim} H_p K(x_1, \dots, x_{r-1}; \bar{M}).$$

3. Assume  $A$  and  $M$  Noetherian. Let  $I$  be an ideal of  $A$ . Let  $a_1, \dots, a_k$  be an  $M$ -regular sequence in  $I$ . Show that this sequence can be extended to a maximal  $M$ -regular sequence  $a_1, \dots, a_q$  in  $I$ , in other words an  $M$ -regular sequence such that there is no  $M$ -regular sequence  $a_1, \dots, a_{q+1}$  in  $I$ .  
 4. Again assume  $A$  and  $M$  Noetherian. Let  $I = (x_1, \dots, x_r)$  and let  $a_1, \dots, a_q$  be a maximal  $M$ -regular sequence in  $I$ . Assume  $IM \neq M$ . Prove that

$$H_{r-q}(x; M) \neq 0 \text{ but } H_p(x; M) = 0 \text{ for } p > r - q.$$

[See [No 68], 8.5 Theorem 6. The result is similar to the result in Exercise 5, and generalizes Theorem 4.5(a). See also [Mat 80], pp. 100-103. The result shows that

all maximal  $M$ -regular sequences in  $M$  have the same length, which is called the  **$I$ -depth** of  $M$  and is denoted by  $\text{depth}_I(M)$ . For the proof, let  $s$  be the maximal integer such that  $H_s K(x; M) \neq 0$ . By assumption,  $H_0(x; M) = M/IM \neq 0$ , so  $s$  exists. We have to prove that  $q + s = r$ . First note that if  $q = 0$  then  $s = r$ . Indeed, if  $q = 0$  then every element of  $I$  is zero divisor in  $M$ , whence  $I$  is contained in the union of the associated primes of  $M$ , whence in some associated prime of  $M$ . Hence  $H_r(x; M) \neq 0$ .

Next assume  $q > 0$  and proceed by induction. Consider the exact sequence

$$0 \rightarrow M \xrightarrow{a_1} M \rightarrow M/a_1M \rightarrow 0$$

where the first map is  $m(a_1)$ . Since  $I$  annihilates  $H_p(x; M)$  by Theorem 4.5(c), we get an exact sequence

$$0 \rightarrow H_p(x; M) \rightarrow H_p(x; M/a_1M) \rightarrow H_{p-1}(x; M) \rightarrow 0.$$

Hence  $H_{s+1}(x; M/a_1M) \neq 0$ , but  $H_p(x; M/a_1M) = 0$  for  $p \geq s+2$ . From the hypothesis that  $a_1, \dots, a_q$  is a maximal  $M$ -regular sequence, it follows at once that  $a_2, \dots, a_q$  is maximal  $M/a_1M$ -regular in  $I$ , so by induction,  $q-1 = r-(s+1)$  and hence  $q+s = r$ , as was to be shown.]

5. The following exercise combines some notions of Chapter XX on homology, and some notions covered in this chapter and in Chapter X, §5. Let  $M$  be an  $A$ -module.

Let  $A$  be Noetherian,  $M$  finite module over  $A$ , and  $I$  an ideal of  $A$  such that  $IM \neq M$ . Let  $r$  be an integer  $\geq 1$ . Prove that the following conditions are equivalent:

- (i)  $\text{Ext}^i(N, M) = 0$  for all  $i < r$  and all finite modules  $N$  such that  $\text{supp}(N) \subset \mathfrak{X}(I)$ .
- (ii)  $\text{Ext}^i(A/I, M) = 0$  for all  $i < r$ .
- (iii) There exists a finite module  $N$  with  $\text{supp}(N) = \mathfrak{X}(I)$  such that

$$\text{Ext}^i(N, M) = 0 \quad \text{for all } i < r.$$

- (iv) There exists an  $M$ -regular sequence  $a_1, \dots, a_r$  in  $I$ .

[Hint: (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (iii) is clear. For (iii)  $\Rightarrow$  (iv), first note that

$$0 = \text{Ext}^0(N, M) = \text{Hom}(N, M).$$

Assume  $\text{supp}(N) = \mathfrak{X}(I)$ . Find an  $M$ -regular element in  $I$ . If there is no such element, then  $I$  is contained in the set of divisors of 0 of  $M$  in  $A$ , which is the union of the associated primes. Hence  $I \subset P$  for some associated prime  $P$ . This yields an injection  $A/P \subset M$ , so

$$0 \neq \text{Hom}_{A_P}(A_P/PA_P, M).$$

By hypothesis,  $N_P \neq 0$  so  $N_P/PN_P \neq 0$ , and  $N_P/PN_P$  is a vector space over  $A_P/PA_P$ , so there exists a non-zero  $A_P/PA_P$  homomorphism

$$N_P/PN_P \rightarrow M_P,$$

so  $\text{Hom}_{A_P}(N_P, M_P) \neq 0$ , whence  $\text{Hom}(N, M) \neq 0$ , a contradiction. This proves the existence of one regular element  $a_1$ .

Now let  $M_1 = M/a_1M$ . The exact sequence

$$0 \rightarrow M \xrightarrow{a_1} M \rightarrow M/a_1M \rightarrow 0$$

yields the exact cohomology sequence

$$\rightarrow \text{Ext}^i(N, M) \rightarrow \text{Ext}^i(N, M/a_1M) \rightarrow \text{Ext}^{i+1}(N, M) \rightarrow$$

so  $\text{Ext}^i(N, M/a_1M) = 0$  for  $i < r - 1$ . By induction there exists an  $M_1$ -regular sequence  $a_2, \dots, a_r$  and we are done.

Last, (iv)  $\Rightarrow$  (i). Assume the existence of the regular sequence. By induction,  $\text{Ext}^i(N, a_1M) = 0$  for  $i < r - 1$ . We have an exact sequence for  $i < r$ :

$$0 \rightarrow \text{Ext}^i(N, M) \xrightarrow{a_1} \text{Ext}^i(N, M)$$

But  $\text{supp}(N) = \mathcal{L}(\text{ann}(N)) \subset \mathcal{L}(I)$ , so  $I \subset \text{rad}(\text{ann}(N))$ , so  $a_1$  is nilpotent on  $N$ . Hence  $a_1$  is nilpotent on  $\text{Ext}^i(N, M)$ , so  $\text{Ext}^i(N, M) = 0$ . Done.] See Matsumura's [Mat 70], p. 100, Theorem 28. The result is useful in algebraic geometry, with for instance  $M = A$  itself. One thinks of  $A$  as the affine coordinate ring of some variety, and one thinks of the equations  $a_i = 0$  as defining hypersurface sections of this variety, and the simultaneous equations  $a_1 = \dots = a_r = 0$  as defining a complete intersection. The theorem gives a cohomological criterion in terms of  $\text{Ext}$  for the existence of such a complete intersection.

---

## APPENDIX 1

---

# The Transcendence of $e$ and $\pi$

The proof which we shall give here follows the classical method of Gelfond and Schneider, properly formulated. It is based on a theorem concerning values of functions satisfying differential equations, and it had been recognized for some time that such values are subject to severe restrictions, in various contexts. Here, we deal with the most general algebraic differential equation.

We shall assume that the reader is acquainted with elementary facts concerning functions of a complex variable. Let  $f$  be an entire function (i.e. a function which is holomorphic on the complex plane). For our purposes, we say  $f$  is of order  $\leq \rho$  if there exists a number  $C > 1$  such that for all large  $R$  we have

$$|f(z)| \leq C^{R^\rho}$$

whenever  $|z| \leq R$ . A meromorphic function is said to be of order  $\leq \rho$  if it is a quotient of entire functions of order  $\leq \rho$ .

**Theorem.** *Let  $K$  be a finite extension of the rational numbers. Let  $f_1, \dots, f_N$  be meromorphic functions of order  $\leq \rho$ . Assume that the field  $K(f_1, \dots, f_N)$  has transcendence degree  $\geq 2$  over  $K$ , and that the derivative  $D = d/dz$  maps the ring  $K[f_1, \dots, f_N]$  into itself. Let  $w_1, \dots, w_m$  be distinct complex numbers not lying among the poles of the  $f_i$ , such that*

$$f_i(w_v) \in K$$

*for all  $i = 1, \dots, N$  and  $v = 1, \dots, m$ . Then  $m \leq 10\rho[K : \mathbf{Q}]$ .*

**Corollary 1.** (Hermite-Lindemann). *If  $\alpha$  is algebraic (over  $\mathbf{Q}$ ) and  $\neq 0$ , then  $e^\alpha$  is transcendental. Hence  $\pi$  is transcendental.*

*Proof.* Suppose that  $\alpha$  and  $e^\alpha$  are algebraic. Let  $K = \mathbf{Q}(\alpha, e^\alpha)$ . The two functions  $z$  and  $e^z$  are algebraically independent over  $K$  (trivial), and the ring  $K[z, e^z]$  is obviously mapped into itself by the derivative. Our functions take on algebraic values in  $K$  at  $\alpha, 2\alpha, \dots, m\alpha$  for any  $m$ , contradiction. Since  $e^{2\pi i} = 1$ , it follows that  $2\pi i$  is transcendental.

**Corollary 2.** (Gelfond-Schneider). *If  $\alpha$  is algebraic  $\neq 0, 1$  and if  $\beta$  is algebraic irrational, then  $\alpha^\beta = e^{\beta \log \alpha}$  is transcendental.*

*Proof.* We proceed as in Corollary 1, considering the functions  $e^{\beta t}$  and  $e^t$  which are algebraically independent because  $\beta$  is assumed irrational. We look at the numbers  $\log \alpha, 2 \log \alpha, \dots, m \log \alpha$  to get a contradiction as in Corollary 1.

Before giving the main arguments proving the theorem, we state some lemmas. The first two, due to Siegel, have to do with integral solutions of linear homogeneous equations.

**Lemma 1.** *Let*

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= 0 \\ &\dots \\ a_{r1}x_1 + \cdots + a_{rn}x_n &= 0 \end{aligned}$$

*be a system of linear equations with integer coefficients  $a_{ij}$ , and  $n > r$ . Let  $A$  be a number such that  $|a_{ij}| \leq A$  for all  $i, j$ . Then there exists an integral, non-trivial solution with*

$$|x_j| \leq 2(2nA)^{r/(n-r)}.$$

*Proof.* We view our system of linear equations as a linear equation  $L(X) = 0$ , where  $L$  is a linear map,  $L: \mathbf{Z}^{(n)} \rightarrow \mathbf{Z}^{(r)}$ , determined by the matrix of coefficients. If  $B$  is a positive number, we denote by  $\mathbf{Z}^{(n)}(B)$  the set of vectors  $X$  in  $\mathbf{Z}^{(n)}$  such that  $|X| \leq B$  (where  $|X|$  is the maximum of the absolute values of the coefficients of  $X$ ). Then  $L$  maps  $\mathbf{Z}^{(n)}(B)$  into  $\mathbf{Z}^{(r)}(nBA)$ . The number of elements in  $\mathbf{Z}^{(n)}(B)$  is  $\geq B^n$  and  $\leq (2B + 1)^n$ . We seek a value of  $B$  such that there will be two distinct elements  $X, Y$  in  $\mathbf{Z}^{(n)}(B)$  having the same image,  $L(X) = L(Y)$ . For this, it will suffice that  $B^n > (2nBA)^r$ , and thus it will suffice that

$$B = (2nA)^{r/(n-r)}.$$

We take  $X - Y$  as the solution of our problem.

Let  $K$  be a finite extension of  $\mathbf{Q}$ , and let  $I_K$  be the integral closure of  $\mathbf{Z}$  in  $K$ . From Exercise 5 of Chapter IX, we know that  $I_K$  is a free module over  $\mathbf{Z}$ , of dimension  $[K : \mathbf{Q}]$ . We view  $K$  as contained in the complex numbers. If

$\alpha \in K$ , a conjugate of  $\alpha$  will be taken to be an element  $\sigma\alpha$ , where  $\sigma$  is an embedding of  $K$  in  $\mathbb{C}$ . By the **size** of a set of elements of  $K$  we shall mean the maximum of the absolute values of all conjugates of these elements.

By the size of a vector  $X = (x_1, \dots, x_n)$  we shall mean the size of the set of its coordinates.

Let  $\omega_1, \dots, \omega_M$  be a basis of  $I_K$  over  $\mathbb{Z}$ . Let  $\alpha \in I_K$ , and write

$$\alpha = a_1\omega_1 + \dots + a_M\omega_M.$$

Let  $\omega'_1, \dots, \omega'_M$  be the dual basis of  $\omega_1, \dots, \omega_M$  with respect to the trace. Then we can express the (Fourier) coefficients  $a_j$  of  $\alpha$  as a trace,

$$a_j = \text{Tr}(\alpha\omega'_j).$$

The trace is a sum over the conjugates. Hence the size of these coefficients is bounded by the size of  $\alpha$ , times a fixed constant, depending on the size of the elements  $\omega'_j$ .

**Lemma 2.** *Let  $K$  be a finite extension of  $\mathbb{Q}$ . Let*

$$\begin{aligned} \alpha_{11}x_1 + \dots + \alpha_{1n}x_n &= 0 \\ &\dots \\ \alpha_{r1}x_1 + \dots + \alpha_{rn}x_n &= 0 \end{aligned}$$

*be a system of linear equations with coefficients in  $I_K$ , and  $n > r$ . Let  $A$  be a number such that  $\text{size}(\alpha_{ij}) \leq A$ , for all  $i, j$ . Then there exists a non-trivial solution  $X$  in  $I_K$  such that*

$$\text{size}(X) \leq C_1(C_2 n A)^{r/(n-r)},$$

*where  $C_1, C_2$  are constants depending only on  $K$ .*

*Proof.* Let  $\omega_1, \dots, \omega_M$  be a basis of  $I_K$  over  $\mathbb{Z}$ . Each  $x_j$  can be written

$$x_j = \xi_{j1}\omega_1 + \dots + \xi_{jM}\omega_M$$

with unknowns  $\xi_{j\lambda}$ . Each  $\alpha_{ij}$  can be written

$$\alpha_{ij} = a_{ij1}\omega_1 + \dots + a_{ijM}\omega_M$$

with integers  $a_{ij\lambda} \in \mathbb{Z}$ . If we multiply out the  $\alpha_{ij}x_j$ , we find that our linear equations with coefficients in  $I_K$  are equivalent to a system of  $rM$  linear equations in the  $nM$  unknowns  $\xi_{j\lambda}$ , with coefficients in  $\mathbb{Z}$ , whose size is bounded by  $CA$ , where  $C$  is a number depending only on  $M$  and the size of the elements  $\omega_\lambda$ , together with the products  $\omega_\lambda\omega_\mu$ , in other words where  $C$  depends only on  $K$ . Applying Lemma 1, we obtain a solution in terms of the  $\xi_{j\lambda}$ , and hence a solution  $X$  in  $I_K$ , whose size satisfies the desired bound.

The next lemma has to do with estimates of derivatives. By the size of a polynomial with coefficients in  $K$ , we shall mean the size of its set of coefficients. A **denominator** for a set of elements of  $K$  will be any positive rational integer whose product with every element of the set is an algebraic integer. We define in a similar way a denominator for a polynomial with coefficients in  $K$ . We abbreviate “denominator” by den.

Let

$$P(T_1, \dots, T_N) = \sum \alpha_{(v)} M_{(v)}(T)$$

be a polynomial with complex coefficients, and let

$$Q(T_1, \dots, T_N) = \sum \beta_{(v)} M_{(v)}(T)$$

be a polynomial with real coefficients  $\geq 0$ . We say that  $Q$  **dominates**  $P$  if  $|\alpha_{(v)}| \leq \beta_{(v)}$  for all  $(v)$ . It is then immediately verified that the relation of dominance is preserved under addition, multiplication, and taking partial derivatives with respect to the variables  $T_1, \dots, T_N$ .

**Lemma 3.** *Let  $K$  be of finite degree over  $\mathbf{Q}$ . Let  $f_1, \dots, f_N$  be functions, holomorphic on a neighborhood of a point  $w \in \mathbf{C}$ , and assume that  $D = d/dz$  maps the ring  $K[f_1, \dots, f_N]$  into itself. Assume that  $f_i(w) \in K$  for all  $i$ . Then there exists a number  $C_1$  having the following property. Let  $P(T_1, \dots, T_N)$  be a polynomial with coefficients in  $K$ , of degree  $\leq r$ . If we set  $f = P(f_1, \dots, f_N)$ , then we have, for all positive integers  $k$ ,*

$$\text{size}(D^k f(w)) \leq \text{size}(P) r^k k! C_1^{k+r}$$

Furthermore, there is a denominator for  $D^k f(w)$  bounded by  $\text{den}(P) C_1^{k+r}$ .

*Proof.* There exist polynomials  $P_i(T_1, \dots, T_N)$  with coefficients in  $K$  such that

$$Df_i = P_i(f_1, \dots, f_N).$$

Let  $h$  be the maximum of their degrees. There exists a unique derivation  $\bar{D}$  on  $K[T_1, \dots, T_N]$  such that  $\bar{D}T_i = P_i(T_1, \dots, T_N)$ . For any polynomial  $P$  we have

$$\bar{D}(P(T_1, \dots, T_N)) = \sum_{i=1}^N (D_i P)(T_1, \dots, T_N) \cdot P_i(T_1, \dots, T_N),$$

where  $D_1, \dots, D_N$  are the partial derivatives. The polynomial  $P$  is dominated by

$$\text{size}(P)(1 + T_1 + \dots + T_N)^r,$$

and each  $P_i$  is dominated by  $\text{size}(P_i)(1 + T_1 + \dots + T_N)^h$ . Thus  $\bar{D}P$  is dominated by

$$\text{size}(P) C_2 r (1 + T_1 + \dots + T_N)^{r+h}.$$

Proceeding inductively, one sees that  $\bar{D}^k P$  is dominated by

$$\text{size}(P) C_3^k r^k k! (1 + T_1 + \dots + T_N)^{r+k}.$$

Substituting values  $f_i(w)$  for  $T_i$ , we obtain the desired bound on  $D^k f(w)$ . The second assertion concerning denominators is proved also by a trivial induction.

We now come to the main part of the proof of our theorem. Let  $f, g$  be two functions among  $f_1, \dots, f_N$  which are algebraically independent over  $K$ . Let  $r$  be a positive integer divisible by  $2m$ . We shall let  $r$  tend to infinity at the end of the proof.

Let

$$F = \sum_{i,j=1}^r b_{ij} f^i g^j$$

have coefficients  $b_{ij}$  in  $K$ . Let  $n = r^2/2m$ . We can select the  $b_{ij}$  not all equal to 0, and such that

$$D^k F(w_v) = 0$$

for  $0 \leq k < n$  and  $v = 1, \dots, m$ . Indeed, we have to solve a system of  $mn$  linear equations in  $r^2 = 2mn$  unknowns. Note that

$$\frac{mn}{2mn - mn} = 1.$$

We multiply these equations by a denominator for the coefficients. Using the estimate of Lemma 3, and Lemma 2, we can in fact take the  $b_{ij}$  to be algebraic integers, whose size is bounded by

$$O(r^n n! C_1^{n+r}) \leq O(n^{2n})$$

for  $n \rightarrow \infty$ .

Since  $f, g$  are algebraically independent over  $K$ , our function  $F$  is not identically zero. We let  $s$  be the smallest integer such that all derivatives of  $F$  up to order  $s-1$  vanish at all points  $w_1, \dots, w_m$ , but such that  $D^s F$  does not vanish at one of the  $w$ , say  $w_1$ . Then  $s \geq n$ . We let

$$\gamma = D^s F(w_1) \neq 0.$$

Then  $\gamma$  is an element of  $K$ , and by Lemma 3, it has a denominator which is bounded by  $O(C_1^s)$  for  $s \rightarrow \infty$ . Let  $c$  be this denominator. The norm of  $c\gamma$  from  $K$  to  $\mathbf{Q}$  is then a non-zero rational integer. Each conjugate of  $c\gamma$  is bounded by  $O(s^{5s})$ . Consequently, we get

$$(1) \quad 1 \leq |N_{\mathbf{Q}}^K(c\gamma)| \leq O(s^{5s})^{[K:\mathbf{Q}]-1} |\gamma|,$$

where  $|\gamma|$  is the fixed absolute value of  $\gamma$ , which will now be estimated very well by global arguments.

Let  $\theta$  be an entire function of order  $\leq \rho$ , such that  $\theta f$  and  $\theta g$  are entire, and  $\theta(w_1) \neq 0$ . Then  $\theta^{2r}F$  is entire. We consider the entire function

$$H(z) = \frac{\theta(z)^{2r}F(z)}{\prod_{v=1}^m (z - w_v)^s}.$$

Then  $H(w_1)$  differs from  $D^s F(w_1)$  by obvious factors, bounded by  $C_4^s s!$ . By the maximum modulus principle, its absolute value is bounded by the maximum of  $H$  on a large circle of radius  $R$ . If we take  $R$  large, then  $z - w_v$  has approximately the same absolute value as  $R$ , and consequently, on the circle of radius  $R$ ,  $H(z)$  is bounded in absolute value by an expression of type

$$\frac{s^{3s} C_5^{2rR\rho}}{R^{ms}}.$$

We select  $R = s^{1/2\rho}$ . We then get the estimate

$$|\gamma| \leq \frac{s^{4s} C_6^s}{s^{ms/2\rho}}.$$

We now let  $r$  tend to infinity. Then both  $n$  and  $s$  tend to infinity. Combining this last inequality with inequality (1), we obtain the desired bound on  $m$ . This concludes the proof.

Of course, we made no effort to be especially careful in the powers of  $s$  occurring in the estimates, and the number 10 can obviously be decreased by exercising a little more care in the estimates.

The theorem we proved is only the simplest in an extensive theory dealing with problems of transcendence degree. In some sense, the theorem is best possible without additional hypotheses. For instance, if  $P(t)$  is a polynomial with integer coefficients, then  $e^{P(t)}$  will take the value 1 at all roots of  $P$ , these being algebraic. Furthermore, the functions

$$t, e^t, e^{t^2}, \dots, e^{t^n}$$

are algebraically independent, but take on values in  $\mathbf{Q}(e)$  for all integral values of  $t$ .

However, one expects rather strong results of algebraic independence to hold. Lindemann proved that if  $\alpha_1, \dots, \alpha_n$  are algebraic numbers, linearly independent over  $\mathbf{Q}$ , then

$$e^{\alpha_1}, \dots, e^{\alpha_n}$$

are algebraically independent.

More generally, Schanuel has made the following conjecture: If  $\alpha_1, \dots, \alpha_n$  are complex numbers, linearly independent over  $\mathbf{Q}$ , then the transcendence degree of

$$\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n}$$

should be  $\geq n$ .

From this one would deduce at once the algebraic independence of  $e$  and  $\pi$  (looking at  $1, 2\pi i, e, e^{2\pi i}$ ), and all other independence statements concerning the ordinary exponential function and logarithm which one feels to be true, for instance, the statement that  $\pi$  cannot lie in the field obtained by starting with the algebraic numbers, adjoining values of the exponential function, taking algebraic closure, and iterating these two operations. Such statements have to do with values of the exponential function lying in certain fields of transcendence degree  $< n$ , and one hopes that by a suitable deepening of Theorem 1, one will reach the desired results.

---

## APPENDIX 2

---

# Some Set Theory

---

### §1. DENUMERABLE SETS

Let  $n$  be a positive integer. Let  $J_n$  be the set consisting of all integers  $k$ ,  $1 \leq k \leq n$ . If  $S$  is a set, we say that  $S$  has  $n$  elements if there is a bijection between  $S$  and  $J_n$ . Such a bijection associates with each integer  $k$  as above an element of  $S$ , say  $k \mapsto a_k$ . Thus we may use  $J_n$  to “count”  $S$ . Part of what we assume about the basic facts concerning positive integers is that if  $S$  has  $n$  elements, then the integer  $n$  is uniquely determined by  $S$ .

One also agrees to say that a set has 0 elements if the set is empty.

We shall say that a set  $S$  is **denumerable** if there exists a bijection of  $S$  with the set of positive integers  $\mathbf{Z}^+$ . Such a bijection is then said to **enumerate** the set  $S$ . It is a mapping

$$n \mapsto a_n$$

which to each positive integer  $n$  associates an element of  $S$ , the mapping being injective and surjective.

If  $D$  is a denumerable set, and  $f : S \rightarrow D$  is a bijection of some set  $S$  with  $D$ , then  $S$  is also denumerable. Indeed, there is a bijection  $g : D \rightarrow \mathbf{Z}^+$ , and hence  $g \circ f$  is a bijection of  $S$  with  $\mathbf{Z}^+$ .

Let  $T$  be a set. A **sequence** of elements of  $T$  is simply a mapping of  $\mathbf{Z}^+$  into  $T$ . If the map is given by the association  $n \mapsto x_n$ , we also write the sequence as  $\{x_n\}_{n \geq 1}$ , or also  $\{x_1, x_2, \dots\}$ . For simplicity, we also write  $\{x_n\}$  for the sequence. Thus we think of the sequence as prescribing a first, second,  $\dots$ ,  $n$ -th element of  $T$ . We use the same braces for sequences as for sets, but the context will always make our meaning clear.

**Examples.** The even positive integers may be viewed as a sequence  $\{x_n\}$  if we put  $x_n = 2n$  for  $n = 1, 2, \dots$ . The odd positive integers may also be viewed as a sequence  $\{y_n\}$  if we put  $y_n = 2n - 1$  for  $n = 1, 2, \dots$ . In each case, the sequence gives an enumeration of the given set.

We also use the word *sequence* for mappings of the natural numbers into a set, thus allowing our sequences to start from 0 instead of 1. If we need to specify whether a sequence starts with the 0-th term or the first term, we write

$$\{x_n\}_{n \geq 0} \quad \text{or} \quad \{x_n\}_{n \geq 1}$$

according to the desired case. Unless otherwise specified, however, we always assume that a sequence will start with the first term. Note that from a sequence  $\{x_n\}_{n \geq 0}$  we can define a new sequence by letting  $y_n = x_{n-1}$  for  $n \geq 1$ . Then  $y_1 = x_0, y_2 = x_1, \dots$ . Thus there is no essential difference between the two kinds of sequences.

Given a sequence  $\{x_n\}$ , we call  $x_n$  the  $n$ -th term of the sequence. A sequence may very well be such that all its terms are equal. For instance, if we let  $x_n = 1$  for all  $n \geq 1$ , we obtain the sequence  $\{1, 1, 1, \dots\}$ . Thus there is a difference between a sequence of elements in a set  $T$ , and a subset of  $T$ . In the example just given, the set of all terms of the sequence consists of one element, namely the single number 1.

Let  $\{x_1, x_2, \dots\}$  be a sequence in a set  $S$ . By a **subsequence** we shall mean a sequence  $\{x_{n_1}, x_{n_2}, \dots\}$  such that  $n_1 < n_2 < \dots$ . For instance, if  $\{x_n\}$  is the sequence of positive integers,  $x_n = n$ , the sequence of even positive integers  $\{x_{2n}\}$  is a subsequence.

An enumeration of a set  $S$  is of course a sequence in  $S$ .

A set is **finite** if the set is empty, or if the set has  $n$  elements for some positive integer  $n$ . If a set is not finite, it is called **infinite**.

Occasionally, a map of  $J_n$  into a set  $T$  will be called a **finite sequence** in  $T$ . A finite sequence is written as usual,

$$\{x_1, \dots, x_n\} \quad \text{or} \quad \{x_i\}_{i=1, \dots, n}.$$

When we need to specify the distinction between finite sequences and maps of  $\mathbb{Z}^+$  into  $T$ , we call the latter infinite sequences. Unless otherwise specified, we shall use the word sequence to mean infinite sequence.

**Proposition 1.1.** *Let  $D$  be an infinite subset of  $\mathbb{Z}^+$ . Then  $D$  is denumerable, and in fact there is a unique enumeration of  $D$ , say  $\{k_1, k_2, \dots\}$  such that*

$$k_1 < k_2 < \dots < k_n < k_{n+1} < \dots$$

*Proof.* We let  $k_1$  be the smallest element of  $D$ . Suppose inductively that we have defined  $k_1 < \dots < k_n$ , in such a way that any element  $k$  in  $D$  which is not equal to  $k_1, \dots, k_n$  is  $> k_n$ . We define  $k_{n+1}$  to be the smallest element of  $D$  which is  $> k_n$ . Then the map  $n \mapsto k_n$  is the desired enumeration of  $D$ .

**Corollary 1.2.** *Let  $S$  be a denumerable set and  $D$  an infinite subset of  $S$ . Then  $D$  is denumerable.*

*Proof.* Given an enumeration of  $S$ , the subset  $D$  corresponds to a subset of  $\mathbf{Z}^+$  in this enumeration. Using Proposition 1.1, we conclude that we can enumerate  $D$ .

**Proposition 1.3.** *Every infinite set contains a denumerable subset.*

*Proof.* Let  $S$  be an infinite set. For every non-empty subset  $T$  of  $S$ , we select a definite element  $a_T$  in  $T$ . We then proceed by induction. We let  $x_1$  be the chosen element  $a_S$ . Suppose that we have chosen  $x_1, \dots, x_n$  having the property that for each  $k = 2, \dots, n$  the element  $x_k$  is the selected element in the subset which is the complement of  $\{x_1, \dots, x_{k-1}\}$ . We let  $x_{n+1}$  be the selected element in the complement of the set  $\{x_1, \dots, x_n\}$ . By induction, we thus obtain an association  $n \mapsto x_n$  for all positive integers  $n$ , and since  $x_n \neq x_k$  for all  $k < n$  it follows that our association is injective, i.e. gives an enumeration of a subset of  $S$ .

**Proposition 1.4.** *Let  $D$  be a denumerable set, and  $f: D \rightarrow S$  a surjective mapping. Then  $S$  is denumerable or finite.*

*Proof.* For each  $y \in S$ , there exists an element  $x_y \in D$  such that  $f(x_y) = y$  because  $f$  is surjective. The association  $y \mapsto x_y$  is an injective mapping of  $S$  into  $D$ , because if

$$y, z \in S \quad \text{and} \quad x_y = x_z$$

then

$$y = f(x_y) = f(x_z) = z.$$

Let  $g(y) = x_y$ . The image of  $g$  is a subset of  $D$  and  $D$  is denumerable. Since  $g$  is a bijection between  $S$  and its image, it follows that  $S$  is denumerable or finite.

**Proposition 1.5.** *Let  $D$  be a denumerable set. Then  $D \times D$  (the set of all pairs  $(x, y)$  with  $x, y \in D$ ) is denumerable.*

*Proof.* There is a bijection between  $D \times D$  and  $\mathbf{Z}^+ \times \mathbf{Z}^+$ , so it will suffice to prove that  $\mathbf{Z}^+ \times \mathbf{Z}^+$  is denumerable. Consider the mapping of  $\mathbf{Z}^+ \times \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$  given by

$$(m, n) \mapsto 2^m 3^n.$$

It is injective, and by Proposition 1.1, our result follows.

**Proposition 1.6.** *Let  $\{D_1, D_2, \dots\}$  be a sequence of denumerable sets. Let  $S$  be the union of all sets  $D_i$  ( $i = 1, 2, \dots$ ). Then  $S$  is denumerable.*

*Proof.* For each  $i = 1, 2, \dots$  we enumerate the elements of  $D_i$ , as indicated in the following notation:

$$\begin{aligned} D_1 &: \{x_{11}, x_{12}, x_{13}, \dots\} \\ D_2 &: \{x_{21}, x_{22}, x_{23}, \dots\} \\ &\dots \\ D_i &: \{x_{i1}, x_{i2}, x_{i3}, \dots\} \\ &\dots \end{aligned}$$

The map  $f: \mathbf{Z}^+ \times \mathbf{Z}^+ \rightarrow D$  given by

$$f(i, j) = x_{ij}$$

is then a surjective map of  $\mathbf{Z}^+ \times \mathbf{Z}^+$  onto  $S$ . By Proposition 1.4, it follows that  $S$  is denumerable.

**Corollary 1.7.** *Let  $F$  be a non-empty finite set and  $D$  a denumerable set. Then  $F \times D$  is denumerable. If  $S_1, S_2, \dots$  are a sequence of sets, each of which is finite or denumerable, then the union  $S_1 \cup S_2 \cup \dots$  is denumerable or finite.*

*Proof.* There is an injection of  $F$  into  $\mathbf{Z}^+$  and a bijection of  $D$  with  $\mathbf{Z}^+$ . Hence there is an injection of  $F \times D$  into  $\mathbf{Z}^+ \times \mathbf{Z}^+$  and we can apply Corollary 1.2 and Proposition 1.6 to prove the first statement. One could also define a surjective map of  $\mathbf{Z}^+ \times \mathbf{Z}^+$  onto  $F \times D$ . (Cf. Exercises 1 and 4.) As for the second statement, each finite set is contained in some denumerable set, so that the second statement follows from Proposition 1.1 and 1.6.

For convenience, we shall say that a set is **countable** if it is either finite or denumerable.

## §2. ZORN'S LEMMA

In order to deal efficiently with infinitely many sets simultaneously, one needs a special property. To state it, we need some more terminology.

Let  $S$  be a set. An **ordering** (also called partial ordering) of  $S$  is a relation, written  $x \leqq y$ , among some pairs of elements of  $S$ , having the following properties.

**ORD 1.** *We have  $x \leqq x$ .*

**ORD 2.** *If  $x \leqq y$  and  $y \leqq z$  then  $x \leqq z$ .*

**ORD 3.** *If  $x \leqq y$  and  $y \leqq x$  then  $x = y$ .*

We sometimes write  $y \geq x$  for  $x \leq y$ . Note that we don't require that the relation  $x \leq y$  or  $y \leq x$  hold for every pair of elements  $(x, y)$  of  $S$ . Some pairs may not be comparable. If the ordering satisfies this additional property, then we say that it is a **total ordering**.

**Example 1.** Let  $G$  be a group. Let  $S$  be the set of subgroups. If  $H, H'$  are subgroups of  $G$ , we define

$$H \leq H'$$

if  $H$  is a subgroup of  $H'$ . One verifies immediately that this relation defines an ordering on  $S$ . Given two subgroups  $H, H'$  of  $G$ , we do not necessarily have  $H \leq H'$  or  $H' \leq H$ .

**Example 2.** Let  $R$  be a ring, and let  $S$  be the set of left ideals of  $R$ . We define an ordering in  $S$  in a way similar to the above, namely if  $L, L'$  are left ideals of  $R$ , we define

$$L \leq L'$$

if  $L \subset L'$ .

**Example 3.** Let  $X$  be a set, and  $S$  the set of subsets of  $X$ . If  $Y, Z$  are subsets of  $X$ , we define  $Y \leq Z$  if  $Y$  is a subset of  $Z$ . This defines an ordering on  $S$ .

In all these examples, the relation of ordering is said to be that of inclusion.

In an ordered set, if  $x \leq y$  and  $x \neq y$  we then write  $x < y$ .

Let  $A$  be an ordered set, and  $B$  a subset. Then we can define an ordering on  $B$  by defining  $x \leq y$  for  $x, y \in B$  to hold if and only if  $x \leq y$  in  $A$ . We shall say that  $R_0$  is the ordering on  $B$  **induced** by  $R$ , or is the **restriction** to  $B$  of the partial ordering of  $A$ .

Let  $S$  be an ordered set. By a **least element** of  $S$  (or a **smallest element**) one means an element  $a \in S$  such that  $a \leq x$  for all  $x \in S$ . Similarly, by a **greatest element** one means an element  $b$  such that  $x \leq b$  for all  $x \in S$ .

By a **maximal element**  $m$  of  $S$  one means an element such that if  $x \in S$  and  $x \geq m$ , then  $x = m$ . Note that a maximal element need not be a greatest element. There may be many maximal elements in  $S$ , whereas if a greatest element exists, then it is unique (proof?).

Let  $S$  be an ordered set. We shall say that  $S$  is **totally ordered** if given  $x, y \in S$  we have necessarily  $x \leq y$  or  $y \leq x$ .

**Example 4.** The integers  $\mathbf{Z}$  are totally ordered by the usual ordering. So are the real numbers.

Let  $S$  be an ordered set, and  $T$  a subset. An **upper bound** of  $T$  (in  $S$ ) is an element  $b \in S$  such that  $x \leq b$  for all  $x \in T$ . A **least upper bound** of  $T$  in  $S$  is an upper bound  $b$  such that, if  $c$  is another upper bound, then  $b \leq c$ . We shall say

that  $S$  is **inductively ordered** if every non-empty totally ordered subset has an upper bound.

We shall say that  $S$  is **strictly inductively ordered** if every non-empty totally ordered subset has a least upper bound.

In Examples 1, 2, 3, in each case, the set is strictly inductively ordered. To prove this, let us take Example 1. Let  $T$  be a non-empty totally ordered subset of the set of subgroups of  $G$ . This means that if  $H, H' \in T$ , then  $H \subset H'$  or  $H' \subset H$ . Let  $U$  be the union of all sets in  $T$ . Then:

1.  $U$  is a subgroup. *Proof:* If  $x, y \in U$ , there exist subgroups  $H, H' \in T$  such that  $x \in H$  and  $y \in H'$ . If, say,  $H \subset H'$ , then both  $x, y \in H'$  and hence  $xy \in H'$ . Hence  $xy \in U$ . Also,  $x^{-1} \in H'$ , so  $x^{-1} \in U$ . Hence  $U$  is a subgroup.
2.  $U$  is an upper bound for each element of  $T$ . *Proof:* Every  $H \in T$  is contained in  $U$ , so  $H \leq U$  for all  $H \in T$ .
3.  $U$  is a least upper bound for  $T$ . *Proof:* Any subgroup of  $G$  which contains all the subgroups  $H \in T$  must then contain their union  $U$ .

The proof that the sets in Examples 2, 3 are strictly inductively ordered is entirely similar.

We can now state the property mentioned at the beginning of the section.

**Zorn's Lemma.** *Let  $S$  be a non-empty inductively ordered set. Then there exists a maximal element in  $S$ .*

As an example of Zorn's lemma, we shall now prove the infinite version of a theorem given in Chapters 1, §7, and XIV, §2, namely:

*Let  $R$  be an entire, principal ring and let  $E$  be a free module over  $R$ . Let  $F$  be a submodule. Then  $F$  is free. In fact, if  $\{v_i\}_{i \in I}$  is a basis for  $E$ , and  $F \neq \{0\}$ , then there exists a basis for  $F$  indexed by a subset of  $I$ .*

*Proof.* For each subset  $J$  of  $I$  we let  $E_J$  be the free submodule of  $E$  generated by all  $v_j, j \in J$ , and we let  $F_J = E_J \cap F$ . We let  $S$  be the set of all pairs  $(F_J, w)$  where  $J$  is a subset of  $I$ , and  $w: J' \rightarrow F_J$  is a basis of  $F_J$  indexed by a subset  $J'$  of  $J$ . We write  $w_j$  instead of  $w(j)$  for  $j \in J'$ . If  $(F_J, w)$  and  $(F_K, u)$  are such pairs, we define  $(F_J, w) \leq (F_K, u)$  if  $J \subset K$ , if  $J' \subset K'$ , and if the restriction of  $u$  to  $J'$  is equal to  $w$ . (In other words, the basis  $u$  for  $F_K$  is an extension of the basis  $w$  for  $F_J$ .) This defines an ordering on  $S$ , and it is immediately verified that  $S$  is in fact inductively ordered, and non-empty (say by the finite case of the result). We can therefore apply Zorn's lemma. Let  $(F_J, w)$  be a maximal element. We contend that  $J = I$  (this will prove our result). Suppose  $J \neq I$  and let  $k \in I$  but  $k \notin J$ . Let  $K = J \cup \{k\}$ . If

$$E_{J \cup \{k\}} \cap F = F_J,$$

then  $(F_K, w)$  is a bigger pair than  $(F_J, w)$  contradicting the maximality assumption. Otherwise there exist elements of  $F_K$  which can be written in the form

$$cv_k + y$$

with some  $y \in E_J$  and  $c \in R$ ,  $c \neq 0$ . The set of all elements  $c \in R$  such that there exists  $y \in E_J$  for which  $cv_k + y \in F$  is an ideal. Let  $a$  be a generator of this ideal, and let

$$w_k = av_k + y$$

be an element of  $F$ , with  $y \in E_J$ . If  $z \in F_K$  then there exists  $b \in R$  such that  $z - bw_k \in E_J$ . But  $z - bw_k \in F$ , whence  $z - bw_k \in F_J$ . It follows at once that the family consisting of  $w_j$  ( $j \in J$ ) and  $w_k$  is a basis for  $F_K$ , thus contradicting the maximality again. This proves what we wanted.

Zorn's lemma could be just taken as an axiom of set theory. However, it is not psychologically completely satisfactory as an axiom, because its statement is too involved, and one does not visualize easily the existence of the maximal element asserted in that statement. We show how one can prove Zorn's lemma from other properties of sets which everyone would immediately grant as acceptable psychologically.

From now on to the end of the proof of Theorem 2.1, we let  $A$  be a non-empty partially ordered and strictly inductively ordered set. We recall that **strictly inductively ordered** means that every nonempty totally ordered subset has a least upper bound. We assume given a map  $f: A \rightarrow A$  such that for all  $x \in A$  we have  $x \leqq f(x)$ . We could call such a map an **increasing** map.

Let  $a \in A$ . Let  $B$  be a subset of  $A$ . We shall say that  $B$  is **admissible** if:

1.  $B$  contains  $a$ .
2. We have  $f(B) \subset B$ .
3. Whenever  $T$  is a non-empty totally ordered subset of  $B$ , the least upper bound of  $T$  in  $A$  lies in  $B$ .

Then  $B$  is also strictly inductively ordered, by the induced ordering of  $A$ . We shall prove:

**Theorem 2.1.** (Bourbaki). *Let  $A$  be a non-empty partially ordered and strictly inductively ordered set. Let  $f: A \rightarrow A$  be an increasing mapping. Then there exists an element  $x_0 \in A$  such that  $f(x_0) = x_0$ .*

*Proof.* Suppose that  $A$  were totally ordered. By assumption, it would have a least upper bound  $b \in A$ , and then

$$b \leqq f(b) \leqq b,$$

so that in this case, our theorem is clear. The whole problem is to reduce the theorem to that case. In other words, what we need to find is a totally ordered admissible subset of  $A$ .

If we throw out of  $A$  all elements  $x \in A$  such that  $x$  is not  $\geq a$ , then what remains is obviously an admissible subset. Thus without loss of generality, we may assume that  $A$  has a least element  $a$ , that is  $a \leq x$  for all  $x \in A$ .

Let  $M$  be the intersection of all admissible subsets of  $A$ . Note that  $A$  itself is an admissible subset, and that all admissible subsets of  $A$  contain  $a$ , so that  $M$  is not empty. Furthermore,  $M$  is itself an admissible subset of  $A$ . To see this, let  $x \in M$ . Then  $x$  is in every admissible subset, so  $f(x)$  is also in every admissible subset, and hence  $f(x) \in M$ . Hence  $f(M) \subset M$ . If  $T$  is a totally ordered non-empty subset of  $M$ , and  $b$  is the least upper bound of  $T$  in  $A$ , then  $b$  lies in every admissible subset of  $A$ , and hence lies in  $M$ . It follows that  $M$  is the smallest admissible subset of  $A$ , and that any admissible subset of  $A$  contained in  $M$  is equal to  $M$ .

We shall prove that  $M$  is totally ordered, and thereby prove Theorem 2.1.

[First we make some remarks which don't belong to the proof, but will help in the understanding of the subsequent lemmas. Since  $a \in M$ , we see that  $f(a) \in M$ ,  $f \circ f(a) \in M$ , and in general  $f^n(a) \in M$ . Furthermore,

$$a \leq f(a) \leq f^2(a) \leq \dots$$

If we had an equality somewhere, we would be finished, so we may assume that the inequalities hold. Let  $D_0$  be the totally ordered set  $\{f^n(a)\}_{n \geq 0}$ . Then  $D_0$  looks like this:

$$a < f(a) < f^2(a) < \dots < f^n(a) < \dots$$

Let  $a_1$  be the least upper bound of  $D_0$ . Then we can form

$$a_1 < f(a_1) < f^2(a_1) < \dots$$

in the same way to obtain  $D_1$ , and we can continue this process, to obtain

$$D_1, D_2, \dots$$

It is clear that  $D_1, D_2, \dots$  are contained in  $M$ . If we had a precise way of expressing the fact that we can establish a never-ending string of such denumerable sets, then we would obtain what we want. The point is that we are now trying to prove Zorn's lemma, which is the natural tool for guaranteeing the existence of such a string. However, given such a string, we observe that its elements have two properties: If  $c$  is an element of such a string and  $x < c$ , then  $f(x) \leq c$ . Furthermore, there is no element between  $c$  and  $f(c)$ , that is if  $x$  is an element of the string, then  $x \leq c$  or  $f(c) \leq x$ . We shall now prove two lemmas which show that elements of  $M$  have these properties.]

Let  $c \in M$ . We shall say that  $c$  is an **extreme point** of  $M$  if whenever  $x \in M$  and  $x < c$ , then  $f(x) \leq c$ . For each extreme point  $c \in M$  we let

$$M_c = \text{set of } x \in M \text{ such that } x \leq c \text{ or } f(c) \leq x.$$

Note that  $M_c$  is not empty because  $a$  is in it.

**Lemma 2.2.** *We have  $M_c = M$  for every extreme point  $c$  of  $M$ .*

*Proof.* It will suffice to prove that  $M_c$  is an admissible subset. Let  $x \in M_c$ . If  $x < c$  then  $f(x) \leq c$  so  $f(x) \in M_c$ . If  $x = c$  then  $f(x) = f(c)$  is again in  $M_c$ . If  $f(c) \leq x$ , then  $f(c) \leq x \leq f(x)$ , so once more  $f(x) \in M_c$ . Thus we have proved that  $f(M_c) \subset M_c$ .

Let  $T$  be a totally ordered subset of  $M_c$  and let  $b$  be the least upper bound of  $T$  in  $M$ . If all elements  $x \in T$  are  $\leq c$ , then  $b \leq c$  and  $b \in M_c$ . If some  $x \in T$  is such that  $f(c) \leq x$ , then  $f(c) \leq x \leq b$ , and so  $b$  is in  $M_c$ . This proves our lemma.

**Lemma 2.3.** *Every element of  $M$  is an extreme point.*

*Proof.* Let  $E$  be the set of extreme points of  $M$ . Then  $E$  is not empty because  $a \in E$ . It will suffice to prove that  $E$  is an admissible subset. We first prove that  $f$  maps  $E$  into itself. Let  $c \in E$ . Let  $x \in M$  and suppose  $x < f(c)$ . We must prove that  $f(x) \leq f(c)$ . By Lemma 2.2,  $M = M_c$ , and hence we have  $x < c$ , or  $x = c$ , or  $f(c) \leq x$ . This last possibility cannot occur because  $x < f(c)$ . If  $x < c$  then

$$f(x) \leq c \leq f(c).$$

If  $x = c$  then  $f(x) = f(c)$ , and hence  $f(E) \subset E$ .

Next let  $T$  be a totally ordered subset of  $E$ . Let  $b$  be the least upper bound of  $T$  in  $M$ . We must prove that  $b \in E$ . Let  $x \in M$  and  $x < b$ . If for all  $c \in T$  we have  $f(c) \leq x$ , then  $c \leq f(c) \leq x$  implies that  $x$  is an upper bound for  $T$ , whence  $b \leq x$ , which is impossible. Since  $M_c = M$  for all  $c \in E$ , we must therefore have  $x \leq c$  for some  $c \in T$ . If  $x < c$ , then  $f(x) \leq c \leq b$ , and if  $x = c$ , then

$$c = x < b.$$

Since  $c$  is an extreme point and  $M_c = M$ , we get  $f(x) \leq b$ . This proves that  $b \in E$ , that  $E$  is admissible, and thus proves Lemma 2.3.

We now see trivially that  $M$  is totally ordered. For let  $x, y \in M$ . Then  $x$  is an extreme point of  $M$  by Lemma 2, and  $y \in M_x$  so  $y \leq x$  or

$$x \leq f(x) \leq y,$$

thereby proving that  $M$  is totally ordered. As remarked previously, this concludes the proof of Theorem 2.1.

We shall obtain Zorn's lemma essentially as a corollary of Theorem 2.1. We first obtain Zorn's lemma in a slightly weaker form.

**Corollary 2.4.** *Let  $A$  be a non-empty strictly inductively ordered set. Then  $A$  has a maximal element.*

*Proof.* Suppose that  $A$  does not have a maximal element. Then for each  $x \in A$  there exists an element  $y_x \in A$  such that  $x < y_x$ . Let  $f: A \rightarrow A$  be the map such that  $f(x) = y_x$  for all  $x \in A$ . Then  $A, f$  satisfy the hypotheses of Theorem 2.1 and applying Theorem 2.1 yields a contradiction.

The only difference between Corollary 2.4 and Zorn's lemma is that in Corollary 2.4, we assume that a non-empty totally ordered subset has a *least* upper bound, rather than an upper bound. It is, however, a simple matter to reduce Zorn's lemma to the seemingly weaker form of Corollary 2.4. We do this in the second corollary.

**Corollary 2.5. (Zorn's lemma).** *Let  $S$  be a non-empty inductively ordered set. Then  $S$  has a maximal element.*

*Proof.* Let  $A$  be the set of non-empty totally ordered subsets of  $S$ . Then  $A$  is not empty since any subset of  $S$  with one element belongs to  $A$ . If  $X, Y \in A$ , we define  $X \leqq Y$  to mean  $X \subset Y$ . Then  $A$  is partially ordered, and is in fact strictly inductively ordered. For let  $T = \{X_i\}_{i \in I}$  be a totally ordered subset of  $A$ . Let

$$Z = \bigcup_{i \in I} X_i.$$

Then  $Z$  is totally ordered. To see this, let  $x, y \in Z$ . Then  $x \in X_i$  and  $y \in X_j$  for some  $i, j \in I$ . Since  $T$  is totally ordered, say  $X_i \subset X_j$ . Then  $x, y \in X_j$  and since  $X_j$  is totally ordered,  $x \leqq y$  or  $y \leqq x$ . Thus  $Z$  is totally ordered, and is obviously a least upper bound for  $T$  in  $A$ . By Corollary 2.4, we conclude that  $A$  has a maximal element  $X_0$ . This means that  $X_0$  is a maximal totally ordered subset of  $S$  (non-empty). Let  $m$  be an upper bound for  $X_0$  in  $S$ . Then  $m$  is the desired maximal element of  $S$ . For if  $x \in S$  and  $m \leqq x$  then  $X_0 \cup \{x\}$  is totally ordered, whence equal to  $X_0$  by the maximality of  $X_0$ . Thus  $x \in X_0$  and  $x \leqq m$ . Hence  $x = m$ , as was to be shown.

### §3. CARDINAL NUMBERS

Let  $A, B$  be sets. We shall say that the **cardinality** of  $A$  is the same as the cardinality of  $B$ , and write

$$\text{card}(A) = \text{card}(B)$$

if there exists a bijection of  $A$  onto  $B$ .

We say  $\text{card}(A) \leq \text{card}(B)$  if there exists an injective mapping (injection)  $f: A \rightarrow B$ . We also write  $\text{card}(B) \geq \text{card}(A)$  in this case. It is clear that if  $\text{card}(A) \leq \text{card}(B)$  and  $\text{card}(B) \leq \text{card}(C)$ , then  $\text{card}(A) \leq \text{card}(C)$ .

This amounts to saying that a composite of injective mappings is injective. Similarly, if  $\text{card}(A) = \text{card}(B)$  and  $\text{card}(B) = \text{card}(C)$  then  $\text{card}(A) = \text{card}(C)$ .

This amounts to saying that a composite of bijective mappings is bijective. We clearly have  $\text{card}(A) = \text{card}(A)$ . Using Zorn's lemma, it is easy to show (see Exercise 14) that

$$\text{card}(A) \leq \text{card}(B) \quad \text{or} \quad \text{card}(B) \leq \text{card}(A).$$

Let  $f: A \rightarrow B$  be a surjective map of a set  $A$  onto a set  $B$ . Then

$$\text{card}(B) \leq \text{card}(A).$$

This is easily seen, because for each  $y \in B$  there exists an element  $x \in A$ , denoted by  $x_y$ , such that  $f(x_y) = y$ . Then the association  $y \mapsto x_y$  is an injective mapping of  $B$  into  $A$ , whence by definition,  $\text{card}(B) \leq \text{card}(A)$ .

Given two nonempty sets  $A, B$  we have  $\text{card}(A) \leq \text{card}(B)$  or  $\text{card}(B) \leq \text{card}(A)$ .

This is a simple application of Zorn's lemma. We consider the family of pairs  $(S, f)$  where  $S$  is a subset of  $A$  and  $f: S \rightarrow B$  is an injective mapping. From the existence of a maximal element, the assertion follows at once.

**Theorem 3.1.** (Schroeder-Bernstein). *Let  $A, B$  be sets, and suppose that  $\text{card}(A) \leq \text{card}(B)$ , and  $\text{card}(B) \leq \text{card}(A)$ . Then*

$$\text{card}(A) = \text{card}(B).$$

*Proof.* Let

$$f: A \rightarrow B \quad \text{and} \quad g: B \rightarrow A$$

be injections. We separate  $A$  into two disjoint sets  $A_1$  and  $A_2$ . We let  $A_1$  consist of all  $x \in A$  such that, when we lift back  $x$  by a succession of inverse maps,

$$x, g^{-1}(x), f^{-1} \circ g^{-1}(x), g^{-1} \circ f^{-1} \circ g^{-1}(x), \dots$$

then at some stage we reach an element of  $A$  which cannot be lifted back to  $B$  by  $g$ . We let  $A_2$  be the complement of  $A_1$ , in other words, the set of  $x \in A$  which can be lifted back indefinitely, or such that we get stopped in  $B$  (i.e. reach an element of  $B$  which has no inverse image in  $A$  by  $f$ ). Then  $A = A_1 \cup A_2$ . We shall define a bijection  $h$  of  $A$  onto  $B$ .

If  $x \in A_1$ , we define  $h(x) = f(x)$ .

If  $x \in A_2$ , we define  $h(x) = g^{-1}(x) = \text{unique element } y \in B \text{ such that } g(y) = x$ .

Then trivially,  $h$  is injective. We must prove that  $h$  is surjective. Let  $b \in B$ . If, when we try to lift back  $b$  by a succession of maps

$$\dots \circ f^{-1} \circ g^{-1} \circ f^{-1} \circ g^{-1} \circ f^{-1}(b)$$

we can lift back indefinitely, or if we get stopped in  $B$ , then  $g(b)$  belongs to  $A_2$  and consequently  $b = h(g(b))$ , so  $b$  lies in the image of  $h$ . On the other hand, if we cannot lift back  $b$  indefinitely, and get stopped in  $A$ , then  $f^{-1}(b)$  is defined (i.e.,  $b$  is in the image of  $f$ ), and  $f^{-1}(b)$  lies in  $A_1$ . In this case,  $b = h(f^{-1}(b))$  is also in the image of  $h$ , as was to be shown.

Next we consider theorems concerning sums and products of cardinalities.

We shall reduce the study of cardinalities of products of arbitrary sets to the denumerable case, using Zorn's lemma. Note first that an infinite set  $A$  always contains a denumerable set. Indeed, since  $A$  is infinite, we can first select an element  $a_1 \in A$ , and the complement of  $\{a_1\}$  is infinite. Inductively, if we have selected distinct elements  $a_1, \dots, a_n$  in  $A$ , the complement of  $\{a_1, \dots, a_n\}$  is infinite, and we can select  $a_{n+1}$  in this complement. In this way, we obtain a sequence of distinct elements of  $A$ , giving rise to a denumerable subset of  $A$ .

Let  $A$  be a set. By a **covering** of  $A$  one means a set  $\Gamma$  of subsets of  $A$  such that the union

$$\bigcup_{C \in \Gamma} C$$

of all the elements of  $\Gamma$  is equal to  $A$ . We shall say that  $\Gamma$  is a **disjoint covering** if whenever  $C, C' \in \Gamma$ , and  $C \neq C'$ , then the intersection of  $C$  and  $C'$  is empty.

**Lemma 3.2.** *Let  $A$  be an infinite set. Then there exists a disjoint covering of  $A$  by denumerable sets.*

*Proof.* Let  $S$  be the set whose elements are pairs  $(B, \Gamma)$  consisting of a subset  $B$  of  $A$ , and a disjoint covering of  $B$  by denumerable sets. Then  $S$  is not empty. Indeed, since  $A$  is infinite,  $A$  contains a denumerable set  $D$ , and the pair  $(D, \{D\})$  is in  $S$ . If  $(B, \Gamma)$  and  $(B', \Gamma')$  are elements of  $S$ , we define

$$(B, \Gamma) \leqq (B', \Gamma')$$

to mean that  $B \subset B'$ , and  $\Gamma \subset \Gamma'$ . Let  $T$  be a totally ordered non-empty subset of  $S$ . We may write  $T = \{(B_i, \Gamma_i)\}_{i \in I}$  for some indexing set  $I$ . Let

$$B = \bigcup_{i \in I} B_i \quad \text{and} \quad \Gamma = \bigcup_{i \in I} \Gamma_i.$$

If  $C, C' \in \Gamma$ ,  $C \neq C'$ , then there exists some indices  $i, j$  such that  $C \in \Gamma_i$  and  $C' \in \Gamma_j$ . Since  $T$  is totally ordered, we have, say,

$$(B_i, \Gamma_i) \leqq (B_j, \Gamma_j).$$

Hence in fact,  $C, C'$  are both elements of  $\Gamma_j$ , and hence  $C, C'$  have an empty intersection. On the other hand, if  $x \in B$ , then  $x \in B_i$  for some  $i$ , and hence there is some  $C \in \Gamma_i$  such that  $x \in C$ . Hence  $\Gamma$  is a disjoint covering of  $B$ . Since the

elements of each  $\Gamma_i$  are denumerable subsets of  $A$ , it follows that  $\Gamma$  is a disjoint covering of  $B$  by denumerable sets, so  $(B, \Gamma)$  is in  $S$ , and is obviously an upper bound for  $T$ . Therefore  $S$  is inductively ordered.

Let  $(M, \Delta)$  be a maximal element of  $S$ , by Zorn's lemma. Suppose that  $M \neq A$ . If the complement of  $M$  in  $A$  is infinite, then there exists a denumerable set  $D$  contained in this complement. Then

$$(M \cup D, \Delta \cup \{D\})$$

is a bigger pair than  $(M, \Delta)$ , contradicting the maximality of  $(M, \Delta)$ . Hence the complement of  $M$  in  $A$  is a finite set  $F$ . Let  $D_0$  be an element of  $\Delta$ . Let

$$D_1 = D_0 \cup F.$$

Then  $D_1$  is denumerable. Let  $\Delta_1$  be the set consisting of all elements of  $\Delta$ , except  $D_0$ , together with  $D_1$ . Then  $\Delta_1$  is a disjoint covering of  $A$  by denumerable sets, as was to be shown.

**Theorem 3.3.** *Let  $A$  be an infinite set, and let  $D$  be a denumerable set. Then*

$$\text{card}(A \times D) = \text{card}(A).$$

*Proof.* By the lemma, we can write

$$A = \bigcup_{i \in I} D_i$$

as a disjoint union of denumerable sets. Then

$$A \times D = \bigcup_{i \in I} (D_i \times D).$$

For each  $i \in I$ , there is a bijection of  $D_i \times D$  on  $D_i$  by Proposition 1.5. Since the sets  $D_i \times D$  are disjoint, we get in this way a bijection of  $A \times D$  on  $A$ , as desired.

**Corollary 3.4.** *If  $F$  is a finite non-empty set, then*

$$\text{card}(A \times F) = \text{card}(A).$$

*Proof.* We have

$$\text{card}(A) \leqq \text{card}(A \times F) \leqq \text{card}(A \times D) = \text{card}(A).$$

We can then use Theorem 3.1 to get what we want.

**Corollary 3.5.** *Let  $A, B$  be non-empty sets,  $A$  infinite, and suppose*

$$\text{card}(B) \leqq \text{card}(A).$$

*Then*

$$\text{card}(A \cup B) = \text{card}(A).$$

*Proof.* We can write  $A \cup B = A \cup C$  for some subset  $C$  of  $B$ , such that  $C$  and  $A$  are disjoint. (We let  $C$  be the set of all elements of  $B$  which are not elements of  $A$ .) Then  $\text{card}(C) \leq \text{card}(A)$ . We can then construct an injection of  $A \cup C$  into the product

$$A \times \{1, 2\}$$

of  $A$  with a set consisting of 2 elements. Namely, we have a bijection of  $A$  with  $A \times \{1\}$  in the obvious way, and also an injection of  $C$  into  $A \times \{2\}$ . Thus

$$\text{card}(A \cup C) \leq \text{card}(A \times \{1, 2\}).$$

We conclude the proof by Corollary 3.4 and Theorem 3.1.

**Theorem 3.6.** *Let  $A$  be an infinite set. Then*

$$\text{card}(A \times A) = \text{card}(A).$$

*Proof.* Let  $S$  be the set consisting of pairs  $(B, f)$  where  $B$  is an infinite subset of  $A$ , and  $f$  is a bijection of  $B$  onto  $B \times B$ . Then  $S$  is not empty because if  $D$  is a denumerable subset of  $A$ , we can always find a bijection of  $D$  on  $D \times D$ . If  $(B, f)$  and  $(B', f')$  are in  $S$ , we define  $(B, f) \leq (B', f')$  to mean  $B \subset B'$ , and the restriction of  $f'$  to  $B$  is equal to  $f$ . Then  $S$  is partially ordered, and we contend that  $S$  is inductively ordered. Let  $T$  be a non-empty totally ordered subset of  $S$ , and say  $T$  consists of the pairs  $(B_i, f_i)$  for  $i$  in some indexing set  $I$ . Let

$$M = \bigcup_{i \in I} B_i.$$

We shall define a bijection  $g : M \rightarrow M \times M$ . If  $x \in M$ , then  $x$  lies in some  $B_i$ . We define  $g(x) = f_i(x)$ . This value  $f_i(x)$  is independent of the choice of  $B_i$  in which  $x$  lies. Indeed, if  $x \in B_j$  for some  $j \in I$ , then say

$$(B_i, f_i) \leq (B_j, f_j).$$

By assumption,  $B_i \subset B_j$ , and  $f_j(x) = f_i(x)$ , so  $g$  is well defined. To show  $g$  is surjective, let  $x, y \in M$  and  $(x, y) \in M \times M$ . Then  $x \in B_i$  for some  $i \in I$  and  $y \in B_j$  for some  $j \in I$ . Again since  $T$  is totally ordered, say  $(B_i, f_i) \leq (B_j, f_j)$ . Thus  $B_i \subset B_j$ , and  $x, y \in B_j$ . There exists an element  $b \in B_j$  such that

$$f_j(b) = (x, y) \in B_j \times B_j.$$

By definition,  $g(b) = (x, y)$ , so  $g$  is surjective. We leave the proof that  $g$  is injective to the reader to conclude the proof that  $g$  is a bijection. We then see

that  $(M, g)$  is an upper bound for  $T$  in  $S$ , and therefore that  $S$  is inductively ordered.

Let  $(M, g)$  be a maximal element of  $S$ , and let  $C$  be the complement of  $M$  in  $A$ . If  $\text{card}(C) \leqq \text{card}(M)$ , then

$$\text{card}(A) = \text{card}(M \cup C) = \text{card}(M)$$

by Corollary 3.5, and hence  $\text{card}(M) = \text{card}(A)$ . Since  $\text{card}(M) = \text{card}(M \times M)$ , we are done with the proof in this case. If

$$\text{card}(M) \leqq \text{card}(C),$$

then there exists a subset  $M_1$  of  $C$  having the same cardinality as  $M$ . We consider

$$\begin{aligned} (M \cup M_1) \times (M \cup M_1) \\ = (M \times M) \cup (M_1 \times M) \cup (M \times M_1) \cup (M_1 \times M_1). \end{aligned}$$

By the assumption on  $M$  and Corollary 3.5, the last three sets in parentheses on the right of this equation have the same cardinality as  $M$ . Thus

$$(M \cup M_1) \times (M \cup M_1) = (M \times M) \cup M_2$$

where  $M_2$  is disjoint from  $M \times M$ , and has the same cardinality as  $M$ . We now define a bijection

$$g_1 : M \cup M_1 \rightarrow (M \cup M_1) \times (M \cup M_1).$$

We let  $g_1(x) = g(x)$  if  $x \in M$ , and we let  $g_1$  on  $M_1$  be any bijection of  $M_1$  on  $M_2$ . In this way we have extended  $g$  to  $M \cup M_1$ , and the pair  $(M \cup M_1, g_1)$  is in  $S$ , contradicting the maximality of  $(M, g)$ . The case  $\text{card}(M) \leqq \text{card}(C)$  therefore cannot occur, and our theorem is proved (using Exercise 14 below).

**Corollary 3.7.** *If  $A$  is an infinite set, and  $A^{(n)} = A \times \cdots \times A$  is the product taken  $n$  times, then*

$$\text{card}(A^{(n)}) = \text{card}(A).$$

*Proof.* Induction.

**Corollary 3.8.** *If  $A_1, \dots, A_n$  are non-empty sets with  $A_n$  infinite, and*

$$\text{card}(A_i) \leqq \text{card}(A_n)$$

*for  $i = 1, \dots, n$ , then*

$$\text{card}(A_1 \times \cdots \times A_n) = \text{card}(A_n).$$

*Proof.* We have

$$\text{card}(A_n) \leqq \text{card}(A_1 \times \cdots \times A_n) \leqq \text{card}(A_n \times \cdots \times A_n)$$

and we use Corollary 3.7 and the Schroeder-Bernstein theorem to conclude the proof.

**Corollary 3.9.** *Let  $A$  be an infinite set, and let  $\Phi$  be the set of finite subsets of  $A$ . Then*

$$\text{card}(\Phi) = \text{card}(A).$$

*Proof.* Let  $\Phi_n$  be the set of subsets of  $A$  having exactly  $n$  elements, for each integer  $n = 1, 2, \dots$ . We first show that  $\text{card}(\Phi_n) \leqq \text{card}(A)$ . If  $F$  is an element of  $\Phi_n$ , we order the elements of  $F$  in any way, say

$$F = \{x_1, \dots, x_n\}.$$

and we associate with  $F$  the element  $(x_1, \dots, x_n) \in A^{(n)}$ ,

$$F \mapsto (x_1, \dots, x_n).$$

If  $G$  is another subset of  $A$  having  $n$  elements, say  $G = \{y_1, \dots, y_n\}$ , and  $G \neq F$ , then

$$(x_1, \dots, x_n) \neq (y_1, \dots, y_n).$$

Hence our map

$$F \mapsto (x_1, \dots, x_n)$$

of  $\Phi_n$  into  $A^{(n)}$  is injective. By Corollary 3.7, we conclude that

$$\text{card}(\Phi_n) \leqq \text{card}(A).$$

Now  $\Phi$  is the disjoint union of the  $\Phi_n$  for  $n = 1, 2, \dots$  and it is an exercise to show that  $\text{card}(\Phi) \leqq \text{card}(A)$  (cf. Exercise 1). Since

$$\text{card}(A) \leqq \text{card}(\Phi),$$

because in particular,  $\text{card}(\Phi_1) = \text{card}(A)$ , we see that our corollary is proved.

In the next theorem, we shall see that given a set, there always exists another set whose cardinality is bigger.

**Theorem 3.10.** *Let  $A$  be an infinite set, and  $T$  the set consisting of two elements  $\{0, 1\}$ . Let  $M$  be the set of all maps of  $A$  into  $T$ . Then*

$$\text{card}(A) \leqq \text{card}(M) \quad \text{and} \quad \text{card}(A) \neq \text{card}(M).$$

*Proof.* For each  $x \in A$  we let

$$f_x : A \rightarrow \{0, 1\}$$

be the map such that  $f_x(x) = 1$  and  $f_x(y) = 0$  if  $y \neq x$ . Then  $x \mapsto f_x$  is obviously an injection of  $A$  into  $M$ , so that  $\text{card}(A) \leq \text{card}(M)$ . Suppose that

$$\text{card}(A) = \text{card}(M).$$

Let

$$x \mapsto g_x$$

be a bijection between  $A$  and  $M$ . We define a map  $h : A \rightarrow \{0, 1\}$  by the rule

$$h(x) = 0 \quad \text{if} \quad g_x(x) = 1,$$

$$h(x) = 1 \quad \text{if} \quad g_x(x) = 0.$$

Then certainly  $h \neq g_x$  for any  $x$ , and this contradicts the assumption that  $x \mapsto g_x$  is a bijection, thereby proving Theorem 3.10.

**Corollary 3.11.** *Let  $A$  be an infinite set, and let  $S$  be the set of all subsets of  $A$ . Then  $\text{card}(A) \leq \text{card}(S)$  and  $\text{card}(A) \neq \text{card}(S)$ .*

*Proof.* We leave it as an exercise. [Hint: If  $B$  is a non-empty subset of  $A$ , use the characteristic function  $\varphi_B$  such that

$$\varphi_B(x) = 1 \quad \text{if} \quad x \in B,$$

$$\varphi_B(x) = 0 \quad \text{if} \quad x \notin B.$$

What can you say about the association  $B \mapsto \varphi_B$ ?]

## §4. WELL-ORDERING

An ordered set  $A$  is said to be **well-ordered** if it is totally ordered, and if every non-empty subset  $B$  has a least element, that is, an element  $a \in B$  such that  $a \leq x$  for all  $x \in B$ .

**Example 1.** The set of positive integers  $\mathbf{Z}^+$  is well-ordered. Any finite set can be well-ordered, and a denumerable set  $D$  can be well-ordered: Any bijection of  $D$  with  $\mathbf{Z}^+$  will give rise to a well-ordering of  $D$ .

**Example 2.** Let  $S$  be a well-ordered set and let  $b$  be an element of some set,  $b \notin S$ . Let  $A = S \cup \{b\}$ . We define  $x \leq b$  for all  $x \in S$ . Then  $A$  is totally ordered, and is in fact well-ordered.

*Proof.* Let  $B$  be a non-empty subset of  $A$ . If  $B$  consists of  $b$  alone, then  $b$  is a least element of  $B$ . Otherwise,  $B$  contains some element  $a \in A$ . Then  $B \cap A$  is not empty, and hence has a least element, which is obviously also a least element for  $B$ .

**Theorem 4.1.** *Every non-empty set can be well-ordered.*

*Proof.* Let  $A$  be a non-empty set. Let  $S$  be the set of all pairs  $(X, \omega)$ , where  $X$  is a subset of  $A$  and  $\omega$  is a well-ordering of  $X$ . Note that  $S$  is not empty because any single element of  $A$  gives rise to such a pair. If  $(X, \omega)$  and  $(X', \omega')$  are such pairs, we define  $(X, \omega) \leq (X', \omega')$  if  $X \subset X'$ , if the ordering induced on  $X$  by  $\omega'$  is equal to  $\omega$ , and if  $X$  is an initial segment of  $X'$ . It is obvious that this defines an ordering on  $S$ , and we contend that  $S$  is inductively ordered. Let  $\{(X_i, \omega_i)\}$  be a totally ordered non-empty subset of  $S$ . Let  $X = \bigcup X_i$ . If  $a, b \in X$ , then  $a, b$  lie in some  $X_i$ , and we define  $a \leq b$  in  $X$  if  $a \leq b$  with respect to the ordering  $\omega_i$ . This is independent of the choice of  $i$  (immediate from the assumption of total ordering). In fact,  $X$  is well ordered, for if  $Y$  is a non-empty subset of  $X$ , then there is some element  $y \in Y$  which lies in some  $X_j$ . Let  $c$  be a least element of  $X_j \cap Y$ . One verifies at once that  $c$  is a least element of  $Y$ . We can therefore apply Zorn's lemma. Let  $(X, \omega)$  be a maximal element in  $S$ . If  $X \neq A$ , then, using Example 2, we can define a well-ordering on a bigger subset than  $X$ , contradicting the maximality assumption. This proves Theorem 4.1.

**Note.** Theorem 4.1 is an immediate and straightforward consequence of Zorn's lemma. Usually in mathematics, Zorn's lemma is the most efficient tool when dealing with infinite processes.

## EXERCISES

1. Prove the statement made in the proof of Corollary 3.9.
2. If  $A$  is an infinite set, and  $\Phi_n$  is the set of subsets of  $A$  having exactly  $n$  elements, show that

$$\text{card}(A) \leq \text{card}(\Phi_n)$$

for  $n \geq 1$ .

3. Let  $A_i$  be infinite sets for  $i = 1, 2, \dots$  and assume that

$$\text{card}(A_i) \leq \text{card}(A)$$

for some set  $A$ , and all  $i$ . Show that

$$\text{card}\left(\bigcup_{i=1}^{\infty} A_i\right) \leq \text{card}(A).$$

4. Let  $K$  be a subfield of the complex numbers. Show that for each integer  $n \geq 1$ , the cardinality of the set of extensions of  $K$  of degree  $n$  in  $\mathbf{C}$  is  $\leq \text{card}(K)$ .
5. Let  $K$  be an infinite field, and  $E$  an algebraic extension of  $K$ . Show that

$$\text{card}(E) = \text{card}(K).$$

6. Finish the proof of the Corollary 3.11.
7. If  $A, B$  are sets, denote by  $M(A, B)$  the set of all maps of  $A$  into  $B$ . If  $B, B'$  are sets with the same cardinality, show that  $M(A, B)$  and  $M(A, B')$  have the same cardinality. If  $A, A'$  have the same cardinality, show that  $M(A, B)$  and  $M(A', B)$  have the same cardinality.
8. Let  $A$  be an infinite set and abbreviate  $\text{card}(A)$  by  $\alpha$ . If  $B$  is an infinite set, abbreviate  $\text{card}(B)$  by  $\beta$ . Define  $\alpha\beta$  to be  $\text{card}(A \times B)$ . Let  $B'$  be a set disjoint from  $A$  such that  $\text{card}(B) = \text{card}(B')$ . Define  $\alpha + \beta$  to be  $\text{card}(A \cup B')$ . Denote by  $B^A$  the set of all maps of  $A$  into  $B$ , and denote  $\text{card}(B^A)$  by  $\beta^\alpha$ . Let  $C$  be an infinite set and abbreviate  $\text{card}(C)$  by  $\gamma$ . Prove the following statements:
- $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ .
  - $\alpha\beta = \beta\alpha$ .
  - $\alpha^{\beta + \gamma} = \alpha^\beta\alpha^\gamma$ .
9. Let  $K$  be an infinite field. Prove that there exists an algebraically closed field  $K^a$  containing  $K$  as a subfield, and algebraic over  $K$ . [Hint: Let  $\Omega$  be a set of cardinality strictly greater than the cardinality of  $K$ , and containing  $K$ . Consider the set  $S$  of all pairs  $(E, \varphi)$  where  $E$  is a subset of  $\Omega$  such that  $K \subset E$ , and  $\varphi$  denotes a law of addition and multiplication on  $E$  which makes  $E$  into a field such that  $K$  is a subfield, and  $E$  is algebraic over  $K$ . Define a partial ordering on  $S$  in an obvious way; show that  $S$  is inductively ordered, and that a maximal element is algebraic over  $K$  and algebraically closed. You will need Exercise 5 in the last step.]
10. Let  $K$  be an infinite field. Show that the field of rational functions  $K(t)$  has the same cardinality as  $K$ .
11. Let  $J_n$  be the set of integers  $\{1, \dots, n\}$ . Let  $\mathbf{Z}^+$  be the set of positive integers. Show that the following sets have the same cardinality:
  - The set of all maps  $M(\mathbf{Z}^+, J_n)$ .
  - The set of all maps  $M(\mathbf{Z}^+, J_2)$ .
  - The set of all real numbers  $x$  such that  $0 \leq x < 1$ .
  - The set of all real numbers.
12. Show that  $M(\mathbf{Z}^+, \mathbf{Z}^+)$  has the same cardinality as the real numbers.
13. Let  $S$  be a non-empty set. Let  $S'$  denote the product  $S$  with itself taken denumerably many times. Prove that  $(S')'$  has the same cardinality as  $S'$ . [Given a set  $S$  whose cardinality is strictly greater than the cardinality of  $\mathbf{R}$ , I do not know whether it is always true that  $\text{card } S = \text{card } S'$ .] Added 1994: The grapevine communicates to me that according to Solovay, the answer is “no.”
14. Let  $A, B$  be non-empty sets. Prove that

$$\text{card}(A) \leq \text{card}(B) \quad \text{or} \quad \text{card}(B) \leq \text{card}(A).$$

[Hint: consider the family of pairs  $(C, f)$  where  $C$  is a subset of  $A$  and  $f: C \rightarrow B$  is an injective map. By Zorn's lemma there is a maximal element. Now finish the proof].

## Bibliography

- [Ad 62] F. ADAMS, Vector Fields on Spheres, *Ann. Math.* **75** (1962) pp. 603–632
- [Ara 31] H. ARAMATA, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **7** (1931) pp. 334–336
- [Ara 33] H. ARAMATA, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **9** (1933) pp. 31–34
- [Art 24] E. ARTIN, Kennzeichnung des Körpers der reellen algebraischen Zahlen, *Abh. Math. Sem. Hansischen Univ.* **3** (1924) pp. 319–323
- [Art 27] E. ARTIN, Über die Zerlegung definiter Funktionen in Quadrate, *Abh. Math. Sem. Hansischen Univ.* **5** (1927) pp. 100–115
- [Art 44] E. ARTIN, *Galois Theory*, University of Notre Dame, 1944
- [ArS 27] E. ARTIN and E. SCHREIER, Algebraische Konstruktion reeller Körper, *Abh. Math. Sem. Hansischen Univ.* **5** (1927) pp. 85–99
- [ArT 68] E. ARTIN and J. TATE, *Class Field Theory*, Benjamin-Addison Wesley, 1968 (reprinted by Addison-Wesley, 1991)
- [Art 68] M. ARTIN, On the solutions of analytic equations, *Invent. Math.* **5** (1968) pp. 277–291
- [ArM 65] M. ARTIN and B. MAZUR, On periodic points, *Ann. Math.* (2) **81** (1965) pp. 89–99
- [At 61] M. ATIYAH, Characters and cohomology of finite groups, *Pub. IHES* **9** (1961) pp. 5–26
- [At 67] M. ATIYAH, *K-Theory*, Addison-Wesley, (reprinted from the Benjamin Lecture Notes, 1967)
- [ABP 73] M. ATIYAH, R. BOTT, V. PATODI, On the heat equation and the index theorem, *Invent. Math.* **19** (1973) pp. 270–330
- [ABS 64] M. ATIYAH, R. BOTT, A. SHAPIRO, Clifford Modules, *Topology* **Vol. 3 Supp. 1** (1964) pp. 3–38
- [AtM 69] M. ATIYAH and I. McDONALD, *Introduction to commutative algebra*, Addison-Wesley, 1969
- [Ba 68] H. BASS, *Algebraic K-theory*, Benjamin, 1968
- [BaH 62] P. T. BATEMAN and R. HORN, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962) pp. 363–367
- [Be 80] G. BELYI, Galois extensions of the maximal cyclotomic field, *Izv. Akad. Nauk SSSR* **43** (1979) pp. 267–276 (= *Math. USSR Izv.* **14** (1980), pp. 247–256)
- [Be 83] G. BELYI, On extensions of the maximal cyclotomic field having a given classical Galois group, *J. reine angew. Math.* **341** (1983) pp. 147–156
- [BeY 91] C. BERENSTEIN and A. YGER, Effective Bezout identities in  $\mathbb{Q}[z_1, \dots, z_n]$ , *Acta Math.* **166** (1991) pp. 69–120
- [BGV 92] N. BERLINE, E. GETZLER, M. VERGNE, *Heat kernels and Dirac operators*, Springer-Verlag, 1992
- [BCHS 65] B. BIRCH, S. CHOWLA, M. HALL, and A. SCHINZEL, On the difference  $x^3 - y^2$ , *Norske Vid. Selsk. Forrh.* **38** (1965) pp. 65–69
- [Bott 69] R. BOTT, *Lectures on K(X)*, Benjamin 1969
- [Boun 1854] V. BOUNIAKOWSKY, Sur les diviseurs numériques invariables des fonctions

- rationnelles entières, *Mémoires sc. math. et phys.* **T. VI** (1854–1855) pp. 307–329
- [Bour 82] N. BOURBAKI, *Lie algebras and Lie groups*, Masson, 1982
- [Bra 47a] R. BRAUER, On the zeta functions of algebraic number fields, *Amer. J. Math.* **69** (1947) pp. 243–250
- [Bra 47b] R. BRAUER, On Artin's L-series with general group characters, *Ann. Math.* **48** (1947) pp. 502–514
- [BLSTW 83] J. BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, B. TUCKERMAN, and S. WAGSTAFF, Factorization of  $b^n \pm 1$ ,  $b = 2, 3, 5, 6, 7, 10, 11$  up to high powers, *Contemporary Mathematics* **Vol. 22**, AMS, Providence, RI, 1983
- [BtD 85] T. BRÖCKER and T. TOM DIECK, *Representations of Compact Lie Groups*, Springer-Verlag, 1985
- [Br 87] D. BROWNAWELL, Bounds for the degree in Nullstellensatz, *Ann. of Math.* **126** (1987) pp. 577–592
- [Br 88] D. BROWNAWELL, Local diophantine nullstellen inequalities, *J. Amer. Math. Soc.* **1** (1988) pp. 311–322
- [Br 89] D. BROWNAWELL, Applications of Cayley-Chow forms, *Springer Lecture Notes 1380: Number Theory, Ulm*, 1987, H. P. Schlickewei and E. Wirsing (eds.) pp. 1–18
- [BrCDT 01] C. BREUIL, B. CONRAD, F. DIAMOND, R. TAYLOR, On the modularity of elliptic curves over  $\mathbb{Q}$ : Wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001) pp. 843–939
- [CaE 57] E. CARTAN and S. EILENBERG, *Homological Algebra*, Princeton University Press, 1957
- [CCFT 91] P. CASSOU-NOGUES, T. CHINBURG, A. FROLICH, M. J. TAYLOR, L-functions and Galois modules, in *L-functions and Arithmetic*, J. Coates and M. J. Taylor (eds.), Proceedings of the Durham symposium July 1989, *London Math. Soc. Lecture Notes Series 153*, Cambridge University Press (1991) pp. 75–139
- [CuR 81] C. W. CURTIS and I. REINER, *Methods of Representation Theory*, John Wiley and Sons, 1981
- [Da 65] H. DAVENPORT, On  $f^3(t) - g^2(t)$ , *Norske Vid. Selsk. Forrh.* **38** (1965) pp. 86–87
- [De 68] P. DELIGNE, Formes modulaires et représentations  $l$ -adiques, *Séminaire Bourbaki* 1968–1969, pp. 55–105
- [De 73] P. DELIGNE, Formes modulaires et représentations de  $GL(2)$ , *Springer Lecture Notes 349* (1973) pp. 507–530
- [DeS 74] P. DELIGNE and J.-P. SERRE, Formes modulaires de poids 1, *Ann. Sci. ENS* **7** (1974) pp. 507–530
- [Dou 64] A. DOUADY, Determination d'un groupe de Galois, *C.R. Acad. Sci.* **258** (1964), pp. 5305–5308
- [ES 52] S. EILENBERG and N. STEENROD, *Foundations of Algebraic Topology*, Princeton University Press, 1952
- [Fa 91] G. FALTINGS, *Lectures on the arithmetic Riemann-Roch theorem*, *Ann. Math. Studies 127*, 1991
- [Fr 87] G. FREY, Links between stable elliptic curves and certain diophantine equations, *Number Theory, Lecture Notes 1380*, Springer-Verlag 1987 pp. 31–62

- [Fro 83] A. FRÖLICH, *Galois Module Structures of Algebraic Integers*, *Ergebnisse der Math. 3 Folge Vol. 1*, Springer-Verlag (1983)
- [FuL 85] W. FULTON and S. LANG, *Riemann-Roch Algebra*, Springer-Verlag, 1985
- [God 58] R. GODEMENT, *Théorie des faisceaux*, Hermann Paris, 1958
- [Gor 68] D. GORENSTEIN, *Finite groups*, Harper and Row, 1968
- [Gor 82] D. GORENSTEIN, *Finite simple groups*, Plenum Press, 1982
- [Gor 83] D. GORENSTEIN, The classification of finite simple groups, Plenum Press, 1983
- [Gor 86] D. GORENSTEIN, Classifying the finite simple groups, *Bull. AMS* **14** No. 1 (1986) pp. 1–98
- [GreH 81] M. GREENBERG and J. HARPER, *Algebraic Topology: A First Course*, Benjamin-Addison Wesley, 1981
- [GriH 78] P. GRIFFITHS and J. HARRIS, *Principles of Algebraic Geometry*, Wiley Interscience, New York, 1978
- [Gro 57] A. GROTHENDIECK, Sur quelques points d'algèbre homologique, *Tohoku Math. J.* **9** (1957) pp. 119–221
- [Gro 68] A. GROTHENDIECK, Classes de Chern et représentations linéaires des groupes discrets, *Dix exposés sur la cohomologie étale des schémas*, North-Holland, Amsterdam, 1968
- [Gu 90] R. GUNNING, *Introduction to Holomorphic Functions of Several Variables*, Vol. II: Local Theory; Vol. III, Wadsworth and Brooks/Cole, 1990
- [HalR 74] H. HALBERSTAM and H.-E. RICHERT, *Sieve methods*, Academic Press, 1974
- [Hal 71] M. HALL, The diophantine equation  $x^3 - y^2 = k$ , *Computers and Number Theory*, ed. by A. O. L. Atkin and B. Birch, Academic Press, London 1971 pp. 173–198
- [HardW 71] G. H. HARDY and E. M. WRIGHT, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, UK, 1938–01971 (several editions)
- [Hart 77] R. HARTSHORNE, *Algebraic Geometry*, Springer-Verlag, New York, 1977
- [Has 34] H. HASSE, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, *Abh. Math. Sem. Univ. Hamburg* **10** (1934) pp. 325–348
- [HilS 70] P. J. HILTON and U. STAMMBACH, *A course in homological algebra*, Graduate Texts in Mathematics, Springer-Verlag 1970
- [Hir 66] F. HIRZEBRUCH, *Topological methods in algebraic geometry*, Springer-Verlag, New York, 1966 (Translated and expanded from the original German, 1956)
- [Hu 75] D. HUSEMOLLER, *Fibre Bundles*, Springer-Verlag, second edition, 1975
- [Ih 66] Y. IHARA, On discrete subgroups of the two by two projective linear group over  $p$ -adic fields, *J. Math Soc. Japan* **18** (1966) pp. 219–235
- [Ik 77] M. IKEDA, Completeness of the absolute Galois group of the rational number field, *J. reine angew. Math.* **291** (1977) pp. 1–22
- [Iw 53] K. IWASAWA, On solvable extensions of algebraic number fields, *Ann. Math.* **548** (1953) pp. 548–572
- [Ja 79] N. JACOBSON, *Lie algebras*, Dover, 1979 (reprinted from Interscience, 1962)

- [Ja 85] N. JACOBSON, *Basic Algebra I and II*, second edition, Freeman, 1985
- [JoL 01] J. JORGENSEN and S. LANG, *Spherical Inversion on  $SL_n(\mathbb{R})$* , Springer Verlag 2001
- [Jou 80] J.-P. JOUANOLOU, Idéaux résultants, *Advances in Mathematics* **37** No. 3 (1980) pp. 212–238
- [Jou 90] J.-P. JOUANOLOU, Le formalisme du résultant, *Advances in Mathematics* **90** No. 2 (1991) pp. 117–263
- [Jou 91] J.-P. JOUANOLOU, *Aspects invariants de l'élimination*, Département de Mathématiques, Université Louis Pasteur, Strasbourg, France (1991)
- [Ko 88] J. KOLLAR, Sharp effective nullstellensatz, *J. Amer. Math. Soc.* **1** No. 4 (1988) pp. 963–975
- [Kr 32] W. KRULL, Allgemeine Bewertungstheorie, *J. reine angew. Math.* (1932) pp. 169–196
- [La 52] S. LANG, On quasi algebraic closure, *Ann. Math.* **55** (1952) pp. 373–390
- [La 53] S. LANG, The theory of real places, *Ann. Math.* **57** No. 2 (1953) pp. 378–391
- [La 58] S. LANG, *Introduction to Algebraic Geometry*, Interscience, 1958
- [La 70] S. LANG, *Algebraic Number Theory*, Addison-Wesley, 1970; reprinted by Springer-Verlag; second edition 1994
- [La 72] S. LANG, *Differential Manifolds*, Addison-Wesley, 1972; reprinted by Springer-Verlag, 1985; superceded by [La 99a]
- [La 73] S. LANG, *Elliptic Functions*, Springer-Verlag, 1973; second edition 1987
- [La 76] S. LANG, *Introduction to Modular Forms*, Springer-Verlag 1976
- [La 78] S. LANG, Elliptic Curves: Diophantine Analysis, Springer 1978
- [La 82] S. LANG, Units and class groups in number theory and algebraic geometry, *Bull. AMS* Vol. **6** No. 3 (1982) pp. 253–316
- [La 83] S. LANG, *Fundamentals of Diophantine Geometry*, Springer-Verlag 1983
- [La 85] S. LANG, *Real Analysis*, Second edition, Addison-Wesley, 1985; third edition *Real and Functional Analysis*, Springer-Verlag, 1993
- [La 90a] S. LANG, *Undergraduate Algebra*, second edition, Springer-Verlag, 1990
- [La 90b] S. LANG, *Cyclotomic fields, I and II*, Springer-Verlag, New York, 1990, combined edition of the original editions, 1978, 1980
- [La 90c] S. LANG, Old and new conjectured diophantine inequalities, *Bull. AMS* Vol. **23** No. 1 (1990) pp. 37–75
- [La 96] S. LANG, *Topics in Cohomology of Groups*, Springer Lecture Notes 1996, reproduced in Lang's *Collected Papers*, Vol. IV, Springer 2000
- [La 99a] S. LANG, *Fundamentals of Differential Geometry*, Springer Verlag, 1999
- [La 99b] S. LANG, *Math Talks for Undergraduates*, Springer Verlag, 1999
- [LaT 75] S. LANG and H. TROTTER, *Distribution of Frobenius Elements in  $GL_2$ -Extensions of the Rational Numbers*, Springer Lecture Notes **504**
- [Ma 16] F. MACAULAY, *The algebraic theory of modular systems*, Cambridge University Press, Cambridge UK, 1916
- [Mack 51] G. MACKEY, On induced representations of groups, *Amer. J. Math.* **73** (1951) pp. 576–592
- [Mack 53] G. MACKEY, Symmetric and anti-symmetric Kronecker squares of induced representations of finite groups, *Amer. J. Math.* **75** (1953) pp. 387–405

- [Man 69] J. MANIN, *Lectures on the K-functor in algebraic geometry*, Russian Math. Surveys 24(5) (1969) pp. 1–89
- [Man 71] A. MANNING, Axiom A diffeomorphisms have rational zeta functions, *Bull. Lond. Math. Soc.* **3** (1971) pp. 215–220
- [Mas 84a] R. C. MASON, Equations over function fields, Springer Lecture Notes **1068** (1984) pp. 149–157; in *Number Theory, Proceedings of the Noordwijkerhout, 1983*
- [Mas 84b] R. C. MASON, Diophantine equations over function fields, *London Math. Soc. Lecture Note Series* **96**, Cambridge University Press, 1984
- [Mas 84c] R. C. MASON, The hyperelliptic equation over function fields, *Math. Proc. Cambridge Philos. Soc.* **93** (1983) pp. 219–230
- [MaW 85] D. MASSER and G. WÜSTHOLZ, Zero estimates on group varieties II, *Invent. Math.* **80** (1985) pp. 233–267
- [Mat 80] H. MATSUMURA, *Commutative algebra*, second edition, Benjamin-Cummings, New York 1980
- [Mat 86] H. MATSUMURA, *Commutative rings*, Cambridge University Press, 1986
- [Matz 87] B. MATZAT, Konstruktive Galoistheorie, Springer Lecture Notes **1284**, 1987
- [Matz 88] B. MATZAT, Über das Umkehrproblem der Galoischen Theorie, *Jahrsbericht Deutsch. Mat.-Verein.* **90** (1988) pp. 155–183
- [Neu 69a] J. NEUKIRCH, Über eine algebraische Kennzeichnung der Henselkörper, *J. reine angew. Math.* **231** (1968) pp. 75–81
- [Neu 69b] J. NEUKIRCH, Kennzeichnung der  $p$ -adischen und endlichen algebraischen Zahlkörper, *Invent. Math.* **6** (1969) pp. 269–314
- [Neu 69c] J. NEUKIRCH, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, *J. für Math.* **238** (1969) pp. 135–147
- [No 76] D. NORTHCOTT, *Finite Free Resolutions*, Cambridge University Press, 1976
- [Ph 86] P. PHILIPPON, Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France* **114** (1986) pp. 355–383
- [Ph 91–95] P. PHILIPPON, Sur des hauteurs alternatives I, *Math. Ann.* **289** (1991) pp. 255–283; II *Ann. Inst. Fourier* **44** (1994) pp. 1043–1065; III *J. Math. Pures Appl.* **74** (1995) pp. 345–365
- [Pop 94] F. POP, On Grothendieck's conjecture of birational anabelian geometry, *Annals of Math.* (2) **139** (1994) pp. 145–182
- [Pop 95] F. POP, Etale Galois covers of affine smooth curves, *Invent. Math.* **120** (1995), pp. 555–578
- [Ri 90a] K. RIBET, On modular representations of  $\text{Gal}(\mathbb{Q}^\text{ab}/\mathbb{Q})$  arising from modular forms, *Invent. Math.* **100** (1990) pp. 431–476
- [Rib 90b] K. RIBET, From the Taniyama-Shimura conjecture to Fermat's last theorem, *Annales de la Fac. des Sci. Toulouse* (1990) pp. 116–170
- [Ric 60] C. RICKART, *Banach Algebras*, Van Nostrand (1960), Theorems 1.7.1 and 4.2.2
- [Ro 79] J. ROTMAN, *Introduction to Homological Algebra*, Academic Press, 1979
- [Ru 73] W. RUDIN, *Functional Analysis*, McGraw Hill (1973) Theorems 10.14, and 11.18
- [Schi 58] A. SCHINZEL and W. SIERPINSKI, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1948) pp. 185–208
- [Schulz 37] W. SCHULZ, Über die Galoissche Gruppe der Hermitschen Polynome, *J. reine angew. math.* **177** (1937) pp. 248–252

- [Schur 31] J. SCHUR, Affektlose Gleichungen in der Theorie der Laguereschen und Hermiteschen Polynome, *J. reine angew. math.* **165** (1931) pp. 52–58
- [Se 62] J.-P. SERRE, Endomorphismes complètement continus des espaces de Banach p-adiques, *Pub. Math. IHES* **12** (1962) pp. 69–85
- [Se 64] J.-P. SERRE, *Cohomologie Galoisiennne*, Springer Lecture Notes **5**, 1964
- [Se 65a] J.-P. SERRE, *Algèbre locale, multiplicités*, Springer Lecture Notes **11** (1965) Third Edition 1975
- [Se 65b] J.-P. SERRE, *Lie algebras and Lie groups*, Benjamin, 1965; reprinted *Springer Lecture Notes 1500*, Springer-Verlag 1992
- [Se 68a] J.-P. SERRE, *Abelian l-adic representations and Elliptic Curves*, Benjamin, 1968
- [Se 68b] J.-P. SERRE, Une interprétation des congruences relatives à la fonction de Ramanujan, *Séminaire Delange-Poitou-Pisot*, 1971–1972
- [Se 72a] J.-P. SERRE, Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) pp. 259–331
- [Se 72b] J.-P. SERRE, Congruences et formes modulaires (d'après Swinnerton-Dyer), *Séminaire Bourbaki*, 1971–1972
- [Se 73] J.-P. SERRE, *A Course in Arithmetic*, Springer-Verlag, New York, 1973
- [Se 80] J.-P. SERRE, *Trees*, Springer-Verlag, 1980
- [Se 87] J.-P. SERRE, Sur les représentations modulaires de degré 2 de  $\text{Gal}(\mathbb{Q}^*/\mathbb{Q})$ , *Duke Math. J.* **54** (1987), pp. 179–230
- [Se 88] J.-P. SERRE, Groupes de Galois sur  $\mathbb{Q}$ , *Séminaire Bourbaki*, 1987–1988, *Astérisque* **161–162**, pp. 73–85
- [Se 92] J.-P. SERRE, *Topics in Galois theory*, course at Harvard, 1989, Jones and Bartlett, Boston 1992
- [SGA 6] P. BERTHELOT, A. GROTHENDIECK, L. ILLUSIE et al., *Théorie des intersections et théorème de Riemann-Roch*, Springer Lecture Notes **146** (1967)
- [Shaf 54] I. SHAFAREVICH, Construction of fields of algebraic number with given solvable Galois group, *Izv. Akad. Nauk SSSR* **18** (1954) pp. 525–578 (*Amer. math. Soc. Transl.* **4** (1956)) pp. 185–237
- [Shat 72] S. SHATZ, *Profinite groups, arithmetic and geometry*, Ann. of Math. Studies, Princeton University Press 1972
- [Shih 74] R.-Y. SHIH, On the construction of Galois extensions of function fields and number fields, *Math. Ann.* **207** (1974), pp. 99–120
- [Shim 66] G. SHIMURA, A Reciprocity law in non-solvable extensions, *J. reine angew. Math.* **224** (1966) pp. 209–220
- [Shim 71] G. SHIMURA, *Introduction to the arithmetic theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971
- [Shu 87] M. SHUB, *Global Stability of Dynamical Systems*, Springer-Verlag, New York 1987
- [Sil 88] J. SILVERMAN, Wieferich's criterion and the abc conjecture, *J. Number Theory* **30** (1988) pp. 226–237
- [Sn 00] N. SNYDER, An alternate proof of Mason's theorem, *Elemente der Math.* **55** (2000) pp. 93–94
- [Sol 01] R. SOLOMON, A brief history of the classification of the finite simple groups, *Bull. AMS* Vol. **38** No. 3 (2001) pp. 315–322

- [Sou 90] C. SOULÉ, Géometrie d'Arakelov et théorie des nombres transcendants, Preprint, 1990
- [SteT 86] C.L. STEWART and R. Tijdeman, On the Oesterle–Masser Conjecture, *Mon. Math.* **102** (1986) pp. 251–257
- [Sto 81] W. STOTHERS, Polynomial identites and hauptmoduln, *Quart. J. Math. Oxford* (2) **32** (1981) pp. 349–370
- [Sw 69] R. SWAN, Invariant rational functions and a problem of Steenrod, *Invent. Math.* **7** (1969) pp. 148–158
- [Sw 83] R. SWAN, Noether's problem in Galois theory, *Emmy Noether in Bryn Mawr*, J. D. Sally and B. Srinivasan, eds., Springer-Verlag, 1983, p. 40
- [SwD 73] H. P. SWINNERTON-DYER, On  $l$ -adic representations and congruences for coefficients of modular forms, Antwerp conference, *Springer Lecture Notes* **350** (1973)
- [TaW 95] R. TAYLOR and A. WILES, Ring-theoretic properties of certain Hecke algebras, *Annals of Math.* **141** (1995) pp. 553–572
- [Uch 77] K. UCHIDA, Isomorphisms of Galois groups of algebraic function fields, *Ann. of Math.* **106** (1977) pp. 589–598
- [Uch 79] K. UCHIDA, Isomorphisms of Galois groups of solvable closed Galois extensions, *Tohoku Math. J.* **31** (1979) pp. 359–362
- [Uch 81] K. UCHIDA, Homomorphisms of Galois groups of solvably closed Galois extensions, *J. Math. Soc. Japan* **33** (1981) pp. 595–604
- [vdW 29] B. L. VAN DER WAERDEN, On Hilbert's function, series of composition of ideals and a generalization of the theorem of Bezout, *Proc. R. Soc. Amsterdam* **31** (1929) pp. 749–770
- [vdW 30] B. L. VAN DER WAERDEN, *Modern Algebra*, Springer-Verlag, 1930
- [Wil 95] A. WILES, Modular elliptic curves and Fermat's last theorem, *Annals of Math.* **141** (1995) pp. 443–551
- [Win 91] K. WINBERG, On Galois groups of  $p$ -closed algebraic number fields with restricted ramification, I, *J. reine angew. Math.* **400** (1989) pp. 185–202 and II, *ibid.* **416** (1991) pp. 187–194
- [Wit 35] E. WITT, Der Existenzsatz für abelsche Funktionenkörper, *J. reine angew. Math.* **173** (1936) pp. 43–51
- [Wit 36] E. WITT, Konstruktion von galoisschen Körpern der Charakteristik  $p$  mit vorgegebener Gruppe der Ordnung  $p^f$ , *J. reine angew. Math.* **174** (1936) pp. 237–245
- [Wit 37] E. WITT, Zyklische Körper und Algebren der Charakteristik  $p$  vom Grad  $p^n$ . Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik  $p$ , *J. reine angew. Math.* **176** (1937) pp. 126–140
- [Za 95] U. ZANNIER, On Davenport's bound for the degree of  $f^3 - g^2$  and Riemann's existence theorem, *Acta Arithm.* **LXXI.2** (1995) pp. 107–137

# INDEX

---

---

*abc* conjecture, 195  
abelian, 4  
    category, 133  
    extension, 266, 278  
    group, 4, 42, 79  
    Kummer theory, 293  
    tower, 18  
absolute value, 465  
absolutely semisimple, 659  
abstract nonsense, 759  
abut, 815  
action of a group, 25  
acyclic, 795  
Adams operations, 726, 782  
additive category, 133  
additive functor, 625, 790  
additive polynomial, 308  
adic  
    completion, 163, 206  
    expansion, 190  
    topology, 162, 206  
adjoint, 533, 581  
affine space, 383  
algebra, 121, 629, 749  
algebraic  
    closure, 178, 231, 272  
    element, 223  
    extension, 224  
    group, 549  
    integer, 371  
    set, 379  
    space, 383, 386  
algebraically  
    closed, 272  
    independent, 102, 308, 356  
almost all, 5  
alternating  
    algebra, 733  
    form, 511, 526, 530, 571, 598  
    group, 31, 32, 722  
    matrix, 530, 587  
    multilinear map, 511, 731  
    product, 733, 780

annihilator, 417  
anti-dual, 532  
anti-linear, 562  
anti-module, 532  
approximation theorem, 467  
Aramata's theorem, 701  
archimedean ordering, 450  
Artin  
    conjectures, 256, 301  
    theorems, 264, 283, 290, 429  
artinian, 439, 443, 661  
Artin-Rees theorem, 429  
Artin-Schreier theorem, 290  
associated  
    graded ring, 428, 430  
    group and field, 301  
    ideal of algebraic set, 381  
    linear map, 507  
    matrix of bilinear map, 528  
    object, 814  
    prime, 418  
associative, 3  
asymptotic Fermat, 196  
automorphism, 10, 54  
    inner, 26  
    of a form, 525, 533  
Banach space, 475  
balanced, 660  
base change, 625  
basis, 135, 140  
Bateman-Horn conjecture, 323  
belong  
    group and field, 263  
    ideal and algebraic set, 381  
    prime and primary ideal, 421  
Bernoulli  
    numbers, 218  
    polynomials, 219  
bifunctor, 806  
bijective, ix  
bilinear form, 146, 522

- bilinear map, 48, 121, 144
- binomial polynomial, 434
- Blichfeldt theorem, 702
- blocks, 555
- Borel subgroup, 537
- boundaries, 767
- bounded complex, 762
- Bourbaki theorems
  - on sets, 881
  - on traces and semisimplicity, 650
- bracket product, 121
- Brauer's theorems, 701, 709
- Bruhat decomposition, 539
- Burnside theorems
  - on simple modules, 648
  - on tensor representations, 726
- butterfly lemma, 20
  
- C**-dimension, 772
- cancellation law, 40
- canonical map, 14, 16
- cardinal number, 885
- Cartan subgroup, 712
- Casimir, 628, 639
- category, 53
- Cauchy
  - family, 52
  - sequence, 51, 162, 206, 469
- Cayley-Hamilton theorem, 561
- center
  - of a group, 26, 29
  - of a ring, 84
- central element, 714
- centralizer, 14
- chain condition, 407
- character, 282, 327, 667, 668
  - independence, 283, 676
- characteristic, 90
- characteristic polynomial, 256, 434, 561
  - of tensor product, 569
- Chevalley's theorem, 214
- Chinese remainder theorem, 94
- class formula, 29
- class function, 673
- class number, 674
- Clifford algebra, 749, 757
- closed
  - complex, 765
  - subgroup, 329
  - under law of composition, 6
- coboundary, 302
  
- cocycle
  - $GL_n$ , 549
  - Hilbert's theorem, 90, 288
  - Sah's theorem, 303
- coefficient function, 681
- coefficients
  - of linear combination, 129
  - of matrix, 503
  - of polynomial, 98, 101
- coerasable, 805
- cofinal, 52
- cohomology, 288, 302, 303, 549, 764
  - of groups, 826
- cokernel, 119, 133
- column
  - operation, 154
  - rank, 506
  - vector, 503
- commutative, 4
  - diagram, ix
  - group, 4
  - ring, 83, 84, 86
- commutator, 20, 69, 75
- commutator subgroup, 20, 75
  - of  $SL_n$ , 539, 541
- commute, 29
- compact
  - Krull topology, 329
  - spec of a ring, 411
- complete
  - family, 837
  - field, 469
  - ring and local ring, 206
- completely reducible, 554
- completion, 52, 469, 486
- complex, 445, 761, 765
- complex numbers, 272
- component, 503, 507
  - of a matrix, 503
- composition of mappings, 85
- compositum of fields, 226
- conjugacy class, 673
- conjugate elements
  - of a group, 26
  - of a field, 243
- conjugate
  - embeddings, 243, 476
  - fields, 243, 477
  - subgroups, 26, 28, 35
- conjugation, 26, 552, 570, 662
- connected, 411
- connected sum, 6
- connection, 755

- constant polynomial, 175
- constant term, 100
- content, 181
- contragredient, 665
- contravariant functor, 62
- convergence, 206
- convolution, 85, 116
- coordinates, 408
- coproduct, 59, 80
  - of commutative rings, 630
  - of groups, 70, 72
  - of modules, 128
- correspondence, 76
- coset, 12
  - representative, 12
- countable, 878
- covariant functor, 62
- Cramer's rule, 513
- cubic extension, 270
- cuspidal, 318
- cycle
  - in homology, 767
  - in permutations, 30
- cyclic
  - endomorphism, 96
  - extension, 266, 288
  - group, 8, 23, 96, 830
  - module, 147, 149
  - tower, 18
- cyclotomic
  - field, 277–282, 314, 323
  - polynomials, 279
- Davenport theorem, 195
- decomposable, 439
- decomposition
  - field, 341
  - group, 341
- Dedekind
  - determinant, 548
  - ring, 88, 116, 168, 353
- defined, 710, 769
- definite form, 593
- degree
  - of extension, 224
  - of morphism, 765
  - of polynomial, 100, 190
  - of variety, 438
  - Weierstrass, 208
- Deligne-Serre theorem, 319
- density theorem, 647
- denumerable set, 875
- dependent absolute values, 465
- de Rham complex, 748
- derivation, 214, 368, 746, 754
  - over a subfield, 369
  - universal, 746
- derivative, 178
- derived functor, 791
- descending chain condition, 408, 439, 443, 661
- determinant, 513
  - ideal, 738, 739
  - of cohomology, 738
  - of linear map, 513, 520
  - of module, 735
  - of Witt group, 595
- diagonal element, 504
- diagonalizable, 568
- diagonalized form, 576
- difference equations, 256
- differential, 747, 762, 814
- dihedral group, 78, 723
- dimension
  - of character, 670
  - of module, 146, 507
  - of transcendental extension, 355
  - of vector space, 141
- dimension in homology, 806, 811, 823
  - shifting, 805
- direct
  - limit, 160, 170, 639
  - product, 9, 127
  - sum, 36, 130, 165
- directed family, 51, 160
- discrete valuation ring, 487
- discriminant, 193, 204, 270, 325
- distinguished extensions
  - of fields, 227, 242
  - of rings, 335, 291
- distinguished polynomials, 209
- distributivity, 83
- divide, 111, 116
- divisible, 50
- division ring, 84, 642
- Dolbeault complex, 764
- dominate (polynomials), 870
- double coset, 75, 693
- doubly transitive, 80
- dual
  - basis, 142, 287
  - group, 46, 145
  - module, 142, 145, 523, 737
  - representation, 665

- effective character, 668, 685
- eigenvalue, 562
- eigenvector, 562, 582–585
- Eisenstein criterion, 183
- elementary
  - divisors, 153, 168, 521, 547
  - group, 705
  - matrix, 540
  - symmetric polynomials, 190, 217
- elimination, 391
  - ideal, 392
- embedding, 11, 120
  - of fields, 229
  - of rings, 91
- endomorphism, 10, 24, 54
  - of cyclic groups, 96
- enough
  - injectives, 787
  - T-exacts, 810
- entire, 91
  - functions, 87
- epimorphism, 120
- equivalent
  - norms, 470
  - places, 349
  - valuations, 480
- erasable, 800
- euclidean algorithm, 173, 207
- Euler characteristic, 769
- Euler-Grothendieck group, 771
- Euler phi function, 94
- Euler-Poincaré
  - characteristic, 769, 824
  - map, 156, 433, 435, 770
- evaluation, 98, 101
- even permutation, 31
- exact, 15, 120
  - for a functor, 619
  - sequence of complexes, 767
- expansion of determinant, 515
- exponent
  - of an element, 23, 149
  - of a field extension, 293
  - of a group, 23
  - of a module, 149
- exponential, 497
- Ext, 791, 808, 810, 831, 857
- extension
  - of base, 623
  - of derivations, 375
  - of fields, 223
  - of homomorphisms, 347, 378
  - of modules, 831
- exterior
  - algebra, 733
  - product, 733
- extreme point, 883
- factor
  - group, 14
  - module, 119, 141
  - ring, 89
- factorial, 111, 115, 175, 209
- faithful, 28, 334, 649, 664
- faithfully flat, 638
- Fermat theorem, 195, 319
- fiber product, 61, 81
- field, 93
  - of definition of a representation, 710
- filtered complex, 817
- filtration, 156, 172, 426, 814, 817
- finite
  - complex, 762
  - dimension, 141, 772, 823
  - extension, 223
  - field, 244
  - free resolution, 840
  - homological dimension, 772, 823
  - module, 129
  - resolution, 763
  - sequence, 877
  - set, 877
  - type, 129
  - under a place, 349
- finitely generated
  - algebra, 121
  - extension, 226
  - group, 66
  - module, 129
  - ring, 90
- finitely presented, 171
- Fitting ideal, 738–745
- Fitting lemma, 440
- five lemma, 169
- fixed
  - field, 261
  - point, 28, 34, 80
- flat, 612, 808
  - for a module, 616
- forgetful functor, 62
- form
  - multilinear, 450, 466
  - polynomial, 384
- formal power series, 205
- Fourier coefficients, 679

- fractional ideal, 88
- fractions, 107
- free
  - abelian group, 38, 39
  - extension, 362
  - generators, 137
  - group, 66, 82
  - module, 135
  - module generated by a set, 137
  - resolution, 763
- Frey polynomial, 198
- Frobenius
  - element, 180, 246, 316, 346
  - reciprocity, 686, 689
- functionals, 142
- functor, 62
- fundamental group, 63
  
- G* or  $(G, k)$ -module, 664, 779
- G*-homomorphism, 779
- G*-object, 55
- G*-regular, 829
- G*-set, 25, 27, 55
- Galois
  - cohomology, 288, 302
  - extension, 261
  - group, 252, 262, 269
  - theory, 262
- Gauss lemma, 181, 209, 495
- Gauss sum, 277
- g.c.d., 111
- Gelfand-Mazur theorem, 471
- Gelfand-Naimark theorem, 406
- Gelfond-Schneider, 868
- generate and generators
  - for a group, 9, 23, 68
  - for an ideal, 87
  - for a module, 660
  - for a ring, 90
- generating function or power series, 211
- generators and relations, 68
- generic
  - forms, 390, 392
  - hyperplane, 374
  - pfaffian, 589
  - point, 383, 408
  - polynomial, 272, 345
- ghost components, 330
- $GL_2$ , 300, 317, 537, 715
- $GL_n$ , 19, 521, 543, 546, 547
- global sections, 792
- Goursat's lemma, 75
  
- graded
  - algebra, 172, 631
  - module, 427, 751, 765
  - morphism, 765, 766
  - object, 814
  - ring, 631
- Gram-Schmidt orthogonalization, 579, 599
- Grassman algebra, 733
- greatest common divisor, 111
- Grothendieck
  - algebra and ring, 778–782
  - group, 40, 139
  - power series, 218
  - spectral sequence, 819
- group, 7
  - algebra, 104, 121
  - automorphism, 10
  - extensions, 827
  - homomorphism, 10
  - object, 65
  - ring, 85, 104, 126
  
- Hall conjecture, 197
- harmonic polynomials, 354, 550
- Hasse zeta function, 255
- height, 167
- Herbrand quotient, 79
- Hermite-Lindemann, 867
- hermitian
  - form, 533, 571, 579
  - linear map, 534
  - matrix, 535
- Hilbert
  - Nullstellensatz, 380, 551
  - polynomial, 433
  - Serre theorem, 431
  - syzygy theorem, 862
  - theorem on polynomial rings, 185
  - theorem 90, 288
  - Zariski theorem, 409
- homogeneous, 410, 427, 631
  - algebraic space, 385
  - ideal, 385, 436, 733
  - integral closure, 409
  - point, 385
  - polynomial, 103, 107, 190, 384, 436
  - quadratic map, 575
- homology, 445, 767
  - isomorphism, 767, 836
- homomorphisms in categories, 765
- homomorphism
  - of complex, 445, 765

- homomorphism (*continued*)
  - of groups, 10
  - of inverse systems, 163
  - of modules, 119, 122
  - of monoid, 10
  - of representations, 125
  - of rings, 88
- homotopies of complexes, 787
- Horrock's theorem, 847
- Howe's proof, 258
- hyperbolic
  - enlargement, 593
  - pair, 586, 590
  - plane, 586, 590
  - space, 590
- hyperplane, 542
  - section, 374, 410
- Ideal, 86
  - class group, 88, 126
- idempotent, 443
- image, 11
- indecomposable, 440
- independent
  - absolute values, 465
  - characters, 283, 676
  - elements of module, 151
  - extensions, 362
  - variables, 102, 103
- index, 12
- induced
  - character, 686
  - homomorphism, 16
  - module, 688
  - ordering, 879
  - representation, 688
- inductively ordered, 880
- inertia
  - form, 393
  - group, 344
- infinite
  - cyclic group, 8, 23
  - cyclic module, 147
  - extension, 223, 235
  - Galois extensions, 313
  - period, 8, 23
  - set, 876
    - under a place, 349
- infinitely
  - large, 450
  - small, 450
- injective
- map, ix
- module, 782, 830
- resolution, 788, 801, 819
- inner automorphism, 26
- inseparable
  - degree, 249
  - extension, 247
- integers mod  $n$ , 94
- integral, 334, 351, 352, 409
  - closure, 336, 409
  - domain, 91
  - equation, 334
  - extension, 340
  - homomorphism, 337
  - map, 357
  - root test, 185
  - valued polynomials, 216, 435
- integrally closed, 337
- integrality criterion, 352, 409
- invariant
  - bases, 550
  - submodule, 665
- invariant
  - of linear map, 557, 560
  - of matrix, 557
  - of module, 153, 557, 563
  - of submodule, 153, 154
- inverse, ix, 7
- inverse limit, 50, 51, 161, 163, 169
  - of Galois groups, 313, 328
- inverse matrix, 518
- invertible, 84
- $\text{Irr}(z, k, X)$ , 224
- irreducible
  - algebraic set, 382, 408
  - character, 669, 696
  - element, 111
  - module, 554
  - polynomial, 175, 183
  - polynomial of a field element, 224
- irrelevant prime, 436
- isolated prime, 422
- isometry, 572
- isomorphism, 10, 54
  - of representations, 56, 667
- isotropy group, 27
- Iss'sa-Hironaka theorem, 498
- Jacobson
  - density, 647
  - radical, 658
- Jordan-Hölder, 22, 156
- Jordan canonical form, 559

- K*-family, 771
- K*-theory, 139, 771–782
- kernel
  - of bilinear map, 48, 144, 522, 572
  - of homomorphism, 11, 133
- Kolchin's theorem, 661
- Koszul complex, 853
- Krull
  - theorem, 429
  - topology, 329
- Krull-Remak-Schmidt, 441
- Kummer extensions
  - abelian, 294–296, 332
  - non-abelian, 297, 304, 326
- L*-functions, 727
- lambda operation, 217
- lambda-ring, 218, 780
- Langlands conjectures, 316, 319
- lattice, 662
- law of composition, 3
- Lazard's theorem, 639
- leading coefficient, 100
- least
  - common multiple, 113
  - element, 879
  - upper bound, 879
- left
  - coset, 12
  - derived functor, 791
  - exact, 790
  - ideal, 86
  - module, 117
- length
  - of complex, 765
  - of filtration, 433
  - of module, 433, 644
- Lie algebra, 548
- lie above
  - prime, 338
  - valuation ring, 350
- lifting, 227
- linear
  - combination, 129
  - dependence, 130
  - independence, 129, 150, 283
  - map, 119
  - polynomial, 100
- linearly disjoint, 360
- local
  - degree, 477
  - homomorphism, 444
- norm, 478
- parameter, 487
- ring, 110, 425, 441
- uniformization, 498
- localization, 110
- locally nilpotent, 418
- logarithm, 497, 597
- logarithmic derivative, 214, 375
- Mackey's theorems, 694
- MacLane's criterion, 364
- mapping cylinder, 838
- Maschke's theorem, 666
- Mason-Stothers theorem, 194, 220
- matrix, 503
  - of bilinear map, 528
  - over non-commutative ring, 641
- maximal
  - abelian extension, 269
  - archimedean, 450
  - element, 879
  - ideal, 92
- metric linear map, 573
- minimal polynomial, 556, 572
- Mittag-Leffler condition, 164
- modular forms, 318, 319
- module, 117
  - over principal ring, 146, 521
  - modulo an ideal, 90
- Moebius inversion, 116, 254
- monic, 175
- monoid, 3
  - algebra, 106, 126
  - homomorphism, 10
- monomial, 101
- monomorphism, 120
- Morita's theorem, 660
- morphism, 53
  - of complex, 765
  - of functor, 65, 625, 800
  - or representation, 125
- multilinear map, 511, 521, 602
- multiple root, 178, 247
- multiplicative
  - function, 116
  - subgroup of a field, 177
  - subset, 107
- multiplicity
  - of character, 670
  - of root, 178
  - of simple module, 644
- Nakayama's lemma, 424, 661
- natural transformation, 65

- negative, 449
- definite, 578
- Newton approximation, 493
- nilpotent, 416, 559, 569
- Noether normalization, 357
- Noetherian, 186, 210, 408–409, 415, 427
  - graded ring, 427
  - module, 413
- non-commutative variables, 633
- non-degenerate, 522, 572
- non-singular, 523, 529
- norm, 284, 578, 637
  - on a vector space, 469
  - on a finitely generated abelian group, 166
- normal
  - basis theorem, 312
  - endomorphism, 597
  - extension, 238
  - subgroup, 14
  - tower, 18
- normalizer, 14
- Northcott theorems, 864
- null
  - sequence, 52
  - space, 586
- nullstellensatz, 380, 383
- occur, 102, 176
- odd permutation, 31
- one-dimensional
  - character, 671
  - representation, 671
- open complex, 761
- open set, 406
- operate
  - on a module, 664
  - on an object, 55
  - on a set, 25, 76
- orbit, 28
  - decomposition formula, 29
- order
  - of a group, 12
  - at  $p$ , 113, 488
  - at a valuation, 488
  - of a zero, 488
- ordering, 449, 480, 878
- ordinary tensor product, 630
- orthogonal
  - basis, 572–585
  - element, 48, 144, 572
  - group, 535
  - map, 535
  - sum, 572
- orthogonality relations, 677
- orthogonalization, 579
- orthonormal, 577
- over a map, 229
- $p$ -adic
  - integers, 51, 162, 169, 488
  - numbers, 488
- $p$ -class, 706
- $p$ -conjugate, 706
- $p$ -divisible, 50
- $p$ -elementary, 705
- $p$ -group, 33
- $p$ -regular, 705
- $p$ -singular, 705
- $p$ -subgroup, 33
- pairing, 48
- parallelogram law, 598
- partial fractions, 187
- partition, 79
  - function, 211
- perfect, 252
- period, 23, 148
- periodicity of Clifford algebra, 758
- permutation, 8, 30
- perpendicular, 48, 144, 522
- Pfaffian, 589
- Pic or Picard group, 88, 126
- place, 349, 482
- Poincaré series, 211, 431
- point
  - of algebraic set, 383
  - in a field, 408
- polar decomposition, 584
- polarization identity, 580
- pole, 488
- polynomial, 97
  - algebra, 97, 633
  - function, 98
  - invariants, 557
  - irreducible, 175, 183
  - Noetherian, 185
- Pontrjagin dual, 145
- positive, 449
  - definite, 578, 583
- power map, 10
- power series, 205
  - factorial, 209
  - Noetherian, 210
- primary
  - decomposition, 422
  - ideal, 421
  - module, 421

- prime
  - element, 113
  - field, 90
  - ideal, 92
  - ring, 90
- primitive
  - element, 243, 244
  - group, 80
  - operation, 79
  - polynomials, 181, 182
  - power series, 209
  - root, 301
  - root of unity, 277, 278
- principal
  - homomorphism, 418
  - ideal, 86, 88
  - module, 554, 556
  - representation, 554
  - ring, 86, 146, 521
- product
  - in category, 58
  - of groups, 9
  - of modules, 127
  - of rings, 91
- profinite, 51
- projection, 388
- projective
  - module, 137, 168, 848, 850
  - resolution, 763
  - space, 386
- proper, ix
  - congruence, 492
- pull-back, 61
- purely inseparable
  - element, 249
  - extension, 250
- push-out, 62, 81
- quadratic
  - extension, 269
  - form, 575
  - map, 574
  - symbol, 281
- quadratically closed, 462
- quaternions, 9, 545, 723, 758
- Quillen-Suslin theorem, 848
- quotient
  - field, 110
  - ring, 107
- radical
  - of an ideal, 388, 417
- of a ring, 661
- of an integer, 195
- Ramanujan power series, 212
- ramification index, 483
- rank, 42, 46
  - of a matrix, 506
- rational
  - conjugacy class, 276, 326, 725
  - element, 714
  - function, 110
- real, 451
  - closed, 451
  - closure, 452
  - place, 462
  - zero, 457
- reduced
  - decomposition, 422, 443
  - polynomial, 177
- reduction
  - criterion, 185
  - map, 99, 102
  - modulo an ideal, 446, 623
  - mod  $p$ , 623
- refinement of a tower, 18
- regular
  - character, 675, 699
  - extension, 366
  - module, 699, 829
  - representation, 675, 829
  - sequence, 850
- relations, 68
- relative invariant, 171, 327
- relatively prime, 113
- representation, 55, 124, 126
  - functor, 64
  - of a group, 55, 317, 664
  - of a ring, 553
  - space, 667
- residue class, 91
  - degree, 422, 483
  - ring, 91
- resolution, 763, 798
- resultant, 200, 398, 410
  - system, 403
  - variety, 393
- Ribet, 319
- Rieffel's theorem, 655
- Riemann surface, 275
- Riemann-Roch, 212, 218, 220, 258
- right
  - coset, 12, 75
  - derived functor, 791
  - exact functor, 791, 798

- right (*continued*)
  - ideal, 66
  - module, 117
- rigid, 275
- rigidity theorem, 276
- ring, 83
  - homomorphism, 88
  - of fractions, 107
- root, 175
  - of unity, 177, 276
- row
  - operation, 154
  - rank, 506
  - vector, 503
- $S_3$  and  $S_4$ , 722
- scalar product, 571
- Schanuel
  - conjecture, 873
  - lemma, 841
- Schreier's theorem, 22
- Schroeder-Bernstein theorem, 885
- Schur
  - Galois groups, 274
  - lemma, 643
- Schwarz inequality, 578, 580
- section, 64, 792
- self-adjoint, 581
- semidirect product, 15, 76
- semilinear, 532
- seminorm, 166, 475
- semipositive, 583, 597
- semisimple
  - endomorphism, 569, 661
  - module, 554, 647, 659
  - representation, 554, 712
  - ring, 651
- separable
  - closure, 243
  - degree, 239
  - element, 240
  - extension, 241, 658
  - polynomial, 241
- separably generated, 363
- separating transcendence basis, 363
- sequence, 875
- Serre's conjecture, 848
  - theorem, 844
- sesquilinear form, 532
- Shafarevich conjecture, 314
- sheaf, 792
- sign of a permutation, 31, 77
- simple
  - character, 669
  - group, 20
  - module, 156, 554, 643
  - ring, 653, 655
  - root, 247
- simplicity of  $SL_n$ , 539, 542
- size of a matrix, 503
- skew symmetric, 526
- $SL_2$ , 69, 537, 539, 546
  - generators and relations, 69, 70, 537
- $SL_n$ , 521, 539, 541, 547
- snake lemma, 158, 169, 614–621
- Snyder's proof, 220
- solvable
  - extension, 291, 314
  - group, 18, 293, 314
  - by radicals, 292
- spec of a ring, 405, 410
- special linear group, 14, 52, 59, 69, 541, 546, 547
- specializing, 101
- specialization, 384
- spectral
  - sequence, 815–825
  - theorem, 581, 583, 585
- split exact sequence, 132
- splitting field, 235
- square
  - matrix, 504
  - group, 9, 77, 270
  - root of operator, 584
- stably free, 840
  - dimension, 840
- stably isomorphic, 841
- stalk, 161
- standard
  - complex, 764
  - alternating matrix, 587
- Steinberg theorem, 726
- Stewart-Tijdeman, 196
- strictly inductively ordered, 881
- stripping functor, 62
- Sturm's theorem, 454
- subgroup, 9
- submodule, 118
- submonoid, 6
- subobject, 134
- subring, 84
- subsequence, 876
- subspace, 141
- substituting, 98, 101

- super
  - algebra, 632
  - commutator, 757
  - product, 631, 751
  - tensor product, 632, 751
- supersolvable, 702
- support, 419
- surjective, ix
- Sylow group, 33
- Sylvester's theorem, 577
- symmetric
  - algebra, 635
  - endomorphism, 525, 585, 597
  - form, 525, 571
  - group, 28, 30, 269, 272–274
  - matrix, 530
  - multilinear map, 635
  - polynomial, 190, 217
  - product, 635, 781, 861
- symplectic, 535
  - basis, 599
- syzygy theorem, 862
- Szpiro conjecture, 198
- Taniyama-Shimura conjecture, 316, 319
- Tate group, 50, 163, 169
  - limit, 598
- Taylor series, 213
- tensor, 581, 628
  - algebra, 633
  - exact, 612
  - product, 602, 725
  - product of complexes, 832, 851
  - product representation, 725, 799
- Tits construction of free group, 81
- tor (for torsion), 42, 47, 149
- Tor, 622, 791
  - dimension, 622
- Tornheim proof, 471
- torsion
  - free, 45, 147
  - module, 147, 149
- total
  - complex, 815
  - degree, 103
- totally ordered, 879
- tower
  - of fields, 225
  - of groups, 18
- trace
  - of element, 284, 666
  - of linear map, 511, 570
  - of matrix, 505, 511
- transcendence
  - basis, 356
  - degree, 355
  - of  $e$ , 867
- transcendental, 99
- transitive, 28, 79
- translation, 26, 227
- transpose
  - of bifunctor, 808
  - of linear map, 524
  - of matrix, 505
- transposition, 13
- transvection, 542
- trigonometric degree, 115
  - polynomial, 114, 115
- trivial
  - character, 282
  - operation, 664
  - representation, 664
  - subgroup, 9
  - valuation, 465
- two-sided ideal, 86, 655
- type
  - of abelian group, 43
  - of module, 149
- unimodular, 846
  - extension property, 849
- unipotent, 714
- unique factorization, 111, 116
- uniquely divisible, 575
- unit, 84
  - element, 3, 83
  - ideal, 87
- unitary, 535, 583
- universal, 37
  - delta-functor, 800
  - derivation, 746
- universally
  - attracting, 57
  - repelling, 57
- upper bound, 879
- upper diagonal group, 19
- valuation, 465
- valuation ring, 348, 481
  - determined by ordering, 450, 452
- value group, 480
- Vandermonde determinant, 257–259, 516
- vanishing ideal, 38
- variable, 99, 104
- variation of signs, 454

- variety, 382
- vector space, 118, 139
- volume, 735
- Warning's theorem, 214
- Wedderburn's theorem, 649
- Weierstrass
  - degree, 208
  - polynomial, 208
  - preparation theorem, 208
- weight, 191
- well-behaved, 410, 478
- well-defined, x
- well-ordering, 891
- Weyl group, 570
- Witt group, 594, 599
  - theorem, 591
  - vector, 330, 492
- Witt-Grothendieck group, 595
- Zariski-Matsusaka theorem, 372
- Zariski topology, 407
- Zassenhaus lemma, 20
- zero
  - divisor, 91
  - element, 3
  - of ideal, 390, 405
  - of polynomial, 102, 175, 379, 390
- zeta function, 211, 212, 255
- Zorn's lemma, 880, 884

# Graduate Texts in Mathematics

- 1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
- 2 OXTBOY. Measure and Category. 2nd ed.
- 3 SCHAEFER. Topological Vector Spaces. 2nd ed.
- 4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
- 5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
- 6 HUGHES/PIPER. Projective Planes.
- 7 J.-P. SERRE. A Course in Arithmetic.
- 8 TAKEUTI/ZARING. Axiomatic Set Theory.
- 9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
- 10 COHEN. A Course in Simple Homotopy Theory.
- 11 CONWAY. Functions of One Complex Variable I. 2nd ed.
- 12 BEALS. Advanced Mathematical Analysis.
- 13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
- 14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
- 15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
- 16 WINTER. The Structure of Fields.
- 17 ROSENBLATT. Random Processes. 2nd ed.
- 18 HALMOS. Measure Theory.
- 19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
- 20 HUSEMOLLER. Fibre Bundles. 3rd ed.
- 21 HUMPHREYS. Linear Algebraic Groups.
- 22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
- 23 GREUB. Linear Algebra. 4th ed.
- 24 HOLMES. Geometric Functional Analysis and Its Applications.
- 25 HEWITT/STROMBERG. Real and Abstract Analysis.
- 26 MANES. Algebraic Theories.
- 27 KELLEY. General Topology.
- 28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
- 29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
- 30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
- 31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
- 32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
- 33 HIRSCH. Differential Topology.
- 34 SPITZER. Principles of Random Walk. 2nd ed.
- 35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
- 36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
- 37 MONK. Mathematical Logic.
- 38 GRAUERT/FRITZSCHE. Several Complex Variables.
- 39 ARVESON. An Invitation to  $C^*$ -Algebras.
- 40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
- 41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
- 42 J.-P. SERRE. Linear Representations of Finite Groups.
- 43 GILLMAN/JERISON. Rings of Continuous Functions.
- 44 KENDIG. Elementary Algebraic Geometry.
- 45 LOÈVE. Probability Theory I. 4th ed.
- 46 LOÈVE. Probability Theory II. 4th ed.
- 47 MOISE. Geometric Topology in Dimensions 2 and 3.
- 48 SACHS/WU. General Relativity for Mathematicians.
- 49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
- 50 EDWARDS. Fermat's Last Theorem.
- 51 KLINGENBERG. A Course in Differential Geometry.
- 52 HARTSHORNE. Algebraic Geometry.
- 53 MANIN. A Course in Mathematical Logic.
- 54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
- 55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
- 56 MASSEY. Algebraic Topology: An Introduction.
- 57 CROWELL/FOX. Introduction to Knot Theory.
- 58 KOBLITZ.  $p$ -adic Numbers,  $p$ -adic Analysis, and Zeta-Functions. 2nd ed.
- 59 LANG. Cyclotomic Fields.
- 60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
- 61 WHITEHEAD. Elements of Homotopy Theory.
- 62 KARGAPOLOV/MERLJAKOV. Fundamentals of the Theory of Groups.
- 63 BOLLOBAS. Graph Theory.

# Graduate Texts in Mathematics

- 64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
- 65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
- 66 WATERHOUSE. Introduction to Affine Group Schemes.
- 67 SERRE. Local Fields.
- 68 WEIDMANN. Linear Operators in Hilbert Spaces.
- 69 LANG. Cyclotomic Fields II.
- 70 MASSEY. Singular Homology Theory.
- 71 FARKAS/KRA. Riemann Surfaces. 2nd ed.
- 72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
- 73 HUNGERFORD. Algebra.
- 74 DAVENPORT. Multiplicative Number Theory. 3rd ed.
- 75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
- 76 ITAKA. Algebraic Geometry.
- 77 HECKE. Lectures on the Theory of Algebraic Numbers.
- 78 BURRIS/SANKAPPANAVAR. A Course in Universal Algebra.
- 79 WALTERS. An Introduction to Ergodic Theory.
- 80 ROBINSON. A Course in the Theory of Groups. 2nd ed.
- 81 FORSTER. Lectures on Riemann Surfaces.
- 82 BOTT/TU. Differential Forms in Algebraic Topology.
- 83 WASHINGTON. Introduction to Cyclotomic Fields. 2nd ed.
- 84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
- 85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
- 86 VAN LINT. Introduction to Coding Theory. 2nd ed.
- 87 BROWN. Cohomology of Groups.
- 88 PIERCE. Associative Algebras.
- 89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
- 90 BRØNSTED. An Introduction to Convex Polytopes.
- 91 BEARDON. On the Geometry of Discrete Groups.
- 92 DIESTEL. Sequences and Series in Banach Spaces.
- 93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part I. 2nd ed.
- 94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
- 95 SHIRYAEV. Probability. 2nd ed.
- 96 CONWAY. A Course in Functional Analysis. 2nd ed.
- 97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
- 98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
- 99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
- 100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
- 101 EDWARDS. Galois Theory.
- 102 VARADARAJAN. Lie Groups, Lie Algebras and Their Representations.
- 103 LANG. Complex Analysis. 3rd ed.
- 104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part II.
- 105 LANG.  $SL_2(\mathbb{R})$ .
- 106 SILVERMAN. The Arithmetic of Elliptic Curves.
- 107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
- 108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
- 109 LEHTO. Univalent Functions and Teichmüller Spaces.
- 110 LANG. Algebraic Number Theory.
- 111 HUSEMÖLLER. Elliptic Curves. 2nd ed.
- 112 LANG. Elliptic Functions.
- 113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
- 114 KOBLITZ. A Course in Number Theory and Cryptography. 2nd ed.
- 115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
- 116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
- 117 J.-P. SERRE. Algebraic Groups and Class Fields.
- 118 PEDERSEN. Analysis Now.
- 119 ROTMAN. An Introduction to Algebraic Topology.
- 120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.
- 121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
- 122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
- 123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*

- 124 DUBROVIN/FOMENKO/NOVIKOV. *Modern Geometry—Methods and Applications. Part III*
- 125 BERENSTEIN/GAY. *Complex Variables: An Introduction*.
- 126 BOREL. *Linear Algebraic Groups*. 2nd ed.
- 127 MASSEY. *A Basic Course in Algebraic Topology*.
- 128 RAUCH. *Partial Differential Equations*.
- 129 FULTON/HARRIS. *Representation Theory: A First Course. Readings in Mathematics*
- 130 DODSON/POSTON. *Tensor Geometry*.
- 131 LAM. *A First Course in Noncommutative Rings*. 2nd ed.
- 132 BEARDON. *Iteration of Rational Functions*.
- 133 HARRIS. *Algebraic Geometry: A First Course*.
- 134 ROMAN. *Coding and Information Theory*.
- 135 ROMAN. *Advanced Linear Algebra*.
- 136 ADKINS/WEINTRAUB. *Algebra: An Approach via Module Theory*.
- 137 AXLER/BOURDON/RAMEY. *Harmonic Function Theory*. 2nd ed.
- 138 COHEN. *A Course in Computational Algebraic Number Theory*.
- 139 BREDON. *Topology and Geometry*.
- 140 AUBIN. *Optima and Equilibria. An Introduction to Nonlinear Analysis*.
- 141 BECKER/WEISPENNING/KREDEL. *Gröbner Bases. A Computational Approach to Commutative Algebra*.
- 142 LANG. *Real and Functional Analysis*. 3rd ed.
- 143 DOOB. *Measure Theory*.
- 144 DENNIS/FARB. *Noncommutative Algebra*.
- 145 VICK. *Homology Theory. An Introduction to Algebraic Topology*. 2nd ed.
- 146 BRIDGES. *Computability: A Mathematical Sketchbook*.
- 147 ROSENBERG. *Algebraic K-Theory and Its Applications*.
- 148 ROTMAN. *An Introduction to the Theory of Groups*. 4th ed.
- 149 RATCLIFFE. *Foundations of Hyperbolic Manifolds*.
- 150 EISENBUD. *Commutative Algebra with a View Toward Algebraic Geometry*.
- 151 SILVERMAN. *Advanced Topics in the Arithmetic of Elliptic Curves*.
- 152 ZIEGLER. *Lectures on Polytopes*.
- 153 FULTON. *Algebraic Topology: A First Course*.
- 154 BROWN/PEARCY. *An Introduction to Analysis*.
- 155 KASSEL. *Quantum Groups*.
- 156 KECHRIS. *Classical Descriptive Set Theory*.
- 157 MALLIAVIN. *Integration and Probability*.
- 158 ROMAN. *Field Theory*.
- 159 CONWAY. *Functions of One Complex Variable II*.
- 160 LANG. *Differential and Riemannian Manifolds*.
- 161 BORWEIN/ERDÉLYI. *Polynomials and Polynomial Inequalities*.
- 162 ALPERIN/BELL. *Groups and Representations*.
- 163 DIXON/MORTIMER. *Permutation Groups*.
- 164 NATHANSON. *Additive Number Theory: The Classical Bases*.
- 165 NATHANSON. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*.
- 166 SHARPE. *Differential Geometry: Cartan's Generalization of Klein's Erlangen Program*.
- 167 MORANDI. *Field and Galois Theory*.
- 168 EWALD. *Combinatorial Convexity and Algebraic Geometry*.
- 169 BHATIA. *Matrix Analysis*.
- 170 BREDON. *Sheaf Theory*. 2nd ed.
- 171 PETERSEN. *Riemannian Geometry*.
- 172 REMMERT. *Classical Topics in Complex Function Theory*.
- 173 DIESTEL. *Graph Theory*. 2nd ed.
- 174 BRIDGES. *Foundations of Real and Abstract Analysis*.
- 175 LICKORISH. *An Introduction to Knot Theory*.
- 176 LEE. *Riemannian Manifolds*.
- 177 NEWMAN. *Analytic Number Theory*.
- 178 CLARKE/LEDYAEV/STERN/WOLENSKI. *Nonsmooth Analysis and Control Theory*.
- 179 DOUGLAS. *Banach Algebra Techniques in Operator Theory*. 2nd ed.
- 180 SRIVASTAVA. *A Course on Borel Sets*.
- 181 KRESS. *Numerical Analysis*.
- 182 WALTER. *Ordinary Differential Equations*.

- 183 MEGGINSON. An Introduction to Banach Space Theory.
- 184 BOLLOBAS. Modern Graph Theory.
- 185 COX/LITTLE/O'SHEA. Using Algebraic Geometry.
- 186 RAMAKRISHNAN/VALENZA. Fourier Analysis on Number Fields.
- 187 HARRIS/MORRISON. Moduli of Curves.
- 188 GOLDBLATT. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.
- 189 LAM. Lectures on Modules and Rings.
- 190 ESMONDE/MURTY. Problems in Algebraic Number Theory.
- 191 LANG. Fundamentals of Differential Geometry.
- 192 HIRSCH/LACOMBE. Elements of Functional Analysis.
- 193 COHEN. Advanced Topics in Computational Number Theory.
- 194 ENGEL/NAGEL. One-Parameter Semigroups for Linear Evolution Equations.
- 195 NATHANSON. Elementary Methods in Number Theory.
- 196 OSBORNE. Basic Homological Algebra.
- 197 EISENBUD/HARRIS. The Geometry of Schemes.
- 198 ROBERT. A Course in  $p$ -adic Analysis.
- 199 HEDENMALM/KORENBLUM/ZHU. Theory of Bergman Spaces.
- 200 BAO/CHERN/SHEN. An Introduction to Riemann–Finsler Geometry.
- 201 HINDRY/SILVERMAN. Diophantine Geometry: An Introduction.
- 202 LEE. Introduction to Topological Manifolds.
- 203 SAGAN. The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions.
- 204 ESCOFIER. Galois Theory.
- 205 FÉLIX/HALPERIN/THOMAS. Rational Homotopy Theory. 2nd ed.
- 206 MURTY. Problems in Analytic Number Theory.  
*Readings in Mathematics*
- 207 GODSIL/ROYLE. Algebraic Graph Theory.
- 208 CHENEY. Analysis for Applied Mathematics.
- 209 ARVESON. A Short Course on Spectral Theory.
- 210 ROSEN. Number Theory in Function Fields.
- 211 LANG. Algebra. Revised 3rd ed.
- 212 MATOUŠEK. Lectures on Discrete Geometry.
- 213 FRITZSCHE/GRAUERT. From Holomorphic Functions to Complex Manifolds.
- 214 JOST. Partial Differential Equations.
- 215 GOLDSCHMIDT. Algebraic Functions and Projective Curves.
- 216 D. SERRE. Matrices: Theory and Applications.
- 217 MARKER. Model Theory: An Introduction.
- 218 LEE. Introduction to Smooth Manifolds.
- 219 MACLACHLAN/REID. The Arithmetic of Hyperbolic 3-Manifolds.
- 220 NESTREUW. Smooth Manifolds and Observables.
- 221 GRÜNBAUM. Convex Polytopes. 2nd ed.
- 222 HALL. Lie Groups, Lie Algebras, and Representations: An Elementary Introduction.
- 223 VRETBLAD. Fourier Analysis and Its Applications.
- 224 WALSCHAP. Metric Structures in Differential Geometry.