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

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

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 $\dim F_2 \geqq 1$. Then

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

Let $\sigma_1 = \sigma | F_1$ be the restriction of σ to F_1. By induction, we can extend σ_1 to an isometry

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

Then $\bar{\sigma}_1(F_1^{\perp}) = (\sigma_1 F_1)^{\perp}$. Since σF_2 is perpendicular to $\sigma F_1 = \sigma_1 F_1$, it follows that σF_2 is contained in $\bar{\sigma}_1(F_1^{\perp})$. Let $\sigma_2 = \sigma | F_2$. Then the isometry

$$\sigma_2 : F_2 \to \sigma_2 F_2 = \sigma F_2$$

extends by induction to an isometry

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

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 $\sigma : F \to F'$ be an isometry. Then σ 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* $\dim W' \leqq \dim W$, *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 $\dim W' \geqq \dim W$. 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 $\mathrm{id} : F \to F$ to an isometry σ 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*

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

where g_0 is a null form, g_{hyp} is hyperbolic, and g_{def} is definite. The form $g_{\mathrm{hyp}} \oplus g_{\mathrm{def}}$ is non-degenerate. The forms g_0, g_{hyp}, and g_{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_{hyp} by g_h and g_{def} by g_d.

§11. THE WITT GROUP

Let g, φ by symmetric forms on finite dimensional vector spaces over k. We shall say that they are **equivalent** if g_d is isometric to φ_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 $W(k)$. 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

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

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 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

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

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

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

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

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

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

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 $g : E \times E \to \mathbf{C}$ 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 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 ψ on E such that $2ig = h + \psi$. Show that h and ψ 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 $U : E \to E$ 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 $T : E \to E$ 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 $A, B : E \to E$ 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 λ. [*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

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

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 αI for some complex number α. [*Hint*: Let $B_0 \in S$. Let

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

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

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 $|\ |$ on E.*

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

9. (a) Show that $A \geqq 0$ if and only if all eigenvalues of A belonging to non-zero eigenvectors are $\geqq 0$. Both in the hermitian case and the symmetric case, one says that A is **semipositive** if $A \geqq 0$, 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, ${}^tUU = I$), and P is symmetric positive definite. For two hermitian or symmetric endomorphisms A, B, define $A \geqq B$ to mean $A - B \geqq 0$, and similarly for $A > B$. Suppose $A > 0$. Show that there are two real numbers $\alpha > 0$ and $\beta > 0$ such that $\alpha I \leqq A \leqq \beta I$.

10. If A is an endomorphism of E, define its norm $|A|$ to be the greatest lower bound of all numbers C such that $|Ax| \leqq C|x|$ for all $x \in E$.

    (a) Show that this norm satisfies the triangle inequality.

    (b) Show that the series

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

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

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

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 $A : E \to E$ 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 $f: E \to F$ 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 $f: E \to F$ be a map having the following property. There exists a number $C > 0$ such that for all $x, y \in E$ we have

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

Show that there exists a unique additive map $g : E \to F$ 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

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

14. (Tate) Let S be a set and $f: S \to S$ a map of S into itself. Let $h: S \to \mathbf{R}$ be a real valued function. Assume that there exists a real number $d > 1$ such that $h \circ f - dh$ 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 $n \geqq 1$, and let f be a bilinear alternating form on E. Show that there exists a basis $\{e_i\}$ $(i = 1, \ldots, n)$ and an integer r such that $2r \leqq n$,

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

where $a_1, \ldots, a_r \in \mathbf{Z}$, $a_i \neq 0$, and a_i divides a_{i+1} for $i = 1, \ldots, r - 1$ and finally $e_i \cdot e_j = 0$ for all other pairs of indices $i \leqq j$. Show that the ideals $\mathbf{Z}a_i$ are uniquely determined. [*Hint*: Consider the injective homomorphism $\varphi_f : E \to E^\vee$ 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 $\langle\ ,\ \rangle$ be a symmetric positive definite form. Let Ω 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 $U \times A \times K \to UAK \subset G$ is actually a bijection. This amounts to Gram–Schmidt orthogonalization. Prove the similar statement in the complex case, that is, for $G(\mathbf{C}) = GL_n(\mathbf{C})$, $K(\mathbf{C})$ = complex unitary group, $U(\mathbf{C})$ = complex unipotent upper triangular group, and A the same group of positive diagonal matrices as in the real case.

25. Let now $G = SL_n(\mathbf{R})$, and let K, A be the corresponding subgroups having determinant 1. Show that the product $U \times A \times K \to UAK$ again gives a bijection with G.

26. Let $\mathfrak{a}$ be the $\mathbf{R}$-vector space of real diagonal matrices with trace 0. Let $\mathfrak{a}^\vee$ be the dual space. Let α_i $(i = 1, \ldots, n-1)$ be the functional defined on an element $H = \operatorname{diag}(h_1, \ldots, h_n)$ by $\alpha_i(H) = h_i - h_{i+1}$. (a) Show that $\{\alpha_1, \ldots, \alpha_{n-1}\}$ is a basis of $\mathfrak{a}^\vee$ over $\mathbf{R}$. (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 $\{H_{1,2}, \ldots, H_{n-1,n}\}$ is a basis of $\mathfrak{a}$. (c) Abbreviate $H_{i,i+1} = H_i$ $(i = 1, \ldots, n-1)$. 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 $\{\alpha_1', \ldots, \alpha_{n-1}'\}$ is the dual basis of $\{H_1, \ldots, H_{n-1}\}$. Show that

$$\alpha_i'(H) = h_1 + \cdots + h_i.$$

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

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

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

28. **Positivity.** On $\mathfrak{a}$ (real diagonal matrices with trace 0) the form of Exercise 27 can be defined by $\operatorname{tr}(XY)$, since elements $X, Y \in \mathfrak{a}$ are symmetric. Let $\mathscr{A} = \{\alpha_1, \ldots, \alpha_{n-1}\}$ denote the basis of Exercise 26. Define an element $H \in \mathfrak{a}$ to be **semipositive** (writen $H \geqq 0$) if $\alpha_i(H) \geqq 0$ for all $i = 1, \ldots, n-1$. For each $\alpha \in \mathfrak{a}^\vee$, let $H_\alpha \in \mathfrak{a}$ represent α 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

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

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

29. Show that the elements $n\alpha_i'$ $(i = 1, \ldots, n-1)$ can be expressed as linear combinations of $\alpha_1, \ldots, \alpha_{n-1}$ with positive coefficients in $\mathbf{Z}$.

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 $f: A \to B$, 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 $E_1, \ldots, E_n, F$ are modules, we denote by

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

the module of n-multilinear maps

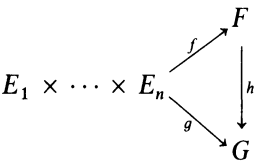
$$f: E_1 \times \cdots \times E_n \to F.$$

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 $E_1, \ldots, E_n$ as the objects of a category. Indeed, if

$$f : E_1 \times \cdots \times E_n \to F \quad \text{and} \quad g : E_1 \times \cdots \times E_n \to G$$

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



A universal object in this category is called a **tensor product** of $E_1, \ldots, E_n$ (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 $(x_1, \ldots, x_n)$, $(x_i \in E_i)$, i.e. generated by the set $E_1 \times \cdots \times E_n$. Let N be the submodule generated by all the elements of the following type:

$$(x_1, \ldots, x_i + x_i', \ldots, x_n) - (x_1, \ldots, x_i, \ldots, x_n) - (x_1, \ldots, x_i', \ldots, x_n)$$
$$(x_1, \ldots, ax_i, \ldots, x_n) - a(x_1, \ldots, x_n)$$

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

$$E_1 \times \cdots \times E_n \to M$$

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

$$\varphi : E_1 \times \cdots \times E_n \to M/N.$$

We contend that φ is multilinear and is a tensor product.

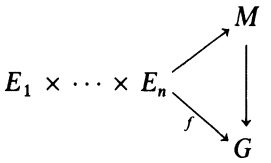
It is obvious that φ is multilinear—our definition was adjusted to this purpose. Let

$$f : E_1 \times \cdots \times E_n \to G$$

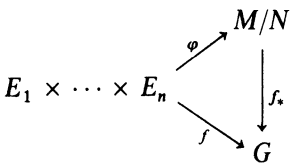
be a multilinear map. By the definition of free module generated by

$$E_1 \times \cdots \times E_n$$

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



Since f is multilinear, the induced map $M \to G$ 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 $f_* : M/N \to G$ which makes the following diagram commutative:



Since the image of φ 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 $E_1, \ldots, E_n$. If $x_i \in E_i$, we write

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

We have for all i,

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

$$x_1 \otimes \cdots \otimes (x_i + x_i') \otimes \cdots \otimes x_n$$

$$= (x_1 \otimes \cdots \otimes x_n) + (x_1 \otimes \cdots \otimes x_i' \otimes \cdots \otimes x_n)$$

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

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

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*

$$(E_1 \otimes E_2) \otimes E_3 \to E_1 \otimes (E_2 \otimes E_3)$$

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

$$\lambda_x : E_2 \times E_3 \to (E_1 \otimes E_2) \otimes E_3$$

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

$$\bar{\lambda}_x : E_2 \otimes E_3 \to (E_1 \otimes E_2) \otimes E_3.$$

The map

$$E_1 \times (E_2 \otimes E_3) \to (E_1 \otimes E_2) \otimes E_3$$

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

$$E_1 \otimes (E_2 \otimes E_3) \to (E_1 \otimes E_2) \otimes E_3,$$

which has the desired property (clear from its construction).

Proposition 1.2. *Let E, F be modules. Then there is a unique isomorphism*

$$E \otimes F \to F \otimes E$$

such that $x \otimes y \mapsto y \otimes x$ for $x \in E$ and $y \in F$.

Proof. The map $E \times F \to F \otimes E$ 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

$$f_i : E_i' \to E_i \qquad (i = 1, \ldots, n)$$

is a collection of linear maps. We get an induced map on the product,

$$\prod f_i : \prod E_i' \to \prod E_i.$$

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 $T(f_1, \ldots, f_n)$ which makes the following diagram commutative:

$$\begin{array}{ccc} E_1' \times \cdots \times E_n' & \longrightarrow & E_1' \otimes \cdots \otimes E_n' \\ \Big\downarrow{\scriptstyle \prod f_i} & & \Big\downarrow{\scriptstyle T(f_1, \ldots, f_n)} \\ E_1 \times \cdots \times E_n & \longrightarrow & E_1 \otimes \cdots \otimes E_n \end{array}$$

It is immediately verified that T is functorial, namely that if we have a composite of linear maps $f_i \circ g_i$ $(i = 1, \ldots, n)$ then

$$T(f_1 \circ g_1, \ldots, f_n \circ g_n) = T(f_1, \ldots, f_n) \circ T(g_1, \ldots, g_n)$$

and

$$T(\mathrm{id}, \ldots, \mathrm{id}) = \mathrm{id}.$$

We observe that $T(f_1, \ldots, f_n)$ is the unique linear map whose effect on an element $x_1' \otimes \cdots \otimes x_n'$ of $E_1' \otimes \cdots \otimes E_n'$ is

$$x_1' \otimes \cdots \otimes x_n' \mapsto f_1(x_1') \otimes \cdots \otimes f_n(x_n').$$

We may view T as a map

$$\prod_{i=1}^{n} L(E_i', E_i) \to L\left(\bigotimes_{i=1}^{n} E_i', \bigotimes_{i=1}^{n} E_i\right),$$

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 $f : F' \to F$ and $g_1, g_2 : E' \to E$, 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 τ gives rise to a linear map

$$\tau : L(E', E) \to L(\tau(E'), \tau(E))$$

for each pair of modules E', E, by the formula

$$\tau(f) = T(\mathrm{id}, f).$$

Remark. By abuse of notation, it is sometimes convenient to write

$$f_1 \otimes \cdots \otimes f_n \quad \text{instead of} \quad T(f_1, \ldots, f_n).$$

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,

$$\boxed{L(E, L(F, G)) \approx L^2(E, F; G) \approx L(E \otimes F, G).}$$

The isomorphisms involved are described in a natural way.

(i) $L^2(E, F; G) \to L(E, L(F, G))$.

If $f : E \times F \to G$ is bilinear, and $x \in E$, then the map

$$f_x : F \to G$$

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) $L(E, L(F, G)) \to L^2(E, F; G)$.

Let $\varphi \in L(E, L(F, G))$. We let $f_\varphi : E \times F \to G$ 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) $L^2(E, F; G) \to L(E \otimes F, G)$.

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 $E \times F \to E \otimes F$ 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, τ is linear. We have projections $\pi_i : E \to E$ of E on E_i. Then

$$\pi_i \circ \pi_i = \pi_i, \qquad \pi_i \circ \pi_j = 0 \qquad \text{if} \quad i \neq j,$$

$$\sum_{i=1}^{n} \pi_i = \mathrm{id}.$$

We apply the functor τ, and see that $\tau(\pi_i)$ satisfies the same relations, hence gives a direct sum decomposition of $\tau(E) = F \otimes E$. Note that $\tau(\pi_i) = \mathrm{id} \otimes \pi_i$.

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

$$\left(\bigoplus_{i \in S} E_i\right) \times F \to \bigoplus_{i \in S} (E_i \otimes F) \to \bigoplus_{i \in I} (E_i \otimes F)$$

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

$$\left(\bigoplus_{i \in S'} E_i\right) \times F \to \bigoplus_{i \in I} (E_i \otimes F)$$

induces our preceding map on the sum for $i \in S$. But we have an *injection*

$$\left(\bigoplus_{i \in S} E_i\right) \times F \to \left(\bigoplus_{i \in S'} E_i\right) \times F.$$

Hence by compatibility, we can define a bilinear map

$$\left(\bigoplus_{i \in I} E_i\right) \times F \to \bigoplus_{i \in I} (E_i \otimes F),$$

and consequently a linear map

$$\left(\bigoplus_{i\in I} E_i\right) \otimes F \to \bigoplus_{i\in I} (E_i \otimes F).$$

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,

$$\sum_{i=1}^{n} (y_i \otimes v) = \left(\sum_{i=1}^{n} y_i\right) \otimes v, \qquad y_i \in F.$$

Hence every element is in fact of type $y \otimes v$ with some $y \in F$.

We have a bilinear map

$$F \times E \to F$$

such that $(y, av) \mapsto ay$, inducing a linear map

$$F \otimes E \mapsto F.$$

We also have a linear map $F \to F \otimes E$ 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*

$$\sum_{i\in I} y_i \otimes v_i, \qquad y_i \in F$$

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*

$$\mathrm{End}_R(E) \otimes \mathrm{End}_R(F) \to \mathrm{End}_R(E \otimes F)$$

which is the unique linear map such that

$$f \otimes g \mapsto T(f, g)$$

for $f \in \mathrm{End}_R(E)$ and $g \in \mathrm{End}_R(F)$.

[We note that the tensor product on the left is here taken in the tensor product of the two modules $\mathrm{End}_R(E)$ and $\mathrm{End}_R(F)$.]

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

$$f(v_i) = v_{i'} \quad \text{and} \quad f(v_\nu) = 0 \quad \text{if } \nu \neq i$$

$$g(w_j) = w_{j'} \quad \text{and} \quad g(w_\mu) = 0 \quad \text{if } \mu \neq j.$$

Furthermore, the families $\{f_{i,i'}\}$ and $\{g_{j,j'}\}$ are bases of $\mathrm{End}_R(E)$ and $\mathrm{End}_R(F)$ respectively. Then

$$T(f, g)(v_\nu \otimes w_\mu) = \begin{cases} v_{i'} \otimes w_{j'} & \text{if } (\nu, \mu) = (i, j) \\ 0 & \text{if } (\nu, \mu) \neq (i, j). \end{cases}$$

Thus the family $\{T(f_{i,i'}, g_{j,j'})\}$ is a basis of $\mathrm{End}_R(E \otimes F)$. Since the family $\{f_{i,i'} \otimes g_{j,j'}\}$ is a basis of $\mathrm{End}_R(E) \otimes \mathrm{End}_R(F)$, 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*

$$0 \to E' \xrightarrow{\varphi} E \xrightarrow{\psi} E'' \to 0$$

be an exact sequence, and F any module. Then the sequence

$$F \otimes E' \to F \otimes E \to F \otimes E'' \to 0$$

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

$$F \otimes E \to F \otimes E''.$$

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

$$F \otimes E' \to F \otimes E$$

is contained in the kernel of

$$F \otimes E \to F \otimes E''.$$

Conversely, let I be the image of $F \otimes E' \to F \otimes E$, and let

$$f : (F \otimes E)/I \to F \otimes E''$$

be the canonical map. We shall define a linear map

$$g : F \otimes E'' \to (F \otimes E)/I$$

such that $g \circ f = \mathrm{id}$. 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 $F \times E'' \to (F \otimes E)/I$ 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

$$0 \to F \otimes E' \to F \otimes E \to F \otimes E'' \to 0$$

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 $(R/\mathfrak{a}) \times E \to E/\mathfrak{a}E$ induced by*

$$(a, x) \mapsto ax \pmod{\mathfrak{a}E}, \qquad a \in R, x \in E$$

is bilinear and induces an isomorphism

$$(R/\mathfrak{a}) \otimes E \xrightarrow{\approx} E/\mathfrak{a}E.$$

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

$$E \to R/\mathfrak{a} \otimes E$$

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

$$E/\mathfrak{a}E \to R/\mathfrak{a} \otimes E,$$

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

$$E' \to E \to E''$$

the sequence

$$F \otimes E' \to F \otimes E \to F \otimes E''$$

is exact.

F 2. For every short exact sequence

$$0 \to E' \to E \to E'' \to 0$$

the sequence

$$0 \to F \otimes E' \to F \otimes E \to F \otimes E'' \to 0$$

is exact.

F 3. For every injection $0 \to E' \to E$ the sequence

$$0 \to F \otimes E' \to F \otimes E$$

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 $E' \to E$ 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 $R = k[[x_1, \ldots, x_n]]$, then x_1, $\ldots$, 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 $n \geqq 2$. The same argument, of course, applies to any local ring R such that $\mathfrak{m}/\mathfrak{m}^2$ has dimension $\geqq 2$ 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*

$$0 \to N \to M \to F \to 0$$

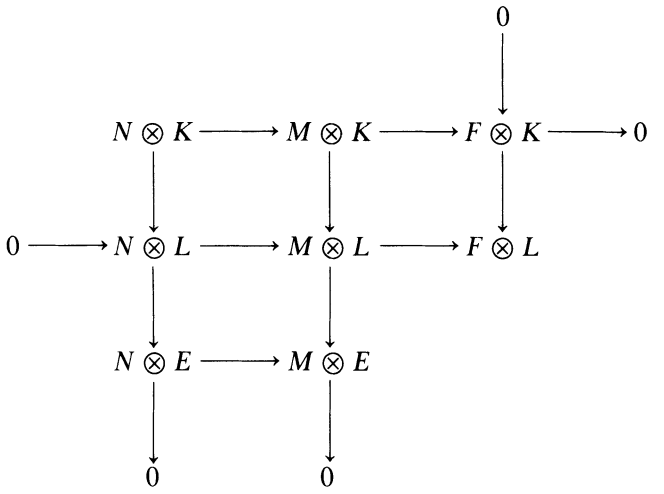
is an exact sequence. Then for any E, we have an exact sequence

$$0 \to N \otimes E \to M \otimes E \to F \otimes E \to 0.$$

Proof. Represent E as a quotient of a flat L by an exact sequence

$$0 \to K \to L \to E \to 0.$$

Then we have the following exact and commutative diagram:



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

$$0 \to N \otimes E \to M \otimes E$$

which proves the lemma.

Proposition 3.4. *Let*

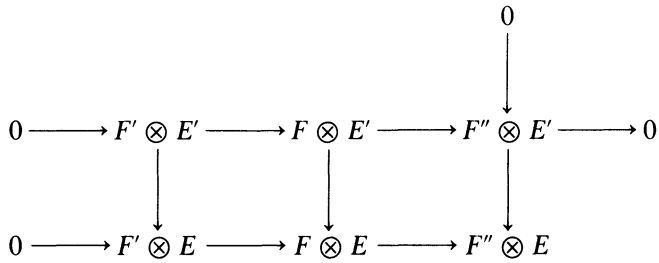
$$0 \to F' \to F \to F'' \to 0$$

be an exact sequence, and assume that F'' is flat. Then F is flat if and only if F' is flat. More generally, let

$$0 \to F^0 \to F^1 \to \cdots \to F^n \to 0$$

be an exact sequence such that $F^1, \ldots, F^n$ are flat. Then F^0 is flat.

Proof. Let $0 \to E' \to E$ be an injection. We have an exact and commutative diagram:



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 $F' \otimes E' \to F' \otimes E$ 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

$$0 \to E' \to E$$

the tensored sequence

$$0 \to F \otimes E' \to F \otimes E$$

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 $F \otimes E_1' \to F \otimes E$ is a monomorphism so is $F \otimes E_1' \to F \otimes E_2'$ since the composite map with $F \otimes E_2' \to F \otimes E$ is a monomorphism. The only question lies with a factor module. Suppose we have an exact sequence

$$0 \to N \to E \to M \to 0.$$

Let M' be a submodule of M and E' its inverse image in E. Then we have a

commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & E' & \longrightarrow & M' & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M & \longrightarrow & 0. \end{array}$$

We tensor with F to get the exact and commutative diagram

$$\begin{array}{ccccccccc} & & & & 0 & & K & & \\ & & & & \downarrow & & \downarrow & & \\ & & F \otimes N & \longrightarrow & F \otimes E' & \longrightarrow & F \otimes M' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F \otimes N & \longrightarrow & F \otimes E & \longrightarrow & F \otimes M & & \\ & & \downarrow & & & & & & \\ & & 0 & & & & & & \end{array}$$

where K is the questionable kernel which we want to prove is 0. But the snake lemma yields the exact sequence

$$0 \to K \to 0$$

which concludes the proof.

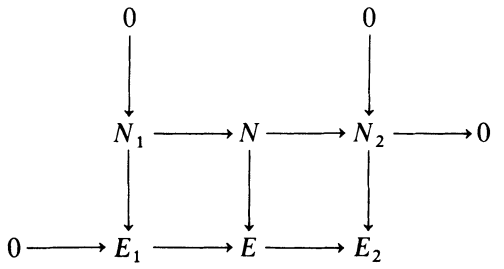
Lemma 3.6. *Let $\{E_i\}$ be a family of modules, and suppose that F is flat for each E_i. Then F is flat for their direct sum.*

Proof. Let $E = \bigoplus E_i$ be their direct sum. We have to prove that given any submodule E' of E, the sequence

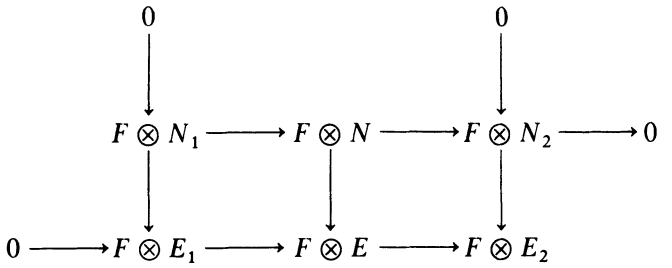
$$0 \to F \otimes E' \to F \otimes E = \bigoplus F \otimes E_i$$

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:



Tensoring with F we get the exact and commutative diagram:



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*

$$\mathfrak{a} \otimes F \to \mathfrak{a}F$$

is an isomorphism. In fact, F is flat if and only for every ideal $\mathfrak{a}$ of R tensoring the sequence

$$0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$$

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 $M \to M/\mathfrak{a}M$. 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 $\mathfrak{A}$ and $\mathfrak{B}$ 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 $\mathfrak{A}$ **T-exact** if $B \mapsto T(A, B)$ is an exact functor; and we call an object L of $\mathfrak{B}$ **${}^tT$-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 $\mathfrak{B}$ there is a ${}^tT$-exact L and an epimorphism

$$L \to E \to 0.$$

For the analog of Proposition 3.7, we need to assume that there is some object R in $\mathfrak{B}$ for which F is R-exact, that is given an exact sequence

$$0 \to \mathfrak{a} \to R$$

then $0 \to T(F, \mathfrak{a}) \to T(F, R)$ 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.

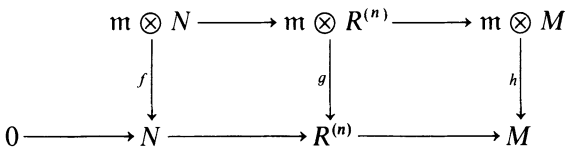
We now pass to somewhat different considerations.

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 $x_1, \ldots, x_n \in M$ are elements of M whose residue classes are a basis of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$, then $x_1, \ldots, x_n$ form a basis of M over R.*

Proof. Let $R^{(n)} \to M$ be the map which sends the unit vectors of $R^{(n)}$ on $x_1, \ldots, x_n$ respectively, and let N be its kernel. We get an exact sequence

$$0 \to N \to R^{(n)} \to M,$$

whence a commutative diagram



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

$$0 \to \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker} h,$$

and the arrow on the right is merely

$$R^{(n)}/\mathfrak{m}R^{(n)} \to M/\mathfrak{m}M,$$

which is an isomorphism by the assumption on $x_1, \ldots, x_n$. It follows that $\operatorname{coker} f = 0$, 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*

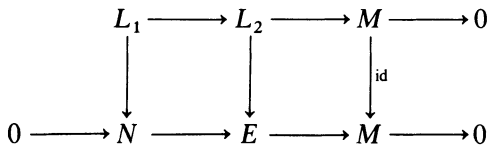
$$0 \to N \to E \to M \to 0$$

be exact, with E finite free. Then N is finitely generated.

Proof. Let

$$L_1 \to L_2 \to M \to 0$$

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



such that $L_2 \to E$ is surjective. Then the snake lemma gives at once the exact sequence

$$0 \to \operatorname{coker}(L_1 \to N) \to 0,$$

so $\operatorname{coker}(L_1 \to N) = 0$, 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 $i = 1, \ldots, n$, 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 $y_j \in M$ $(j = 1, \ldots, s)$ 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

$$0 \to K \to R^{(n)} \to R$$

where the map $R^{(n)} \to R$ is given by

$$(b_1, \ldots, b_n) \mapsto \sum_{i=1}^{n} a_i b_i,$$

and K is its kernel. Since M is flat it follows that

$$K \otimes M \to M^{(n)} \xrightarrow{f_M} M$$

is exact, where f_M is given by

$$f_M(z_1, \ldots, z_n) = \sum_{i=1}^{n} a_i z_i.$$

Therefore there exist elements $\beta_j \in K$ and $y_j \in M$ such that

$$(x_1, \ldots, x_n) = \sum_{j=1}^{s} \beta_j y_j.$$

Write $\beta_j = (b_{1j}, \ldots, b_{nj})$ 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

$$\cdots \to E_i \to E_{i-1} \to E_0 \to M \to 0$$

be a free or projective resolution of M, i.e. an exact sequence where E_i is free or projective for all $i \geqq 0$. We write this sequence as

$$E_M \to M \to 0.$$

Then by definition,

$$\operatorname{Tor}_i(M, N) = i\text{-th homology of the complex } E \otimes N, \text{ that is of}$$

$$\cdots \to E_i \otimes N \to E_{i-1} \otimes N \to \cdots \to E_0 \otimes N \to 0.$$

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 $\operatorname{Tor}_i(M, N)$, 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

$$\operatorname{Tor}_i(M, N) \approx \operatorname{Tor}_i(N, M)$$

for all i. See Propositions 8.2 and 8.2′ of Chapter XX.

Following general principles, we say that M has **Tor-dimension** $\leqq d$ if $\operatorname{Tor}_i(M, N) = 0$ 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) $\operatorname{Tor}_1(M, N) = 0$ *for all N.*

(iii) $\operatorname{Tor}_i(M, N) = 0$ *for all $i \geqq 1$ 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 $R \to R'$ 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

$$R' \times R' \times E \to R' \otimes E$$

defined by the rule

$$(a, b, x) \mapsto ab \otimes x.$$

This induces therefore a R-linear map

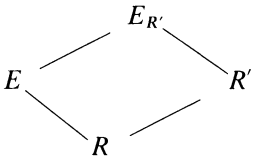
$$R' \otimes (R' \otimes E) \to R' \otimes E$$

and hence a R-bilinear map $R' \times (R' \otimes E) \to R' \otimes E$. 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 $R \to R/\mathfrak{a}$ 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:



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 $R \to R' \to R''$ 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 $R \to A$ 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 $R \to R'$ be a homomorphism of commutative rings. We have a 4-multilinear map

$$R' \times A \times R' \times A \to R' \otimes A$$

defined by

$$(a, x, b, y) \mapsto ab \otimes xy.$$

We get an induced R-linear map

$$R' \otimes A \otimes R' \otimes A \to R' \otimes A$$

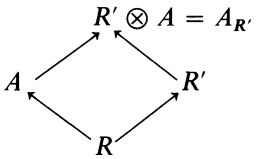
and hence an induced R-bilinear map

$$(R' \otimes A) \times (R' \otimes A) \to R' \otimes A.$$

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,



For the record, we give some routine tests for flatness in the context of base extension.

Proposition 4.2. *Let $R \to A$ 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 $H : L \to M$ is a rule which to each object X of $\mathfrak{A}$ associates a morphism $H_X : L(X) \to M(X)$ in $\mathfrak{B}$, such that for any morphism $f : X \to Y$ in $\mathfrak{A}$, the following diagram is commutative:

$$\begin{array}{ccc} L(X) & \xrightarrow{H_X} & M(X) \\ {\scriptstyle L(f)}\downarrow & & \downarrow{\scriptstyle M(f)} \\ L(Y) & \xrightarrow[H_Y]{} & M(Y) \end{array}$$

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,

$$E \mapsto E^\vee = L(E, R) = \mathrm{Hom}_R(E, R).$$

Similarly, we have a functor in two variables,

$$(E, F) \mapsto L(E, F) = \mathrm{Hom}_R(E, F),$$

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 $H : L \to M$ be a morphism of functors. If $H_E : L(E) \to M(E)$ 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 $(i = 1, \ldots, m)$ be modules over a ring. Let $\varphi_i : E_i \to E$ and $\psi_i : E \to E_i$ be homomorphisms having the following properties:*

$$\psi_i \circ \varphi_i = \mathrm{id}, \qquad \psi_i \circ \varphi_j = 0 \quad \text{if} \quad i \neq j$$

$$\sum_{i=1}^{m} \varphi_i \circ \psi_i = \mathrm{id},$$

Then the map

$$x \mapsto (\psi_1 x, \ldots, \psi_m x)$$

is an isomorphism of E onto the direct product $\prod_{i=1}^{m} E_i$, and the map

$$(x_1, \ldots, x_m) \mapsto \varphi_1 x_1 + \cdots + \varphi_m x_m$$

is an isomorphism of the product onto E. Conversely, if E is equal to the direct sum of submodules E_i $(i = 1, \ldots, m)$, if we let ψ_i be the inclusion of E_i in E, and φ_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

$$\begin{array}{ccc} L(E) & \xrightarrow{H_E} & M(E) \\ {\scriptstyle L(\varphi_i)}\uparrow & & \uparrow{\scriptstyle M(\varphi_i)} \\ L(E_i) & \xrightarrow[H_{E_i}]{} & M(E_i) \end{array}$$

and a similar diagram replacing φ_i by ψ_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 $M(\varphi_i)$ $(i = 1, \ldots, m)$ 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*

$$L(E', E) \otimes L(F', F) \to L(E' \otimes F', E \otimes F)$$

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*

$$\mathrm{End}_R(E) \otimes \mathrm{End}_R(F) \to \mathrm{End}_R(E \otimes F).$$

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*

$$E^\vee \otimes F \to L(E, F)$$

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 $\{v_1, \ldots, v_n\}$ be a basis of E, and let $\{v_1', \ldots, v_n'\}$ 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 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

$$L(E, E) \to E^\vee \otimes E,$$

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*

$$E^\vee \otimes F^\vee \to (E \otimes F)^\vee.$$

given for $\lambda \in E^\vee$ and $\mu \in F^\vee$ by the map

$$\lambda \otimes \mu \mapsto \Lambda,$$

where Λ 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*

$$L(E, E) \to E^\vee \otimes E \to R,$$

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 $R \to A$ 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

$$M_{a,b}: A \times B \to A \otimes B \text{ such that } M_{a,b}(a', b') = aa' \otimes bb'.$$

Hence $M_{a,b}$ induces an R-linear map $m_{a,b}: A \otimes B \to A \otimes B$ 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

$$A \otimes B \times A \otimes B \to A \otimes B$$

such that $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$. This map is obviously associative, and we have a natural ring homomorphism

$$R \to A \otimes B \quad \text{given by} \quad c \mapsto 1 \otimes c = c \otimes 1.$$

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 $R \to A$ and $R \to B$ are two homomorphisms of commutative rings, then their coproduct over R is the homomorphism $R \to A \otimes B$ 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 $R \to A$ and $R \to B$. One can use induction.

Let A, B be commutative rings, and assume given ring-homomorphisms into a commutative ring C,

$$\varphi : A \to C \quad \text{and} \quad \psi : B \to C.$$

Then we can define a $\mathbf{Z}$-bilinear map

$$A \times B \to C$$

by $(x, y) \mapsto \varphi(x)\psi(y)$. From this we get a unique additive homomorphism

$$A \otimes B \to C$$

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 $A \otimes B \to C$ is a ring-homomorphism. We also have two ring-homomorphisms

$$A \xrightarrow{f} A \otimes B \quad \text{and} \quad B \xrightarrow{g} A \otimes B$$

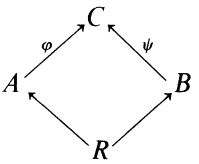
given by

$$x \mapsto x \otimes 1 \quad \text{and} \quad y \mapsto 1 \otimes y.$$

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 φ, ψ make the following diagram com-

mutative,



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 $A \otimes B \to C$ 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 $A_r \times A_s \to A_{r+s}$. 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** $A \otimes A \to A$ 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 $T_{su}(E)$ 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**

$$A \otimes_{su} B$$

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 $A \otimes_{su} B$ 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

$$(a \otimes_{su} b)(a' \otimes_{su} b')(a'' \otimes_{su} b'')$$

in two ways turns out to be the same, namely $(-1)^{ij+js+sr}$. Since bilinearity is trivially satisfied, it follows that $A \otimes_{su} B$ 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 $r \geqq 0$, we let

$$T^r(E) = \bigotimes_{i=1}^{r} E \quad \text{and} \quad T^0(E) = R.$$

Thus $T^r(E) = E \otimes \cdots \otimes E$ (r times). Then T^r is a functor, whose effect on linear maps is given as follows. If $f : E \to F$ is a linear map, then

$$T^r(f) = T(f, \ldots, f)$$

in the sense of §1.

From the associativity of the tensor product, we obtain a bilinear map

$$T^r(E) \times T^s(E) \to T^{r+s}(E),$$

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 $f : E \to F$ be a linear map. Then f induces a linear map

$$T^r(f) : T^r(E) \to T^r(F)$$

for each $r \geqq 0$, 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 $x_1, \ldots, x_r \in E$ 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 $t_1, \ldots, t_n \in P$ such that the elements

$$M_{(i)}(t) = t_{i_1} \cdots t_{i_s}$$

with $1 \leqq i_\nu \leqq n$ 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 $t_1, \ldots, t_n$ 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 $t_1, \ldots, t_n$ 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 $\{v_1, \ldots, v_n\}$ is a basis of E over R, then the elements*

$$M_{(i)}(v) = v_{i_1} \otimes \cdots \otimes v_{i_\nu}, \qquad 1 \leqq i_\nu \leqq n$$

form a basis of $T^r(E)$, and every element of $T(E)$ has a unique expression as a finite sum

$$\sum_{(i)} a_{(i)} M_{(i)}(v), \qquad a_{(i)} \in R$$

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 $\mathrm{End}_R(E)$ *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 $\mathrm{End}_R(T(E))$, 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

$$T(L(E)) \to LT(E)$$

given in each dimension r by the linear map

$$f_1 \otimes \cdots \otimes f_r \mapsto T(f_1, \ldots, f_r) = f_1 \cdots f_r.$$

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*

$$T(L(E)) = T(\mathrm{End}_R(E)) \to LT(E) = \bigoplus_{r=0}^{\infty} \mathrm{End}_R(T^r(E))$$

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 $(1, \ldots, n)$. An r-multilinear map

$$f : E^{(r)} \to F$$

is said to be **symmetric** if $f(x_1, \ldots, x_r) = f(x_{\sigma(1)}, \ldots, x_{\sigma(r)})$ for all $\sigma \in \mathfrak{S}_r$.

In $T^r(E)$, 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

$$S^r(E) = T^r(E)/\mathfrak{b}_r,$$

and let

$$S(E) = \bigoplus_{r=0}^{\infty} S^r(E)$$

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

$$E^{(r)} \to S^r(E)$$

obtained by composing the maps

$$E^{(r)} \to T^r(E) \to T^r(E)/\mathfrak{b}_r = S^r(E)$$

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 $(x_1, \ldots, x_r)$ under the canonical map

$$E^{(r)} \to S^r(E)$$

will be denoted simply by $x_1 \cdots x_r$.

Proposition 8.1. *Let E be free of dimension n over R. Let $\{v_1, \ldots, v_n\}$ 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 $t_1, \ldots, t_n$ be algebraically independent variables over R, and form the polynomial algebra $R[t_1, \ldots, t_n]$. Let P_r be the R-module of homogeneous polynomials of degree r. We define a map of $E^{(r)} \to P_r$ as follows. If $w_1, \ldots, w_r$ are elements of E which can be written

$$w_i = \sum_{v=1}^{n} a_{iv} v_v, \qquad i = 1, \ldots, r,$$

then our map is given by

$$(w_1, \ldots, w_r) \mapsto (a_{11}t_1 + \cdots + a_{1n}t_n) \cdots (a_{r1}t_1 + \cdots + a_{rn}t_n).$$

It is obvious that this map is multilinear and symmetric. Hence it factors through a linear map of $S^r(E)$ into P_r:

$$\begin{array}{ccc} E^{(r)} & \longrightarrow & S^r(E) \\ & \searrow \quad \swarrow & \\ & P_r & \end{array}$$

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 $(i) = (i_1, \ldots, i_r)$. 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 $S^r(E) \to P_r$ 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*

$$S^n(E' \oplus E'') \approx \bigoplus_{p+q=n} S^pE' \otimes S^qE''.$$

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

$$SE' \otimes SE'' \to SE,$$

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 $f(X) = \operatorname{Irr}(\alpha, k, X)$, 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 α 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 $\varphi : A \to B$ 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 φ, 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

$$\operatorname{Hom}_B(B \otimes_A E, F) \approx \operatorname{Hom}_A(E, F_A).$$

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 $\{e_1, \ldots, e_r\}$ is a basis of B over R, then

$$1_A \otimes e_1, \ldots, 1_A \otimes e_r$$

   is a basis of $A \otimes B$ over A. We may then define the **norm**

$$N = N_{A \otimes B, A} : A \otimes B \to A$$

   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 $\varphi : A \to C$ be a homomorphism of R-algebras. Then the following diagram is commutative:

$$\begin{array}{ccc} A \otimes B & \xrightarrow{\varphi \otimes \mathrm{id}} & C \otimes B \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} \\ A & \xrightarrow[\varphi]{} & C \end{array}$$

(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 $u : F \to E$ is a homomorphism of A-modules, $u \neq 0$, then $T_M(u) : M \otimes_A F \to M \otimes_A E$ 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 $N' \to N \to N''$ is exact if and only if the sequence tensored with M is exact.

10. (a) Let $A \to B$ 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 $A \to B$ 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

$$\mathrm{Hom}_A(P, M) \otimes_A E \to \mathrm{Hom}_A(P, M \otimes_A E)$$

is a monomorphism (resp. an isomorphism).

[*Hint*: Let $F_1 \to F_0 \to P \to 0$ be a finite presentation, say. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_A(P, M) \otimes_A E & \longrightarrow & \mathrm{Hom}_A(F_0, M) \otimes_A E & \longrightarrow & \mathrm{Hom}_A(F_1, M) \otimes_A E \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Hom}_A(P, M \otimes_A E) & \longrightarrow & \mathrm{Hom}_A(F_0, M \otimes_A E) & \longrightarrow & \mathrm{Hom}_A(F_1, M \otimes_A E)]. \end{array}$$

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

$$\mathrm{Hom}_A(P, A) \otimes_A E \to \mathrm{Hom}_A(P, E)$$

is surjective.

(iv) For every finitely presented module P and homomorphism $f: P \to E$ there exists a free module F, finitely generated, and homomorphisms

$$g: P \to F \quad \text{and} \quad h: F \to E$$

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 $E \to E^\vee$ of E with its dual space. Let $\{v_1, \ldots, v_n\}$ be a basis of E. The B-dual basis $\{v_1', \ldots, v_n'\}$ 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 $\mathscr{D}: E \to \mathbf{D}$ be an injective linear map of E into $\mathbf{D}$. Show that the element $\sum \mathscr{D}(v_i)\mathscr{D}(v_i') = \omega_{B,\mathscr{D}}$ is independent of the choice of basis. We call it the **Casimir element** in $\mathbf{D}$, determined by $\mathscr{D}$ and B.

Remark. The terminology of the Casimir element is determined by the classical case, when G is a Lie group, $E = \mathfrak{g} = \mathrm{Lie}(G)$ is the Lie algebra of G (tangent space at the origin with the Lie algebra product determined by the Lie derivative), and $\mathscr{D}(v)$ 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 $\mathrm{Mat}_n(k)$ consisting of matrices with trace 0. Let B be the bilinear form defined by $B(X, Y) = \mathrm{tr}(XY)$. Let $G = SL_n(k)$. Prove:

(a) B is $\mathbf{c}(G)$-invariant, where $\mathbf{c}(g)$ is conjugation by an element $g \in G$.

(b) B is invariant under the transpose $(X, Y) \mapsto ({}^tX, {}^tY)$.

(c) Let $k = \mathbf{R}$. 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 $\mathscr{D}: E \to \mathbf{D}$ 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 (φ_{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 $\mathrm{Mat}_n(K)$. We have a ring-homomorphism

$$K \to \mathrm{Mat}_n(K)$$

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

$$E = E_1 \oplus \cdots \oplus E_n, \qquad F = F_1 \oplus \cdots \oplus F_m$$

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

$$\varphi : E_1 \oplus \cdots \oplus E_n \to F$$

be a homomorphism. Let $\varphi_j : E_j \to F$ be the restriction of φ 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 $X = {}^t(x_1, \ldots, x_n)$, whose components are in $E_1, \ldots, E_n$ respectively. We can associate with φ the row vector $(\varphi_1, \ldots, \varphi_n)$, $\varphi_j \in \mathrm{Hom}_R(E_j, F)$, and the effect of φ on the element x of E is described by matrix multiplication, of the row vector times the column vector.

More generally, consider a homomorphism

$$\varphi : E_1 \oplus \cdots \oplus E_n \to F_1 \oplus \cdots \oplus F_m.$$

Let $\pi_i : F_1 \oplus \cdots \oplus F_m \to F_i$ 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 $\varphi_{ij} \in \mathrm{Hom}_R(E_j, F_i)$, such that φ 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 (φ_{ij}) with $\varphi_{ij} \in \mathrm{Hom}_R(E_j, F_i)$, we can define an element of $\mathrm{Hom}_R(E, F)$ by means of this matrix. We have an additive group-isomorphism between $\mathrm{Hom}_R(E, F)$ and this group of matrices.

In particular, let E be a fixed R-module, and let $K = \mathrm{End}_R(E)$. Then we have a ring-isomorphism

$$\mathrm{End}_R(E^{(n)}) \to \mathrm{Mat}_n(K)$$

which to each $\varphi \in \mathrm{End}_R(E^{(n)})$ 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 $f_a : E \to E$ 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 φ_{ij} in $\mathrm{End}_R(E)$, 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 $\mathrm{End}_R(E)$ is a division ring.*

Proof. Let $f : E \to F$ be a non-zero homomorphism. Its image and kernel are submodules, hence $\mathrm{Ker}\, f = 0$ and $\mathrm{Im}\, f = F$. 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, $E_1, \ldots, E_r$ are uniquely determined up to isomorphisms, and the multiplicities $n_1, \ldots, n_r$ are uniquely determined. The ring $\mathrm{End}_R(E)$ *is isomorphic to a ring of matrices, of type*

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

where M_i is an $n_i \times n_i$ matrix over $\mathrm{End}_R(E_i)$. *(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

$$E_1^{(n_1)} \oplus \cdots \oplus E_r^{(n_r)} \to F_1^{(m_1)} \oplus \cdots \oplus F_s^{(m_s)},$$

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

$$E_i^{(n_i)} \to F_i^{(m_i)}$$

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 $\mathrm{End}_R(E^{(n)})$ is isomorphic to the $n \times n$ matrix ring over the division ring $\mathrm{End}_R(E) = K$. 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

$$R \to Rv$$

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

$$R/L \to Rv.$$

We can write $E = Mv \oplus M'$ with some submodule M'. Then

$$Rv = Mv \oplus (M' \cap Rv),$$

because every element $x \in Rv$ 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 Rv. Since Mv is maximal in Rv, it follows that $M' \cap Rv$ 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 $E = F_0 \oplus F_0'$. Every element x of F has a unique expression $x = x_0 + x_0'$ with $x_0 \in F_0$ and $x_0' \in F_0'$. But $x_0' = x - x_0 \in F$. Hence F is the direct sum

$$F = F_0 \oplus (F \cap F_0').$$

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 $E \to E/F$ 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 $\mathrm{End}_R(E)$. 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 $f_\alpha : E \to E$ by the map $f_\alpha(x) = \alpha x$. This is what is meant by the condition

$$\varphi(\alpha x) = \alpha \varphi(x).$$

We let $R'' = R''(E) = \mathrm{End}_{R'}(E)$. We call R' the **commutant** of R and R'' the **bicommutant**. Thus we get a ring-homomorphism

$$R \to \mathrm{End}_{R'}(E) = R''(E) = R''$$

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 $R' = \mathrm{End}_R(E)$, $f \in \mathrm{End}_{R'}(E)$ 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 $\pi: E \to Rx$ 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 $R' = \mathrm{End}_R(E)$. Let $f \in \mathrm{End}_{R'}(E)$. Let $x_1, \ldots, x_n \in E$. Then there exists an element $\alpha \in R$ such that*

$$\alpha x_i = f(x_i) \quad \text{for} \quad i = 1, \ldots, n.$$

If E is finitely generated over R', then the natural map $R \to \mathrm{End}_{R'}(E)$ is surjective.

Proof. For clarity of notation, we shall first carry out the proof in case E is simple. Let $f^{(n)}: E^{(n)} \to E^{(n)}$ be the product map, so that

$$f^{(n)}(y_1, \ldots, y_n) = (f(y_1), \ldots, f(y_n)).$$

Let $R'_n = \mathrm{End}_R(E^{(n)})$. 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 $\mathrm{End}_{R'_n}(E^{(n)})$. By the lemma, there exists an element $\alpha \in R$ such that

$$(\alpha x_1, \ldots, \alpha x_n) = (f(x_1), \ldots, f(x_n)),$$

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:

$$E = E_1^{(n_1)} \oplus \cdots \oplus E_r^{(n_r)} \qquad (E_i \not\approx E_j \quad \text{if} \quad i \neq j),$$

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 $\mathrm{End}_{R_n'}(E^{(n)})$, and that we can apply the lemma.

We add the observation that if E is finitely generated over R', then an element $f \in \mathrm{End}_{R'}(E)$ is determined by its value on a finite number of elements of E, so the asserted surjectivity $R \to \mathrm{End}_{R'}(E)$ 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* $\mathrm{End}_k(E)$. *If E is a simple R-module, then* $R = \mathrm{End}_{R'}(E)$.

Proof. We contend that $\mathrm{End}_R(E) = k$. At any rate, $\mathrm{End}_R(E)$ 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 $\mathrm{End}_k(E)$ 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 $\mathrm{End}_R(E) = k$. Let now $\{v_1, \ldots, v_n\}$ be a basis of E over k. Let $A \in \mathrm{End}_k(E)$. According to the density theorem, there exists $\alpha \in R$ such that

$$\alpha v_i = A v_i \quad \text{for} \quad i = 1, \ldots, n.$$

Since the effect of A is determined by its effect on a basis, we conclude that $R = \mathrm{End}_k(E)$.

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 $\mathrm{End}_k(E)$ 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 $k[G] = \mathrm{End}_k(E)$.

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 $\mathrm{End}_R(E)$ 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 $\mathrm{End}_k(E)$. 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 $D = \mathrm{End}_R(E)$, and assume that E is finite dimensional over D. Then $R = \mathrm{End}_D(E)$.*

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis of E over D. Given $A \in \mathrm{End}_D(E)$, by Theorem 3.2 there exists $\alpha \in R$ such that

$$\alpha v_i = A v_i \quad \text{for} \quad i = 1, \ldots, n.$$

Hence the map $R \to \mathrm{End}_D(E)$ 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

$$R \to \mathrm{End}_k(E)$$

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 $\rho: R \to \mathrm{End}_k(V)$. Then ρ is an isomorphism, in other words, $R \approx \mathrm{Mat}_n(k)$.*

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 $V_1, \ldots, V_m$ are finite dimensional vector spaces over a field k, and that R is a k-algebra with representations

$$R \to \mathrm{End}_k(V_i), \ i = 1, \ldots, m,$$

so V_i is an R-module. If we let

$$E = V_1 \oplus \cdots \oplus V_m,$$

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 $V_1, \ldots, V_m$ 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 $\mathrm{End}_{R'}(E)$, 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 α_E, α_F be the corresponding k-endomorphisms on E and F respectively. Suppose that the traces are equal; that is,*

$$\mathrm{tr}(\alpha_E) = \mathrm{tr}(\alpha_F) \text{ for all } \alpha \in R.$$

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

$$\mathrm{tr}(e_E) = n\dim_k(V) \quad \text{and} \quad \mathrm{tr}(e_F) = m\dim_k(V).$$

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

$$\rho : G \to \mathrm{End}_k(E) \quad \text{and} \quad \rho' : G \to \mathrm{End}_k(F)$$

(so ρ and ρ' map G into the multiplicative monoid of End_k). Assume that $\mathrm{tr}\ \rho(\sigma) = \mathrm{tr}\ \rho'(\sigma)$ for all $\sigma \in G$. Then ρ and ρ' are isomorphic. Indeed, we let $R = k[G]$, so that ρ and ρ' extend to representations of R. By linearity, one has that $\mathrm{tr}\ \rho(\alpha) = \mathrm{tr}\ \rho'(\alpha)$ 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 $R = \mathrm{Mat}_n(k)$ 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

$$R_i = \sum_{L \simeq L_i} L$$

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 $i = 1, \ldots, s$, so that we write

$$1 = e_1 + \cdots + e_s.$$

For any $x \in R$, write

$$x = \sum_{i \in I} x_i, \qquad x_i \in R_i.$$

For $j = 1, \ldots, s$ we have $e_j x = e_j x_j$ and also

$$x_j = 1 \cdot x_j = e_1 x_j + \cdots + e_s x_j = e_j x_j.$$

Furthermore, $x = e_1 x + \cdots + e_s x$. This proves that there is no index i other than $i = 1, \ldots, s$ 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 $R = R_1 + \cdots + R_s$ is direct, and furthermore, e_i is a unit element for R_i, which is therefore a ring. Since

$R_iR_j = 0$ 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 $L_1, \ldots, L_s$. 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 $1 = e_1 + \cdots + e_s$, and $R_i = Re_i$. We have $e_ie_j = 0$ 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*

$$E = \bigoplus_{i=1}^{s} R_iE = \bigoplus_{i=1}^{s} e_iE,$$

and R_iE 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 $L_iV = V$ for some i. By a previous lemma, we have $L_i \approx V$. Hence E is the direct sum of $E_1, \ldots, E_s$. It is then clear that $R_iE = E_i$.

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 $\mathrm{End}_k(E)$. 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

$$x \mapsto (xv_1, \ldots, xv_n)$$

is a R-homomorphism of R into E, and is an injection since R is contained in $\mathrm{End}_k(E)$. 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 $\psi \in \mathrm{End}_R(R)$ 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

$$LR = \bigoplus_{j=1}^{m} L_j, \qquad L = L_1.$$

Let M be a simple left ideal. We have a direct sum decomposition $R = L \oplus L'$. Let $\pi : R \to L$ be the projection. It is an R-endomorphism. Let $\sigma : L \to M$ be an isomorphism (it exists by Theorem 4.3). Then $\sigma \circ \pi : R \to R$ is an R-endomorphism. By the lemma, there exists $\alpha \in R$ such that

$$\sigma \circ \pi(x) = x\alpha \quad \text{for all} \quad x \in R.$$

Apply this to elements $x \in L$. We find

$$\sigma(x) = x\alpha \quad \text{for all} \quad x \in L.$$

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, $R' = \mathrm{End}_R(L)$ and $R'' = \mathrm{End}_{R'}(L)$. Then the natural map $\lambda : R \to R''$ is an isomorphism.*

Proof. The kernel of λ is a two-sided ideal, so λ 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

$$R \to R''$$

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 $R = \mathrm{End}_D(E)$. Then R is simple and E is a simple R-module. Furthermore, $D = \mathrm{End}_R(E)$.*

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 $\{v_1, \ldots, v_m\}$ be a basis of E over D. The map

$$\alpha \mapsto (\alpha v_1, \ldots, \alpha v_m)$$

of R into $E^{(m)}$ is an R-homomorphism of R into $E^{(m)}$, and is injective. Given $(w_1, \ldots, w_m) \in E^{(m)}$, 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 $D = \mathrm{End}_R(E)$. 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 $\varphi \in \mathrm{End}_R(E)$. 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 $R = \mathrm{End}_k(E)$. 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 $R = \mathrm{End}_k(E)$ with the ring of matrices $\mathrm{Mat}_m(k)$, once a basis of E is selected. In that case, we can take the simple left ideals to be the ideals L_i $(i = 1, \ldots, m)$ 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 $M \in \mathrm{Mat}_m(k)$ commutes with all elements of $\mathrm{Mat}_m(k)$, 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 $N = \mathrm{Rad}(R)$.

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

$$\sigma(x \otimes a) = \sigma x \otimes a \quad \text{for} \quad x \in K \quad \text{and} \quad a \in A.$$

Let N be the radical of $K \otimes A$. Since N is nilpotent, it follows that σN is also nilpotent for all $\sigma \in G$, whence $\sigma N = N$ because N is the maximal nilpotent ideal (Exercise 5). Let $\{\alpha_1, \ldots, \alpha_m\}$ 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

$$\mathrm{trace}((y \otimes 1)\xi) = \sum \sigma\xi = \sum \mathrm{Tr}(yx_i) \otimes \alpha_i = \sum 1 \otimes \alpha_i \mathrm{Tr}(yx_i)$$

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 $A \approx \mathrm{End}_k(V)$ and $B \approx \mathrm{End}_k(W)$ where V, W are finite dimensional vector spaces over k, and there is a natural isomorphism*

$$A \otimes_k B \approx \mathrm{End}_k(V \otimes_k W) \approx \mathrm{End}_k(V) \otimes_k \mathrm{End}_k(W).$$

Proof. The formula is a special case of Theorem 2.5 of Chapter XVI, and the isomorphisms $A \approx \mathrm{End}_k(V)$, $B \approx \mathrm{End}_k(W)$ 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 $R'(E) = \mathrm{End}_R(E)$ and

$$R''(E) = \mathrm{End}_{R'}(E).$$

Let $\lambda: R \to R''$ be the natural homomorphism such that $\lambda_x(v) = xv$ for $x \in R$ and $v \in E$. If λ 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 $L \times \cdots \times L \to R$ 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 $(x_1, \ldots, x_n) \mapsto x_1a_1 + \cdots + x_na_n$ is a R-homomorphism of left module onto R.

If E is a generator, then there is a surjective homomorphism $E^{(n)} \to R$ (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 $\psi_w: R \oplus F \to F$ be the map $\psi_w(x + v) = xw$. Then any $f \in R''(R \oplus F)$ commutes with π_1, π_2, and each ψ_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 $E^{(n)} \to R$ 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 λ is obviously injective.

To prove that E is finitely generated over $R'(E)$, we have

$$R'(E)^{(n)} \approx \mathrm{Hom}_R(E^{(n)}, E) \approx \mathrm{Hom}_R(R, E) \oplus \mathrm{Hom}_R(F, E)$$

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 $\mathrm{Hom}_R(R, E)$ 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 $J_1 \supset J_2 \supset \cdots$ 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 $\oplus R/M_i$ 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 $r \geqq 1$ 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 $\mathrm{tr}(A) = \mathrm{tr}(I)$ for all $A \in G$, show that if $A_0 \in G$, $A_0 = I + N$, then $\mathrm{tr}(NX) = 0$ for all $X \in \mathrm{End}_k(E)$, 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 $\mathrm{End}_k(E)$. Let $a, b \in R$. Assume that

$$\mathrm{Ker}\, b_E \supset \mathrm{Ker}\, a_E,$$

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 $R = \mathrm{End}_D(E_0)$ and $E = E_0^{(n)}$. Let $v_1, \ldots, v_r \in E$ 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 $A \in \mathrm{End}_k(E)$. 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 $M = \mathrm{Mat}_n(A)$ 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: $T \to A_r$ 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

$$gL = A_r Q \qquad \text{(multiplication on the right)}.$$

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 $\mathrm{Mat}_n(F)$ is denoted by $\mathbf{c}(a)$, so $\mathbf{c}(a)M = aMa^{-1}$ for $M \in \mathrm{Mat}_n(F)$. (a) Show that $\mathfrak{n}$ is stable under this action. (b) Show that $\mathfrak{n}$ is semisimple under this action. More precisely, for $1 \leqq i < j \leqq n$, 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 $a = \mathrm{diag}(a_1, \ldots, a_n)$, we have

$$aE_{ij}a^{-1} = (a_i/a_j)E_{ij},$$

so the corresponding character χ_{ij} is given by $\chi_{ij}(a) = a_i/a_j$. (c) Show that $\mathrm{Mat}_n(F)$ is semisimple, and in fact is equal to $\mathfrak{d} \oplus \mathfrak{n} \oplus {}^t\mathfrak{n}$, 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

$$R[G] \to \mathrm{End}_R(E)$$

induces a group-homomorphism

$$G \to \mathrm{Aut}_R(E),$$

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 $\rho : G \to \mathrm{Aut}_R(E)$, we can extend ρ 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 ρ has been extended to a ring-homomorphism of $R[G]$ into $\mathrm{End}_R(E)$. We say that ρ is **faithful** on G if the map $\rho : G \to \mathrm{Aut}_R(E)$ is injective. The extension of ρ to $R[G]$ may not be faithful, however.

Given a representation of G on E, we often write simply σx instead of $\rho(\sigma)x$, whenever we deal with a fixed representation throughout a discussion.

An R-module E, together with a representation ρ, 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 $f : E \to F$ 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 $f : E \to F$, 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 $F \to F/f(E)$ is a G-homomorphism.

By a **trivial** representation $\rho : G \to \mathrm{Aut}_R(E)$, 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, $\mathrm{Hom}_R(E, F)$ is a G-module under the action defined for $f \in \mathrm{Hom}_R(E, F)$ by

$$([\sigma]f)(x) = \sigma f(\sigma^{-1}x).$$

The conditions for an operation are trivially verified. Note the σ^{-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 $\mathrm{Hom}_R(E, R) = E^\vee$ is the dual module. In the terminology of representations, if $\rho\colon G \to \mathrm{Aut}_R(E)$ is a representation of G on E, then the action we have just described gives a representation denoted by

$$\rho^\vee : G \to \mathrm{Aut}_R(E^\vee),$$

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 ρ 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

$$M^\vee = {}^tM^{-1}. \tag{1}$$

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

$$E^\vee \otimes F \approx \mathrm{Hom}_R(E, F) \tag{2}$$

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 $\mathrm{inv}_G(E) = R$-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

$$\mathrm{inv}_G(E^\vee \otimes F) \approx \mathrm{Hom}_G(E, F). \tag{3}$$

If $\rho\colon G \to \mathrm{Aut}_R(E)$ and $\rho'\colon G \to \mathrm{Aut}_R(E')$ 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** $\mathrm{Tr}_G\colon E \to E$ which is an R-homomorphism, namely

$$\mathrm{Tr}_G(x) = \sum_{\sigma \in G} \sigma x.$$

We observe that $\mathrm{Tr}_G(x)$ lies in $\mathrm{inv}_G(E)$, i.e. is fixed under the operation of all elements of G. This is because

$$\tau \,\mathrm{Tr}_G(x) = \sum_{\sigma \in G} \tau\sigma x,$$

and multiplying by τ on the left permutes the elements of G.

In particular, if $f\colon E \to F$ is an R-homomorphism of G-modules, then $\mathrm{Tr}_G(f)\colon E \to F$ 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 φ, ψ are G-homomorphisms. Then

$$\mathrm{Tr}_G(\psi \circ f \circ \varphi) = \psi \circ \mathrm{Tr}_G(f) \circ \varphi.$$

Proof. We have

$$\mathrm{Tr}_G(\psi \circ f \circ \varphi) = \sum_{\sigma \in G} \sigma(\psi \circ f \circ \varphi) = \sum_{\sigma \in G} (\sigma\psi) \circ (\sigma f) \circ (\sigma\varphi)$$

$$= \psi \circ \left(\sum_{\sigma \in G} \sigma f \right) \circ \varphi = \psi \circ \mathrm{Tr}_G(f) \circ \varphi.$$

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 $\pi : E \to F$ 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

$$0 \to F \underset{\varphi}{\overset{j}{\rightleftarrows}} E$$

such that j is the inclusion, and $\varphi \circ j = \mathrm{id}$. 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 $\rho : k[G] \to \operatorname{End}_k(E)$ be a representation. By the **character** χ_ρ of the representation, we shall mean the k-valued function

$$\chi_\rho : k[G] \to k$$

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 χ_E instead of χ_ρ.

We also call E the **representation space** of ρ.

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 χ_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 ρ, φ of G on spaces E, F are **isomorphic** if there is a G-isomorphism between E and F. We then see that if ρ, φ 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 σ 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 σ 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 ${}^tM^{-1}$ 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 $\geqq 0$.*

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 χ_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*

$$\chi = \sum_{i=1}^{s} n_i \chi_i, \qquad n_i \in \mathbf{Z}, n_i \geqq 0,$$

where $\chi_1, \ldots, \chi_s$ 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 χ. 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 $n_1, \ldots, n_s$. Namely, n_i is the number of times that L_i occurs (up to an isomorphism) in the representation space of χ, 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 χ_i in χ. In both corollaries, we continue to assume that k has characteristic 0.

Corollary 2.4. *As functions of G into k, the simple characters*

$$\chi_1, \ldots, \chi_s$$

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 σ be a generator of G. Let

$$e_1 = \frac{1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1}}{p}, \qquad e_2 = 1 - e_1.$$

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 ζ 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 $e_1'^2 = e_1'$, 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 $G \to k^*$.

Assume that E is a 1-dimensional vector space over k. Let

$$\rho : G \to \mathrm{Aut}_k(E)$$

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 σ 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 $\chi : G \to k^*$ 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 $\chi : G \to k^*$ 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 χ.

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 χ 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 χ 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 σ. Then H is a cyclic subgroup. A representation of G having character χ 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 $f: G \to k$ 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

$$\operatorname{tr}(MM'M^{-1}) = \operatorname{tr}(M').$$

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 σ is conjugate to σ_0, that is, if there exists an element τ 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 σ is conjugate to σ_0, and this means that we can write

$$\alpha = \sum_{\gamma} a_\gamma \gamma$$

where the sum is taken over all conjugacy classes γ.

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

$$R_i \approx \mathrm{End}_k(L_i).$$

We let

$$d_i = \dim_k L_i.$$

Then

$$\boxed{d_i^2 = \dim_k R_i \quad \text{and} \quad \sum_{i=1}^{s} d_i^2 = n.}$$

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 $\gamma_1, \ldots, \gamma_s$ and the unit elements $e_1, \ldots, e_s$ form bases of the center of $k[G]$.*

The number of elements in γ_i will be denoted by h_i. The number of elements in a conjugacy class γ will be denoted by h_γ. 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 χ_{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 χ_{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 $1 = \sigma_1, \ldots, \sigma_n$ 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 σ permutes $\sigma_1, \ldots, \sigma_n$, and it is immediately clear that all diagonal elements in the matrix representing σ 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 $e_1, \ldots, e_s$ (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*

$$e_i = \sum_{\tau \in G} a_\tau \tau, \qquad a_\tau \in k.$$

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 $\chi_1, \ldots, \chi_s$ 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 $d_i | n$ 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 ζ be a primitive m-th root of unity, and let M be the module over $\mathbf{Z}$ generated by the finite number of elements $\zeta^\nu \sigma e_i$ ($\nu = 0, \ldots, m-1$ 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 $e_1, \ldots, e_s$ 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 $X_R(G) \times X_R(G) \to R$, 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 χ_i and χ_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*

$$X_R(G) \times X_R(G) \to R,$$

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 $\gamma_1, \ldots, \gamma_s$ 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 α^- 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 α by e_i and β by an element τ 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 $\gamma_1, \ldots, \gamma_s$ 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*

$$Z_R(G) \times Z(G) \to R$$

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 γ_i when G operates by conjugation), and hence h_i divides n. The extension of our pairing as stated is obvious, since $\gamma_1, \ldots, \gamma_s$ 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 $\{v_1, \ldots, v_s\}$ be an orthogonal basis for this module. If

$$v = a_1 v_1 + \cdots + a_s v_s$$

with $a_i \in R$, then we call $a_1, \ldots, a_s$ 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 $\gamma_1, \ldots, \gamma_s$ is a Fourier expansion.

Theorem 5.5. *The conjugacy classes $\gamma_1, \ldots, \gamma_s$ 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*

$$Z_R(G) \times Z_R(G) \to R.$$

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 γ_i. But $\{\gamma_1, \ldots, \gamma_s\}$ 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 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*

$$Z_R(G) \times Z_R(G) \to R$$

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 $\gamma_1, \ldots, \gamma_s$ form an orthogonal basis for $Z_R(G)$. If R contains $1/n$, then $e_1, \ldots, e_s$ 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 α, β 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 $\gamma_1, \ldots, \gamma_s$ 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 $\gamma_1, \ldots, \gamma_s$ 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

$$G \to \mathrm{Aut}_k(E).$$

After selecting a basis of E, we get a representation of G by $d \times d$ matrices. If $\{v_1, \ldots, v_d\}$ is the basis, then we have the dual basis $\{\lambda_1, \ldots, \lambda_d\}$ such that $\lambda_i(v_j) = \delta_{ij}$. If an element σ of G is represented by a matrix $(\rho_{ij}(\sigma))$, then each coefficient $\rho_{ij}(\sigma)$ is a function of σ, 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 λ 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*

$$\varphi : E \to F$$

be a homomorphism. Then either $\varphi = 0$ or φ is an isomorphism.

Proof. Indeed, the kernel of φ and the image of φ 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 λ 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 μ 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 μ.

As a corollary, we see that if χ, ψ 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 ρ 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 $\mathrm{End}_{G,k}(E)$ 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 λ be a functional on E, and let $x \in E$. Let $\varphi_{\lambda,x} \in \mathrm{End}_k(E)$ be the endomorphism such that*

$$\varphi_{\lambda,x}(y) = \lambda(y)x.$$

Then $\mathrm{tr}(\varphi_{\lambda,x}) = \lambda(x)$.

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 λ. If $\lambda(x) = 0$, we pick a basis of E consisting of a basis for the kernel of λ, 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 $\rho: G \to \mathrm{Aut}_k(E)$ 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 λ, μ 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 $n \cdot \operatorname{tr}(\varphi_{\lambda, y})$ by Lemma 5.10, and also to dc. Taking λ, 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 χ 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 χ 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 $\chi_1, \ldots, \chi_s$ 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 χ_{reg} with χ_i for $i = 1, \ldots, s$ 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 χ_i, and let ρ_i be the representation of G or $k[G]$ on E_i. For $\alpha \in k[G]$ we let $\rho_i(\alpha) : E_i \to E_i$ be the map such that $\rho_i(\alpha)x = \alpha x$ for all $x \in E_i$.

Proposition 5.14. *We have*

$$\rho_i(e_i) = \text{id} \quad \textit{and} \quad \rho_i(e_j) = 0 \quad \textit{if } i \neq j.$$

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 χ_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 $\rho^{(i)}_{v,\mu}$ be the coefficient functions of this matrix, $i = 1, \ldots, s$ and $v, \mu = 1, \ldots, d_i$. Then the functions $\rho^{(i)}_{v,\mu}$ form an orthogonal basis for the space of all functions on G, and hence for any function f on G we have*

$$f = \sum_{i=1}^{s} \sum_{v,\mu} \frac{1}{d_i} \langle f, \rho^{(i)}_{v,\mu} \rangle \rho^{(i)}_{v,\mu}.$$

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** χ 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 $m_i \geqq 0$ 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 χ be an effective character in $X(G)$. Then χ is simple over $\mathbf{C}$ if and only if $\|\chi\|^2 = 1$, or alternatively,*

$$\sum_{\sigma \in G} |\chi(\sigma)|^2 = \#(G).$$

(b) *Let χ, ψ be effective characters in $X(G)$, and let E, F be their representation spaces over $\mathbf{C}$. Then*

$$\langle \chi, \psi \rangle_G = \dim \operatorname{Hom}_G(E, F).$$

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 χ_i over $\mathbf{C}$, then by Schur's lemma

$$\dim \operatorname{Hom}_G(E_i, E_i) = 1 \text{ and } \dim \operatorname{Hom}_G(E_i, E_j) = 0 \text{ for } i \neq j.$$

Hence $\dim \operatorname{Hom}_G(E, F) = \sum m_i q_i$, 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 $\dim_k \operatorname{inv}_G(E^\vee \otimes F)$.*
(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

$$X_R(G) \times X_R(G) \to R.$$

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

$$\mathrm{res}_S^G : X_R(G) \to X_R(S)$$

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,

$$\mathrm{ind}_S^G : X_R(S) \to X_R(G),$$

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**

$$g^G(\sigma) = \mathrm{ind}_S^G(g)(\sigma) = \frac{1}{(S:1)} \sum_{\tau \in G} g_S(\tau\sigma\tau^{-1}).$$

Then $\mathrm{ind}_S^G(g)$ is a class function on G. It is clear that 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*

$$\langle \mathrm{ind}_S^G(g), f\rangle_G = \langle g, \mathrm{Res}_S^G(f)\rangle_S.$$

(ii) $\mathrm{Ind}_S^G(g)f = \mathrm{ind}_S^G(gf_S)$.

(iii) *If $T \subset S \subset G$ are subgroups of G, then*

$$\mathrm{ind}_S^G \circ \mathrm{ind}_T^S = \mathrm{ind}_T^G.$$

(iv) *If $\sigma \in G$ and g^σ is defined by $g^\sigma(\tau^\sigma) = g(\tau)$, where $\tau^\sigma = \sigma^{-1}\tau\sigma$, then*

$$\mathrm{ind}_S^G(g) = \mathrm{ind}_{S^\sigma}^G(g^\sigma).$$

(v) *If ψ is an effective character of S then $\mathrm{ind}_S^G(\psi)$ 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 τ 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 (σ, τ) 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 $\geqq 0$ because $\mathrm{res}_S^G(\chi)$ is an effective character of S. Therefore the scalar product

$$\langle \psi, \mathrm{res}_S^G(\chi) \rangle_S$$

is $\geqq 0$. Hence ψ^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 $\bar{c}_1, \ldots, \bar{c}_r$ 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*

$$\mathrm{ind}_S^G(g)(\xi) = \sum_{i=1}^{r} g_S(\bar{c}_i \xi \bar{c}_i^{-1}).$$

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

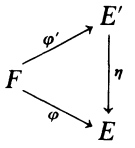
$$G = \bigcup S\bar{c}_i \quad \text{and} \quad S = \bigcup T\bar{d}_j$$

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

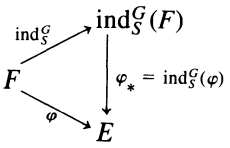
Let G be a group and S a subgroup of finite index. Let F be an S-module. We consider the category $\mathfrak{C}$ whose objects are S-homomorphisms $\varphi : F \to E$ of F into a G-module E. (We note that a G-module E can be regarded as an S-module by restriction.) If $\varphi' : F \to E'$ is another object in $\mathfrak{C}$, we define a morphism $\varphi' \to \varphi$ in $\mathfrak{C}$ to be a G-homomorphism $\eta : E' \to E$ making the following diagram commutative:



A universal object in $\mathfrak{C}$ is determined up to a unique G-isomorphism. It will be denoted by

$$\mathrm{ind}_S^G : F \to \mathrm{ind}_S^G(F).$$

We shall prove below that a universal object always exists. If $\varphi : F \to E$ 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 φ is an inclusion. We shall then call this particular module $\mathrm{ind}_S^G(F)$ **the** G-module **induced** by F. In particular, given an S-homomorphism $\varphi: F \to E$ into a G-module E, there is a unique G-homomorphism $\varphi_*: \mathrm{ind}_S^G(F) \to E$ making the following diagram commutative:



The association $\varphi \mapsto \mathrm{ind}_S^G(\varphi)$ then induces an isomorphism

$$\boxed{\mathrm{Hom}_G(\mathrm{ind}_S^G(F), E) \approx \mathrm{Hom}_S(F, \mathrm{res}_S^G(E)),}$$

for an S-module F and a G-module E. We shall see in a moment that ind_S^G is a functor from $\mathrm{Mod}(S)$ to $\mathrm{Mod}(G)$, 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

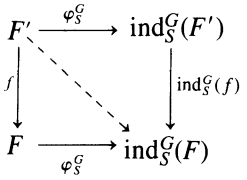
$$\mathrm{ind}^G(F)$$

for the induced module.

Let $f : F' \to F$ be an S-homomorphism. If

$$\varphi_S^G : F' \to \mathrm{ind}_S^G(F')$$

is a G-module induced by F', then there exists a unique G-homomorphism $\mathrm{ind}_S^G(F') \to \mathrm{ind}_S^G(F)$ making the following diagram commutative:



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* 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:

ind_S^G *commutes with direct sums: If we have an* S*-direct sum* $F \oplus F'$*, then*

$$\mathrm{ind}_S^G(F \oplus F') \approx \mathrm{ind}_S^G(F) \oplus \mathrm{ind}_S^G(F'),$$

the direct sum on the right being a G*-direct sum.*

If $f, g : F' \to F$ *are* S*-homomorphisms, then*

$$\mathrm{ind}_S^G(f + g) = \mathrm{ind}_S^G(f) + \mathrm{ind}_S^G(g).$$

If $T \subset S \subset G$ *are subgroups of* G*, and* F *is a* T*-module, then*

$$\mathrm{ind}_S^G \circ \mathrm{ind}_T^S(F) \approx \mathrm{ind}_T^G(F).$$

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 $f: G \to F$ 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 $\varphi: F \to M_G^S(F)$ 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 φ is an S-homomorphism, $\varphi: F \to M_G^S(F)$ is universal, and φ is injective. The image of φ 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 φ is an S-homomorphism, and it is immediately clear that φ 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 φ 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 $\{\bar{c}_1^{-1}, \ldots, \bar{c}_r^{-1}\}$ 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 presceding 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 $G \to \mathrm{Aut}_R(E)$, 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 $\mathrm{ind}_S^G(F)$. Then we deal with the category $\mathfrak{C}$ 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 $\{\lambda_1, \ldots, \lambda_r\}$ 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 $\varphi : F \to E$ be the inclusion mapping. Then φ is universal in our category $\mathfrak{C}$, 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 $\varphi' : F \to E'$ be an S-homomorphism into a G-module E'. We define

$$h : E \to E'$$

by the rule

$$h(\lambda_1 x_1 + \cdots + \lambda_r x_r) = \lambda_1 \varphi'(x_1) + \cdots + \lambda_r \varphi'(x_r)$$

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 σ and i, and $\tau_{\sigma, i}$ is an element of S, also

depending on σ, 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 φ' 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 ψ 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 χ of E is equal to the induced character ψ^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 ψ_0 is the extension of ψ to G obtained by setting $\psi_0(\sigma) = 0$ if $\sigma \notin S$.

Proof. Let $\{w_1, \ldots, w_m\}$ be a basis for F over k. We know that

$$E = \bigoplus \bar{c}^{-1}F.$$

Let σ be an element of G. The elements $\{\overline{c\sigma}^{-1}w_j\}_{c,j}$ form a basis for E over k.

We observe that $\bar{c}\sigma\overline{c\sigma}^{-1}$ is an element of S because

$$S\bar{c}\sigma = Sc\sigma = S\overline{c\sigma}.$$

We have

$$\sigma(\overline{c\sigma}^{-1}w_j) = \bar{c}^{-1}(\bar{c}\sigma\overline{c\sigma}^{-1})w_j.$$

Let

$$(\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}$$

be the components of the matrix representing the effect of $\bar{c}\sigma\overline{c\sigma}^{-1}$ on F with respect to the basis $\{w_1, \ldots, w_m\}$. Then the action of σ on E is given by

$$\begin{aligned}\sigma(\overline{c\sigma}^{-1}w_j) &= \bar{c}^{-1}\sum_\mu (\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}w_\mu \\ &= \sum_\mu (\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}(\bar{c}^{-1}w_\mu).\end{aligned}$$

By definition,

$$\chi(\sigma) = \sum_{c\sigma = c}\sum_j (\bar{c}\sigma\overline{c\sigma}^{-1})_{jj}.$$

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 γ 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 γ.

Lemma 7.5. *The elements $\{\tau_\gamma\gamma\}$ 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 γ represent distinct double cosets,

whence τ_γ 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 γF either according to the formal definition above, or according to the operation of G. The two are naturally isomorphic (essentially equal). We shall write

$$[\gamma] : F \to \gamma F \text{ or } [\gamma]F$$

for the above isomorphism from the S-module F to the $[\gamma]S$-module γF. 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*

$$\operatorname{res}_H^G \circ \operatorname{ind}_S^G \approx \bigoplus_\gamma \operatorname{ind}_{H\cap[\gamma]S}^H \circ \operatorname{res}_{H\cap[\gamma]S}^{[\gamma]S} \circ [\gamma]$$

where the direct sum is taken over double coset representatives γ.

Proof. The induced module $\operatorname{ind}_S^G(F)$ is simply the direct sum

$$\operatorname{ind}_S^G(F) = \bigoplus_{\gamma,\tau_\gamma} \tau_\gamma \gamma F$$

by Lemma 7.5, which gives us coset representatives of S in G, and Theorem 7.3. On the other hand, for each γ, the module

$$\bigoplus_{\tau_\gamma} \tau_\gamma \gamma F$$

is a representation module for the induced representation from $H\cap[\gamma]S$ on γF to H. Taking the direct sum over γ, 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

Hom_G, $E^\vee$, and the tensor product. Let

$$\lambda : E \to \lambda E$$

by a R-isomorphism. Then interpreting elements of G as endomorphisms of E we obtain a group $\lambda G\lambda^{-1}$ operating on λE. We shall also write $[\lambda]G$ instead of $\lambda G\lambda^{-1}$. Let E_1, E_2 be (G, R)-modules. Let $\lambda_1 : E_i \to \lambda_i E_i$ be R-isomorphisms. Then we have a natural R-isomorphism

$$\lambda_2 \mathrm{Hom}_G(E_1, E_2)\lambda_1^{-1} = \mathrm{Hom}_{\lambda_2 G \lambda_1^{-1}}(\lambda_1 E_1, \lambda_2 E_2), \tag{1}$$

and especially

$$[\lambda]\mathrm{Hom}_G(E, E) = \mathrm{Hom}_{[\lambda]G}(\lambda E, \lambda E).$$

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 σ, $\tau \in G$. *Suppose that* $\sigma^{-1}\tau$ lies in the double coset $D = H\gamma S$. Then we have an R-isomorphism

$$\mathrm{Hom}_{[\sigma]H \cap [\tau]S}([\sigma]F_1, [\tau]F_2) \approx \mathrm{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2). \tag{2}$$

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

$$M_D(F_1, F_2) = \mathrm{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2)$$

where γ 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*

$$\mathrm{Hom}_G(\mathrm{ind}_H^G(F_1), \mathrm{ind}_S^G(F_2)) \approx \bigoplus_D M_D(F_1, F_2),$$

where the direct sum is taken over all double cosets $H\gamma S = D$.

Proof. We have the isomorphisms:

$$\begin{aligned}
\mathrm{Hom}_G(\mathrm{ind}_H^G(F_1), \mathrm{ind}_S^G(F_2)) &\approx \mathrm{Hom}_H(F_1, \mathrm{res}_H^G \circ \mathrm{ind}_S^G(F_2)) \\
&\approx \bigoplus_\gamma \mathrm{Hom}_H(F_1, \mathrm{ind}_{H \cap [\gamma]S}^H \circ \mathrm{res}_{H \cap [\gamma]S}^{[\gamma]S} \circ [\gamma]F_2) \\
&\approx \bigoplus_\gamma \mathrm{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2)
\end{aligned}$$

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 γ 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 γ. Let χ be an effective character of H and ψ an effective character of S. Then*

$$\langle \mathrm{ind}_H^G(\chi), \mathrm{ind}_S^G(\psi)\rangle_G = \sum_\gamma \langle \chi, [\gamma]\psi\rangle_{H\cap[\gamma]S}.$$

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 ψ be an effective character of S. Then $\mathrm{ind}_S^G(\psi)$ is irreducible if and only if ψ 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 ψ 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 $\mathrm{ind}_S^G(F)$ 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*

$$\mathrm{ind}_S^G(F^\vee) \approx (\mathrm{ind}_S^G(F))^\vee.$$

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 $\mathrm{ind}_S^G(F)$ as

$$\mathrm{ind}_S^G(F) = \bigoplus \lambda_i F.$$

We may select $\lambda_1 = 1$ (unit element of G). There is a unique R-homomorphism

$$f : F^\vee \to (\mathrm{ind}_S^G(F))^\vee$$

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

$$f([\sigma]\varphi)(\lambda_i x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \sigma(\varphi(\sigma^{-1}x)) & \text{if } i = 1. \end{cases}$$

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

$$[\sigma](f(\varphi))(\lambda_1 x) = \sigma f(\varphi)(\sigma^{-1}\lambda_i x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \sigma(\varphi(\sigma^{-1}x)) & \text{if } i = 1. \end{cases}$$

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

$$\operatorname{ind}_S^G(f) : \operatorname{ind}_S^G(F^\vee) \to (\operatorname{ind}_S^G(F))^\vee,$$

which must be an isomorphism because f was an isomorphism on its image, the λ_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*

$$\operatorname{ind}_S^G(\operatorname{res}_S(E) \otimes F) \approx E \otimes \operatorname{ind}_S^G(F).$$

Proof. The G-module $\operatorname{ind}_S^G(F)$ contains F as a summand, because it is the direct sum $\bigoplus \lambda_i F$ with left coset representatives λ_i as in Theorem 7.3. Hence we have a natural S-isomorphism

$$f : \operatorname{res}_S(E) \otimes F \xrightarrow{\approx} E \otimes \lambda_1 F \subset E \otimes \operatorname{ind}_S^G(F).$$

taking the representative λ_1 to be 1 (the unit element of G). By the universal property of induction, there is a G-homomorphism

$$\operatorname{ind}_S^G(f) : \operatorname{ind}_S^G(\operatorname{res}_S(E) \otimes F) \to E \otimes \operatorname{ind}_S^G(F),$$

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

$$\operatorname{ind}_H^G(F) \approx \operatorname{ind}_{H'}^{G'}(F').$$

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

$$\text{(3)} \qquad \operatorname{ind}^G_{[\sigma]H\cap[\tau]S}([\sigma]F_1 \otimes [\tau]F_2) \approx \operatorname{ind}^G_{H\cap[\gamma]S}(F_1 \otimes [\gamma]F_2).$$

Theorem 7.12. *There is a G-isomorphism*

$$\operatorname{ind}^G_H(F_1) \otimes \operatorname{ind}^G_S(F_2) \approx \bigoplus_\gamma \operatorname{ind}^G_{H\cap[\gamma]S}(F_1 \otimes [\gamma]F_2),$$

where the sum is taken over double coset representatives γ.

Proof. We have:

$$\operatorname{ind}^G_H(F_1) \otimes \operatorname{ind}^G_S(F_2) \approx \operatorname{ind}^G_H(F_1 \otimes \operatorname{res}_H \operatorname{ind}^G_S(F_2)) \qquad \text{by Theorem 7.11}$$

$$\approx \bigoplus_\gamma \operatorname{ind}^G_H(F_1 \otimes \operatorname{ind}^H_{H\cap[\gamma]S} \operatorname{res}_{H\cap{}^{[\gamma]S}_{[\gamma]S}}([\gamma]F_2) \qquad \text{by Theorem 7.6}$$

$$\approx \bigoplus_\gamma \operatorname{ind}^G_H\left(\operatorname{ind}^H_{H\cap[\gamma]S}\left(\operatorname{res}^H_{H\cap[\gamma]S}(F_1) \otimes \operatorname{res}^{[\gamma]S}_{H\cap[\gamma]S}([\gamma]F_2)\right)\right) \qquad \text{by Theorem 7.7}$$

$$\approx \bigoplus_\gamma \operatorname{ind}^G_{H\cap[\gamma]S}(F_1 \otimes [\gamma]F_2) \qquad \text{by transitivity of induction}$$

where we view $F_1 \cap [\gamma]F_2$ 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 ψ be a character of H. Let ψ^G be the induced character. Then the multiplicity of 1_H in ψ is the same as the multiplicity of 1_G in ψ^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 θ_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 φ 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 χ, ψ 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 ψ 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

$$\begin{aligned} \sum_A \langle \psi, \lambda_A^G \rangle &= \sum_A \langle \psi | A, \lambda_A \rangle \\ &= \sum_A \langle \psi | A, \varphi(a)r_A - \theta_A \rangle \\ &= \sum_A \varphi(a)\psi(1) - \sum_A \frac{1}{a} \sum_{\sigma \text{ gen } A} a\psi(\sigma) \\ &= n\psi(1) - \sum_{\sigma \in G} \psi(\sigma). \end{aligned}$$

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 λ_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 λ_A with respect to a character of degree 1 are integers $\geqq 0$. Let ψ 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 ψ 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 ψ 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

$$\log(hR) \sim \log \mathbf{D}^{1/2} \text{ for } [k : \mathbf{Q}]/\log \mathbf{D} \to 0,$$

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 $G \to G/C$. If σ is a generator of $\bar{H}$, then an inverse image σ 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 ψ be its character. If $w \in E$ also generates a 1-dimensional H-space, with the same character ψ, 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_ψ the subspace of E generated by all 1-dimensional H-subspaces having the character ψ, 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 ψ. 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 τ 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_ψ 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 ψ_σ is the function on H given by $\psi_\sigma(\tau) = \psi(\sigma^{-1}\tau\sigma)$. This shows that σ maps F_ψ into F_{ψ_σ}. However, by symmetry, we see that σ^{-1} maps F_{ψ_σ} into F_ψ, and the two maps σ, σ^{-1} give inverse mappings between F_{ψ_σ} and F_ψ. Thus G permutes the spaces $\{F_\psi\}$.

Let $E' = GF_{\psi_0} = \sum \sigma F_{\psi_0}$ for some fixed ψ_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 ψ_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 $G \to \mathrm{Aut}_k(E)$. 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

$$E = \mathrm{ind}_{\bar{H}}^{\bar{G}}(F).$$

Let H be the inverse image of $\bar{H}$ in the natural map $G \to \bar{G}$. 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.

$$E = \mathrm{ind}_H^G(F),$$

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_α in our family. In other words,

$$V_R(G) = \sum_\alpha \operatorname{ind}_{H_\alpha}^G(X_R(H_\alpha)).$$

We could also say that $V_R(G)$ is the subgroup generated over R by all the characters induced from all the H_α.

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 σ is p-singular, τ is p-regular, and σ, τ commute. Indeed, if $p^r m$ is the period of x, with m prime to p, then $1 = vp^r + \mu m$ whence $x = (x^m)^\mu (x^{p^r})^\nu$ 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_α, 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 ζ is a primitive n-th root of unity. There exists a basis of R as a $\mathbf{Z}$-module, namely $1, \zeta, \ldots, \zeta^{N-1}$ for some integer N. This is a trivial fact, and we can take N to be the degree of the irreducible polynomial of ζ over $\mathbf{Q}$. This irreducible polynomial has leading coefficient 1, and

has integer coefficients, so the fact that

$$1, \zeta, \ldots, \zeta^{N-1}$$

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 $d.1_G$ belongs to V_R then $d.1_G$ belongs to $V_{\mathbf{Z}}$.*

Proof. We contend that $1, \zeta, \ldots, \zeta^{N-1}$ 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

$$V_R = V_{\mathbf{Z}} \oplus V_{\mathbf{Z}} \zeta \oplus \cdots \oplus V_{\mathbf{Z}} \zeta^{N-1}$$

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 σ is p-singular, and τ is p-regular, and σ, τ 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 ψ_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 $R = \mathbf{Z}[\zeta]$ be as before. If $a \in \mathbf{Z}$ and $a \in pR$ then $a \in p\mathbf{Z}$.*

Proof. This is immediate from the fact that R has a basis over $\mathbf{Z}$ 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 τ be p-regular in G, and let T be the cyclic subgroup generated by τ. Let C be the subgroup of G consisting of all elements commuting with τ. 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) $f(\sigma) \in \mathbf{Z}$ *for all* $\sigma \in G$.

(ii) $f(\sigma) = 0$ *if* σ *does not belong to the p-class of* τ.

(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 $\psi_1, \ldots, \psi_r$ be the simple characters of the cyclic group T, and assume that these are extended to $T \times P$ by composition with the projection:

$$T \times P \to T \to k^*.$$

We denote the extensions again by $\psi_1, \ldots, \psi_r$. 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

$$\psi(\tau y) = \psi(\tau) = (T : 1) \quad \text{for} \quad y \in P$$

$$\psi(\sigma) = 0 \quad \text{if} \quad \sigma \in TP, \quad \text{and} \quad \sigma \notin \tau P.$$

We contend that ψ^G satisfies our requirements.

First, it is clear that ψ 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 τP. The number $\mu(\sigma)$ is divisible by $(P : 1)$ because if an element x of G moves σ into τP by conjugation, so does every element of Px. Hence the values of ψ^G lie in $\mathbf{Z}$.

Furthermore, $\mu(\sigma) \neq 0$ only if σ is p-conjugate to τ, 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 τ 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_α). 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 γ 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 γ. 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 γ, 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_α. 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 γ, we can find a function f_γ in $V_R(G)$, whose values are 0 on elements outside γ, and $\not\equiv 0 \bmod p$ for elements of γ. 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_α. Let $n = n_0 p^r$ where n_0 is prime to p. Then the constant function $n_0 . 1_G$ belongs to $V_{\mathbf{Z}}(G)$.*

Proof. By Lemma 10.3, it suffices to prove that $n_0 . 1_G$ belongs to $V_R(G)$. Let f be as in Lemma 10.9. Then

$$n_0 . 1_G = n_0(1_G - f) + n_0 f.$$

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_α. Then $X(G) = V_{\mathbf{Z}}(G)$. Every character of G is a linear combination, with integer coefficients, of characters induced from subgroups H_α.*

Proof. Immediate from Lemma 10.10, since we can find functions $n_0 . 1_G$ 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_α belongs to $X(H_\alpha)$ for each α.*

Proof. Assume that the restriction of f to H_α is a character on H_α for each α. 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 $\{v_1, \ldots, v_m\}$ be a basis of E over k. Then

$$\{1 \otimes v_1, \ldots, 1 \otimes v_m\}$$

is a basis of E' over k'. Thus the matrices representing an element σ 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 simle 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 $R_\nu(k)R_\mu(k) = 0$ if $\nu \neq \mu$, 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 $E = L_\nu$ and $F = L_\mu$ with $\nu \neq \mu$. Then $R_\mu E = 0$. Hence $R_{\mu i} E_{k'} = 0$ for each $i = 1, \ldots, m(\mu)$. 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 $\chi_1, \ldots, \chi_{s(k)}$ 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 ζ_m is a primitive m-th root of unity.*

Proof. Let χ be the character of a representation of G over $\mathbf{C}$, i.e. an effective character. By Theorem 10.13, we can write

$$\chi = \sum_j c_j \operatorname{ind}_{S_j}^G(\psi_j), \qquad c_j \in \mathbf{Z},$$

the sum being taken over a finite number of subgroups S_j, and ψ_j being a 1-dimensional character of S_j. It is clear that each ψ_j is definable over $\mathbf{Q}(\zeta_m)$. Thus the induced character ψ_j^G is definable over $\mathbf{Q}(\zeta_m)$. Each ψ_j^G can be written

$$\psi_j^G = \sum_\mu d_{j\mu} \chi_\mu, \qquad d_{j\mu} \in \mathbf{Z}$$

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 χ as a linear combination of the simple characters over k is unique, and hence the coefficient

$$\sum_j c_j d_{j\mu}$$

is $\geqq 0$. 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

$$F[C_K] \subset \mathrm{Mat}_2(F)$$

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 α must lie in $F[C_K]$, for otherwise $\{1, \alpha\}$ would be linearly independent over $F[C_K]$, whence $\mathrm{Mat}_2(F)$ would be commutative, which is not the case. Since α is invertible, α 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

$$\psi, \psi' : H \to F^{s*}$$

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 α, 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 ψ, of the algebra $F[H]$ into K. Since $F[H]$ is semisimple, it follows that $\psi : F[H] \to K$ is an isomorphism. Hence ψ 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 ψ, ψ' are called the **(eigen)characters of the Cartan subgroup**. In the split case, if α 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 σ: $K \to K$ be the non-trivial automorphism. Let $\{\alpha, \sigma\alpha\}$ be a normal basis. With respect to this basis, the matrix of σ 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 α.

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 α 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 α 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

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}, \quad x \in F,$$

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 σ generates $\mathrm{Gal}(K/F)$, 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 σ. 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 = group of unipotent elements $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$;

B = 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 χ 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

$\mu : F^* \to C^*$ denotes a homomorphism. Then we obtain the character

$\mu \circ \det: G \to \mathbf{C}^*$,

which is 1-dimensional. Its values on representatives of the conjugacy classes are given in the following table.

Table 12.5(I)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
$\mu \circ \det$	$\mu(a)^2$	$\mu(a)^2$	$\mu(ad)$	$\mu \circ \det(\alpha)$

The stated values are by definition. The last value can also be written

$$\mu(\det \alpha) = \mu(N_{K/F}(\alpha)),$$

viewing α 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 μ. 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:

$\psi_\mu = \mathrm{res}_A(\mu \circ \det)$, and view ψ_μ therefore as a character on B. Thus

$$\psi_\mu\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \mu(ad).$$

We obtain the induced character

$$\psi_\mu^G = \mathrm{ind}_B^G(\psi_\mu).$$

Then ψ_μ^G is not simple. It contains $\mu \circ \det$, as one sees by Frobenius reciprocity:

$$\langle \mathrm{ind}_B^G \psi_\mu, \mu \circ \det \rangle_G = \langle \psi_\mu, \mu \circ \det \rangle_B = \frac{1}{\#(B)} \sum_{\beta \in B} |\mu \circ \det(\beta)|^2 = 1.$$

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)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
$\psi_\mu^G - \mu \circ \det$	$q\mu(a)^2$	0	$\mu(ad)$	$-\mu \circ \det(\alpha)$

Actually, one computes the values of ψ_μ^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:

$$\mathrm{ind}_H^G(\varphi)(\alpha) = \frac{1}{\#(H)} \sum_{\beta \in G} \varphi_H(\beta\alpha\beta^{-1})$$

where φ_H is the function equal to φ 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

$$\mathrm{ind}_B^G(\psi_\mu)\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \mu(a)^2,$$

which yields the stated value for the character χ. Using Table 12.4, one finds at once that $\sum |\chi(\beta)|^2 = \#(G)$, and hence;

A character χ 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

$\psi : A \to \mathbf{C}^*$ 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 ψ_1, ψ_2: $F^* \to \mathbf{C}^*$. In light of the isomorphism $B/U \approx A$, we view ψ has a character on B. Then we form the induced character

$$\psi^G = \mathrm{ind}_B^G(\psi) = \mathrm{ind}_B^G([w]\psi).$$

With ψ 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)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
ψ^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 ψ^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 β in the various conjugacy classes, and using Table 12.4, we find:

$$\sum_{\beta \in G} |\psi^G(\beta)|^2 = (q+1)^2(q-1) + (q-1)(q^2-1) + (q^2+q) \sum_{\alpha \in (A-F^*)/w} |\psi(\alpha) + \psi(\alpha^w)|^2.$$

The third term can be written

$$\frac{1}{2}(q^2+q) \sum_{\alpha \in A-F^*} (\psi(\alpha) + \psi(\alpha^w))(\psi(\alpha^{-1}) + \psi(\alpha^{-w}))$$

$$= \frac{1}{2}(q^2+q) \sum_{\alpha \in A-F^*} (1 + 1 + \psi(\alpha^{1-w}) + \psi(\alpha^{w-1})).$$

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 ψ, the character

$$\alpha \mapsto \psi(\alpha^{1-w}) \text{ for } \alpha \in A$$

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

$$\sum_{\beta \in G} |\psi^G(\beta)|^2 = (q+1)(q^2-1) + (q-1)(q^2-1) + q(q^2-1)(q-3)$$
$$= q(q-1)(q^2-1) = \#(G),$$

thus proving that ψ^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 ψ such that $[w]\psi \neq \psi$, divided by 2 because each pair ψ and $[w]\psi$ yields the same induced character ψ^G. The table of values shows that up to this coincidence, the induced characters are distinct.

Fourth type

$\theta : K^* \to \mathbf{C}^*$ 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

$$\theta^G = \operatorname{ind}_C^G(\theta) = \operatorname{ind}_C^G([w]\theta).$$

Let $\mu : F^* \to \mathbf{C}^*$ denote a homomorphism as in the first type. Let:

$\lambda : F^+ \to \mathbf{C}^*$ be a *non-trivial* homomorphism.

(μ, λ) = the character on ZU such that

$$(\mu, \lambda)\left(\begin{pmatrix} a & ax \\ 0 & a \end{pmatrix}\right) = \mu(a)\lambda(x).$$

$(\mu, \lambda)^G = \operatorname{ind}_{ZU}^G(\mu, \lambda)$.

A routine computation of the same nature that we have had previously gives the following values for the induced characters θ^G and $(\mu, \lambda)^G$.

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
θ^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 θ^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 μ. Thus we define:

$$\theta' = (\text{res}\,\theta, \lambda)^G - \theta^G = ([w]\theta)',$$

which is an effective character. A character θ' is said to be of **fourth type** if θ 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)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
θ' $\theta \neq [w]\theta$	$(q - 1)\theta(a)$	$-\theta(a)$	0	$-\theta(\alpha) - \theta(\alpha^w)$

We claim that the characters θ' of fourth type are simple.

To prove this, we evaluate

$$\sum_{\beta \in G} |\theta'(\beta)|^2 = (q - 1)^2(q - 1) + (q - 1)(q^2 - 1) + \frac{1}{2}(q^2 - q) \sum_{\alpha \in K^* - F^*} |\theta(\alpha) + \theta(\alpha^w)|^2.$$

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 θ' 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	ψ^G from pairs $\psi \neq [w]\psi$	$\frac{1}{2}(q - 1)(q - 2)$	$q + 1$
IV	θ' 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,
   (a) Show that there are three conjugacy classes.
   (b) There are two characters of dimension 1, on S_3/A_3.
   (c) 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.
   (d) 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 ρ be the representation of (d). Define ρ' by

   $$\rho'(\sigma) = \rho(\sigma) \text{ if } \sigma \text{ is even;}$$
   $$\rho'(\sigma) = -\rho(\sigma) \text{ if } \sigma \text{ is odd.}$$

   Show that ρ' is also irreducible, remains irreducible after tensoring with k^a, and is non-isomorphic to ρ. 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 $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{H} \approx \mathrm{Mat}_2(\mathbf{C})$ (2×2 complex matrices). Relate this to (b).

4. Let S be a normal subgroup of G. Let ψ be a simple character of S over $\mathbf{C}$. Show that $\mathrm{ind}_S^G(\psi)$ 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 ρ be an irreducible representation of G over $\mathbf{C}$. Prove that either the restriction of ρ 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 θ of H such that $\rho \approx \mathrm{ind}_H^G(\theta)$.

6. **Dihedral group D_{2n}.** There is a group of order $2n$ (n even integer $\geqq 2$) generated by two elements σ, τ such that

$$\sigma^n = 1,\ \tau^2 = 1, \quad \text{and} \quad \tau\sigma\tau = \sigma^{-1}.$$

It is called the **dihedral group**.

(a) Show that there are four representations of dimension 1, obtained by the four possible values ± 1 for σ and τ.

(b) Let C_n be the cyclic subgroup of D_{2n} generated by σ. For each integer $r = 0, \ldots, n-1$ let ψ_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 χ_r be the induced character. Show that $\chi_r = \chi_{n-r}$.

(c) Show that for $0 < r < n/2$ the induced character χ_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 $A^\wedge = \mathrm{Hom}(A, \mathbf{C}^*)$ 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 $\psi_1, \ldots, \psi_r$ be representatives of the orbits of H in $A^\wedge$, and let $H_i (i = 1, \ldots, r)$ be the isotropy group of ψ_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 ψ_i is thus extended to a character on G_i.

Let θ be a simple representation of H_i (on a vector space over $\mathbf{C}$). From $H_i = G_i/A$, view θ as a simple representation of G_i. Let

$$\rho_{i,\theta} = \mathrm{ind}_{G_i}^{G}(\psi_i \otimes \theta).$$

(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 ψ be the character of the corresponding representation of G on $\mathbf{C}[S]$.

(a) Let $\sigma \in G$. Show that $\psi(\sigma)$ = number of fixed points of σ 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 $\leqq (G : A)$.

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 $\mu : \mathbf{F}^* \to \mathbf{C}^*$ be a homomorphism and let $\psi_\mu : B \to \mathbf{C}^*$ be the homomorphism such that $\psi_\mu(\alpha) = \mu(a)$. Show that the induced character $\mathrm{ind}_B^G(\psi_\mu)$ 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 $G \to \mathrm{Aut}(V)$ 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 χ 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 σ, we have $\sigma^j \in C$.

15. Let G be a group and let H_1, H_2 be subgroups of finite index. Let ρ_1, ρ_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 $f: G \to \mathrm{Hom}_R(F_1, F_2)$ 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

$$\mathrm{Hom}_R(F_1^G, F_2^G) \xrightarrow{\sim} M_G(F_1, F_2).$$

    By F_i^G we have abbreviated $\mathrm{ind}_{H_i}^G(F_i)$.

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 ρ_1, ρ_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 ρ_1, ρ_2 are irreducible then $\rho_2 \otimes \rho_2$ is also irreducible. [*Hint*: Use Theorem 5.17.]

    (b) Let χ_1, χ_2 be the characters of ρ_1, ρ_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 $x_1, \ldots, x_r$ be distinct elements of P_1 (i.e. linear expressions in the variables $t_1, \ldots, t_n$)

and let $a_1, \ldots, a_r \in k$. If

$$a_1 x_1^v + \cdots + a_r x_r^v = 0$$

for all integers $v = 1, \ldots, r$ show that $a_i = 0$ for $i = 1, \ldots, r$. [*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_σ be an element of k. Show that if

$$\sum_{\sigma \in G} c_\sigma T^r(\sigma) = 0$$

for all integers $r \geqq 1$, 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 $G \to \mathrm{End}_k(E)$ be a faithful representation (i.e. injective), so that we identify G with a multiplicative subset of $\mathrm{End}_k(E)$. 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 $r \geqq 1$, 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 $\geqq 1$ 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 $f(1) \geqq 0$.

23. In this exercise, we assume the next chapter on alternating products. Let ρ 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 χ is the character of ρ, 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

$$-\frac{d}{dt} \log \sigma_t(\chi) = \sum_{n=1}^{\infty} \Psi^n(\chi) t^n \quad \text{and} \quad -\frac{d}{dt} \log \lambda_{-t}(\chi) = \sum_{n=1}^{\infty} \Psi^n(\chi) t^n.$$

(c) Show that

$$nS^n(\chi) = \sum_{r=1}^{n} \Psi^r(\chi) S^{n-r}(\chi) \quad \text{and} \quad n\bigwedge^n(\chi) = \sum_{r=1}^{\infty} (-1)^{r-1} \Psi^r(\chi) \bigwedge^{n-r}(\chi).$$

24. Let χ be a simple character of G. Prove that $\Psi^n(\chi)$ is also simple. (The characters are over $\mathbf{C}$.)

25. We now assume that you know §3 of Chapter XX.
    (a) Prove that the Grothendieck ring defined there for $\mathrm{Mod}_{\mathbf{C}}(G)$ is naturally isomorphic to the character ring $X(G)$.
    (b) Relate the above formulas with Theorem 3.12 of Chapter XX.
    (c) Read Fulton-Lang's *Riemann-Roch Algebra*, Chapter I, especially §6, and show that $X(G)$ is a λ-ring, with Ψ^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 $\rho : G \to \mathrm{Aut}(U)$. We then say that U is a G-object, and also that ρ is a representation of G in U. We say that G operates trivially if $\rho(G) = \mathrm{id}$. For simplicity, we omit the ρ from the notation. By a G-morphism $f : U \to V$ 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 $\pi_{U,G} : U \to U/G$ having the following universal property: If $f : U \to U'$ is a G-morphism, then there exists a unique morphism

$$f/G : U/G \to U'/G$$

    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 $f : U \to U'$ is a morphism, then we get a homomorphism

$$E(f) = f_* : E(U) \to E(U').$$

    (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 $F : U \to U$ a G-morphism. If $P_F(t) = \prod (t - \alpha_i)$ is the characteristic polynomial of the linear map $F_* : E(U) \to E(U)$, 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 χ be a simple character of G. Let d_χ be the dimension of the simple representation of G belonging to χ, and $n = \operatorname{ord}(G)$. 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 μ 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

$$-\frac{1}{N} \sum_{\mu=1}^{\infty} \operatorname{tr}(e_\chi \circ F_*^\mu)t^{\mu-1}.$$

Define $L_F(t, \chi, U/G)$ for any character χ 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 χ, χ' 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 ψ be a character of H. Let $W = U/H$, and let ψ^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 ψ be a character of G/H, and let χ be the character of G obtained by composing ψ with the canonical map $G \to G/H$. 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 χ is the character of G on V, show that χ is also the character on E, and that χ mod $\mathfrak{m}_\mathfrak{p}$ 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 $f: E^{(r)} \to F$ is said to be **alternating** if $f(x_1, \ldots, x_r) = 0$ 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

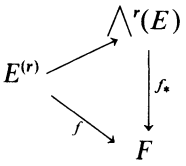
$$\bigwedge^r(E) = T^r(E)/\mathfrak{a}_r.$$

Then we have an r-multilinear map $E^{(r)} \to \bigwedge^r(E)$ (called canonical) obtained

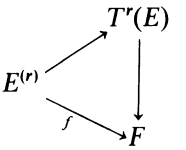
from the composition

$$E^{(r)} \to T^r(E) \to T^r(E)/\mathfrak{a}_r = \bigwedge^r(E).$$

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 $f : E^{(r)} \to F$ is such a map, there exists a unique linear map $f_* : \bigwedge^r(E) \to F$ such that the following diagram is commutative:



Our map f_* exists because we can first get an induced map $T^r(E) \to F$ making the following diagram commutative:



and this induced map vanishes on $\mathfrak{a}_r$, hence inducing our f_*.

The image of an element $(x_1, \ldots, x_r) \in E^{(r)}$ in the canonical map into $\bigwedge^r(E)$ will be denoted by $x_1 \wedge \cdots \wedge x_r$. It is also the image of $x_1 \otimes \cdots \otimes x_r$ in the factor homomorphism $T^r(E) \to \bigwedge^r(E)$.

In this way, $\bigwedge^r$ becomes a functor, from modules to modules. Indeed, let $u : E \to F$ be a homomorphism. Given elements $x_1, \ldots, x_r \in E$, we can map

$$(x_1, \ldots, x_r) \mapsto u(x_1) \wedge \cdots \wedge u(x_r) \in \bigwedge^r(F).$$

This map is multilinear alternating, and therefore induces a homomorphism

$$\bigwedge^r(u) : \bigwedge^r(E) \to \bigwedge^r(F).$$

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

$$A_r \times A_s \to A_{r+s}$$

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

$$A_r/\mathfrak{a}_r \times A_s/\mathfrak{a}_s \to A_{r+s}/\mathfrak{a}_{r+s},$$

and thus a bilinear map $A/\mathfrak{a} \times A/\mathfrak{a} \to A/\mathfrak{a}$, which obviously makes $A/\mathfrak{a}$ into a graded R-algebra.

We apply this to $T^r(E)$ 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 $y_1, \ldots, y_s \in E$ 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 $f : E \to F$ we obtain a map

$$\bigwedge(f) : \bigwedge(E) \to \bigwedge(F)$$

which is such that for $x_1, \ldots, x_r \in E$ 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 $\{v_1, \ldots, v_n\}$ be a basis of E over R. If $1 \leqq r \leqq n$, then $\bigwedge^r(E)$ is free over R, and the elements*

$$v_{i_1} \wedge \cdots \wedge v_{i_r}, \qquad i_1 < \cdots < i_r$$

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 multilinear alternating form f_a on E such that

$$f_a(v_1, \ldots, v_n) = a.$$

Consequently, there exists a unique linear map

$$\bigwedge^n(E) \to R$$

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 $1 \leqq r \leqq n$. 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 $(j) = (j_1, \ldots, j_r)$ such that $j_1 < \cdots < j_r$ and let $j_{r+1}, \ldots, j_n$ be those values of i which do not appear among $(j_1, \ldots, j_r)$. 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 $1 \leqq r \leqq n$.

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 $(1, \ldots, n)$.

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*

$$0 \to E' \to E \to E'' \to 0$$

be an exact sequence of free R-modules of finite ranks r, n, and s respectively. Then there is a natural isomorphism

$$\varphi : \bigwedge^r E' \otimes \bigwedge^s E'' \to \bigwedge^n E.$$

This isomorphism is the unique isomorphism having the following property. For elements $v_1, \ldots, v_r \in E'$ and $w_1, \ldots, w_s \in E''$, let $u_1, \ldots, u_s$ be liftings of $w_1, \ldots, w_s$ 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 φ having the desired effect. The value on the right of the above formula is independent of the choice of $u_1, \ldots, u_s$ lifting $w_1, \ldots, w_s$ by using the alternating property, so we obtain a homomorphism φ. Selecting in particular $\{v_1, \ldots, v_r\}$ and $\{w_1, \ldots, w_s\}$ to be bases of E' and E'' respectively, one then sees that φ 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 $\| \ \|$ 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 $\{e_1, \ldots, e_n\}$ 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 μ 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 $x_1, \ldots, x_n$ 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

$$\bigwedge_i^n E = \text{submodule of } \bigwedge^n E \text{ generated by all elements}$$

$$x_1' \wedge \cdots \wedge x_i' \wedge y_{i+1} \wedge \cdots \wedge y_n$$

$$\text{with } x_1', \ldots, x_i' \in E' \text{ viewed as submodule of } E.$$

Then we have a filtration

$$\bigwedge_i^n E \supset \bigwedge_{i+1}^n E.$$

Proposition 1.3. *There is a natural isomorphism*

$$\bigwedge^i E' \otimes \bigwedge^{n-i} E'' \to \bigwedge_i^n E / \bigwedge_{i+1}^n E.$$

Proof. Let $x_1'', \ldots, x_{n-i}''$ be elements of E'', and lift them to elements $y_1, \ldots, y_{n-i}$ of E. We consider the map

$$(x_1', \ldots, x_i', x_1'', \ldots, x_{n-i}'') \mapsto x_1' \wedge \cdots \wedge x_i' \wedge y_1 \wedge \cdots \wedge y_{n-i}$$

with the right-hand side taken mod $\bigwedge_{i+1}^n E$. Then it is immediate that this map factors through

$$\bigwedge^i E' \otimes \bigwedge^{n-i} E'' \to \bigwedge_i^n E / \bigwedge_{i+1}^n E,$$

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

$$\bigwedge E' \otimes \bigwedge E'' \to \bigwedge E,$$

which is graded, i.e. for $p = 0, \ldots, n$ we have

$$\bigwedge^p E' \otimes \bigwedge^{n-p} E'' \to \bigwedge^n E.$$

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 $L^\vee = \mathrm{Hom}_R(L, R)$, 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:

$$\mathbf{E} : 0 \to E_0 \to E_1 \to \cdots \to E_m \to 0.$$

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 $r \geqq 0$ 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

$$J = (j_1, \ldots, j_r) \text{ with } 1 \leqq j_1 < j_2 < \cdots < j_r \leqq p.$$

Let $A = (a_{ij})$. Let $1 \leqq r \leqq \min(p, q)$. Let $K = (k_1, \ldots, k_r)$ be another element of S_r^p. We *define*

$$A_{JK}^{(r)} = \begin{vmatrix} a_{j_1k_1} & a_{j_1k_2} & \cdots & a_{j_1k_r} \\ a_{j_2k_1} & a_{j_2k_2} & \cdots & a_{j_2k_r} \\ \vdots & \vdots & & \vdots \\ a_{j_rk_1} & a_{j_rk_2} & \cdots & a_{j_rk_r} \end{vmatrix}$$

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 $\{e_1, \ldots, e_p\}$ be a basis of R^p and $\{u_1, \ldots, u_q\}$ a basis of R^q. Then the elements

$$e_{j_1} \wedge \cdots \wedge e_{j_r} \qquad (j_1 < j_2 < \cdots < j_r)$$

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 1×1 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*

$$(AB)^{(r)} = A^{(r)}B^{(r)} \quad \textit{for} \quad r \geqq 0.$$

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 σ ranges over all permutations of the set.

For $r \geqq 0$ 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

$$I_r(A) = 0 \quad \text{for} \quad r > \min(p, q)$$

and the inclusions

$$R = I_0(A) \supset I_1(A) \supset I_2(A) \supset \cdots$$

By Proposition 10.1, we also have

$$I_r(AB) \subset I_r(A) \cap I_r(B). \tag{1}$$

Therefore, if $A = UBU'$ where U, U' are square matrices of determinant 1, then

$$I_r(A) = I_r(B). \tag{2}$$

Next, let E be an R-module. Let $x_1, \ldots, x_q$ be generators of E. Then we may form the matrix of relations $(a_1, \ldots, a_q) \in R^q$ 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:

$$I_r(x_1, \ldots, x_q) = I_r(x) = \text{ideal generated by } I_r(A) \text{ for all } A.$$

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

$$R = I_0(x) \supset I_1(x) \supset I_2(x) \supset \cdots$$
$$I_r(x) = 0 \quad \text{if} \quad r > q.$$

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 $R^q \to E \to 0$ be a representation of E as a quotient of R^q, and let $x_1, \ldots, x_q$ be the images of the unit vectors in R^q. Then $I_r(x)$ is the ideal generated by all values*

$$\lambda(w_1, \ldots, w_r)$$

where $w_1, \ldots, w_r \in \operatorname{Ker}(R^q \to E)$ 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:

$$F_k(x) = I_{q-k}(x) \quad \text{for} \quad 0 \leqq k \leqq q$$

$$F_k(x) = R \qquad \text{when} \quad k > q.$$

Lemma 2.3. *The Fitting ideal $F_k(x)$ does not depend on the choice of generators (x).*

Proof. Let $y_1, \ldots, y_s$ 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 $r \geqq 0$ 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

$$0 \to K \to R^q \to E \to 0,$$

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 $(x_1, \ldots, x_q)$. 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*

$$F_0(E) \subset F_1(E) \subset F_2(E) \subset \cdots$$

(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.