Proof. By Proposition 6.7(c), we may assume that no primary component in the primary decomposition of $\mathfrak{a}$ is irrelevant. Let Z be the algebraic space of zeros of $\mathfrak{a}$ in projective space. We may assume k algebraically closed as noted previously. Then there exists a homogeneous polynomial $L \in k[X]$ of degree 1 (a linear form) which does not lie in any of the prime ideals belonging to the primary ideals in the given decomposition. In particular, L is not a divisor of zero mod $\mathfrak{a}$. Then the components of the algebraic space of zeros of $\mathfrak{a} + (L)$ must have dimension $\leqq r - 1$. By induction and Theorem 6.6, we conclude that the difference

$$\chi(n, \mathfrak{a}) - \chi(n - 1, \mathfrak{a})$$

satisfies the conditions of Lemma 6.4(b), which concludes the proof.

The polynomial in Theorem 6.9 is called the **Hilbert polynomial** of the ideal $\mathfrak{a}$.

Remark. The above results give an introduction for Hartshorne's [Ha 77], Chapter I, especially §7. If Z is not empty, and if we write

$$\chi(n, \mathfrak{a}) = c\frac{n^r}{r!} + \text{lower terms},$$

then $c > 0$ and c can be interpreted as the **degree** of Z, or in geometric terms, the number of points of intersection of Z with a sufficiently general linear variety of complementary dimension (counting the points with certain multiplicities). For explanations and details, see [Ha 77], Chapter I, Proposition 7.6 and Theorem 7.7; van der Waerden [vdW 29] which does the same thing for multihomogeneous polynomial ideals; [La 58], referred to at the end of Chapter VIII, §2; and the papers [MaW 85], [Ph 86], making the link with van der Waerden some six decades before.

Bibliography

[AtM 69] M. ATIYAH and I. MACDONALD, *Introduction to commutative algebra*, Addison-Wesley, 1969

[Ha 77] R. HARTSHORNE, *Algebraic Geometry*, Springer Verlag, 1977

[MaW 85] D. MASSER and G. WÜSTHOLZ, Zero estimates on group varieties II, *Invent. Math.* **80** (1985), pp. 233–267

[Mat 80] H. MATSUMURA, *Commutative algebra*, Second Edition, Benjamin-Cummings, 1980

[Ph 86] P. PHILIPPON, Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France* **114** (1986), pp. 355–383

[vdW 29] B. L. VAN DER WAERDEN, On Hilbert's function, series of composition of ideals and a generalization of the theorem of Bezout, *Proc. R. Soc. Amsterdam* **31** (1929), pp. 749–770

§7. INDECOMPOSABLE MODULES

Let A be a ring, not necessarily commutative, and E an A-module. We say that E is **Artinian** if E satisfies the descending chain condition on submodules, that is a sequence

$$E_1 \supset E_2 \supset E_3 \cdots$$

must stabilize: there exists an integer N such that if $n \geqq N$ then $E_n = E_{n+1}$.

Example 1. If k is a field, A is a k-algebra, and E is a finite-dimensional vector space over k which is also an A-module, then E is Artinian as well as Noetherian.

Example 2. Let A be a commutative Noetherian local ring with maximal ideal $\mathfrak{m}$, and let $\mathfrak{q}$ be an $\mathfrak{m}$-primary ideal. Then for every positive integer n, $A/\mathfrak{q}^n$ is Artinian. Indeed, $A/\mathfrak{q}^n$ has a Jordan-Hölder filtration in which each factor is a finite dimensional vector space over the field $A/\mathfrak{m}$, and is a module of finite length. See Proposition 7.2.

Conversely, suppose that A is a local ring which is both Noetherian and Artinian. Let $\mathfrak{m}$ be the maximal ideal. Then there exists some positive integer n such that $\mathfrak{m}^n = 0$. Indeed, the descending sequence $\mathfrak{m}^n$ stabilizes, and Nakayama's lemma implies our assertion. It then also follows that every primary ideal is nilpotent.

As with Noetherian rings and modules, it is easy to verify the following statements:

Proposition 7.1. *Let A be a ring, and let*

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

be an exact sequence of A-modules. Then E is Artinian if and only if E' and E'' are Artinian.

We leave the proof to the reader. The proof is the same as in the Noetherian case, reversing the inclusion relations between modules.

Proposition 7.2. *A module E has a finite simple filtration if and only if E is both Noetherian and Artinian.*

Proof. A simple module is generated by one element, and so is Noetherian. Since it contains no proper submodule $\neq 0$, it is also Artinian. Proposition 7.2 is then immediate from Proposition 7.1.

A module E is called **decomposable** if E can be written as a direct sum

$$E = E_1 \oplus E_2$$

with $E_1 \neq E$ and $E_2 \neq E$. Otherwise, E is called **indecomposable**. If E is decomposable as above, let e_1 be the projection on the first factor, and $e_2 = 1 - e_1$ the projection on the second factor. Then e_1, e_2 are idempotents such that

$$e_1 \neq 1, \qquad e_2 \neq 1, \qquad e_1 + e_2 = 1 \quad \text{and} \quad e_1 e_2 = e_2 e_1 = 0.$$

Conversely, if such idempotents exist in $\mathrm{End}(E)$ for some module E, then E is decomposable, and e_i is the projection on the submodule $e_i E$.

Let $u : E \to E$ be an endomorphism of some module E. We can form the descending sequence

$$\mathrm{Im}\, u \supset \mathrm{Im}\, u^2 \supset \mathrm{Im}\, u^3 \supset \cdots$$

If E is Artinian, this sequence stabilizes, and we have

$$\mathrm{Im}\, u^n = \mathrm{Im}\, u^{n+1} \qquad \text{for all sufficiently large } n.$$

We call this submodule $u^\infty(E)$, or $\mathrm{Im}\, u^\infty$.

Similarly, we have an ascending sequence

$$\mathrm{Ker}\, u \subset \mathrm{Ker}\, u^2 \subset \mathrm{Ker}\, u^3 \subset \cdots$$

which stabilizes if E is Noetherian, and in this case we write

$$\mathrm{Ker}\, u^\infty = \mathrm{Ker}\, u^n \qquad \text{for } n \text{ sufficiently large.}$$

Proposition 7.3. (Fitting's Lemma). *Assume that E is Noetherian and Artinian. Let $u \in \mathrm{End}(E)$. Then E has a direct sum decomposition*

$$E = \mathrm{Im}\, u^\infty \oplus \mathrm{Ker}\, u^\infty.$$

Furthermore, the restriction of u to $\mathrm{Im}\, u^\infty$ is an automorphism, and the restriction of u to $\mathrm{Ker}\, u^\infty$ is nilpotent.

Proof. Choose n such that $\mathrm{Im}\, u^\infty = \mathrm{Im}\, u^n$ and $\mathrm{Ker}\, u^\infty = \mathrm{Ker}\, u^n$. We have

$$\mathrm{Im}\, u^\infty \cap \mathrm{Ker}\, u^\infty = \{0\},$$

for if x lies in the intersection, then $x = u^n(y)$ for some $y \in E$, and then $0 = u^n(x) = u^{2n}(y)$. So $y \in \mathrm{Ker}\, u^{2n} = \mathrm{Ker}\, u^n$, whence $x = u^n(y) = 0$.

Secondly, let $x \in E$. Then for some $y \in u^n(E)$ we have

$$u^n(x) = u^n(y).$$

Then we can write

$$x = x - u^n(y) + u^n(y),$$

which shows that $E = \operatorname{Im} u^\infty + \operatorname{Ker} u^\infty$. Combined with the first step of the proof, this shows that E is a direct sum as stated.

The final assertion is immediate, since the restriction of u to $\operatorname{Im} u^\infty$ is surjective, and its kernel is 0 by the first part of the proof. The restriction of u to $\operatorname{Ker} u^\infty$ is nilpotent because $\operatorname{Ker} u^\infty = \operatorname{Ker} u^n$. This concludes the proof of the proposition.

We now generalize the notion of a local ring to a non-commutative ring. A ring A is called **local** if the set of non-units is a two-sided ideal.

Proposition 7.4. *Let E be an indecomposable module over the ring A. Assume E Noetherian and Artinian. Any endomorphism of E is either nilpotent or an automorphism. Furthermore* $\operatorname{End}(E)$ *is local.*

Proof. By Fitting's lemma, we know that for any endomorphism u, we have $E = \operatorname{Im} u^\infty$ or $E = \operatorname{Ker} u^\infty$. So we have to prove that $\operatorname{End}(E)$ is local. Let u be an endomorphism which is not a unit, so u is nilpotent. For any endomorphism v it follows that uv and vu are not surjective or injective respectively, so are not automorphisms. Let u_1, u_2 be endomorphisms which are not units. We have to show $u_1 + u_2$ is not a unit. If it is a unit in $\operatorname{End}(E)$, let $v_i = u_i(u_1 + u_2)^{-1}$. Then $v_1 + v_2 = 1$. Furthermore, $v_1 = 1 - v_2$ is invertible by the geometric series since v_2 is nilpotent. But v_1 is not a unit by the first part of the proof, contradiction. This concludes the proof.

Theorem 7.5. (Krull-Remak-Schmidt). *Let $E \neq 0$ be a module which is both Noetherian and Artinian. Then E is a finite direct sum of indecomposable modules. Up to a permutation, the indecomposable components in such a direct sum are uniquely determined up to isomorphism.*

Proof. The existence of a direct sum decomposition into indecomposable modules follows from the Artinian condition. If first $E = E_1 \oplus E_2$, then either E_1, E_2 are indecomposable, and we are done; or, say, E_1 is decomposable. Repeating the argument, we see that we cannot continue this decomposition indefinitely without contradicting the Artinian assumption.

There remains to prove uniqueness. Suppose

$$E = E_1 \oplus \cdots \oplus E_r = F_1 \oplus \cdots \oplus F_s$$

where E_i, F_j are indecomposable. We have to show that $r = s$ and after some permutation, $E_i \approx F_i$. Let e_i be the projection of E on E_i, and let u_j be the projection of E on F_j, relative to the above direct sum decompositions. Let:

$$v_j = e_1 u_j \quad \text{and} \quad w_j = u_j e_1.$$

Then $\sum u_j = \mathrm{id}_E$ implies that

$$\sum_{j=1}^{s} v_j w_j | E_1 = \mathrm{id}_{E_1}.$$

By Proposition 7.4, $\mathrm{End}(E_1)$ is local, and therefore some $v_j w_j$ is an automorphism of E_1. After renumbering, we may assume that $v_1 w_1$ is an automorphism of E_1. We claim that v_1 and w_1 induce isomorphisms between E_1 and F_1, This follows from a lemma.

Lemma 7.6. *Let M, N be modules, and assume N indecomposable. Let $u: M \to N$ and $v: N \to M$ be such that vu is an automorphism. Then u, v are isomorphisms.*

Proof. Let $e = u(vu)^{-1}v$. Then $e^2 = e$ is an idempotent, lying in $\mathrm{End}(N)$, and therefore equal to 0 or 1 since N is assumed indecomposable. But $e \neq 0$ because $\mathrm{id}_M \neq 0$ and

$$0 \neq \mathrm{id}_M = \mathrm{id}_M^2 = (vu)^{-1}vu(vu)^{-1}vu.$$

So $e = \mathrm{id}_N$. Then u is injective because vu is an automorphism; v is injective because $e = \mathrm{id}_N$ is injective; u is surjective because $e = \mathrm{id}_N$; and v is surjective because vu is an automorphism. This concludes the proof of the lemma.

Returning to the theorem, we now see that

$$E = F_1 \oplus (E_2 \oplus \cdots \oplus E_r).$$

Indeed, e_1 induces an isomorphism from F_1 to E_1, and since the kernel of e_1 is $E_2 \oplus \cdots \oplus E_r$ it follows that

$$F_1 \cap (E_2 \oplus \cdots \oplus E_r) = 0.$$

But also, $F_1 \equiv E_1 \pmod{E_2 \oplus \cdots \oplus E_r}$, so E is the sum of F_1 and $E_2 \oplus \cdots \oplus E_r$, whence E is the direct sum, as claimed. But then

$$E/F_1 \approx F_2 \oplus \cdots \oplus F_s \approx E_2 \oplus \cdots \oplus E_r.$$

The proof is then completed by induction.

We apply the preceding results to a commutative ring A. We note that an idempotent in A as a ring is the same thing as an idempotent as an element of $\mathrm{End}(A)$, viewing A as module over itself. Furthermore $\mathrm{End}(A) \approx A$. Therefore, we find the special cases:

Theorem 7.7. *Let A be a Noetherian and Artinian commutative ring.*

(i) *If A is indecomposable as a ring, then A is local.*

(ii) *In general, A is a direct product of local rings, which are Artinian and Noetherian.*

Another way of deriving this theorem will be given in the exercises.

EXERCISES

1. Let A be a commutative ring. Let M be a module, and N a submodule. Let $N = Q_1 \cap \cdots \cap Q_r$ be a primary decomposition of N. Let $\bar{Q}_i = Q_i/N$. Show that $0 = \bar{Q}_1 \cap \cdots \cap \bar{Q}_r$ is a primary decomposition of 0 in M/N. State and prove the converse.
2. Let $\mathfrak{p}$ be a prime ideal, and $\mathfrak{a}$, $\mathfrak{b}$ ideals of A. If $\mathfrak{ab} \subset \mathfrak{p}$, show that $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$.
3. Let $\mathfrak{q}$ be a primary ideal. Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals, and assume $\mathfrak{ab} \subset \mathfrak{q}$. Assume that $\mathfrak{b}$ is finitely generated. Show that $\mathfrak{a} \subset \mathfrak{q}$ or there exists some positive integer n such that $\mathfrak{b}^n \subset \mathfrak{q}$.
4. Let A be Noetherian, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Show that there exists some $n \geqq 1$ such that $\mathfrak{p}^n \subset \mathfrak{q}$.
5. Let A be an arbitrary commutative ring and let S be a multiplicative subset. Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Then $\mathfrak{p}$ intersects S if and only if $\mathfrak{q}$ intersects S. Furthermore, if $\mathfrak{q}$ does not intersect S, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary in $S^{-1}A$.
6. If $\mathfrak{a}$ is an ideal of A, let $\mathfrak{a}_S = S^{-1}\mathfrak{a}$. If $\varphi_S : A \to S^{-1}A$ is the canonical map, abbreviate $\varphi_S^{-1}(\mathfrak{a}_S)$ by $\mathfrak{a}_S \cap A$, even though φ_S is not injective. Show that there is a bijection between the prime ideals of A which do not intersect S and the prime ideals of $S^{-1}A$, given by

$$\mathfrak{p} \mapsto \mathfrak{p}_S \quad \text{and} \quad \mathfrak{p}_S \mapsto \mathfrak{p}_S \cap A = \mathfrak{p}.$$

   Prove a similar statement for primary ideals instead of prime ideals.
7. Let $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ be a reduced primary decomposition of an ideal. Assume that $\mathfrak{q}_1, \ldots, \mathfrak{q}_i$ do not intersect S, but that $\mathfrak{q}_j$ intersects S for $j > i$. Show that

$$\mathfrak{a}_S = \mathfrak{q}_{1S} \cap \cdots \cap \mathfrak{q}_{iS}$$

   is a reduced primary decomposition of $\mathfrak{a}_S$.
8. Let A be a local ring. Show that any idempotent $\neq 0$ in A is necessarily the unit element. (An **idempotent** is an element $e \in A$ such that $e^2 = e$.)
9. Let A be an Artinian commutative ring. Prove:
   (a) All prime ideals are maximal. [*Hint*: Given a prime ideal $\mathfrak{p}$, let $x \in A$, $x(\mathfrak{p}) = 0$. Consider the descending chain $(x) \supset (x^2) \supset (x^3) \supset \cdots$.]

(b) There is only a finite number of prime, or maximal, ideals. [*Hint*: Among all finite intersections of maximal ideals, pick a minimal one.]

(c) The ideal N of nilpotent elements in A is nilpotent, that is there exists a positive integer k such that $N^k = (0)$. [*Hint*: Let k be such that $N^k = N^{k+1}$. Let $\mathfrak{a} = N^k$. Let $\mathfrak{b}$ be a minimal ideal $\neq 0$ such that $\mathfrak{ba} \neq 0$. Then $\mathfrak{b}$ is principal and $\mathfrak{ba} = \mathfrak{b}$.]

(d) A is Noetherian.

(e) There exists an integer r such that

$$A = \prod A/\mathfrak{m}^r$$

where the product is taken over all maximal ideals.

(f) We have

$$A = \prod A_{\mathfrak{p}},$$

where again the product is taken over all prime ideals $\mathfrak{p}$.

10. Let A, B be local rings with maximal ideals $\mathfrak{m}_A$, $\mathfrak{m}_B$, respectively. Let $f: A \to B$ be a homomorphism. We say that f is **local** if $f^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$. Suppose this is the case. Assume A, B Noetherian, and assume that:

1. $A/\mathfrak{m}_A \to B/\mathfrak{m}_B$ is an isomorphism;

2. $\mathfrak{m}_A \to \mathfrak{m}_B/\mathfrak{m}_B^2$ is surjective;

3. B is a finite A-module, via f.

Prove that f is surjective. [*Hint*: Apply Nakayama twice.]

For an ideal $\mathfrak{a}$, recall from Chapter IX, §5 that $\mathfrak{Z}(\mathfrak{a})$ is the set of primes containing $\mathfrak{a}$.

11. Let A be a commutative ring and M an A-module. Define the **support** of M by

$$\operatorname{supp}(M) = \{\mathfrak{p} \in \operatorname{spec}(A) : M_{\mathfrak{p}} \neq 0\}.$$

If M is finite over A, show that $\operatorname{supp}(M) = \mathfrak{Z}(\operatorname{ann}(M))$, where $\operatorname{ann}(M)$ is the annihilator of M in A, that is the set of elements $a \in A$ such that $aM = 0$.

12. Let A be a Noetherian ring and M a finite A-module. Let I be an ideal of A such that $\operatorname{supp}(M) \subset \mathfrak{Z}(I)$. Then $I^n M = 0$ for some $n > 0$.

13. Let A be any commutative ring, and M, N modules over A. If M is finitely presented, and S is a multiplicative subset of A, show that

$$S^{-1}\operatorname{Hom}_A(M, N) \approx \operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N).$$

This is usually applied when A is Noetherian and M finitely generated, in which case M is also finitely presented since the module of relations is a submodule of a finitely generated free module.

14. (a) Prove Proposition 6.7(b).

(b) Prove that the degree of the polynomial P in Theorem 6.9 is exactly r.

Locally constant dimensions

15. Let A be a Noetherian local ring. Let E be a finite A-module. Assume that A has no nilpotent elements. For each prime ideal $\mathfrak{p}$ of A, let $k(\mathfrak{p})$ be the residue class field. If $\dim_{k(\mathfrak{p})} E_{\mathfrak{p}}/\mathfrak{p}E_{\mathfrak{p}}$ is constant for all $\mathfrak{p}$, show that E is free. [*Hint*: Let $x_1, \ldots, x_r \in A$ be

such that the residue classes mod the maximal ideal form a basis for $E/\mathfrak{m}E$ over $k(\mathfrak{m})$. We get a surjective homomorphism

$$A^r \to E \to 0.$$

Let J be the kernel. Show that $J_\mathfrak{p} \subset \mathfrak{m}_\mathfrak{p} A_\mathfrak{p}^r$ for all $\mathfrak{p}$ so $J \subset \mathfrak{p}$ for all $\mathfrak{p}$ and $J = 0$.]

16. Let A be a Noetherian local ring without nilpotent elements. Let $f: E \to F$ be a homomorphism of A-modules, and suppose E, F are finite free. For each prime $\mathfrak{p}$ of A let

$$f_{(\mathfrak{p})}: E_\mathfrak{p}/\mathfrak{p}E_\mathfrak{p} \to F_\mathfrak{p}/\mathfrak{p}F_\mathfrak{p}$$

be the corresponding $k(\mathfrak{p})$-homomorphism, where $k(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is the residue class field at $\mathfrak{p}$. Assume that

$$\dim_{k(\mathfrak{p})} \operatorname{Im} f_{(\mathfrak{p})}$$

is constant.

(a) Prove that $F/\operatorname{Im} f$ and $\operatorname{Im} f$ are free, and that there is an isomorphism

$$F \approx \operatorname{Im} f \oplus (F/\operatorname{Im} f).$$

[*Hint*: Use Exercise 15.]

(b) Prove that $\operatorname{Ker} f$ is free and $E \approx (\operatorname{Ker} f) \oplus (\operatorname{Im} f)$. [*Hint*: Use that finite projective is free.]

The next exercises depend on the notion of a complex, which we have not yet formally defined. A (**finite**) **complex** E is a sequence of homomorphisms of modules

$$0 \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} \cdots \xrightarrow{d^n} E^n \to 0$$

and homorphisms $d^i: E^i \to E^{i+1}$ such that $d^{i+1} \circ d^i = 0$ for all i. Thus $\operatorname{Im}(d^i) \subset \operatorname{Ker}(d^{i+1})$. The **homology** H^i of the complex is defined to be

$$H^i = \operatorname{Ker}(d^{i+1})/\operatorname{Im}(d^i).$$

By definition, $H^0 = E^0$ and $H^n = E^n/\operatorname{Im}(d^n)$. You may want to look at the first section of Chapter XX, because all we use here is the basic notion, and the following property, which you can easily prove. Let E, F be two complexes. By a **homomorphism** $f: E \to F$ we mean a sequence of homomorphisms

$$f_i: E^i \to F^i$$

making the diagram commutative for all i:

$$\begin{array}{ccc} E^i & \xrightarrow{d_E^i} & E^{i+1} \\ \uparrow{\scriptstyle f_i} & & \uparrow{\scriptstyle f_{i+1}} \\ F^i & \xrightarrow[d_F^i]{} & F^{i+1} \end{array}$$

Show that such a homomorphism f induces a homomorphism $H(f): H(E) \to H(F)$ on the homology; that is, for each i we have an induced homomorphism

$$H^i(f): H^i(E) \to H^i(F).$$

The following exercises are inspired from applications to algebraic geometry, as for instance in Hartshorne, *Algebraic Geometry*, Chapter III, Theorem 12.8. See also Chapter XXI, §1 to see how one can construct complexes such as those considered in the next exercises in order to compute the homology with respect to less tractable complexes.

Reduction of a complex mod $\mathfrak{p}$

17. Let $0 \to K^0 \to K^1 \to \cdots \to K^n \to 0$ be a complex of finite free modules over a local Noetherian ring A without nilpotent elements. For each prime $\mathfrak{p}$ of A and module E, let $E(\mathfrak{p}) = E_{\mathfrak{p}}/\mathfrak{p}E_{\mathfrak{p}}$, and similarly let $K(\mathfrak{p})$ be the complex localized and reduced mod $\mathfrak{p}$. For a given integer i, assume that

$$\dim_{k(\mathfrak{p})} H^i(K(\mathfrak{p}))$$

is constant, where H^i is the i-th homology of the reduced complex. Show that $H^i(K)$ is free and that we have a natural isomorphism

$$H^i(K)(\mathfrak{p}) \xrightarrow{\sim} H^i(K(\mathfrak{p})).$$

[*Hint*: First write $d^i_{(\mathfrak{p})}$ for the map induced by d^i on $K^i(\mathfrak{p})$. Write

$$\dim_{k(\mathfrak{p})} \operatorname{Ker} d^i_{(\mathfrak{p})} = \dim_{k(\mathfrak{p})} K^i(\mathfrak{p}) - \dim_{k(\mathfrak{p})} \operatorname{Im} d^i_{(\mathfrak{p})}.$$

Then show that the dimensions $\dim_{k(\mathfrak{p})} \operatorname{Im} d^i_{(\mathfrak{p})}$ and $\dim_{k(\mathfrak{p})} \operatorname{Im} d^{i-1}_{(\mathfrak{p})}$ must be constant. Then apply Exercise 12.]

Comparison of homology at the special point

18. Let A be a Noetherian local ring. Let K be a finite complex, as follows:

$$0 \to K^0 \to \cdots \to K^n \to 0,$$

such that K^i is *finite free* for all i. For some index i assume that

$$H^i(K)(\mathfrak{m}) \to H^i(K(\mathfrak{m}))$$

is surjective. Prove:

(a) This map is an isomorphism.

(b) The following exact sequences split:

$$0 \to \operatorname{Ker} d^i \to K^i \to \operatorname{Im} d^i \to 0$$

$$0 \to \operatorname{Im} d^i \to K^{i+1}$$

(c) Every term in these sequences is free.

19. Let A be a Noetherian local ring. Let K be a complex as in the previous exercise. For some i assume that

$$H^i(K)(\mathfrak{m}) \to H^i(K(\mathfrak{m}))$$

is surjective (or equivalently is an isomorphism by the previous exercise). Prove that

the following conditions are equivalent:

(a) $H^{i-1}(K)(\mathfrak{m}) \to H^{i-1}(K(\mathfrak{m}))$ is surjective.

(b) $H^{i-1}(K)(\mathfrak{m}) \to H^{i-1}(K(\mathfrak{m}))$ is an isomorphism.

(c) $H^i(K)$ is free.

[*Hint*: Lift bases until you are blue in the face.]

(d) If these conditions hold, then each one of the two inclusions

$$\operatorname{Im} d^{i-1} \subset \operatorname{Ker} d^i \subset K^i$$

splits, and each one of these modules is free. Reducing mod $\mathfrak{m}$ yields the corresponding inclusions

$$\operatorname{Im} d^{i-1}_{(\mathfrak{m})} \subset \operatorname{Ker} d^i_{(\mathfrak{m})} \subset K^i(\mathfrak{m}),$$

and induce the isomorphism on cohomology as stated in (b). [*Hint*: Apply the preceding exercise.]

CHAPTER XI

Real Fields

§1. ORDERED FIELDS

Let K be a field. An **ordering** of K is a subset P of K having the following properties:

ORD 1. Given $x \in K$, we have either $x \in P$, or $x = 0$, or $-x \in P$, and these three possibilities are mutually exclusive. In other words, K is the disjoint union of P, $\{0\}$, and $-P$.

ORD 2. If $x, y \in P$, then $x + y$ and $xy \in P$.

We shall also say that K is **ordered by** P, and we call P the set of **positive elements**.

Let us assume that K is ordered by P. Since $1 \neq 0$ and $1 = 1^2 = (-1)^2$ we see that $1 \in P$. By **ORD 2**, it follows that $1 + \cdots + 1 \in P$, whence K has characteristic 0. If $x \in P$, and $x \neq 0$, then $xx^{-1} = 1 \in P$ implies that $x^{-1} \in P$.

Let $x, y \in K$. We define $x < y$ (or $y > x$) to mean that $y - x \in P$. If $x < 0$ we say that x is **negative**. This means that $-x$ is positive. One verifies trivially the usual relations for inequalities, for instance:

$$x < y \quad \text{and} \quad y < z \qquad \text{implies} \qquad x < z,$$

$$x < y \quad \text{and} \quad z > 0 \qquad \text{implies} \qquad xz < yz,$$

$$x < y \quad \text{and} \quad x, y > 0 \qquad \text{implies} \qquad \frac{1}{y} < \frac{1}{x}.$$

We define $x \leqq y$ to mean $x < y$ or $x = y$. Then $x \leqq y$ and $y \leqq x$ imply $x = y$.

If K is ordered and $x \in K$, $x \neq 0$, then x^2 is positive because $x^2 = (-x)^2$ and either $x \in P$ or $-x \in P$. Thus a sum of squares is positive, or 0.

Let E be a field. Then a product of sums of squares in E is a sum of squares. If $a, b \in E$ are sums of squares and $b \neq 0$ then a/b is a sum of squares.

The first assertion is obvious, and the second also, from the expression $a/b = ab(b^{-1})^2$.

If E has characteristic $\neq 2$, and -1 is a sum of squares in E, then every element $a \in E$ is a sum of squares, because $4a = (1 + a)^2 - (1 - a)^2$.

If K is a field with an ordering P, and F is a subfield, then obviously, $P \cap F$ defines an ordering of F, which is called the **induced** ordering.

We observe that our two axioms **ORD 1** and **ORD 2** apply to a ring. If A is an ordered ring, with $1 \neq 0$, then clearly A cannot have divisors of 0, and one can extend the ordering of A to the quotient field in the obvious way: A faction is called positive if it can be written in the form a/b with $a, b \in A$ and $a, b > 0$. One verifies trivially that this defines an ordering on the quotient field.

Example. We define an ordering on the polynomial ring $\mathbf{R}[t]$ over the real numbers. A polynomial

$$f(t) = a_n t^n + \cdots + a_0$$

with $a_n \neq 0$ is defined to be positive if $a_n > 0$. The two axioms are then trivially verified. We note that $t > a$ for all $a \in \mathbf{R}$. Thus t is infinitely large with respect to $\mathbf{R}$. The existence of infinitely large (or infinitely small) elements in an ordered field is the main aspect in which such a field differs from a subfield of the real numbers.

We shall now make some comment on this behavior, i.e. the existence of infinitely large elements.

Let K be an ordered field and let F be a subfield with the induced ordering. As usual, we put $|x| = x$ if $x > 0$ and $|x| = -x$ if $x < 0$. We say that an element α in K is **infinitely large** over F if $|\alpha| \geqq x$ for all $x \in F$. We say that it is **infinitely small** over F if $0 \leqq |\alpha| < |x|$ for all $x \in F, x \neq 0$. We see that α is infinitely large if and only if α^{-1} is infinitely small. We say that K is **archimedean** over F if K has no elements which are infinitely large over F. An intermediate field F_1, $K \supset F_1 \supset F$, is **maximal archimedean over** F in K if it is archimedean over F, and no other intermediate field containing F_1 is archimedean over F. If F_1 is archimedean over F and F_2 is archimedean over F_1 then F_2 is archimedean over F. Hence by Zorn's lemma there always exists a maximal archimedean subfield F_1 of K over F. We say that F is **maximal archimedean in** K if it is maximal archimedean over itself in K.

Let K be an ordered field and F a subfield. Let $\mathfrak{o}$ be the set of elements of K which are not infinitely large over F. Then it is clear that $\mathfrak{o}$ is a ring, and that for any $\alpha \in K$, we have α or $\alpha^{-1} \in \mathfrak{o}$. Hence $\mathfrak{o}$ is what is called a valuation ring, containing F. Let $\mathfrak{m}$ be the ideal of all $\alpha \in K$ which are infinitely small over F. Then $\mathfrak{m}$ is the unique maximal ideal of $\mathfrak{o}$, because any element in $\mathfrak{o}$ which is not in $\mathfrak{m}$ has an inverse in $\mathfrak{o}$. We call $\mathfrak{o}$ the **valuation ring determined by the ordering of K/F.**

Proposition 1.1. *Let K be an ordered field and F a subfield. Let $\mathfrak{o}$ be the valuation ring determined by the ordering of K/F, and let $\mathfrak{m}$ be its maximal ideal. Then $\mathfrak{o}/\mathfrak{m}$ is a real field.*

Proof. Otherwise, we could write

$$-1 = \sum \alpha_i^2 + a$$

with $\alpha_i \in \mathfrak{o}$ and $a \in \mathfrak{m}$. Since $\sum \alpha_i^2$ is positive and a is infinitely small, such a relation is clearly impossible.

§2. REAL FIELDS

A field K is said to be **real** if -1 is not a sum of squares in K. A field K is said to be **real closed** if it is real, and if any algebraic extension of K which is real must be equal to K. In other words, K is maximal with respect to the property of reality in an algebraic closure.

Proposition 2.1. *Let K be a real field.*

(i) *If $a \in K$, then $K(\sqrt{a})$ or $K(\sqrt{-a})$ is real. If a is a sum of squares in K, then $K(\sqrt{a})$ is real. If $K(\sqrt{a})$ is not real, then $-a$ is a sum of squares in K.*

(ii) *If f is an irreducible polynomial of odd degree n in $K[X]$ and if α is a root of f, then $K(\alpha)$ is real.*

Proof. Let $a \in K$. If a is a square in K, then $K(\sqrt{a}) = K$ and hence is real by assumption. Assume that a is not a square in K. If $K(\sqrt{a})$ is not real, then there exist $b_i, c_i \in K$ such that

$$\begin{aligned} -1 &= \sum (b_i + c_i\sqrt{a})^2 \\ &= \sum (b_i^2 + 2c_i b_i\sqrt{a} + c_i^2 a). \end{aligned}$$

Since $\sqrt{a}$ is of degree 2 over K, it follows that

$$-1 = \sum b_i^2 + a \sum c_i^2.$$

If a is a sum of squares in K, this yields a contradiction. In any case, we conclude that

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$$

is a quotient of sums of squares, and by a previous remark, that $-a$ is a sum of squares. Hence $K(\sqrt{a})$ is real, thereby proving our first assertion.

As to the second, suppose $K(\alpha)$ is not real. Then we can write

$$-1 = \sum g_i(\alpha)^2$$

with polynomials g_i in $K[X]$ of degree $\leqq n-1$. There exists a polynomial h in $K[X]$ such that

$$-1 = \sum g_i(X)^2 + h(X)f(X).$$

The sum of $g_i(X)^2$ has even degree, and this degree must be > 0, otherwise -1 is a sum of squares in K. This degree is $\leqq 2n-2$. Since f has odd degree n, it follows that h has odd degree $\leqq n-2$. If β is a root of h then we see that -1 is a sum of squares in $K(\beta)$. Since deg $h <$ deg f, our proof is finished by induction.

Let K be a real field. By a **real closure** we shall mean a real closed field L which is algebraic over K.

Theorem 2.2. *Let K be a real field. Then there exists a real closure of K. If R is real closed, then R has a unique ordering. The positive elements are the squares of R. Every positive element is a square, and every polynomial of odd degree in $R[X]$ has a root in R. We have $R^a = R(\sqrt{-1})$.*

Proof. By Zorn's lemma, our field K is contained in some real closed field algebraic over K. Now let R be a real closed field. Let P be the set of non-zero elements of R which are sums of squares. Then P is closed under addition and multiplication. By Proposition 2.1, every element of P is a square in R, and given $a \in R$, $a \neq 0$, we must have $a \in P$ or $-a \in P$. Thus P defines an ordering. Again by Proposition 2.1, every polynomial of odd degree over R has a root in R. Our assertion follows by Example 5 of Chapter VI, §2.

Corollary 2.3. *Let K be a real field and a an element of K which is not a sum of squares. Then there exists an ordering of K in which a is negative.*

Proof. The field $K(\sqrt{-a})$ is real by Proposition 1.1 and hence has an ordering as a subfield of a real closure. In this ordering, $-a > 0$ and hence a is negative.

Proposition 2.4. *Let R be a field such that $R \neq R^a$ but $R^a = R(\sqrt{-1})$. Then R is real and hence real closed.*

Proof. Let P be the set of elements of R which are squares and $\neq 0$. We contend that P is an ordering of R. Let $a \in R$, $a \neq 0$. Suppose that a is not a square in R. Let α be a root of $X^2 - a = 0$. Then $R(\alpha) = R(\sqrt{-1})$, and hence there exist $c, d \in R$ such that $\alpha = c + d\sqrt{-1}$. Then

$$\alpha^2 = c^2 + 2cd\sqrt{-1} - d^2.$$

Since $1, \sqrt{-1}$ are linearly independent over R, it follows that $c = 0$ (because $a \notin R^2$), and hence $-a$ is a square.

We shall now prove that a sum of squares is a square. For simplicity, write $i = \sqrt{-1}$. Since $R(i)$ is algebraically closed, given $a, b \in R$ we can find $c, d \in R$ such that $(c + di)^2 = a + bi$. Then $a = c^2 - d^2$ and $b = 2cd$. Hence

$$a^2 + b^2 = (c^2 + d^2)^2,$$

as was to be shown.

If $a \in R$, $a \neq 0$, then not both a and $-a$ can be squares in R. Hence P is an ordering and our proposition is proved.

Theorem 2.5. *Let R be a real closed field, and $f(X)$ a polynomial in $R[X]$. Let $a, b \in R$ and assume that $f(a) < 0$ and $f(b) > 0$. Then there exists c between a and b such that $f(c) = 0$.*

Proof. Since $R(\sqrt{-1})$ is algebraically closed, it follows that f splits into a product of irreducible factors of degree 1 or 2. If $X^2 + \alpha X + \beta$ is irreducible ($\alpha, \beta \in R$) then it is a sum of squares, namely

$$\left(X + \frac{\alpha}{2}\right)^2 + \left(\beta - \frac{\alpha^2}{4}\right),$$

and we must have $4\beta > \alpha^2$ since our factor is assumed irreducible. Hence the change of sign of f must be due to the change of sign of a linear factor, which is trivially verified to be a root lying between a and b.

Lemma 2.6. *Let K be a subfield of an ordered field E. Let $\alpha \in E$ be algebraic over K, and a root of the polynomial*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with coefficients in K. Then $|\alpha| \leqq 1 + |a_{n-1}| + \cdots + |a_0|$.

Proof. If $|\alpha| \leqq 1$, the assertion is obvious. If $|\alpha| > 1$, we express $|\alpha|^n$ in terms of the terms of lower degree, divide by $|\alpha|^{n-1}$, and get a proof for our lemma.

Note that the lemma implies that an element which is algebraic over an ordered field cannot be infinitely large with respect to that field.

Let $f(X)$ be a polynomial with coefficients in a real closed field R, and assume that f has no multiple roots. Let $u < v$ be elements of R. By a **Sturm sequence** for f over the interval $[u, v]$ we shall mean a sequence of polynomials

$$S = \{f = f_0, f' = f_1, \ldots, f_m\}$$

having the following properties:

ST 1. The last polynomial f_m is a non-zero constant.

ST 2. There is no point $x \in [u, v]$ such that $f_j(x) = f_{j+1}(x) = 0$ for any value $0 \leqq j \leqq m - 1$.

ST 3. If $x \in [u, v]$ and $f_j(x) = 0$ for some $j = 1, \ldots, m - 1$, then $f_{j-1}(x)$ and $f_{j+1}(x)$ have opposite signs.

ST 4. We have $f_j(u) \neq 0$ and $f_j(v) \neq 0$ for all $j = 0, \ldots, m$.

For any $x \in [u, v]$ which is not a root of any polynomial f_i we denote by $W_S(x)$ the number of sign changes in the sequence

$$\{f(x), f_1(x), \ldots, f_m(x)\},$$

and call $W_S(x)$ the **variation of signs in the sequence**.

Theorem 2.7. (Sturm's Theorem). *The number of roots of f between u and v is equal to $W_S(u) - W_S(v)$ for any Sturm sequence S.*

Proof. We observe that if $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ is the ordered sequence of roots of the polynomials f_j in $[u, v]$ $(j = 0, \ldots, m - 1)$, then $W_S(x)$ is constant on the open intervals between these roots, by Theorem 2.5. Hence it will suffice to prove that if there is precisely one element α such that $u < \alpha < v$ and α is a root of some f_j, then $W_S(u) - W_S(v) = 1$ if α is a root of f, and 0 otherwise. Suppose that α is a root of some f_j, for $1 \leqq j \leqq m - 1$. Then $f_{j-1}(\alpha)$, $f_{j+1}(\alpha)$ have opposite signs by **ST 3**, and these signs do not change when we replace α by u or v. Hence the variation of signs in

$$\{f_{j-1}(u), f_j(u), f_{j+1}(u)\} \quad \text{and} \quad \{f_{j-1}(v), f_j(v), f_{j+1}(v)\}$$

is the same, namely equal to 2. If α is not a root of f, we conclude that

$$W_S(u) = W_S(v).$$

If α is a root of f, then $f(u)$ and $f(v)$ have opposite signs, but $f'(u)$ and $f'(v)$ have the same sign, namely, the sign of $f'(\alpha)$. Hence in this case,

$$W_S(u) = W_S(v) + 1.$$

This proves our theorem.

It is easy to construct a Sturm sequence for a polynomial without multiple roots. We use the Euclidean algorithm, writing

$$\begin{aligned} f &= g_1 f' - f_2, \\ f_2 &= g_2 f_1 - f_3, \\ &\vdots \\ f_{m-2} &= g_{m-1} f_{m-1} - f_m, \end{aligned}$$

using $f' = f_1$. Since f, f' have no common factor, the last term of this sequence is non-zero constant. The other properties of a Sturm sequence are trivially verified, because if two successive polynomials of the sequence have a common zero, then they must all be 0, contradicting the fact that the last one is not.

Corollary 2.8. *Let K be an ordered field, f an irreducible polynomial of degree $\geqq 1$ over K. The number of roots of f in two real closures of K inducing the given ordering on K is the same.*

Proof. We can take v sufficiently large positive and u sufficiently large negative in K so that all roots of f and all roots of the polynomials in the Sturm sequence lie between u and v, using Lemma 2.6. Then $W_S(u) - W_S(v)$ is the total number of roots of f in any real closure of K inducing the given ordering.

Theorem 2.9. *Let K be an ordered field, and let R, R' be real closures of K, whose orderings induce the given ordering on K. Then there exists a unique isomorphism $\sigma : R \to R'$ over K, and this isomorphism is order-preserving.*

Proof. We first show that given a finite subextension E of R over K, there exists an embedding of E into R' over K. Let $E = K(\alpha)$, and let

$$f(X) = \operatorname{Irr}(\alpha, K, X).$$

Then $f(\alpha) = 0$ and the corollary of Sturm's Theorem (Corollary 2.8) shows that f has a root β in R'. Thus there exists an isomorphism of $K(\alpha)$ on $K(\beta)$ over K, mapping α on β.

Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of f in R, and let $\beta_1, \ldots, \beta_m$ be the distinct roots of f in R'. Say

$$\alpha_1 < \cdots < \alpha_n \quad \text{in the ordering of } R,$$
$$\beta_1 < \cdots < \beta_m \quad \text{in the ordering of } R'.$$

We contend that $m = n$ and that we can select an embedding σ of $K(\alpha_1, \ldots, \alpha_n)$ into R' such that $\sigma\alpha_i = \beta_i$ for $i = 1, \ldots, n$. Indeed, let γ_i be an element of R such that

$$\gamma_i^2 = \alpha_{i+1} - \alpha_i \quad \text{for} \quad i = 1, \ldots, n-1$$

and let $E_1 = K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1})$. By what we have seen, there exists an embedding σ of E_1 into R', and then $\sigma\alpha_{i+1} - \sigma\alpha_i$ is a square in R'. Hence

$$\sigma\alpha_1 < \cdots < \sigma\alpha_n.$$

This proves that $m \geqq n$. By symmetry, it follows that $m = n$. Furthermore, the condition that $\sigma\alpha_i = \beta_i$ for $i = 1, \ldots, n$ determines the effect of σ on

$K(\alpha_1, \ldots, \alpha_n)$. We contend that σ is order-preserving. Let $y \in K(\alpha_1, \ldots, \alpha_n)$ and $0 < y$. Let $\gamma \in R$ be such that $\gamma^2 = y$. There exists an embedding of

$$K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1}, \gamma)$$

into R' over K which must induce σ on $K(\alpha_1, \ldots, \alpha_n)$ and is such that σy is a square, hence > 0, as contended.

Using Zorn's lemma, it is now clear that we get an isomorphism of R onto R' over K. This isomorphism is order-preserving because it maps squares on squares, thereby proving our theorem.

Proposition 2.10. *Let K be an ordered field, K' an extension such that there is no relation*

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

with $a_i \in K, a_i > 0$, and $\alpha_i \in K'$. Let L be the field obtained from K' by adjoining the square roots of all positive elements of K. Then L is real.

Proof. If not, there exists a relation of type

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

with $a_i \in K$, $a_i > 0$, and $\alpha_i \in L$. (We can take $a_i = 1$.) Let r be the smallest integer such that we can write such a relation with α_i in a subfield of L, of type

$$K'(\sqrt{b_1}, \ldots, \sqrt{b_r})$$

with $b_j \in K$, $b_j > 0$. Write

$$\alpha_i = x_i + y_i\sqrt{b_r}$$

with $x_i, y_i \in K'(\sqrt{b_1}, \ldots, \sqrt{b_{r-1}})$. Then

$$\begin{aligned} -1 &= \sum a_i(x_i + y_i\sqrt{b_r})^2 \\ &= \sum a_i(x_i^2 + 2x_i y_i\sqrt{b_r} + y_i^2 b_r). \end{aligned}$$

By hypothesis, $\sqrt{b_r}$ is not in $K'(b_1, \ldots, \sqrt{b_{r-1}})$. Hence

$$-1 = \sum a_i x_i^2 + \sum a_i b_r y_i^2,$$

contradicting the minimality of r.

Theorem 2.11. *Let K be an ordered field. There exists a real closure R of K inducing the given ordering on K.*

Proof. Take $K' = K$ in Proposition 2.10. Then L is real, and is contained in a real closure. Our assertion is clear.

Corollary 2.12. *Let K be an ordered field, and K' an extension field. In order that there exist an ordering on K' inducing the given ordering of K, it is necessary and sufficient that there is no relation of type*

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

with $a_i \in K$, $a_i > 0$, and $\alpha_i \in K'$.

Proof. If there is no such relation, then Proposition 2.10 states that L is contained in a real closure, whose ordering induces an ordering on K', and the given ordering on K, as desired. The converse is clear.

Example. Let $\mathbf{Q}^a$ be the field of algebraic numbers. One sees at once that $\mathbf{Q}$ admits only one ordering, the ordinary one. Hence any two real closures of $\mathbf{Q}$ in $\mathbf{Q}^a$ are isomorphic, by means of a unique isomorphism. The real closures of $\mathbf{Q}$ in $\mathbf{Q}^a$ are precisely those subfields of $\mathbf{Q}^a$ which are of finite degree under $\mathbf{Q}^a$. Let K be a finite real extension of $\mathbf{Q}$, contained in $\mathbf{Q}^a$. An element α of K is a sum of squares in K if and only if every conjugate of α in the real numbers is positive, or equivalently, if and only if every conjugate of α in one of the real closures of $\mathbf{Q}$ in $\mathbf{Q}^a$ is positive.

Note. The theory developed in this and the preceding section is due to Artin-Schreier. See the bibliography at the end of the chapter.

§3. REAL ZEROS AND HOMOMORPHISMS

Just as we developed a theory of extension of homomorphisms into an algebraically closed field, and Hilbert's Nullstellensatz for zeros in an algebraically closed field, we wish to develop the theory for values in a real closed field. One of the main theorems is the following:

Theorem 3.1. *Let k be a field, $K = k(x_1, \ldots, x_n)$ a finitely generated extension. Assume that K is ordered. Let R_k be a real closure of k inducing the same ordering on k as K. Then there exists a homomorphism*

$$\varphi : k[x_1, \ldots, x_n] \to R_k$$

over k.

As applications of Theorem 3.1, one gets:

Corollary 3.2. *Notation being as in the theorem, let* $y_1, \ldots, y_m \in k[x]$ *and assume*

$$y_1 < y_2 < \cdots < y_m$$

is the given ordering of K. *Then one can choose* φ *such that*

$$\varphi y_1 < \cdots < \varphi y_m.$$

Proof. Let $\gamma_i \in K^a$ be such that $\gamma_i^2 = y_{i+1} - y_i$. Then $K(\gamma_1, \ldots, \gamma_{n-1})$ has an ordering inducing the given ordering on K. We apply the theorem to the ring

$$k[x_1, \ldots, x_n, \gamma_1^{-1}, \ldots, \gamma_{m-1}^{-1}, \gamma_1, \ldots, \gamma_{m-1}].$$

Corollary 3.3. (Artin). *Let* k *be a real field admitting only one ordering. Let* $f(X_1, \ldots, X_n) \in k(X)$ *be a rational function having the property that for all* $(a) = (a_1, \ldots, a_n) \in R_k^{(n)}$ *such that* $f(a)$ *is defined, we have* $f(a) \geqq 0$. *Then* $f(X)$ *is a sum of squares in* $k(X)$.

Proof. Assume that our conclusion is false. By Corollary 2.3, there exists an ordering of $k(X)$ in which f is negative. Apply Corollary 3.2 to the ring

$$k[X_1, \ldots, X_n, h(X)^{-1}]$$

where $h(X)$ is a polynomial denominator for $f(X)$. We can find a homomorphism φ of this ring into R_k (inducing the identity on k) such that $\varphi(f) < 0$. But

$$\varphi(f) = f(\varphi X_1, \ldots, \varphi X_n).$$

contradiction. We let $a_i = \varphi(X_i)$ to conclude the proof.

Corollary 3.3 was a Hilbert problem. The proof which we shall describe for Theorem 3.1 differs from Artin's proof of the corollary in several technical aspects.

We shall first see how one can reduce Theorem 3.1 to the case when K has transcendence degree 1 over k, and k is real closed.

Lemma 3.4. *Let* R *be a real closed field and let* R_0 *be a subfield which is algebraically closed in* R (*i.e. such that every element of* R *not in* R_0 *is transcendental over* R_0). *Then* R_0 *is real closed.*

Proof. Let $f(X)$ be an irreducible polynomial over R_0. It splits in R into linear and quadratic factors. Its coefficients in R are algebraic over R_0, and hence must lie in R_0. Hence $f(X)$ is linear itself, or quadratic irreducible already over R_0. By the intermediate value theorem, we may assume that f is positive

definite, i.e. $f(a) > 0$ for all $a \in R_0$. Without loss of generality, we may assume that $f(X) = X^2 + b^2$ for some $b \in R_0$. Any root of this polynomial will bring $\sqrt{-1}$ with it and therefore the only algebraic extension of R_0 is $R_0(\sqrt{-1})$. This proves that R_0 is real closed.

Let R_K be a real closure of K inducing the given ordering on K. Let R_0 be the algebraic closure of k in R_K. By the lemma, R_0 is real closed.

We consider the field $R_0(x_1, \ldots, x_n)$. If we can prove our theorem for the ring $R_0[x_1, \ldots, x_n]$, and find a homomorphism

$$\psi : R_0[x_1, \ldots, x_n] \to R_0,$$

then we let $\sigma : R_0 \to R_K$ be an isomorphism over k (it exists by Theorem 2.9), and we let $\varphi = \sigma \circ \psi$ to solve our problem over k. This reduces our theorem to the case when k is real closed.

Next, let F be an intermediate field, $K \supset F \supset k$, such that K is of transcendence degree 1 over F. Again let R_K be a real closure of K preserving the ordering, and let R_F be the real closure of F contained in R_K. If we know our theorem for extensions of dimension 1, then we can find a homomorphism

$$\psi : R_F[x_1, \ldots, x_n] \to R_F.$$

We note that the field $k(\psi x_1, \ldots, \psi x_n)$ has transcendence degree $\leqq n - 1$, and is real, because it is contained in R_F. Thus we are reduced inductively to the case when K has dimension 1, and as we saw above, when k is real closed.

One can interpret our statement geometrically as follows. We can write $K = R(x, y)$ with x transcendental over R, and (x, y) satisfying some irreducible polynomial $f(X, Y) = 0$ in $R[X, Y]$. What we essentially want to prove is that there are infinitely many points on the curve $f(X, Y) = 0$, with coordinates lying in R, i.e. infinitely many real points.

The main idea is that we find some point $(a, b) \in R^{(2)}$ such that $f(a, b) = 0$ but $D_2 f(a, b) \neq 0$. We can then use the intermediate value theorem. We see that $f(a, b + h)$ changes sign as h changes from a small positive to a small negative element of R. If we take $a' \in R$ close to a, then $f(a', b + h)$ also changes sign for small h, and hence $f(a', Y)$ has a zero in R for all a' sufficiently close to a. In this way we get infinitely many zeros.

To find our point, we consider the polynomial $f(x, Y)$ as a polynomial in one variable Y with coefficients in $R(x)$. Without loss of generality we may assume that this polynomial has leading coefficient 1. We construct a Sturm sequence for this polynomial, say

$$\{f(x, Y), f_1(x, Y), \ldots, f_m(x, Y)\}.$$

Let $d = \deg f$. If we denote by $A(x) = (a_{d-1}(x), \ldots, a_0(x))$ the coefficients of $f(x, Y)$, then from the Euclidean alogrithm, we see that the coefficients of the

polynomials in the Sturm sequence can be expressed as rational functions

$$\{G_v(A(x))\}$$

in terms of $a_{d-1}(x), \ldots, a_0(x)$.

Let

$$v(x) = 1 \pm a_{d-1}(x) \pm \cdots \pm a_0(x) + s,$$

where s is a positive integer, and the signs are selected so that each term in this sum gives a positive contribution. We let $u(x) = -v(x)$, and select s so that neither u nor v is a root of any polynomial in the Sturm sequence for f. Now we need a lemma.

Lemma 3.5. *Let R be a real closed field, and $\{h_i(x)\}$ a finite set of rational functions in one variable with coefficients in R. Suppose the rational field $R(x)$ ordered in some way, so that each $h_i(x)$ has a sign attached to it. Then there exist infinitely many special values c of x in R such that $h_i(c)$ is defined and has the same sign as $h_i(x)$, for all i.*

Proof. Considering the numerators and denominators of the rational functions, we may assume without loss of generality that the h_i are polynomials. We then write

$$h_i(x) = \alpha \prod (x - \lambda) \prod p(x),$$

where the first product is extended over all roots λ of h_i in R, and the second product is over positive definite quadratic factors over R. For any $\xi \in R$, $p(\xi)$ is positive. It suffices therefore to show that the signs of $(x - \lambda)$ can be preserved for all λ by substituting infinitely many values α for x. We order all values of λ and of x and obtain

$$\cdots < \lambda_1 < x < \lambda_2 < \cdots$$

where possibly λ_1 or λ_2 is omitted if x is larger or smaller than any λ. Any value α of x in R selected between λ_1 and λ_2 will then satisfy the requirements of our lemma.

To apply the lemma to the existence of our point, we let the rational functions $\{h_1(x)\}$ consist of all coefficients $a_{d-1}(x), \ldots, a_0(x)$, all rational functions $G_v(A(x))$, and all values $f_j(x, u(x))$, $f_j(x, v(x))$ whose variation in signs satisfied Sturm's theorem. We then find infinitely many special values α of x in R which preserve the signs of these rational functions. Then the polynomials $f(\alpha, Y)$ have roots in R, and for all but a finite number of α, these roots have multiplicity 1.

It is then a matter of simple technique to see that for all but a finite number of points on the curve, the elements $x_1, \ldots, x_n$ lie in the local ring of the homomorphism $R[x, y] \to R$ mapping (x, y) on (a, b) such that $f(a, b) = 0$ but

$D_2 f(a, b) \neq 0$. (Cf. for instance the example at the end of §4, Chapter XII, and Exercise 18 of that chapter.) One could also give direct proofs here. In this way, we obtain homomorphisms

$$R[x_1, \ldots, x_n] \to R,$$

thereby proving Theorem 3.1.

Theorem 3.6. *Let k be a real field, $K = k(x_1, \ldots, x_n, y) = k(x, y)$ a finitely generated extension such that $x_1, \ldots, x_n$ are algebraically independent over k, and y is algebraic over $k(x)$. Let $f(X, Y)$ be the irreducible polynomial in $k[X, Y]$ such that $f(x, y) = 0$. Let R be a real closed field containing k, and assume that there exists $(a, b) \in R^{(n+1)}$ such that $f(a, b) = 0$ but*

$$D_{n+1} f(a, b) \neq 0.$$

Then K is real.

Proof. Let $t_1, \ldots, t_n$ be algebraically independent over R. Inductively, we can put an ordering on $R(t_1, \ldots, t_n)$ such that each t_i is infinitely small with respect to R, (cf. the example in §1). Let R' be a real closure of $R(t_1, \ldots, t_n)$ preserving the ordering. Let $u_i = a_i + t_i$ for each $i = 1, \ldots, n$. Then $f(u, b + h)$ changes sign for small h positive and negative in R, and hence $f(u, Y)$ has a root in R', say v. Since f is irreducible, the isomorphism of $k(x)$ on $k(u)$ sending x_i on u_i extends to an embedding of $k(x, y)$ into R', and hence K is real, as was to be shown.

In the language of algebraic geometry, Theorems 3.1 and 3.6 state that the function field of a variety over a real field k is real if and only if the variety has a simple point in some real closure of k.

EXERCISES

1. Let α be algebraic over $\mathbf{Q}$ and assume that $\mathbf{Q}(\alpha)$ is a real field. Prove that α is a sum of squares in $\mathbf{Q}(\alpha)$ if and only if for every embedding σ of $\mathbf{Q}(\alpha)$ in $\mathbf{R}$ we have $\sigma\alpha > 0$.
2. Let F be a finite extension of $\mathbf{Q}$. Let $\varphi : F \to \mathbf{Q}$ be a $\mathbf{Q}$-linear functional such that $\varphi(x^2) > 0$ for all $x \in F, x \neq 0$. Let $\alpha \in F, \alpha \neq 0$. If $\varphi(\alpha x^2) \geqq 0$ for all $x \in F$, show that α is a sum of squares in F, and that F is totally real, i.e. every embedding of F in the complex numbers is contained in the real numbers. [*Hint*: Use the fact that the trace gives an identification of F with its dual space over $\mathbf{Q}$, and use the approximation theorem of Chapter XII, §1.]

3. Let $\alpha \leqq t \leqq \beta$ be a real interval, and let $f(t)$ be a real polynomial which is positive on this interval. Show that $f(t)$ can be written in the form

$$c(\sum Q_\nu^2 + \sum (t - \alpha)Q_\mu^2 + \sum (\beta - t)Q_\lambda^2)$$

where Q^2 denotes a square, and $c \geqq 0$. *Hint*: Split the polynomial, and use the identity:

$$(t - \alpha)(\beta - t) = \frac{(t - \alpha)^2(\beta - t) + (t - \alpha)(\beta - t)^2}{\beta - \alpha}.$$

Remark. The above seemingly innocuous result is a key step in developing the spectral theorem for bounded hermitian operators on Hilbert space. See the appendix of [La 72] and also [La 85].

4. Show that the field of real numbers has only the identity automorphism. [*Hint*: Show that an automorphism preserves the ordering.]

Real places

For the next exercises, cf. Krull [Kr 32] and Lang [La 53]. These exercises form a connected sequence, and solutions will be found in [La 53].

5. Let K be a field and suppose that there exists a real place of K; that is, a place φ with values in a real field L. Show that K is real.

6. Let K be an ordered real field and let F be a subfield which is maximal archimedean in K. Show that the canonical place of K with respect to F is algebraic over F (i.e. if $\mathfrak{o}$ is the valuation ring of elements of K which are not infinitely large over F, and $\mathfrak{m}$ is its maximal ideal, then $\mathfrak{o}/\mathfrak{m}$ is algebraic over F).

7. Let K be an ordered field and let F be a subfield which is maximal archimedean in K. Let K' be the real closure of K (preserving the ordering), and let F' be the real closure of F contained in K'. Let φ be the canonical place of K' with respect to F'. Show that $\varphi(K')$ is F'-valued, and that the restriction of φ to K is equivalent to the canonical place of K over F.

8. Define a real field K to be **quadratically closed** if for all $\alpha \in K$ either $\sqrt{\alpha}$ or $\sqrt{-\alpha}$ lies in K. The ordering of a quadratically closed real field K is then uniquely determined, and so is the real closure of such a field, up to an isomorphism over K. Suppose that K is quadratically closed. Let F be a subfield of K and suppose that F is maximal archimedean in K. Let φ be a place of K over F, with values in a field which is algebraic over F. Show that φ is equivalent to the canonical place of K over F.

9. Let K be a quadratically closed real field. Let φ be a real place of K, taking its values in a real closed field R. Let F be a maximal subfield of K such that φ is an isomorphism on F, and identify F with $\varphi(F)$. Show that such F exists and is maximal archimedean in K. Show that the image of φ is algebraic over F, and that φ is induced by the canonical place of K over F.

10. Let K be a real field and let φ be a real place of K, taking its values in a real closed field R. Show that there is an extension of φ to an R-valued place of a real closure of K. [*Hint*: first extend φ to a quadratic closure of K. Then use Exercise 5.]

11. Let $K \subset K_1 \subset K_2$ be real closed fields. Suppose that K is maximal archimedean in K_1 and K_1 is maximal archimedean in K_2. Show that K is maximal archimedean in K_2.

12. Let K be a real closed field. Show that there exists a real closed field R containing K and having arbitrarily large transcendence degree over K, and such that K is maximal archimedean in R.

13. Let R be a real closed field. Let $f_1, \ldots, f_r$ be homogeneous polynomials of odd degrees in n variables over R. If $n > r$, show that these polynomials have a non-trivial common zero in R. (*Comments*: If the forms are generic (in the sense of Chapter IX), and $n = r + 1$, it is a theorem of Bezout that in the algebraic closure R^a the forms have exactly $d_1 \cdots d_m$ common zeros, where d_i is the degree of f_i. You may assume this to prove the result as stated. If you want to see this worked out, see [La 53], Theorem 15. Compare with Exercise 3 of Chapter IX.)

Bibliography

[Ar 24] E. ARTIN, Kennzeichnung des Körpers der reellen algebraischen Zahlen, *Abh. Math. Sem. Hansischen Univ.* **3** (1924), pp. 319–323

[Ar 27] E. ARTIN, Über die Zerlegung definiter Funktionen in Quadrate, *Abh. Math. Sem. Hansischen Univ.* **5** (1927), pp. 100–115

[ArS 27] E. ARTIN and E. SCHREIER, Algebraische Konstruktion reeller Körper, *Abh. Math. Sem. Hansischen Univ.* **5** (1927), pp. 85–99

[Kr 32] W. KRULL, Allgemeine Bewertungstheorie, *J. reine angew. Math.* (1932), pp. 169–196

[La 53] S. LANG, The theory of real places, *Ann. Math.* **57** No. 2 (1953), pp. 378–391

[La 72] S. LANG, *Differential manifolds*, Addison-Wesley, 1972; reprinted by Springer Verlag, 1985; superceded by [La 99a].

[La 85] S. LANG, *Real and functional analysis*. Third edition, Springer Verlag, 1993

[La 99a] S. LANG, *Fundamentals of Differential Geometry*, Springer Verlag, 1999

CHAPTER XII

Absolute Values

§1. DEFINITIONS, DEPENDENCE, AND INDEPENDENCE

Let K be a field. An **absolute value** v on K is a real-valued function $x \mapsto |x|_v$ on K satisfying the following three properties:

AV 1. We have $|x|_v \geqq 0$ for all $x \in K$, and $|x|_v = 0$ if and only if $x = 0$.

AV 2. For all $x, y \in K$, we have $|xy|_v = |x|_v |y|_v$.

AV 3. For all $x, y \in K$, we have $|x + y|_v \leqq |x|_v + |y|_v$.

If instead of **AV 3** the absolute value satisfies the stronger condition

AV 4. $|x + y|_v \leqq \max(|x|_v, |y|_v)$

then we shall say that it is a **valuation**, or that it is non-archimedean.

The absolute value which is such that $|x|_v = 1$ for all $x \neq 0$ is called **trivial**.

We shall write $|x|$ instead of $|x|_v$ if we deal with just one fixed absolute value. We also refer to v as the absolute value.

An absolute value of K defines a metric. The distance between two elements x, y of K in this metric is $|x - y|$. Thus an absolute value defines a topology on K. Two absolute values are called **dependent** if they define the same topology. If they do not, they are called independent.

We observe that $|1| = |1^2| = |(-1)^2| = |1|^2$ whence

$$|1| = |-1| = 1.$$

Also, $|-x| = |x|$ for all $x \in K$, and $|x^{-1}| = |x|^{-1}$ for $x \neq 0$.

Proposition 1.1. *Let* $|\ |_1$ *and* $|\ |_2$ *be non-trivial absolute values on a field* K. *They are dependent if and only if the relation*

$$|x|_1 < 1$$

implies $|x|_2 < 1$. *If they are dependent, then there exists a number* $\lambda > 0$ *such that* $|x|_1 = |x|_2^{\lambda}$ *for all* $x \in K$.

Proof. If the two absolute values are dependent, then our condition is satisfied, because the set of $x \in K$ such that $|x|_1 < 1$ is the same as the set such that $\lim x^n = 0$ for $n \to \infty$. Conversely, assume the condition satisfied. Then $|x|_1 > 1$ implies $|x|_2 > 1$ since $|x^{-1}|_1 < 1$. By hypothesis, there exists an element $x_0 \in K$ such that $|x_0|_1 > 1$. Let $a = |x_0|_1$ and $b = |x_0|_2$. Let

$$\lambda = \frac{\log b}{\log a}.$$

Let $x \in K, x \neq 0$. Then $|x|_1 = |x_0|_1^{\alpha}$ for some number α. If m, n are integers such that $m/n > \alpha$ and $n > 0$, we have

$$|x|_1 > |x_0|_1^{m/n}$$

whence

$$|x^n/x_0^m|_1 < 1,$$

and thus

$$|x^n/x_0^m|_2 < 1.$$

This implies that $|x|_2 < |x_0|_2^{m/n}$. Hence

$$|x|_2 \leqq |x_0|_2^{\alpha}.$$

Similarly, one proves the reverse inequality, and thus one gets

$$|x|_2 = |x_0|_2^{\alpha}$$

for all $x \in K$, $x \neq 0$. The assertion of the proposition is now obvious, i.e. $|x|_2 = |x|_1^{\lambda}$.

We shall give some examples of absolute values.

Consider first the rational numbers. We have the ordinary absolute value such that $|m| = m$ for any positive integer m.

For each prime number p, we have the p-adic absolute value v_p, defined by the formula

$$|p^r m/n|_p = 1/p^r$$

where r is an integer, and m, n are integers $\neq 0$, not divisible by p. One sees at once that the p-adic absolute value is non-archimedean.

One can give a similar definition of a valuation for any field K which is the quotient field of a principal ring. For instance, let $K = k(t)$ where k is a field and t is a variable over k. We have a valuation v_p for each irreducible polynomial $p(t)$ in $k[t]$, defined as for the rational numbers, but there is no way of normalizing it in a natural way. Thus we select a number c with $0 < c < 1$ and for any rational function $p^r f/g$ where f, g are polynomials not divisible by p, we define

$$|p^r f/g|_p = c^r.$$

The various choices of the constant c give rise to dependent valuations.

Any subfield of the complex numbers (or real numbers) has an absolute value, induced by the ordinary absolute value on the complex numbers. We shall see later how to obtain absolute values on certain fields by embedding them into others which are already endowed with natural absolute values.

Suppose that we have an absolute value on a field which is bounded on the prime ring (i.e. the integers $\mathbf{Z}$ *if the characteristic is* 0, *or the integers* mod p *if the characteristic is* p). *Then the absolute value is necessarily non-archimedean.*

Proof. For any elements x, y and any positive integer n, we have

$$|(x + y)^n| \leqq \sum \left| \binom{n}{v} x^v y^{n-v} \right| \leqq nC \max(|x|, |y|)^n.$$

Taking n-th roots and letting n go to infinity proves our assertion. We note that this is always the case in characteristic > 0 because the prime ring is finite!

If the absolute value is archimedean, then we refer the reader to any other book in which there is a discussion of absolute values for a proof of the fact that it is dependent on the ordinary absolute value. This fact is essentially useless (and is never used in the sequel), because we always start with a concretely given set of absolute values on fields which interest us.

In Proposition 1.1 we derived a strong condition on dependent absolute values. We shall now derive a condition on independent ones.

Theorem 1.2. (Approximation Theorem). (Artin-Whaples). *Let K be a field and $|\ |_1, \ldots, |\ |_s$ non-trivial pairwise independent absolute values on K. Let $x_1, \ldots, x_s$ be elements of K, and $\epsilon > 0$. Then there exists $x \in K$ such that*

$$|x - x_i|_i < \epsilon$$

for all i.

Proof. Consider first two of our absolute values, say v_1 and v_2. By hypothesis we can find $\alpha \in K$ such that $|\alpha|_1 < 1$ and $|\alpha|_s \geqq 1$. Similarly, we can find $\beta \in K$ such that $|\beta|_1 \geqq 1$ and $|\beta|_s < 1$. Put $y = \beta/\alpha$. Then $|y|_1 > 1$ and $|y|_s < 1$.

We shall now prove that there exists $z \in K$ such that $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, s$. We prove this by induction, the case $s = 2$ having just been proved. Suppose we have found $z \in K$ satisfying

$$|z|_1 > 1 \quad \text{and} \quad |z|_j < 1 \qquad \text{for} \quad j = 2, \ldots, s-1.$$

If $|z|_s \leqq 1$ then the element $z^n y$ for large n will satisfy our requirements.

If $|z|_s > 1$, then the sequence

$$t_n = \frac{z^n}{1 + z^n}$$

tends to 1 at v_1 and v_s, and tends to 0 at $v_j (j = 2, \ldots, s-1)$. For large n, it is then clear that $t_n y$ satisfies our requirements.

Using the element z that we have just constructed, we see that the sequence $z^n/(1 + z^n)$ tends to 1 at v_1 and to 0 at v_j for $j = 2, \ldots, s$. For each $i = 1, \ldots, s$ we can therefore construct an element z_i which is very close to 1 at v_i and very close to 0 at v_j $(j \neq i)$. The element

$$x = z_1 x_1 + \cdots + z_s x_s$$

then satisfies the requirement of the theorem.

§2. COMPLETIONS

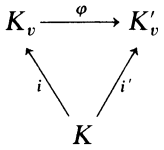
Let K be a field with a non-trivial absolute value v, which will remain fixed throughout this section. One can then define in the usual manner the notion of a Cauchy sequence. It is a sequence $\{x_n\}$ of elements in K such that, given $\epsilon > 0$, there exists an integer N such that for all $n, m > N$ we have

$$|x_n - x_m| < \epsilon.$$

We say that K is **complete** if every Cauchy sequence converges.

Proposition 2.1. *There exists a pair (K_v, i) consisting of a field K_v, complete under an absolute value, and an embedding $i : K \to K_v$ such that the absolute value on K is induced by that of K_v (i.e. $|x|_v = |ix|$ for $x \in K$), and such that iK is dense in K_v. If (K_v', i') is another such pair, then there exists a unique*

isomorphism $\varphi : K_v \to K'_v$ *preserving the absolute values, and making the following diagram commutative:*



Proof. The uniqueness is obvious. One proves the existence in the well-known manner, which we shall now recall briefly, leaving the details to the reader.

The Cauchy sequences form a ring, addition and multiplication being taken componentwise.

One defines a null sequence to be a sequence $\{x_n\}$ such that $\lim_{n\to\infty} x_n = 0$. The null sequences form an ideal in the ring of Cauchy sequences, and in fact form a maximal ideal. (If a Cauchy sequence is not a null sequence, then it stays away from 0 for all n sufficiently large, and one can then take the inverse of almost all its terms. Up to a finite number of terms, one then gets again a Cauchy sequence.)

The residue class field of Cauchy sequences modulo null sequences is the field K_v. We embed K in K_v "on the diagonal", i.e. send $x \in K$ on the sequence $(x, x, x, \ldots)$.

We extend the absolute value of K to K_v by continuity. If $\{x_n\}$ is a Cauchy sequence, representing an element ξ in K_v, we define $|\xi| = \lim |x_n|$. It is easily proved that this yields an absolute value (independent of the choice of representative sequence $\{x_n\}$ for ξ), and this absolute value induces the given one on K.

Finally, one proves that K_v is complete. Let $\{\xi_n\}$ be a Cauchy sequence in K_v. For each n, we can find an element $x_n \in K$ such that $|\xi_n - x_n| < 1/n$. Then one verifies immediately that $\{x_n\}$ is a Cauchy sequence in K. We let ξ be its limit in K_v. By a three-ϵ argument, one sees that $\{\xi_n\}$ converges to ξ, thus proving the completeness.

A pair (K_v, i) as in Proposition 2.1 may be called a **completion** of K. The standard pair obtained by the preceding construction could be called **the completion** of K.

Let K have a non-trivial archimedean absolute value v. If one knows that the restriction of v to the rationals is dependent on the ordinary absolute value, then the completion K_v is a complete field, containing the completion of $\mathbf{Q}$ as a closed subfield, i.e. containing the real numbers $\mathbf{R}$ as a closed subfield. It will be worthwhile to state the theorem of Gelfand-Mazur concerning the structure of such fields. First we define the notion of normed vector space.

Let K be a field with a non-trivial absolute value, and let E be a vector space over K. By a **norm** on E (compatible with the absolute value of K) we shall mean a function $\xi \to |\xi|$ of E into the real numbers such that:

NO 1. $|\xi| \geqq 0$ for all $\xi \in E$, and $= 0$ if and only if $\xi = 0$.

NO 2. For all $x \in K$ and $\xi \in E$ we have $|x\xi| = |x||\xi|$.

NO 3. If $\xi, \xi' \in E$ then $|\xi + \xi'| \leqq |\xi| + |\xi'|$.

Two norms $|\ |_1$ and $|\ |_2$ are called **equivalent** if there exist numbers $C_1, C_2 > 0$ such that for all $\xi \in E$ we have

$$C_1|\xi|_1 \leqq |\xi|_2 \leqq C_2|\xi|_1.$$

Suppose that E is finite dimensional, and let $\omega_1, \ldots, \omega_n$ be a basis of E over K. If we write an element

$$\xi = x_1\omega_1 + \cdots + x_n\omega_n$$

in terms of this basis, with $x_i \in K$, then we can define a norm by putting

$$|\xi| = \max_i |x_i|.$$

The three properties defining a norm are trivially satisfied.

Proposition 2.2. *Let K be a complete field under a non-trivial absolute value, and let E be a finite-dimensional space over K. Then any two norms on E (compatible with the given absolute value on K) are equivalent.*

Proof. We shall first prove that the topology on E is that of a product space, i.e. if $\omega_1, \ldots, \omega_n$ is a basis of E over K, then a sequence

$$\xi^{(v)} = x_1^{(v)}\omega_1 + \cdots + x_n^{(v)}\omega_n, \qquad x_i^{(v)} \in K,$$

is a Cauchy sequence in E only if each one of the n sequences $x_i^{(v)}$ is a Cauchy sequence in K. We do this by induction on n. It is obvious for $n = 1$. Assume $n \geqq 2$. We consider a sequence as above, and without loss of generality, we may assume that it converges to 0. (If necessary, consider $\xi^{(v)} - \xi^{(\mu)}$ for $v, \mu \to \infty$.) We must then show that the sequences of the coefficients converge to 0 also. If this is not the case, then there exists a number $a > 0$ such that we have for some j, say $j = 1$,

$$|x_1^{(v)}| > a$$

for arbitrarily large v. Thus for a subsequence of (v), $\xi^{(v)}/x_1^{(v)}$ converges to 0, and we can write

$$\frac{\xi^{(v)}}{x_1^{(v)}} - \omega_1 = \frac{x_2^{(v)}}{x_1^{(v)}}\omega_2 + \cdots + \frac{x_n^{(v)}}{x_1^{(v)}}\omega_n.$$

We let $\eta^{(v)}$ be the right-hand side of this equation. Then the subsequence $\eta^{(v)}$ converges (according to the left-hand side of our equation). By induction, we

conclude that its coefficients in terms of $\omega_2, \ldots, \omega_n$ also converge in K, say to $y_2, \ldots, y_n$. Taking the limit, we get

$$\omega_1 = y_2\omega_2 + \cdots + y_n\omega_n,$$

contradicting the linear independence of the ω_i.

We must finally see that two norms inducing the same topology are equivalent. Let $|\ |_1$ and $|\ |_2$ be these norms. There exists a number $C > 0$ such that for any $\xi \in E$ we have

$$|\xi|_1 \leqq C \quad \text{implies} \quad |\xi|_2 \leqq 1.$$

Let $a \in K$ be such that $0 < |a| < 1$. For every $\xi \in E$ there exists a unique integer s such that

$$C|a| < |a^s\xi|_1 \leqq C.$$

Hence $|a^s\xi|_2 \leqq 1$ whence we get at once

$$|\xi|_2 \leqq C^{-1}|a|^{-1}|\xi|_1.$$

The other inequality follows by symmetry, with a similar constant.

Theorem 2.3. (Gelfand-Mazur). *Let A be a commutative algebra over the real numbers, and assume that A contains an element j such that $j^2 = -1$. Let $\mathbf{C} = \mathbf{R} + \mathbf{R}j$. Assume that A is normed (as a vector space over $\mathbf{R}$), and that $|xy| \leqq |x|\,|y|$ for all $x, y \in A$. Given $x_0 \in A$, $x_0 \neq 0$, there exists an element $c \in \mathbf{C}$ such that $x_0 - c$ is not invertible in A.*

Proof. (Tornheim). Assume that $x_0 - z$ is invertible for all $z \in \mathbf{C}$. Consider the mapping $f : \mathbf{C} \to A$ defined by

$$f(z) = (x_0 - z)^{-1}.$$

It is easily verified (as usual) that taking inverses is a continuous operation. Hence f is continuous, and for $z \neq 0$ we have

$$f(z) = z^{-1}(x_0 z^{-1} - 1)^{-1} = \frac{1}{z}\left(\frac{1}{\dfrac{x_0}{z} - 1}\right).$$

From this we see that $f(z)$ approaches 0 when z goes to infinity (in $\mathbf{C}$). Hence the map $z \mapsto |f(z)|$ is a continuous map of $\mathbf{C}$ into the real numbers $\geqq 0$, is bounded, and is small outside some large circle. Hence it has a maximum, say M. Let D

be the set of elements $z \in \mathbf{C}$ such that $|f(z)| = M$. Then D is not empty; D is bounded and closed. We shall prove that D is open, hence a contradiction.

Let c_0 be a point of D, which, after a translation, we may assume to be the origin. We shall see that if r is real > 0 and small, then all points on the circle of radius r lie in D. Indeed, consider the sum

$$S(n) = \frac{1}{n} \sum_{k=1}^{n} \frac{1}{x_0 - \omega^k r}$$

where ω is a primitive n-th root of unity. Taking formally the logarithmic derivative of $X^n - r^n = \prod_{k=1}^{n} (X - \omega^k r)$ shows that

$$\frac{nX^{n-1}}{X^n - r^n} = \sum_{k=1}^{n} \frac{1}{X - \omega^k r},$$

and hence, dividing by n, and by X^{n-1}, and substituting x_0 for X, we obtain

$$S(n) = \frac{1}{x_0 - r(r/x_0)^{n-1}}.$$

If r is small (say $|r/x_0| < 1$), then we see that

$$\lim_{n \to \infty} |S(n)| = \left| \frac{1}{x_0} \right| = M.$$

Suppose that there exists a complex number λ of absolute value 1 such that

$$\left| \frac{1}{x_0 - \lambda r} \right| < M.$$

Then there exists an interval on the unit circle near λ, and there exists $\epsilon > 0$ such that for all roots of unity ζ lying in this interval, we have

$$\left| \frac{1}{x_0 - \zeta r} \right| < M - \epsilon.$$

(This is true by continuity.) Let us take n very large. Let b_n be the number of n-th roots of unity lying in our interval. Then b_n/n is approximately equal to the length of the interval (times 2π): We can express $S(n)$ as a sum

$$S(n) = \frac{1}{n} \left[\sum_{\mathrm{I}} \frac{1}{x_0 - \omega^k r} + \sum_{\mathrm{II}} \frac{1}{x_0 - \omega^k r} \right],$$

the first sum $\sum_{\text{I}}$ being taken over those roots of unity ω^k lying in our interval, and the second sum being taken over the others. Each term in the second sum has norm $\leqq M$ because M is a maximum. Hence we obtain the estimate

$$|S(n)| \leqq \frac{1}{n}[|\sum_{\text{I}}| + |\sum_{\text{II}}|]$$

$$\leqq \frac{1}{n}(b_n(M - \epsilon) + (n - b_n)M)$$

$$\leqq M - \frac{b_n}{n}\epsilon.$$

This contradicts the fact that the limit of $|S(n)|$ is equal to M.

Corollary 2.4. *Let K be a field, which is an extension of $\mathbf{R}$, and has an absolute value extending the ordinary absolute value on $\mathbf{R}$. Then $K = \mathbf{R}$ or $K = \mathbf{C}$.*

Proof. Assume first that K contains $\mathbf{C}$. Then the assumption that K is a field and Theorem 2.3 imply that $K = \mathbf{C}$.

If K does not contain $\mathbf{C}$, in other words, does not contain a square root of -1, we let $L = K(j)$ where $j^2 = -1$. We define a norm on L (as an $\mathbf{R}$-space) by putting

$$|x + yj| = |x| + |y|$$

for $x, y \in K$. This clearly makes L into a normed $\mathbf{R}$-space. Furthermore, if $z = x + yj$ and $z' = x' + y'j$ are in L, then

$$\begin{aligned} |zz'| &= |xx' - yy'| + |xy' + x'y| \\ &\leqq |xx'| + |yy'| + |xy'| + |x'y| \\ &\leqq |x||x'| + |y||y'| + |x||y'| + |x'||y| \\ &\leqq (|x| + |y|)(|x'| + |y'|) \\ &\leqq |z||z'|, \end{aligned}$$

and we can therefore apply Theorem 2.3 again to conclude the proof.

As an important application of Proposition 2.2, we have:

Proposition 2.5. *Let K be complete with respect to a nontrivial absolute value v. If E is any algebraic extension of K, then v has a unique extension to E. If E is finite over K, then E is complete.*

Proof. In the archimedean case, the existence is obvious since we deal with the real and complex numbers. In the non-archimedean case, we postpone

the existence proof to a later section. It uses entirely different ideas from the present ones. As to uniqueness, we may assume that E is finite over K. By Proposition 2.2, an extension of v to E defines the same topology as the max norm obtained in terms of a basis as above. Given a Cauchy sequence $\xi^{(\nu)}$ in E,

$$\xi^{(\nu)} = x_{\nu 1}\omega_1 + \cdots + x_{\nu n}\omega_n,$$

the n sequences $\{x_{\nu i}\}(i = 1, \ldots, n)$ must be Cauchy sequences in K by the definition of the max norm. If $\{x_{\nu i}\}$ converges to an element z_i in K, then it is clear that the sequence $\xi^{(\nu)}$ converges to $z_1\omega_1 + \cdots + z_n\omega_n$. Hence E is complete. Furthermore, since any two extensions of v to E are equivalent, we can apply Proposition 1.1, and we see that we must have $\lambda = 1$, since the extensions induce the same absolute value v on K. This proves what we want.

From the uniqueness we can get an explicit determination of the absolute value on an algebraic extension of K. Observe first that if E is a normal extension of K, and σ is an automorphism of E over K, then the function

$$x \mapsto |\sigma x|$$

is an absolute value on E extending that of K. Hence we must have

$$|\sigma x| = |x|$$

for all $x \in E$. If E is algebraic over K, and σ is an embedding of E over K in K^a, then the same conclusion remains valid, as one sees immediately by embedding E in a normal extension of K. In particular, if α is algebraic over K, of degree n, and if $\alpha_1, \ldots, \alpha_n$ are its conjugates (counting multiplicities, equal to the degree of inseparability), then all the absolute values $|\alpha_i|$ are equal. Denoting by N the norm from $K(\alpha)$ to K, we see that

$$|N(\alpha)| = |\alpha|^n,$$

and taking the n-th root, we get:

Proposition 2.6. *Let K be complete with respect to a non-trivial absolute value. Let α be algebraic over K, and let N be the norm from $K(\alpha)$ to K. Let $n = [K(\alpha) : K]$. Then*

$$|\alpha| = |N(\alpha)|^{1/n}.$$

In the special case of the complex numbers over the real numbers, we can write $\alpha = a + bi$ with $a, b \in \mathbf{R}$, and we see that the formula of Proposition 2.6 is a generalization of the formula for the absolute value of a complex number,

$$\alpha = (a^2 + b^2)^{1/2},$$

since $a^2 + b^2$ is none other than the norm of α from $\mathbf{C}$ to $\mathbf{R}$.

Comments and examples. The process of completion is widespread in mathematics. The first example occurs in getting the real numbers from the rational numbers, with the added property of ordering. I carry this process out in full in [La 90a], Chapter IX, §3. In all other examples I know, the ordering property does not intervene. We have seen examples of completions of fields in this chapter, especially with the p-adic absolute values which are far away from ordering the field. But the real numbers are nevertheless needed as the range of values of absolute values, or more generally norms.

In analysis, one completes various spaces with various norms. Let V be a vector space over the complex numbers, say. For many applications, one must also deal with a seminorm, which satisfies the same conditions except that in **NO 1** we require only that $\|\xi\| \geqq 0$. We allow $\|\xi\| = 0$ even if $\xi \neq 0$.

One may then form the space of Cauchy sequences, the subspace of null sequences, and the factor space $\overline{V}$. The seminorm can be extended to a seminorm on $\overline{V}$ by continuity, and this extension actually turns out to be a norm. It is a general fact that $\overline{V}$ is then complete under this extension. A **Banach space** is a complete normed vector space.

Example. Let V be the vector space of step functions on $\mathbf{R}$, a step function being a complex valued function which is a finite sum of characteristic functions of intervals (closed, open, or semiclosed, i.e. the intervals may or may not contain their endpoints). For $f \in V$ we define the **L^1-seminorm** by

$$\|f\|_1 = \int_{\mathbf{R}} |f(x)|\, dx.$$

The completion of V with respect to this seminorm is defined to be $L^1(\mathbf{R})$. One then wants to get a better idea of what elements of $L^1(\mathbf{R})$ look like. It is a simple lemma that given an L^1-Cauchy sequence in V, and given $\varepsilon > 0$, there exists a subsequence which converges uniformly except on a set of measure less than ε. Thus elements of $L^1(\mathbf{R})$ can be identified with pointwise limits of L^1-Cauchy sequences in V. The reader will find details carried out in [La 85].

Analysts use other norms or seminorms, of course, and other spaces, such as the space of C^∞ functions on $\mathbf{R}$ with compact support, and norms which may bound the derivatives. There is no end to the possible variations.

Theorem 2.3 and Corollary 2.4 are also used in the theory of Banach algebras, representing a certain type of Banach algebra as the algebra of continuous functions on a compact space, with the Gelfand-Mazur and Gelfand-Naimark theorems. Cf. [Ri 60] and [Ru 73].

Arithmetic example. For p-adic Banach spaces in connection with the number theoretic work of Dwork, see for instance Serre [Se 62], or also [La 90b], Chapter 15.

In this book we limit ourselves to complete fields and their finite extensions.

Bibliography

[La 85] S. LANG, *Real and Functional Analysis*, Springer Verlag, 1993

[La 90a] S. LANG, *Undergraduate Algebra*, Second Edition, Springer Verlag, 1990

[La 90b] S. LANG, *Cyclotomic Fields* I *and* II, Springer Verlag 1990 (combined from the first editions, 1978 and 1980)

[Ri 60] C. RICKART, *Banach Algebras*, Van Nostrand (1960), Theorems 1.7.1 and 4.2.2.

[Ru 73] W. RUDIN, *Functional Analysis*, McGraw Hill (1973) Theorems 10.14 and 11.18.

[Se 62] J. P. SERRE, Endomorphismes complêtement continus des espaces de Banach p-adiques, *Pub. Math. IHES* **12** (1962), pp. 69–85

§3. FINITE EXTENSIONS

Throughout this section we shall deal with a field K having a non-trivial absolute value v.

We wish to describe how this absolute value extends to finite extensions of K. If E is an extension of K and w is an absolute value on E extending v, then we shall write $w|v$.

If we let K_v be the completion, we know that v can be extended to K_v, and then uniquely to its algebraic closure K_v^a. If E is a finite extension of K, or even an algebraic one, then we can extend v to E by embedding E in K_v^a by an isomorphism over K, and taking the induced absolute value on E. We shall now prove that every extension of v can be obtained in this manner.

Proposition 3.1. *Let E be a finite extension of K. Let w be an absolute value on E extending v, and let E_w be the completion. Let K_w be the closure of K in E_w and identify E in E_w. Then $E_w = EK_w$ (the composite field).*

Proof. We observe that K_w is a completion of K, and that the composite field EK_w is algebraic over K_w and therefore complete by Proposition 2.5. Since it contains E, it follows that E is dense in it, and hence that $E_w = EK_w$.

If we start with an embedding $\sigma : E \to K_v^a$ (always assumed to be over K), then we know again by Proposition 2.5 that $\sigma E \cdot K_v$ is complete. Thus this construction and the construction of the proposition are essentially the same, up to an isomorphism. In the future, we take the embedding point of view. We must now determine when two embeddings give us the same absolute value on E.

Given two embeddings $\sigma, \tau : E \to K_v^a$, we shall say that they are **conjugate over K_v** if there exists an automorphism λ of K_v^a over K_v such that $\sigma = \lambda\tau$. We see that actually λ is determined by its effect on τE, or $\tau E \cdot K_v$.

Proposition 3.2. *Let E be an algebraic extension of K. Two embeddings $\sigma, \tau : E \to K_v^a$ give rise to the same absolute value on E if and only if they are conjugate over K_v.*

Proof. Suppose they are conjugate over K_v. Then the uniqueness of the extension of the absolute value from K_v to K_v^a guarantees that the induced absolute values on E are equal. Conversely, suppose this is the case. Let $\lambda : \tau E \to \sigma E$ be an isomorphism over K. We shall prove that λ extends to an isomorphism of $\tau E \cdot K_v$ onto $\sigma E \cdot K_v$ over K_v. Since τE is dense in $\tau E \cdot K_v$, an element $x \in \tau E \cdot K_v$ can be written

$$x = \lim \tau x_n$$

with $x_n \in E$. Since the absolute values induced by σ and τ on E coincide, it follows that the sequence $\lambda \tau x_n = \sigma x_n$ converges to an element of $\sigma E \cdot K_v$ which we denote by λx. One then verifies immediately that λx is independent of the particular sequence τx_n used, and that the map $\lambda : \tau E \cdot K_v \to \sigma E \cdot K_v$ is an isomorphism, which clearly leaves K_v fixed. This proves our proposition.

In view of the previous two propositions, if w is an extension of v to a finite extension E of K, then we may identify E_w and a composite extension EK_v of E and K_v. If $N = [E : K]$ is finite, then we shall call

$$N_w = [E_w : K_v]$$

the **local degree**.

Proposition 3.3. *Let E be a finite separable extension of K, of degree N. Then*

$$N = \sum_{w|v} N_w.$$

Proof. We can write $E = K(\alpha)$ for a single element α. Let $f(X)$ be its irreducible polynomial over K. Then over K_v, we have a decomposition

$$f(X) = f_1(X) \cdots f_r(X)$$

into irreducible factors $f_i(X)$. They all appear with multiplicity 1 according to our hypothesis of separability. The embeddings of E into K_v^a correspond to the maps of α onto the roots of the f_i. Two embeddings are conjugate if and only if they map α onto roots of the same polynomial f_i. On the other hand, it is clear that the local degree in each case is precisely the degree of f_i. This proves our proposition.

Proposition 3.4. *Let E be a finite extension of K. Then*

$$\sum_{w|v} [E_w : K_v] \leqq [E : K].$$

If E is purely inseparable over K, then there exists only one absolute value w on E extending v.

Proof. Let us first prove the second statement. If E is purely inseparable over K, and p^r is its inseparable degree, then $\alpha^{p^r} \in K$ for every α in E. Hence v has a unique extension to E. Consider now the general case of a finite extension, and let $F = E^{p^r}K$. Then F is separable over K and E is purely inseparable over F. By the preceding proposition,

$$\sum_{w|v} [F_w : K_v] = [F : K],$$

and for each w, we have $[E_w : F_w] \leqq [E : F]$. From this our inequality in the statement of the proposition is obvious.

Whenever v is an absolute value on K such that for any finite extension E of K we have $[E : K] = \sum_{w|v} [E_w : K_v]$ we shall say that v is **well behaved**. Suppose we have a tower of finite extensions, $L \supset E \supset K$. Let w range over the absolute values of E extending v, and u over those of L extending v. If $u|w$ then L_u contains E_w. Thus we have:

$$\begin{aligned}
\sum_{u|v} [L_u : K_v] &= \sum_{w|v} \sum_{u|w} [L_u : E_w][E_w : K_v] \\
&= \sum_{w|v} [E_w : K_v] \sum_{u|w} [L_u : E_w] \\
&\leqq \sum_{w|v} [E_w : K_v][L : E] \\
&\leqq [E : K][L : E].
\end{aligned}$$

From this we immediately see that if v is well behaved, E finite over K, and w extends v on E, then w is well behaved (we must have an equality everywhere).

Let E be a finite extension of K. Let p^r be its inseparable degree. We recall that the norm of an element $\alpha \in K$ is given by the formula

$$N_K^E(\alpha) = \prod_\sigma \sigma\alpha^{p^r}$$

where σ ranges over all distinct isomorphisms of E over K (into a given algebraic closure).

If w is an absolute value extending v on E, then the norm from E_w to K_v will be called the **local norm**.

Replacing the above product by a sum, we get the trace, and the local trace. We abbreviate the trace by Tr.

Proposition 3.8. *Let E be a finite extension of K, and assume that v is well*

behaved. Let $\alpha \in E$. *Then*:

$$N_K^E(\alpha) = \prod_{w|v} N_{K_v}^{E_w}(\alpha)$$

$$\mathrm{Tr}_K^E(\alpha) = \sum_{w|v} \mathrm{Tr}_{K_v}^{E_w}(\alpha)$$

Proof. Suppose first that $E = K(\alpha)$, and let $f(X)$ be the irreducible polynomial of α over K. If we factor $f(X)$ into irreducible terms over K_v, then

$$f(X) = f_1(X) \cdots f_r(X)$$

where each $f_i(X)$ is irreducible, and the f_i are distinct because of our hypothesis that v is well behaved. The norm $N_K^E(\alpha)$ is equal to $(-1)^{\deg f}$ times the constant term of f, and similarly for each f_i. Since the constant term of f is equal to the product of the constant terms of the f_i, we get the first part of the proposition. The statement for the trace follows by looking at the penultimate coefficient of f and each f_i.

If E is not equal to $K(\alpha)$, then we simply use the transitivity of the norm and trace. We leave the details to the reader.

One can also argue directly on the embeddings. Let $\sigma_1, \ldots, \sigma_m$ be the distinct embeddings of E into K_v^a over K, and let p^r be the inseparable degree of E over K. The inseparable degree of $\sigma E \cdot K_v$ over K_v for any σ is at most equal to p^r. If we separate $\sigma_1, \ldots, \sigma_m$ into distinct conjugacy classes over K_v, then from our hypothesis that v is well behaved, we conclude at once that the inseparable degree of $\sigma_i E \cdot K_v$ over K_v must be equal to p^r also, for each i. Thus the formula giving the norm as a product over conjugates with multiplicity p^r breaks up into a product of factors corresponding to the conjugacy classes over K_v.

Taking into account Proposition 2.6, we have:

Proposition 3.6. *Let* K *have a well-behaved absolute value* v. *Let* E *be a finite extension of* K, *and* $\alpha \in E$. *Let*

$$N_w = [E_w : K_v]$$

for each absolute value w *on* E *extending* v. *Then*

$$\prod_{w|v} |\alpha|_w^{N_w} = |N_K^E(\alpha)|_v.$$

§4. VALUATIONS

In this section, we shall obtain, among other things, the existence theorem concerning the possibility of extending non-archimedean absolute values to algebraic extensions. We introduce first a generalization of the notion of non-archimedean absolute value.

Let Γ be a multiplicative commutative group. We shall say that an **ordering** is defined in Γ if we are given a subset S of Γ closed under multiplication such that Γ is the disjoint union of S, the unit element 1, and the set S^{-1} consisting of all inverses of elements of S.

If $\alpha, \beta \in \Gamma$ we define $\alpha < \beta$ to mean $\alpha\beta^{-1} \in S$. We have $\alpha < 1$ if and only if $\alpha \in S$. One easily verifies the following properties of the relation $<$:

1. For $\alpha, \beta \in \Gamma$ we have $\alpha < \beta$, or $\alpha = \beta$, or $\beta < \alpha$, and these possibilities are mutually exclusive.
2. $\alpha < \beta$ implies $\alpha\gamma < \beta\gamma$ for any $\gamma \in \Gamma$.
3. $\alpha < \beta$ and $\beta < \gamma$ implies $\alpha < \gamma$.

(Conversely, a relation satisfying the three properties gives rise to a subset S consisting of all elements < 1. However, we don't need this fact in the sequel.)

It is convenient to attach to an ordered group formally an extra element 0, such that $0\alpha = 0$, and $0 < \alpha$ for all $\alpha \in \Gamma$. The ordered group is then analogous to the multiplicative group of positive reals, except that there may be non-archimedean ordering.

If $\alpha \in \Gamma$ and n is an integer $\neq 0$, such that $\alpha^n = 1$, then $\alpha = 1$. This follows at once from the assumption that S is closed under multiplication and does not contain 1. In particular, the map $\alpha \mapsto \alpha^n$ is injective.

Let K be a field. By a **valuation** of K we shall mean a map $x \mapsto |x|$ of K into an ordered group Γ, together with the extra element 0, such that:

VAL 1. $|x| = 0$ if and only if $x = 0$.

VAL 2. $|xy| = |x||y|$ for all $x, y \in K$.

VAL 3. $|x + y| \leqq \max(|x|, |y|)$.

We see that a valuation gives rise to a homomorphism of the multiplicative group K^* into Γ. The valuation is called **trivial** if it maps K^* on 1. If the map giving the valuation is not surjective, then its image is an ordered subgroup of Γ, and by taking its restriction to this image, we obtain a valuation onto an ordered group, called the **value group**.

We shall denote valuations also by v. If v_1, v_2 are two valuations of K, we shall say that they are **equivalent** if there exists an order-preserving isomorphism λ of the image of v_1 onto the image of v_2 such that

$$|x|_2 = \lambda|x|_1$$

for all $x \in K$. (We agree that $\lambda(0) = 0$.)

Valuations have additional properties, like absolute values. For instance, $|1| = 1$ because $|1| = |1|^2$. Furthermore,

$$|\pm x| = |x|$$

for all $x \in K$. Proof obvious. Also, if $|x| < |y|$ then

$$|x + y| = |y|.$$

To see this, note that under our hypothesis, we have

$$|y| = |y + x - x| \leqq \max(|y + x|, |x|) = |x + y| \leqq \max(|x|, |y|) = |y|.$$

Finally, in a sum

$$x_1 + \cdots + x_n = 0,$$

at least two elements of the sum have the same value. This is an immediate consequence of the preceding remark.

Let K be a field. A subring $\mathfrak{o}$ of K is called a **valuation ring** if it has the property that for any $x \in K$ we have $x \in \mathfrak{o}$ or $x^{-1} \in \mathfrak{o}$.

We shall now see that valuation rings give rise to valuations. Let $\mathfrak{o}$ be a valuation ring of K and let U be the group of units of $\mathfrak{o}$. We contend that $\mathfrak{o}$ is a local ring. Indeed suppose that $x, y \in \mathfrak{o}$ are not units. Say $x/y \in \mathfrak{o}$. Then

$$1 + x/y = (x + y)/y \in \mathfrak{o}.$$

If $x + y$ were a unit then $1/y \in \mathfrak{o}$, contradicting the assumption that y is not a unit. Hence $x + y$ is not a unit. One sees trivially that for $z \in \mathfrak{o}$, zx is not a unit. Hence the nonunits form an ideal, which must therefore be the unique maximal ideal of $\mathfrak{o}$.

Let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$ and let $\mathfrak{m}^*$ be the multiplicative system of nonzero elements of $\mathfrak{m}$. Then

$$K^* = \mathfrak{m}^* \cup U \cup \mathfrak{m}^{*-1}$$

is the disjoint union of $\mathfrak{m}^*$, U, and $\mathfrak{m}^{*-1}$. The factor group K^*/U can now be given an ordering. If $x \in K^*$, we denote the coset xU by $|x|$. We put $|0| = 0$. We define $|x| < 1$ (i.e. $|x| \in S$) if and only if $x \in \mathfrak{m}^*$. Our set S is clearly closed under multiplication, and if we let $\Gamma = K^*/U$ then Γ is the disjoint union of S, 1, S^{-1}. In this way we obtain a valuation of K.

We note that if $x, y \in K$ and $x, y \neq 0$, then

$$|x| < |y| \Leftrightarrow |x/y| < 1 \Leftrightarrow x/y \in \mathfrak{m}^*.$$

Conversely, given a valuation of K into an ordered group we let $\mathfrak{o}$ be the subset of K consisting of all x such that $|x| < 1$. It follows at once from the

axioms of a valuation that $\mathfrak{o}$ is a ring. If $|x| < 1$ then $|x^{-1}| > 1$ so that x^{-1} is not in $\mathfrak{o}$. If $|x| = 1$ then $|x^{-1}| = 1$. We see that $\mathfrak{o}$ is a valuation ring, whose maximal ideal consists of those elements x with $|x| < 1$ and whose units consist of those elements x with $|x| = 1$. The reader will immediately verify that there is a bijection between valuation rings of K and equivalence classes of valuations.

The extension theorem for places and valuation rings in Chapter VII now gives us immediately the extension theorem for valuations.

Theorem 4.1. *Let K be a subfield of a field L. Then a valuation on K has an extension to a valuation on L.*

Proof. Let $\mathfrak{o}$ be the valuation ring on K corresponding to the given valuation. Let $\varphi : \mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ be the canonical homomorphism on the residue class field, and extend φ to a homomorphism of a valuation ring $\mathfrak{O}$ of L as in §3 of Chapter VII. Let $\mathfrak{M}$ be the maximal ideal of $\mathfrak{O}$. Since $\mathfrak{M} \cap \mathfrak{o}$ contains $\mathfrak{m}$ but does not contain 1, it follows that $\mathfrak{M} \cap \mathfrak{o} = \mathfrak{m}$. Let U' be the group of units of $\mathfrak{O}$. Then $U' \cap K = U$ is the group of units of $\mathfrak{o}$. Hence we have a canonical injection

$$K^*/U \to L^*/U'$$

which is immediately verified to be order-preserving. Identifying K^*/U in L^*/U' we have obtained an extension of our valuation of K to a valuation of L.

Of course, when we deal with absolute values, we require that the value group be a subgroup of the multiplicative reals. Thus we must still prove something about the nature of the value group L^*/U', whenever L is algebraic over K.

Proposition 4.2. *Let L be a finite extension of K, of degree n. Let w be a valuation of L with value group Γ'. Let Γ be the value group of K. Then $(\Gamma' : \Gamma) \leqq n$.*

Proof. Let $y_1, \ldots, y_r$ be elements of L whose values represent distinct cosets of Γ in Γ'. We shall prove that the y_j are linearly independent over K. In a relation $a_1 y_1 + \cdots + a_r y_r = 0$ with $a_j \in K$, $a_j \neq 0$ two terms must have the same value, say $|a_i y_i| = |a_j y_j|$ with $i \neq j$, and hence

$$|y_i| = |a_i^{-1} a_j| |y_j|.$$

This contradicts the assumption that the values of y_i, y_j $(i \neq j)$ represent distinct cosets of Γ in Γ', and proves our proposition.

Corollary 4.3. *There exists an integer $e \geqq 1$ such that the map $\gamma \mapsto \gamma^e$ induces an injective homomorphism of Γ' into Γ.*

Proof. Take e to be the index $(\Gamma' : \Gamma)$.

Corollary 4.4. *If K is a field with a valuation v whose value group is an ordered subgroup of the ordered group of positive real numbers, and if L is an algebraic extension of K, then there exists an extension of v to L whose value group is also an ordered subgroup of the positive reals.*

Proof. We know that we can extend v to a valuation w of L with some value group Γ', and the value group Γ of v can be identified with a subgroup of $\mathbf{R}^+$. By Corollary 4.3, every element of Γ' has finite period modulo Γ. Since every element of $\mathbf{R}^+$ has a unique e-th root for every integer $e \geqq 1$, we can find in an obvious way an order-preserving embedding of Γ' into $\mathbf{R}^+$ which induces the identity on Γ. In this way we get our extension of v to an absolute value on L.

Corollary 4.5. *If L is finite over K, and if Γ is infinite cyclic, then Γ' is also infinite cyclic.*

Proof. Use Corollary 4.3 and the fact that a subgroup of a cyclic group is cyclic.

We shall now strengthen our preceding proposition to a slightly stronger one. We call $(\Gamma' : \Gamma)$ the **ramification index**.

Proposition 4.6. *Let L be a finite extension of degree n of a field K, and let $\mathfrak{O}$ be a valuation ring of L. Let $\mathfrak{M}$ be its maximal ideal, let $\mathfrak{o} = \mathfrak{O} \cap K$, and let $\mathfrak{m}$ be the maximal ideal of $\mathfrak{o}$, i.e. $\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o}$. Then the residue class degree $[\mathfrak{O}/\mathfrak{M} : \mathfrak{o}/\mathfrak{m}]$ is finite. If we denote it by f, and if e is the ramification index, then $ef \leqq n$.*

Proof. Let $y_1, \ldots, y_e$ be representatives in L^* of distinct cosets of Γ'/Γ and let $z_1, \ldots, z_s$ be elements of $\mathfrak{O}$ whose residue classes mod $\mathfrak{M}$ are linearly independent over $\mathfrak{o}/\mathfrak{m}$. Consider a relation

$$\sum_{i,j} a_{ij} z_j y_i = 0$$

with $a_{ij} \in K$, not all $a_{ij} = 0$. In an inner sum

$$\sum_{j=1}^{s} a_{ij} z_j,$$

divide by the coefficient a_{iv} having the biggest valuation. We obtain a linear combination of $z_1, \ldots, z_s$ with coefficients in $\mathfrak{o}$, and at least one coefficient equal to a unit. Since $z_1, \ldots, z_s$ are linearly independent mod $\mathfrak{M}$ over $\mathfrak{o}/\mathfrak{m}$, it follows that our linear combination is a unit. Hence

$$\left| \sum_{j=1}^{s} a_{ij} z_j \right| = |a_{iv}|$$

for some index v. In the sum

$$\sum_{i=1}^{e}\left(\sum_{j=1}^{s} a_{ij}z_j\right)y_i = 0$$

viewed as a sum on i, at least two terms have the same value. This contradicts the independence of $|y_1|, \ldots, |y_e| \bmod \Gamma$ just as in the proof of Proposition 4.2.

Remark. Our proof also shows that the elements $\{z_j y_i\}$ are linearly independent over K. This will be used again later.

If w is an extension of a valuation v, then the ramification index will be denoted by $e(w|v)$ and the residue class degree will be denoted by $f(w|v)$.

Proposition 4.7. *Let K be a field with a valuation v, and let $K \subset E \subset L$ be finite extensions of K. Let w be an extension of v to E and let u be an extension of w to L. Then*

$$e(u|w)e(w|v) = e(u|v),$$
$$f(u|w)f(w|v) = f(u|v).$$

Proof. Obvious.

We can express the above proposition by saying that the ramification index and the residue class degree are multiplicative in towers.

We conclude this section by relating valuation rings in a finite extension with the integral closure.

Proposition 4.8. *Let $\mathfrak{o}$ be a valuation ring in a field K. Let L be a finite extension of K. Let $\mathfrak{O}$ be a valuation ring of L lying above $\mathfrak{o}$, and $\mathfrak{M}$ its maximal ideal. Let B be the integral closure of $\mathfrak{o}$ in L, and let $\mathfrak{P} = \mathfrak{M} \cap B$. Then $\mathfrak{O}$ is equal to the local ring $B_{\mathfrak{P}}$.*

Proof. It is clear that $B_{\mathfrak{P}}$ is contained in $\mathfrak{O}$. Conversely, let x be an element of $\mathfrak{O}$. Then x satisfies an equation with coefficients in K, not all 0, say

$$a_n x^n + \cdots + a_0 = 0, \qquad a_i \in K.$$

Suppose that a_s is the coefficient having the biggest value among the a_i for the valuation associated with the valuation ring $\mathfrak{o}$, and that it is the coefficient farthest to the left having this value. Let $b_i = a_i/a_s$. Then all $b_i \in \mathfrak{o}$ and

$$b_n, \ldots, b_{s+1} \in \mathfrak{M}.$$

Divide the equation by x^s. We get

$$(b_n x^{n-s} + \cdots + b_{s+1}x + 1) + \frac{1}{x}\left(b_{s-1} + \cdots + b_0 \frac{1}{x^{s-1}}\right) = 0.$$

Let y and z be the two quantities in parentheses in the preceding equation, so that we can write

$$-y = z/x \quad \text{and} \quad -xy = z.$$

To prove our proposition it will suffice to show that y and z lie in B and that y is not in $\mathfrak{P}$.

We use Proposition 3.5 of Chapter VII. If a valuation ring of L above contains x, then it contains y because y is a polynomial in x with coefficients in

Hence such a valuation ring also contains $z = -xy$. If on the other hand the valuation ring of L above contains $1/x$, then it contains z because z is a polynomial in $1/x$ with coefficients in . Hence this valuation ring also contains y. From this we conclude by Chapter VII, Proposition 3.5, that y, z lie in B.

Furthermore, since $x \in \mathfrak{O}$, and $b_n, \ldots, b_{s+1}$ are in $\mathfrak{M}$ by construction, it follows that y cannot be in $\mathfrak{M}$, and hence cannot be in $\mathfrak{P}$. This concludes the proof.

Corollary 4.9. *Let the notation be as in the proposition. Then there is only a finite number of valuation rings of L lying above* $\mathfrak{P}$.

Proof. This comes from the fact that there is only a finite number of maximal ideals $\mathfrak{P}$ of B lying above the maximal ideal of $\mathfrak{o}$ (Corollary of Proposition 2.1, Chapter VII).

Corollary 4.10. *Let the notation be as in the proposition. Assume in addition that L is Galois over K. If* $\mathfrak{O}$ *and* $\mathfrak{O}'$ *are two valuation rings of L lying above* $\mathfrak{o}$, *with maximal ideals* $\mathfrak{M}$, $\mathfrak{M}'$ *respectively, then there exists an automorphism* σ *of L over K such that* $\sigma\mathfrak{O} = \mathfrak{O}'$ *and* $\sigma\mathfrak{M} = \mathfrak{M}'$.

Proof. Let $\mathfrak{P} = \mathfrak{O} \cap B$ and $\mathfrak{P}' = \mathfrak{O}' \cap B$. By Proposition 2.1 of Chapter VII, we know that there exists an automorphism σ of L over K such that $\sigma\mathfrak{P} = \mathfrak{P}'$. From this our assertion is obvious.

Example. Let k be a field, and let K be a finitely generated extension of transcendence degree 1. If t is a transcendence base of K over k, then K is finite algebraic over $k(t)$. Let $\mathfrak{O}$ be a valuation ring of K containing k, and assume that $\mathfrak{O}$ is $\neq K$. Let $\mathfrak{o} = \mathfrak{O} \cap k(t)$. Then $\mathfrak{o}$ is obviously a valuation ring of $k(t)$ (the

condition about inverses is *a fortiori* satisfied), and the corresponding valuation of $k(t)$ cannot be trivial. Either t or $t^{-1} \in \mathfrak{o}$. Say $t \in \mathfrak{o}$. Then $\mathfrak{o} \cap k[t]$ cannot be the zero ideal, otherwise the canonical homomorphism $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ of $\mathfrak{o}$ modulo its maximal ideal would induce an isomorphism on $k[t]$ and hence an isomorphism on $k(t)$, contrary to hypothesis. Hence $\mathfrak{m} \cap k[t]$ is a prime ideal $\mathfrak{p}$, generated by an irreducible polynomial $p(t)$. The local ring $k[t]_{\mathfrak{p}}$ is obviously a valuation ring, which must be $\mathfrak{o}$ because every element of $k(t)$ has an expression of type $p^r u$ where u is a unit in $k[t]_{\mathfrak{p}}$. Thus we have determined all valuation rings of $k(t)$ containing k, and we see that the value group is cyclic. Such valuations will be called discrete and are studied in greater detail below. In view of Corollary 4.5, it follows that the valuation ring $\mathfrak{O}$ of K is also discrete.

The residue class field $\mathfrak{o}/\mathfrak{m}$ is equal to $k[t]/\mathfrak{p}$ and is therefore a finite extension of k. By Proposition 4.6, it follows that $\mathfrak{O}/\mathfrak{M}$ is finite over k (if $\mathfrak{M}$ denotes the maximal ideal of $\mathfrak{O}$).

Finally, we observe that there is only a finite number of valuation rings $\mathfrak{O}$ of K containing k such that t lies in the maximal ideal of $\mathfrak{O}$. Indeed, such a valuation ring must lie above $k[t]_{\mathfrak{p}}$ where $\mathfrak{p} = (t)$ is the prime ideal generated by t, and we can apply Corollary 4.9.

§5. COMPLETIONS AND VALUATIONS

Throughout this section, we deal with a non-archimedean absolute value v on a field K. This absolute value is then a valuation, whose value group Γ_K is a subgroup of the positive reals. We let $\mathfrak{o}$ be its valuation ring, $\mathfrak{m}$ the maximal ideal.

Let us denote by $\hat{K}$ the completion of K at v, and let $\hat{\mathfrak{o}}$ (resp. $\hat{\mathfrak{m}}$) be the closure of $\mathfrak{o}$ (resp. $\mathfrak{m}$) in $\hat{K}$. By continuity, every element of $\hat{\mathfrak{o}}$ has value $\leqq 1$, and every element of $\hat{K}$ which is not in $\hat{\mathfrak{o}}$ has value > 1. If $x \in \hat{K}$ then there exists an element $y \in K$ such that $|x - y|$ is very small, and hence $|x| = |y|$ for such an element y (by the non-archimedean property). Hence $\hat{\mathfrak{o}}$ is a valuation ring in $\hat{K}$, and $\hat{\mathfrak{m}}$ is its maximal ideal. Furthermore,

$$\hat{\mathfrak{o}} \cap K = \mathfrak{o} \quad \text{and} \quad \hat{\mathfrak{m}} \cap K = \mathfrak{m},$$

and we have an isomorphism

$$\mathfrak{o}/\mathfrak{m} \xrightarrow{\sim} \hat{\mathfrak{o}}/\hat{\mathfrak{m}}.$$

Thus the residue class field $\mathfrak{o}/\mathfrak{m}$ does not change under completion.

Let E be an extension of K, and let $\mathfrak{o}_E$ be a valuation ring of E lying above $\mathfrak{o}$. Let $\mathfrak{m}_E$ be its maximal ideal. We assume that the valuation corresponding to $\mathfrak{o}_E$ is in fact an absolute value, so that we can form the completion E. We then have

a commutative diagram:

$$\begin{array}{ccc} \mathfrak{o}_E/\mathfrak{m}_E & \xrightarrow{\approx} & \hat{\mathfrak{o}}_E/\hat{\mathfrak{m}}_E \\ \uparrow & & \uparrow \\ \mathfrak{o}/\mathfrak{m} & \xrightarrow{\approx} & \hat{\mathfrak{o}}/\hat{\mathfrak{m}} \end{array}$$

the vertical arrows being injections, and the horizontal ones being isomorphisms. Thus the residue class field extension of our valuation can be studied over the completions E of K.

We have a similar remark for the ramification index. Let $\Gamma_v(K)$ and $\Gamma_v(\hat{K})$ denote the value groups of our valuation on K and $\hat{K}$ respectively (i.e. the image of the map $x \mapsto |x|$ for $x \in K^*$ and $x \in \hat{K}^*$ respectively). We saw above that $\Gamma_v(K) = \Gamma_v(\hat{K})$; in other words, the value group is the same under completion, because of the non-archimedean property. (This is of course false in the archimedean case.) If E is again an extension of K and w is an absolute value of E extending v, then we have a commutative diagram

$$\begin{array}{ccc} \Gamma_w(E) & \xrightarrow{=} & \Gamma_w(\hat{E}) \\ \uparrow & & \uparrow \\ \Gamma_v(K) & \xrightarrow{=} & \Gamma_v(\hat{K}) \end{array}$$

from which we see that the ramification index $(\Gamma_w(E) : \Gamma_v(K))$ also does not change under completion.

§6. DISCRETE VALUATIONS

A valuation is called **discrete** if its value group is cyclic. In that case, the valuation is an absolute value (if we consider the value group as a subgroup of the positive reals). The p-adic valuation on the rational numbers is discrete for each prime number p. By Corollary 4.5, an extension of a discrete valuation to a finite extension field is also discrete. Aside from the absolute values obtained by embedding a field into the reals or complex numbers, discrete valuations are the most important ones in practice. We shall make some remarks concerning them.

Let v be a discrete valuation on a field K, and let $\mathfrak{o}$ be its valuation ring. Let $\mathfrak{m}$ be the maximal ideal. There exists an element π of $\mathfrak{m}$ which is such that its value $|\pi|$ generates the value group. (The other generator of the value group is $|\pi^{-1}|$.) Such an element π is called a **local parameter** for v (or for $\mathfrak{m}$). Every

element x of K can be written in the form

$$x = u\pi^r$$

with some unit u of $\mathfrak{o}$, and some integer r. Indeed, we have $|x| = |\pi|^r = |\pi^r|$ for some $r \in \mathbf{Z}$, whence x/π^r is a unit in $\mathfrak{o}$. We call r the **order** of x at v. It is obviously independent of the choice of parameter selected. We also say that x has a **zero of order** r. (If r is negative, we say that x has a **pole** of order $-r$.)

In particular, we see that $\mathfrak{m}$ is a principal ideal, generated by π. As an exercise, we leave it to the reader to verify that every ideal of $\mathfrak{o}$ is principal, and is a power of $\mathfrak{m}$. Furthermore, we observe that $\mathfrak{o}$ is a factorial ring with exactly one prime element (up to units), namely π.

If $x, y \in K$, we shall write $x \sim y$ if $|x| = |y|$. Let π_i $(i = 1, 2, \ldots)$ be a sequence of elements of $\mathfrak{o}$ such that $\pi_i \sim \pi^i$. Let R be a set of representatives of $\mathfrak{o}/\mathfrak{m}$ in $\mathfrak{o}$. This means that the canonical map $\mathfrak{o} \to \mathfrak{o}/\mathfrak{m}$ induces a bijection of R onto $\mathfrak{o}/\mathfrak{m}$.

Assume that K is complete under our valuation. Then every element x of $\mathfrak{o}$ can be written as a convergent series

$$x = a_0 + a_1\pi_1 + a_2\pi_2 + \cdots$$

with $a_i \in R$, and the a_i are uniquely determined by x.

This is easily proved by a recursive argument. Suppose we have written

$$x \equiv a_0 + \cdots + a_n\pi_n \pmod{\mathfrak{m}^{n+1}}$$

then $x - (a_0 + \cdots + a_n\pi_n) = \pi_{n+1}y$ for some $y \in \mathfrak{o}$. By hypothesis, we can write $y = a_{n+1} + \pi z$ with some $a_{n+1} \in R$. From this we get

$$x \equiv a_0 + \cdots + a_{n+1}\pi_{n+1} \pmod{\mathfrak{m}^{n+2}},$$

and it is clear that the n-th term in our series tends to 0. Therefore our series converges (by the non-archimedean behavior!). The fact that R contains precisely one representative of each residue class mod $\mathfrak{m}$ implies that the a_i are uniquely determined.

Examples. Consider first the case of the rational numbers with the p-adic valuation v_p. The completion is denoted by $\mathbf{Q}_p$. It is the field of ***p*-adic numbers**. The closure of $\mathbf{Z}$ in $\mathbf{Q}_p$ is the ring of ***p*-adic integers** $\mathbf{Z}_p$. We note that the prime number p is a prime element in both $\mathbf{Z}$ and its closure $\mathbf{Z}_p$. We can select our set of representatives R to be the set of integers $(0, 1, \ldots, p-1)$. Thus every p-adic integer can be written uniquely as a convergent sum $\sum a_i p^i$ where a_i is an integer, $0 \leqq a_i \leqq p - 1$. This sum is called its p-adic expansion. Such sums are added and multiplied in the ordinary manner for convergent series.

For instance, we have the usual formalism of geometric series, and if we take $p = 3$, then

$$-1 = \frac{2}{1-3} = 2(1 + 3 + 3^2 + \cdots).$$

We note that the representatives $(0, 1, \ldots, p-1)$ are by no means the only ones which can be used. In fact, it can be shown that $\mathbf{Z}_p$ contains the $(p-1)$-th roots of unity, and it is often more convenient to select these roots of unity as representatives for the non-zero elements of the residue class field.

Next consider the case of a rational field $k(t)$, where k is any field and t is transcendental over k. We have a valuation determined by the prime element t in the ring $k[t]$. This valuation is discrete, and the completion of $k[t]$ under this valuation is the power series ring $k[[t]]$. In that case, we can take the elements of k itself as repersentatives of the residue class field, which is canonically isomorphic to k. The maximal ideal of $k[[t]]$ is the ideal generated by t.

This situation amounts to an algebraization of the usual situation arising in the theory of complex variables. For instance, let z_0 be a point in the complex plane. Let $\mathfrak{o}$ be the ring of functions which are holomorphic in some disc around z_0. Then $\mathfrak{o}$ is a discrete valuation ring, whose maximal ideal consists of those functions having a zero at z_0. Every element of $\mathfrak{o}$ has a power series expansion

$$f(z) = \sum_{\nu=m}^{\infty} a_\nu (z - z_0)^\nu.$$

The representatives of the residue class field can be taken to be complex numbers, a_ν. If $a_m \neq 0$, then we say that $f(z)$ has a zero of order m. The order is the same, whether viewed as order with respect to the discrete valuation in the algebraic sense, or the order in the sense of the theory of complex variables. We can select a canonical uniformizing parameter namely $z - z_0$, and

$$f(z) = (z - z_0)^m g(z)$$

where $g(z)$ is a power series beginning with a non-zero constant. Thus $g(z)$ is invertible.

Let K be again complete under a discrete valuation, and let E be a finite extension of K. Let $\mathfrak{o}_E$, $\mathfrak{m}_E$ be the valuation ring and maximal ideal in E lying above $\mathfrak{o}$, $\mathfrak{m}$ in K. Let π be a prime element in E. If Γ_E and Γ_K are the value groups of the valuations in E and K respectively, and

$$e = (\Gamma_E : \Gamma_K)$$

is the ramification index, then

$$|\Pi^e| = |\pi|,$$

and the elements

$$\Pi^i \pi^j, \qquad 0 \leqq i \leqq e-1, j = 0, 1, 2, \ldots$$

have order $je + i$ in E.

Let $\omega_1, \ldots, \omega_f$ be elements of E such that their residue classes mod $\mathfrak{m}_E$ from a basis of $\mathfrak{o}_E/\mathfrak{m}_E$. If R is as before a set of representatives of $\mathfrak{o}/\mathfrak{m}$ in $\mathfrak{o}$, then the set consisting of all elements

$$a_1\omega_1 + \cdots + a_f\omega_f$$

with $a_j \in R$ is a set of representatives of $\mathfrak{o}_E/\mathfrak{m}_E$ in $\mathfrak{o}_E$. From this we see that every element of $\mathfrak{o}_E$ admits a convergent expansion

$$\sum_{i=0}^{e-1} \sum_{v=1}^{f} \sum_{j=0}^{\infty} a_{v,i,j} \pi^j \omega_v \Pi^i.$$

Thus the elements $\{\omega_v \Pi^i\}$ form a set of generators of $\mathfrak{o}_E$ as a module over $\mathfrak{o}$. On the other hand, we have seen in the proof of Proposition 4.6 that these elements are linearly independent over K. Hence we obtain:

Proposition 6.1. *Let K be complete under a discrete valuation. Let E be a finite extension of K, and let e, f be the ramification index and residue class degree respectively. Then*

$$ef = [E : K].$$

Corollary 6.2. *Let $\alpha \in E$, $\alpha \neq 0$. Let v be the valuation on K and w its extension to E. Then*

$$\operatorname{ord}_v N_K^E(\alpha) = f(w|v) \operatorname{ord}_w \alpha.$$

Proof. This is immediate from the formula

$$|N_K^E(\alpha)| = |\alpha|^{ef}$$

and the definitions.

Corollary 6.3. *Let K be any field and v a discrete valuation on K. Let E be a finite extension of K. If v is well behaved in E (for instance if E is separable over K), then*

$$\sum_{w|v} e(w|v) f(w|v) = [E : K].$$

If E is Galois over K, then all e_w are equal to the same number e, all f_w are

equal to the same number f, and so

$$efr = [E : K],$$

where r is the number of extensions of v to E.

Proof. Our first assertion comes from our assumption, and Proposition 3.3. If E is Galois over K, we know from Corollary 4.10 that any two valuations of E lying above v are conjugate. Hence all ramification indices are equal, and similarly for the residue class degrees. Our relation $efr = [E : K]$ is then obvious.

§7. ZEROS OF POLYNOMIALS IN COMPLETE FIELDS

Let K be complete under a non-trivial absolute value.

Let

$$f(X) = \prod (X - \alpha_i)^{r_i}$$

be a polynomial in $K[X]$ having leading coefficient 1, and assume the roots α_i are distinct, with multiplicities r_i. Let d be the degree of f. Let g be another polynomial with coefficients in K^a, and assume that the degree of g is also d, and that g has leading coefficient 1. We let $|g|$ be the maximum of the absolute values of the coefficients of g. One sees easily that if $|g|$ is bounded, then the absolute values of the roots of g are also bounded.

Suppose that g comes close to f, in the sense that $|f - g|$ is small. If β is any root of g, then

$$|f(\beta) - g(\beta)| = |f(\beta)| = \prod |\alpha_i - \beta|^{r_i}$$

is small, and hence β must come close to some root of f. As β comes close to say $\alpha = \alpha_1$, its distance from the other roots of f approaches the distance of α_1 from the other roots, and is therefore bounded from below. In that case, we say that β **belongs to** α.

Proposition 7.1. *If g is sufficiently close to f, and $\beta_1, \ldots, \beta_s$ are the roots of g belonging to α (counting multiplicities), then $s = r_1$ is the multiplicity of α in f.*

Proof. Assume the contrary. Then we can find a sequence g_v of polynomials approaching f with precisely s roots $\beta_1^{(v)}, \ldots, \beta_s^{(v)}$ belonging to α, but with $s \neq r$. (We can take the same multiplicity s since there is only a finite number of choices for such multiplicities.) Furthermore, the other roots of g also

belong to roots of f, and we may suppose that these roots are bunched together, according to which root of f they belong to. Since $\lim g_v = f$, we conclude that α must have multiplicity s in f, contradiction.

Next we investigate conditions under which a polynomial has a root in a complete field.

We assume that K is complete under a discrete valuation, with valuation ring $\mathfrak{o}$, *maximal ideal* $\mathfrak{p}$. We let π be a fixed prime element of $\mathfrak{p}$.

We shall deal with n-space over $\mathfrak{o}$. We denote a vector $(a_1, \ldots, a_n)$ with $a_i \in \mathfrak{o}$ by A. If $f(X_1, \ldots, X_n) \in \mathfrak{o}[X]$ is a polynomial in n variables, with integral coefficients, we shall say that A is a **zero** of f if $f(A) = 0$, and we say that A is a **zero** of f mod $\mathfrak{p}^m$ if $f(A) \equiv 0 \pmod{\mathfrak{p}^m}$.

Let $C = (c_0, \ldots, c_n)$ be in $\mathfrak{o}^{(n+1)}$. Let m be an integer $\geqq 1$. We consider the nature of the solutions of a congruence of type

$$(*) \qquad \pi^m(c_0 + c_1x_1 + \cdots + c_nx_n) \equiv 0 \pmod{\mathfrak{p}^{m+1}}.$$

This congruence is equivalent with the linear congruence

$$(**) \qquad c_0 + c_1x_1 + \cdots + c_nx_n \equiv 0 \pmod{\mathfrak{p}}.$$

If some coefficient c_i $(i = 1, \ldots, n)$ is not $\equiv 0 \pmod{\mathfrak{p}}$, then the set of solutions is not empty, and has the usual structure of a solution of one inhomogeneous linear equation over the field $\mathfrak{o}/\mathfrak{p}$. In particular, it has dimension $n - 1$. A congruence (*) or (**) with some $c_i \not\equiv 0 \pmod{\mathfrak{p}}$ will be called a **proper congruence**.

As a matter of notation, we write $D_i f$ for the formal partial derivative of f with respect to X_i. We write

$$\operatorname{grad} f(X) = (D_1 f(X), \ldots, D_n f(X)).$$

Proposition 7.2. *Let* $f(X) \in \mathfrak{o}[X]$. *Let* r *be an integer* $\geqq 1$ *and let* $A \in \mathfrak{o}^{(n)}$ *be such that*

$$f(A) \equiv 0 \pmod{\mathfrak{p}^{2r-1}},$$

$$D_i f(A) \equiv 0 \pmod{\mathfrak{p}^{r-1}}, \qquad \text{for all} \quad i = 1, \ldots, n,$$

$$D_i f(A) \not\equiv 0 \pmod{\mathfrak{p}^r}, \qquad \text{for some } i = 1, \ldots, n.$$

Let v *be an integer* $\geqq 0$ *and let* $B \in \mathfrak{o}^{(n)}$ *be such that*

$$B \equiv A \pmod{\mathfrak{p}^r} \quad \text{and} \quad f(B) \equiv 0 \pmod{\mathfrak{p}^{2r-1+v}}.$$

A vector $Y \in \mathfrak{o}^{(n)}$ *satisfies*

$$Y \equiv B \pmod{\mathfrak{p}^{r+v}} \quad \text{and} \quad f(Y) \equiv 0 \pmod{\mathfrak{p}^{2r+v}}$$

if and only if Y can be written in the form $Y = B + \pi^{r+v}C$, with some $C \in \mathfrak{o}^{(n)}$ satisfying the proper congruence

$$f(B) + \pi^{r+v} \operatorname{grad} f(B) \cdot C \equiv 0 \pmod{\mathfrak{p}^{2r+v}}.$$

Proof. The proof is shorter than the statement of the proposition. Write $Y = B + \pi^{r+v}C$. By Taylor's expansion,

$$f(B + \pi^{r+v}C) = f(B) + \pi^{r+v} \operatorname{grad} f(B) \cdot C \pmod{\mathfrak{p}^{2r+2v}}.$$

To solve this last congruence mod $\mathfrak{p}^{2r+v}$, we obtain a proper congruence by hypothesis, because $\operatorname{grad} f(B) \equiv \operatorname{grad} f(A) \equiv 0 \pmod{\mathfrak{p}^{r-1}}$.

Corollary 7.3. *Assumptions being as in Proposition 7.2, there exists a zero of f in $\mathfrak{o}^{(n)}$ which is congruent to A mod $\mathfrak{p}^r$.*

Proof. We can write this zero as a convergent sum

$$A + \pi^{r+1}C_1 + \pi^{r+2}C_2 + \cdots$$

solving for $C_1, C_2, \ldots$ inductively as in the proposition.

Corollary 7.4. *Let f be a polynomial in one variable in $\mathfrak{o}[X]$, and let $a \in \mathfrak{o}$ be such that $f(a) \equiv 0 \pmod{\mathfrak{p}}$ but $f'(a) \not\equiv 0 \pmod{\mathfrak{p}}$. Then there exists $b \in \mathfrak{o}$, $b \equiv a \pmod{\mathfrak{p}}$ such that $f(b) = 0$.*

Proof. Take $n = 1$ and $r = 1$ in the proposition, and apply Corollary 7.3.

Corollary 7.5. *Let m be a positive integer not divisible by the characteristic of K. There exists an integer r such that for any $a \in \mathfrak{o}$, $a \equiv 1 \pmod{\mathfrak{p}^r}$, the equation $X^m - a = 0$ has a root in K.*

Proof. Apply the proposition.

Example. In the 2-adic field $\mathbf{Q}_2$, there exists a square root of -7, i.e. $\sqrt{-7} \in \mathbf{Q}_2$, because $-7 = 1 - 8$.

When the absolute value is not discrete, it is still possible to formulate a criterion for a polynomial to have a zero by **Newton approximation**. (Cf. my paper, "On quasi-algebraic closure," *Annals of Math.* (1952) pp. 373–390.

Proposition 7.6. *Let K be a complete under a non-archimedean absolute value (nontrivial). Let $\mathfrak{o}$ be the valuation ring and let $f(X) \in \mathfrak{o}[X]$ be a polynomial in one variable. Let $\alpha_0 \in \mathfrak{o}$ be such that*

$$|f(\alpha_0)| < |f'(\alpha_0)^2|$$

(here f' denotes the formal derivative of f). Then the sequence

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

converges to a root α of f in $\mathfrak{o}$, and we have

$$|\alpha - \alpha_0| \leqq \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1.$$

Proof. Let $c = |f(\alpha_0)/f'(\alpha_0)^2| < 1$. We show inductively that:

1. $|\alpha_i| \leqq 1$,
2. $|\alpha_i - \alpha_0| \leqq c$,
3. $\left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leqq c^{2^i}$.

These three conditions obviously imply our proposition. If $i = 0$, they are hypotheses. By induction, assume them for i. Then:

1. $|f(\alpha_i)/f'(\alpha_i)^2| \leqq c^{2^i}$ gives $|\alpha_{i+1} - \alpha_i| \leqq c^{2^i} < 1$, whence $|\alpha_{i+1}| \leqq 1$.
2. $|\alpha_{i+1} - \alpha_0| \leqq \max\{|\alpha_{i+1} - \alpha_i|, |\alpha_i - \alpha_0|\} = c$.
3. By Taylor's expansion, we have

$$f(\alpha_{i+1}) = f(\alpha_i) - f'(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2$$

for some $\beta \in \mathfrak{o}$, and this is less than or equal to

$$\left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2$$

in absolute value.

Using Taylor's expansion on $f'(\alpha_{i+1})$ we conclude that

$$|f'(\alpha_{i+1})| = |f'(\alpha_i)|.$$

From this we get

$$\left|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\right| \leqq c^{2^{i+1}}$$

as desired.

The technique of the proposition is also useful when dealing with rings, say a local ring $\mathfrak{o}$ with maximal ideal $\mathfrak{m}$ such that $\mathfrak{m}^r = 0$ for some integer $r > 0$. If one has a polynomial f in $\mathfrak{o}[X]$ and an approximate root α_0 such that

$$f'(\alpha_0) \not\equiv 0 \bmod \mathfrak{m},$$

then the Newton approximation sequence shows how to refine α_0 to a root of f.

Example in several variables. *Let K be complete under a non-archimedean absolute value. Let $f(X_1, \ldots, X_{n+1}) \in K[X]$ be a polynomial with coefficients in K. Let $(a_1, \ldots, a_n, b) \in K^{n+1}$. Assume that $f(a, b) = 0$. Let D_{n+1} be the*

partial derivative with respect to the $(n+1)$*-th variable, and assume that* $D_{n+1}f(a, b) \neq 0$. *Let* $(\bar{a}) \in K^n$ *be sufficiently close to* (a). *Then there exists an element* $\bar{b}$ *of* K *close to* b *such that* $f(\bar{a}, \bar{b}) = 0$.

This statement is an immediate corollary of Proposition 7.6. By multiplying all a_i, b by a suitable non-zero element of K one can change them to elements of $\mathfrak{o}$. Changing the variables accordingly, one may assume without loss of generality that a_i, $b \in \mathfrak{o}$, and the condition on the partial derivative not vanishing is preserved. Hence Proposition 7.6 may be applied. After perturbing (a) to $(\bar{a})$, the element b becomes an approximate solution of $f(\bar{a}, X)$. As $(\bar{a})$ approaches (a), $f(\bar{a}, b)$ approaches 0 and $D_{n+1}f(\bar{a}, b)$ approaches $D_{n+1}f(a, b) \neq 0$. Hence for $(\bar{a})$ sufficiently close to (a), the conditions of Proposition 7.6 are satisfied, and one may refine b to a root of $f(\bar{a}, X)$, thus proving the assertion.

The result was used in a key way in my paper "On Quasi Algebraic Closure". It is the analogue of Theorem 3.6 of Chapter XI, for real fields.

In the language of algebraic geometry (which we now assume), the result can be reformulated as follows. Let V be a variety defined over K. Let P be a simple point of V in K. Then there is a whole neighborhood of simple points of V in K. Especially, suppose that V is defined by a finite number of polynomial equations over a finitely generated field k over the prime field. After a suitable projection, one may assume that the variety is affine, and defined by one equation $f(X_1, \ldots, X_{n+1}) = 0$ as in the above statement, and that the point is $P = (a_1, \ldots, a_n, b)$ as above. One can then select $\bar{a}_i = x_i$ close to a_i but such that $(x_1, \ldots, x_n)$ are algebraically independent over k. Let y be the refinement of b such that $f(x, y) = 0$. Then (x, y) is a generic point of V over k, and the coordinates of (x, y) lie in K. In geometric terms, this means that the function field of the variety can be embedded in K over k, just as Theorem 3.6 of Chapter XI gave the similar result for an embedding in a real closed field, e.g. the real numbers.

EXERCISES

1. (a) Let K be a field with a valuation. If

$$f(X) = a_0 + a_1X + \cdots + a_nX^n$$

is a polynomial in $K[X]$, define $|f|$ to be the max on the values $|a_i|(i = 0, \ldots, n)$. Show that this defines an extension of the valuation to $K[X]$, and also that the valuation can be extended to the rational field $K(X)$. How is Gauss' lemma a special case of the above statement? Generalize to polynomials in several variables.

(b) Let f be a polynomial with complex coefficients. Define $|f|$ to be the maximum of the absolute values of the coefficients. Let d be an integer $\geqq 1$. Show that

there exist constants C_1, C_2 (depending only on d) such that, if f, g are polynomials in $\mathbf{C}[X]$ of degrees $\leqq d$, then

$$C_1|f||g| \leqq |fg| \leqq C_2|f||g|.$$

[*Hint*: Induction on the number of factors of degree 1. Note that the right inequality is trivial.]

2. Let $M_{\mathbf{Q}}$ be the set of absolute values consisting of the ordinary absolute value and all p-adic absolute values v_p on the field of rational numbers $\mathbf{Q}$. Show that for any rational number $a \in \mathbf{Q}$, $a \neq 0$, we have

$$\prod_{v \in M_{\mathbf{Q}}} |a|_v = 1.$$

If K is a finite extension of $\mathbf{Q}$, and M_K denotes the set of absolute values on K extending those of $M_{\mathbf{Q}}$, and for each $w \in M_K$ we let N_w be the local degree $[K_w : \mathbf{Q}_v]$, show that for $\alpha \in K$, $\alpha \neq 0$, we have

$$\prod_{w \in M_K} |\alpha|_w^{N_w} = 1.$$

3. Show that the p-adic numbers $\mathbf{Q}_p$ have no automorphisms other than the identity. [*Hint*: Show that such automorphisms are continuous for the p-adic topology. Use Corollary 7.5 as an algebraic characterization of elements close to 1.]

4. Let A be a principal entire ring, and let K be its quotient field. Let $\mathfrak{o}$ be a valuation ring of K containing A, and assume $\mathfrak{o} \neq K$. Show that $\mathfrak{o}$ is the local ring $A_{(p)}$ for some prime element p. [This applies both to the ring $\mathbf{Z}$ and to a polynomial ring $k[X]$ over a field k.]

5. Let A be the subring of polynomials $f(X) \in \mathbf{Q}[X]$ such that the constant coefficient of f is in $\mathbf{Z}$. Show that every finitely generated ideal in A is principal, but the ideal of polynomials in A with 0 constant coefficient is not principal. [Laura Wesson showed me the above, which gives a counterexample to the exercise stated in previous editions and printings, using the valuation ring $\mathfrak{o}$ on $\mathbf{Q}(X)$ containing $\mathbf{Q}$ and such that X has order 1. Then $\mathfrak{o} \neq A_{(p)}$ for any element p of A.]

6. Let $\mathbf{Q}_p$ be a p-adic field. Show that $\mathbf{Q}_p$ contains infinitely many quadratic fields of type $\mathbf{Q}(\sqrt{-m})$, where m is a positive integer.

7. Show that the ring of p-adic integers $\mathbf{Z}_p$ is compact. Show that the group of units in $\mathbf{Z}_p$ is compact.

8. If K is a field complete with respect to a discrete valuation, with finite residue class field, and if $\mathfrak{o}$ is the ring of elements of K whose orders are $\geqq 0$, show that $\mathfrak{o}$ is compact. Show that the group of units of $\mathfrak{o}$ is closed in $\mathfrak{o}$ and is compact.

9. Let K be a field complete with respect to a discrete valuation, let $\mathfrak{o}$ be the ring of integers of K, and assume that $\mathfrak{o}$ is compact. Let $f_1, f_2, \ldots$ be a sequence of polynomials in n variables, with coefficients in $\mathfrak{o}$. Assume that all these polynomials have degree $\leqq d$, and that they converge to a polynomial f (i.e. that $|f - f_i| \to 0$ as $i \to \infty$). If each f_i has a zero in $\mathfrak{o}$, show that f has a zero in $\mathfrak{o}$. If the polynomials f_i are homogeneous of degree d, and if each f_i has a non-trivial zero in $\mathfrak{o}$, show that f has a non-trivial zero in $\mathfrak{o}$. [*Hint*: Use the compactness of $\mathfrak{o}$ and of the units of $\mathfrak{o}$ for the homogeneous case.]

(For applications of this exercise, and also of Proposition 7.6, cf. my paper "On quasi-algebraic closure," *Annals of Math.*, **55** (1952), pp. 412–444.)

10. Show that if p, p' are two distinct prime numbers, then the fields $\mathbf{Q}_p$ and $\mathbf{Q}_{p'}$ are not isomorphic.
11. Prove that the field $\mathbf{Q}_p$ contains all $(p-1)$-th roots of unity. [*Hint*: Use Proposition 7.6, applied to the polynomial $X^{p-1}-1$ which splits into factors of degree 1 in the residue class field.] Show that two distinct $(p-1)$-th roots of unity cannot be congruent mod p.
12. (a) Let $f(X)$ be a polynomial of degree $\geqq 1$ in $\mathbf{Z}[X]$. Show that the values $f(a)$ for $a \in \mathbf{Z}$ are divisible by infinitely many primes.
    (b) Let F be a finite extension of $\mathbf{Q}$. Show that there are infinitely many primes p such that all conjugates of F (in an algebraic closure of $\mathbf{Q}_p$) actually are contained in $\mathbf{Q}_p$. [*Hint*: Use the irreducible polynomial of a generator for a Galois extension of $\mathbf{Q}$ containing F.]
13. Let K be a field of characteristic 0, complete with respect to a non-archimedean absolute value. Show that the series

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

converge in some neighborhood of 0. (The main problem arises when the characteristic of the residue class field is $p > 0$, so that p divides the denominators $n!$ and n. Get an expression which determines the power of p occurring in $n!$.) Prove that the exp and log give mappings inverse to each other, from a neighborhood of 0 to a neighborhood of 1.

14. Let K be as in the preceding exercise, of characteristic 0, complete with respect to a non-archimedean absolute value. For every integer $n > 0$, show that the usual binomial expansion for $(1+x)^{1/n}$ converges in some neighborhood of 0. Do this first assuming that the characteristic of the residue class field does not divide n, in which case the assertion is much simpler to prove.
15. Let F be a complete field with respect to a discrete valuation, let $\mathfrak{o}$ be the valuation ring, π a prime element, and assume that $\mathfrak{o}/(\pi) = k$. Prove that if $a, b \in \mathfrak{o}$ and $a \equiv b \pmod{\pi^r}$ with $r > 0$ then $a^{p^n} \equiv b^{p^n} \pmod{\pi^{r+n}}$ for all integers $n \geqq 0$.
16. Let F be as above. Show that there exists a system of representatives R for $\mathfrak{o}/(\pi)$ in $\mathfrak{o}$ such that $R^p = R$ and that this system is unique (Teichmüller). [*Hint*: Let α be a residue class in k. For each $v \geqq 0$ let a_v be a representative in $\mathfrak{o}$ of $a^{p^{-v}}$ and show that the sequence $a_v^{p^v}$ converges for $v \to \infty$, and in fact converges to a representative a of α, independent of the choices of a_v.] Show that the system of representatives R thus obtained is closed under multiplication, and that if F has characteristic p, then R is closed under addition, and is isomorphic to k.
17. (a) **(Witt vectors again).** Let k be a perfect field of characteristic p. We use the Witt vectors as described in the exercises of Chapter VI. One can define an absolute value on $W(k)$, namely $|x| = p^{-r}$ if x_r is the first non-zero component of x. Show that this is an absolute value, obviously discrete, defined on the ring, and which can be extended at once to the quotient field. Show that this quotient field is complete, and note that $W(k)$ is the valuation ring. The maximal ideal consists of those x such that $x_0 = 0$, i.e. is equal to $pW(k)$.

(b) Assume that F has characteristic 0. Map each vector $x \in W(k)$ on the element

$$\sum \xi_i^{p^{-i}} p^i$$

where ξ_i is a representative of x_i in the special system of Exercise 15. Show that this map is an embedding of $W(k)$ into $\mathfrak{o}$.

18. **(Local uniformization).** Let k be a field, K a finitely generated extension of transcendence degree 1, and $\mathfrak{o}$ a discrete valuation ring of K over k, with maximal ideal $\mathfrak{m}$. Assume that $\mathfrak{o}/\mathfrak{m} = k$. Let x be a generator of $\mathfrak{m}$, and assume that K is separable over $k(x)$. Show that there exists an element $y \in \mathfrak{o}$ such that $K = k(x, y)$, and also having the following property. Let φ be the place on K determined by $\mathfrak{o}$. Let $a = \varphi(x), b = \varphi(y)$ (of course $a = 0$). Let $f(X, Y)$ be the irreducible polynomial in $k[X, Y]$ such that $f(x, y) = 0$. Then $D_2 f(a, b) \neq 0$. [*Hint:* Write first $K = k(x, z)$ where z is integral over $k[x]$. Let $z = z_1, \ldots, z_n (n \geqq 2)$ be the conjugates of z over $k(x)$, and extend $\mathfrak{o}$ to a valuation ring $\mathfrak{O}$ of $k(x, z_1, \ldots, z_n)$. Let

$$z = a_0 + a_1 x + \cdots + a_r x^r + \cdots$$

be the power series expansion of z with $a_i \in k$, and let $P_r(x) = a_0 + \cdots + a_r x^r$. For $i = 1, \ldots, n$ let

$$y_i = \frac{z_i - P_r(x)}{x^r}.$$

Taking r large enough, show that y_1 has no pole at $\mathfrak{O}$ but $y_2, \ldots, y_n$ have poles at $\mathfrak{O}$. The elements $y_1, \ldots, y_n$ are conjugate over $k(x)$. Let $f(X, Y)$ be the irreducible polynomial of (x, y) over k. Then $f(x, Y) = \psi_n(x)Y^n + \cdots + \psi_0(x)$ with $\psi_i(x) k[x]$. We may also assume $\psi_i(0) \neq 0$ (since f is irreducible). Write $f(x, Y)$ in the form

$$f(x, Y) = \psi_n(x) y_2 \cdots y_n (Y - y_1)(y_2^{-1} Y - 1) \cdots (y_n^{-1} Y - 1).$$

Show that $\psi_n(x) y_2 \cdots y_n = u$ does not have a pole at $\mathfrak{O}$. If $w \in \mathfrak{O}$, let w denote its residue class modulo the maximal ideal of $\mathfrak{O}$. Then

$$0 \neq f(\bar{x}, Y) = (-1)^{n-1} \bar{u}(Y - \bar{y}_1).$$

Let $y = y_1, \bar{y} = b$. We find that $D_2 f(a, b) = (-1)^{n-1} \bar{u} \neq 0$.]

19. Prove the converse of Exercise 17, i.e. if $K = k(x, y)$, $f(X, Y)$ is the irreducible polynomial of (x, y) over k, and if $a, b \in k$ are such that $f(a, b) = 0$, but $D_2 f(a, b) \neq 0$, then there exists a unique valuation ring $\mathfrak{o}$ of K with maximal ideal $\mathfrak{m}$ such that $x \equiv a$ and $y \equiv b \pmod{\mathfrak{m}}$. Furthermore, $\mathfrak{o}/\mathfrak{m} = k$, and $x - a$ is a generator of $\mathfrak{m}$. [*Hint:* If $g(x, y) \in k[x, y]$ is such that $g(a, b) = 0$, show that $g(x, y) = (x - a)A(x, y)/B(x, y)$ where A, B are polynomials such that $B(a, b) \neq 0$. If $A(a, b) = 0$ repeat the process. Show that the process cannot be repeated indefinitely, and leads to a proof of the desired assertion.]

20. (**Iss'sa-Hironaka** *Ann. of Math* 83 (1966), pp. 34–46). This exercise requires a good working knowledge of complex variables. Let K be the field of meromorphic functions on the complex plane $\mathbf{C}$. Let $\mathfrak{O}$ be a discrete valuation ring of K (containing the

constants $\mathbf{C}$). Show that the function z is in $\mathfrak{O}$. [*Hint:* Let $a_1, a_2, \ldots$ be a discrete sequence of complex numbers tending to infinity, for instance the positive integers. Let $v_1, v_2, \ldots$, be a sequence of integers, $0 \leqq v_i \leqq p - 1$, for some prime number p, such that $\sum v_i p^i$ is not the p-adic expansion of a rational number. Let f be an entire function having a zero of order $v_i p^i$ at a_i for each i and no other zero. If z is not in $\mathfrak{o}$, consider the quotient

$$g(z) = \frac{f(z)}{\prod_{i=1}^{n} (z - a_i)^{v_i p^i}}.$$

From the Weierstrass factorization of an entire function, show that $g(z) = h(z)^{p^{n+1}}$ for some entire function $h(z)$. Now analyze the zero of g at the discrete valuation of $\mathfrak{o}$ in terms of that of f and $\prod (z - a_i)^{v_i p^i}$ to get a contradiction.]

If U is a non-compact Riemann surface, and L is the field of meromorphic functions on U, and if $\mathfrak{o}$ is a discrete valuation ring of L containing the constants, show that every holomorphic function φ on U lies in $\mathfrak{o}$. [*Hint*: Map $\varphi : U \to \mathbf{C}$, and get a discrete valuation of K by composing φ with meromorphic functions on $\mathbf{C}$. Apply the first part of the exercise.] Show that the valuation ring is the one associated with a complex number. [*Further hint*: If you don't know about Riemann surfaces, do it for the complex plane. For each $z \in U$, let f_z be a function holomorphic on U and having only a zero of order 1 at z. If for some z_0 the function f_{z_0} has order $\geqq 1$ at $\mathfrak{o}$, then show that $\mathfrak{o}$ is the valuation ring associated with z_0. Otherwise, every function f_z has order 0 at $\mathfrak{o}$. Conclude that the valuation of $\mathfrak{o}$ is trivial on any holomorphic function by a limit trick analogous to that of the first part of the exercise.]

Part Three

LINEAR ALGEBRA and REPRESENTATIONS

We shall be concerned with modules and vector spaces, going into their structure under various points of view. The main theme here is to study a pair, consisting of a module, and an endomorphism, or a ring of endomorphisms, and try to decompose this pair into a direct sum of components whose structure can then be described explicitly. The direct sum theme recurs in every chapter. Sometimes, we use a duality to obtain our direct sum decomposition relative to a pairing, and sometimes we get our decomposition directly. If a module refuses to decompose into a direct sum of simple components, then there is no choice but to apply the Grothendieck construction and see what can be obtained from it.

The extension theme occurs only once, in Witt's theorem, in a brief counterpoint to the decomposition theme.

CHAPTER XIII

Matrices and Linear Maps

Presumably readers of this chapter will have had some basic acquaintance with linear algebra in elementary courses. We go beyond such courses by pointing out that a lot of results hold for free modules over a commutative ring. This is useful when one wants to deal with families of linear maps, and reduction modulo an ideal.

Note that §8 and §9 give examples of group theory in the context of linear groups.

Throughout this chapter, we let R be a commutative ring, and we let E, F be R-modules. We suppress the prefix R in front of linear maps and modules.

§1. MATRICES

By an $m \times n$ **matrix** in R one means a doubly indexed family of elements of R, (a_{ij}), $(i = 1, \ldots, m$ and $j = 1, \ldots, n)$, usually written in the form

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \cdots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

We call the elements a_{ij} the **coefficients** or **components** of the **matrix**. A $1 \times n$ matrix is called a **row vector** (of dimension, or size, n) and a $m \times 1$ matrix is called a **column vector** (of dimension, or size, m). In general, we say that (m, n) is the **size** of the matrix, or also $m \times n$.

We define addition for matrices of the same size by components. If $A = (a_{ij})$ and $B = (b_{ij})$ are matrices of the same size, we define $A + B$ to be the matrix whose ij-component is $a_{ij} + b_{ij}$. Addition is obviously associative. We define the multiplication of a matrix A by an element $c \in R$ to be the matrix (ca_{ij}),

whose ij-component is ca_{ij}. Then the set of $m \times n$ matrices in R is a module (i.e. an R-module).

We define the product AB of two matrices only under certain conditions. Namely, when A has size (m, n) and B has size (n, r), i.e. only when the size of the rows of A is the same as the size of the columns of B. If that is the case, let $A = (a_{ij})$ and let $B = (b_{jk})$. We define AB to be the $m \times r$ matrix whose ik-component is

$$\sum_{j=1}^{n} a_{ij} b_{jk}.$$

If A, B, C are matrices such that AB is defined and BC is defined, then so is $(AB)C$ and $A(BC)$ and we have

$$(AB)C = A(BC).$$

This is trivial to prove. If $C = (c_{kl})$, then the reader will see at once that the il-component of either of the above products is equal to

$$\sum_{j} \sum_{k} a_{ij} b_{jk} c_{kl}.$$

An $m \times n$ matrix is said to be a **square matrix** if $m = n$. For example, a 1×1 matrix is a square matrix, and will sometimes be identified with the element of R occurring as its single component.

For a given integer $n \geqq 1$ the set of square $n \times n$ matrices forms a ring.

This is again trivially verified and will be left to the reader.

The unit element of the ring of $n \times n$ matrices is the matrix

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

whose components are equal to 0 except on the diagonal, in which case they are equal to 1. We sometimes write I instead of I_n.

If $A = (a_{ij})$ is a square matrix, we define in general its **diagonal components** to be the elements a_{ii}.

We have a natural ring-homomorphism of R into the ring of $n \times n$ matrices, given by

$$c \mapsto cI_n.$$

Thus cI_n is the square $n \times n$ matrix having all its components equal to 0 except the diagonal components, which are equal to c. Let us denote the ring of $n \times n$

matrices in R by $\mathrm{Mat}_n(R)$. Then $\mathrm{Mat}_n(R)$ is an algebra over R (with respect to the above homomorphism).

Let $A = (a_{ij})$ be an $m \times n$ matrix. We define its **transpose** ${}^tA$ to be the matrix (a_{ji}) ($j = 1, \ldots, n$ and $i = 1, \ldots, m$). Then ${}^tA$ is an $n \times m$ matrix. The reader will verify at once that if A, B are of the same size, then

$$ {}^t(A + B) = {}^tA + {}^tB. $$

If $c \in R$ then ${}^t(cA) = c\,{}^tA$. If A, B can be multiplied, then ${}^tB\,{}^tA$ is defined and we have

$$ {}^t(AB) = {}^tB\,{}^tA. $$

We note the operations on matrices commute with homomorphisms. More precisely, let $\varphi : R \to R'$ be a ring-homomorphism. If A, B are matrices in R, we define φA to be the matrix obtained by applying φ to all the components of A. Then

$$ \varphi(A + B) = \varphi A + \varphi B, \qquad \varphi(AB) = (\varphi A)(\varphi B), \qquad \varphi(cA) = \varphi(c)\varphi A, $$
$$ \varphi({}^tA) = {}^t\varphi(A). $$

A similar remark will hold throughout our discussion of matrices (for instance in the next section).

Let $A = (a_{ij})$ be a square $n \times n$ matrix in a commutative ring R. We define the **trace** of A to be

$$ \mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}; $$

in other words, the trace is the sum of the diagonal elements.

If A, B are $n \times n$ matrices, then

$$ \mathrm{tr}(AB) = \mathrm{tr}(BA). $$

Indeed, if $A = (a_{ij})$ and $B = (b_{ij})$ then

$$ \mathrm{tr}(AB) = \sum_i \sum_v a_{iv} b_{vi} = \mathrm{tr}(BA). $$

As an application, we observe that if B is an invertible $n \times n$ matrix, then

$$ \mathrm{tr}(B^{-1}AB) = \mathrm{tr}(A). $$

Indeed, $\mathrm{tr}(B^{-1}AB) = \mathrm{tr}(ABB^{-1}) = \mathrm{tr}(A)$.

§2. THE RANK OF A MATRIX

Let k be a field and let A be an $m \times n$ matrix in k. By the **row rank** of A we shall mean the maximum number of linearly independent rows of A, and by the **column rank** of A we shall mean the maximum number of linearly independent columns of A. Thus these ranks are the dimensions of the vector spaces generated respectively by the rows of A and the columns of A. We contend that these ranks are equal to the same number, and we define the **rank** of A to be that number.

Let $A^1, \ldots, A^n$ be the columns of A, and let $A_1, \ldots, A_m$ be the rows of A. Let ${}^tX = (x_1, \ldots, x_m)$ have components $x_i \in k$. We have a linear map

$$X \mapsto x_1 A_1 + \cdots + x_m A_m$$

of $k^{(m)}$ onto the space generated by the row vectors. Let W be its kernel. Then W is a subspace of $k^{(m)}$ and

$$\dim W + \text{row rank} = m.$$

If Y is a column vector of dimension m, then the map

$$(X, Y) \mapsto {}^tXY = X \cdot Y$$

is a bilinear map into k, if we view the 1×1 matrix ${}^tXY$ as an element of k. We observe that W is the orthogonal space to the column vectors $A^1, \ldots, A^n$, i.e. it is the space of all X such that $X \cdot A^j = 0$ for all $j = 1, \ldots, n$. By the duality theorem of Chapter III, we know that $k^{(m)}$ is its own dual under the pairing

$$(X, Y) \mapsto X \cdot Y$$

and that $k^{(m)}/W$ is dual to the space generated by $A^1, \ldots, A^n$. Hence

$$\dim k^{(m)}/W = \text{column rank},$$

or

$$\dim W + \text{column rank} = m.$$

From this we conclude that

$$\text{column rank} = \text{row rank},$$

as desired.

We note that W may be viewed as the space of solutions of the system of n linear equations

$$x_1 A_1 + \cdots + x_m A_m = 0,$$

in m unknowns $x_1, \ldots, x_m$. Indeed, if we write out the preceding vector equation in terms of all the coordinates, we get the usual system of n linear equations. We let the reader do this if he or she wishes.

§3. MATRICES AND LINEAR MAPS

Let E be a module, and assume that there exists a basis $\mathfrak{B} = \{\xi_1, \ldots, \xi_n\}$ for E over R. This means that every element of E has a unique expression as a linear combination

$$x = x_1\xi_1 + \cdots + x_n\xi_n$$

with $x_i \in R$. We call $(x_1, \ldots, x_n)$ the **components** of x with respect to the basis. We may view this n-tuple as a row vector. We shall denote by X the transpose of the row vector $(x_1, \ldots, x_n)$. We call X the **column vector of x with respect to the basis**.

We observe that if $\{\xi'_1, \ldots, \xi'_m\}$ is another basis of E over R, then $m = n$. Indeed, let $\mathfrak{p}$ be a maximal ideal of R. Then $E/\mathfrak{p}E$ is a vector space over the field $R/\mathfrak{p}R$, and it is immediately clear that if we denote by $\bar{\xi}_i$ the residue class of ξ_i mod $\mathfrak{p}E$, then $\{\bar{\xi}_1, \ldots, \bar{\xi}_n\}$ is a basis for $E/\mathfrak{p}E$ over $R/\mathfrak{p}R$. Hence n is also the dimension of this vector space, and we know the invariance of the cardinality for bases of vector spaces over fields. Thus $m = n$. We shall call n the **dimension** of the module E over R.

We shall view $R^{(n)}$ as the module of column vectors of size n. It is a free module of dimension n over R. It has a basis consisting of the unit vectors $e^1, \ldots, e^n$ such that

$${}^t e^i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

has components 0 except for its i-th component, which is equal to 1.

An $m \times n$ matrix A gives rise to a linear map

$$L_A : R^{(n)} \to R^{(m)}$$

by the rule

$$X \mapsto AX.$$

Namely, we have $A(X + Y) = AX + AY$ and $A(cX) = cAX$ for column vectors X, Y and $c \in R$.

The above considerations can be extended to a slightly more general context, which can be very useful. Let E be an abelian group and assume that R is a commutative subring of

$$\mathrm{End}_{\mathbf{Z}}(E) = \mathrm{Hom}_{\mathbf{Z}}(E, E).$$

Then E is an R-module. Furthermore, if A is an $m \times n$ matrix in R, then we get a linear map

$$L_A : E^{(n)} \to E^{(m)}$$

defined by a rule similar to the above, namely $X \mapsto AX$. However, this has to be interpreted in the obvious way. If $A = (a_{ij})$ and X is a column vector of elements of E, then

$$AX = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \cdots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix},$$

where $y_i = \sum_{j=1}^{n} a_{ij}x_j$.

If A, B are matrices in R whose product is defined, then for any $c \in R$ we have

$$L_{AB} = L_A L_B \quad \text{and} \quad L_{cA} = cL_A.$$

Thus we have associativity, namely

$$A(BX) = (AB)X.$$

An arbitrary commutative ring R may be viewed as a module over itself. In this way we recover the special case of our map from $R^{(n)}$ into $R^{(m)}$. Furthermore, if E is a module over R, then R may be viewed as a ring of endomorphisms of E.

Proposition 3.1. *Let E be a free module over R, and let $\{x_1, \ldots, x_n\}$ be a basis. Let $y_1, \ldots, y_n$ be elements of E. Let A be the matrix in R such that*

$$A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Then $\{y_1, \ldots, y_n\}$ is a basis of E if and only if A is invertible.

Proof. Let X, Y be the column vectors of our elements. Then $AX = Y$. Suppose Y is a basis. Then there exists a matrix C in R such that $CY = X$.

Then $CAX = X$, whence $CA = I$ and A is invertible. Conversely, assume that A is invertible. Then $X = A^{-1}Y$ and hence $x_1, \ldots, x_n$ are in the module generated by $y_1, \ldots, y_n$. Suppose that we have a relation

$$b_1 y_1 + \cdots + b_n y_n = 0$$

with $b_i \in R$. Let B be the row vector $(b_1, \ldots, b_n)$. Then

$$BY = 0$$

and hence $BAX = 0$. But $\{x_1, \ldots, x_n\}$ is a basis. Hence $BA = 0$, and hence $BAA^{-1} = B = 0$. This proves that the components of Y are linearly independent over R, and proves our proposition.

We return to our situation of modules over an arbitrary commutative ring R.

Let E, F be modules. We shall see how we can associate a matrix with a linear map whenever bases of E and F are given. We assume that E, F are free. We let $\mathfrak{B} = \{\xi_1, \ldots, \xi_n\}$ and $\mathfrak{B}' = \{\xi'_1, \ldots, \xi'_m\}$ be bases of E and F respectively. Let

$$f: E \to F$$

be a linear map. There exist unique elements $a_{ij} \in R$ such that

$$\begin{aligned} f(\xi_1) &= a_{11}\xi'_1 + \cdots + a_{m1}\xi'_m, \\ &\cdots \\ f(\xi_n) &= a_{1n}\xi'_1 + \cdots + a_{mn}\xi'_m, \end{aligned}$$

or in other words,

$$f(\xi_j) = \sum_{i=1}^{m} a_{ij}\xi'_i$$

(Observe that the sum is over the *first* index.) We define

$$M_{\mathfrak{B}'}^{\mathfrak{B}}(f) = (a_{ij}).$$

If $x = x_1\xi_1 + \cdots + x_n\xi_n$ is expressed in terms of the basis, let us denote the column vector X of components of x by $M_{\mathfrak{B}}(x)$. We see that

$$M_{\mathfrak{B}'}(f(x)) = M_{\mathfrak{B}'}^{\mathfrak{B}}(f) M_{\mathfrak{B}}(x).$$

In other words, if X' is the column vector of $f(x)$, and M is the matrix associated with f then $X' = MX$. Thus the operation of the linear map is reflected by the matrix multiplication, and we have $f = L_M$.

Proposition 3.2. *Let E, F, D be modules, and let $\mathfrak{B}$, $\mathfrak{B}'$, $\mathfrak{B}''$ be finite bases of E, F, D, respectively. Let*

$$E \xrightarrow{f} F \xrightarrow{g} D$$

be linear maps. Then

$$M_{\mathfrak{B}''}^{\mathfrak{B}}(g \circ f) = M_{\mathfrak{B}''}^{\mathfrak{B}'}(g) M_{\mathfrak{B}'}^{\mathfrak{B}}(f).$$

Proof. Let A and B be the matrices associated with the maps f, g respectively, with respect to our given bases. If X is the column vector associated with $x \in E$, the vector associated with $g(f(x))$ is $B(AX) = (BA)X$. Hence BA is the matrix associated with $g \circ f$. This proves what we wanted.

Corollary 3.3. *Let $E = F$. Then*

$$M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id}) M_{\mathfrak{B}}^{\mathfrak{B}'}(\mathrm{id}) = M_{\mathfrak{B}'}^{\mathfrak{B}'}(\mathrm{id}) = I.$$

Each matrix $M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id})$ is invertible (i.e. is a unit in the ring of matrices).

Proof. Obvious.

Corollary 3.4. *Let $N = M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id})$. Then*

$$M_{\mathfrak{B}'}^{\mathfrak{B}'}(f) = M_{\mathfrak{B}'}^{\mathfrak{B}}(\mathrm{id}) M_{\mathfrak{B}}^{\mathfrak{B}}(f) M_{\mathfrak{B}}^{\mathfrak{B}'}(\mathrm{id}) = N M_{\mathfrak{B}}^{\mathfrak{B}}(f) N^{-1}.$$

Proof. Obvious

Corollary 3.5. *Let E be a free module of dimension n over R. Let $\mathfrak{B}$ be a basis of E over R. The map*

$$f \mapsto M_{\mathfrak{B}}^{\mathfrak{B}}(f)$$

is a ring-isomorphism of the ring of endomorphisms of E onto the ring of $n \times n$ matrices in R. In fact, the isomorphism is one of algebras over R.

We shall call the matrix $M_{\mathfrak{B}}^{\mathfrak{B}}(f)$ the **matrix associated with f with respect to the basis $\mathfrak{B}$.**

Let E be a free module of dimension n over R. By $GL(E)$ or $\mathrm{Aut}_R(E)$ one means the group of linear automorphisms of E. It is the group of units in $\mathrm{End}_R(E)$. By $GL_n(R)$ one means the group of invertible $n \times n$ matrices in R. Once a basis is selected for E over R, we have a group-isomorphism

$$GL(E) \leftrightarrow GL_n(R)$$

with respect to this basis.

Let E be as above. If

$$f: E \to E$$

is a linear map, we select a basis $\mathfrak{B}$ and let M be the matrix associated with f relative to $\mathfrak{B}$. We define the **trace** of f to be the trace of M, thus

$$\operatorname{tr}(f) = \operatorname{tr}(M).$$

If M' is the matrix of f with respect to another basis, then there exists an invertible matrix N such that $M' = N^{-1}MN$, and hence the trace is independent of the choice of basis.

§4. DETERMINANTS

Let $E_1, \ldots, E_n, F$ be modules. A map

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

is said to be ***R*-multilinear** (or simply multilinear) if it is linear in each variable, i.e. if for every index i and elements $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n, x_j \in E_j$, the map

$$x \mapsto f(x_1, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n)$$

is a linear map of E_i into F.

A multilinear map defined on an n-fold product is also called n-multilinear. If $E_1 = \cdots = E_n = E$, we also say that f is a **multilinear map on E**, instead of saying that it is multilinear on $E^{(n)}$.

Let f be an n-multilinear map. If we take two indices i, j and $i \neq j$ then fixing all the variables except the i-th and j-th variable, we can view f as a bilinear map on $E_i \times E_j$.

Assume that $E_1 = \cdots = E_n = E$. We say that the multilinear map f is **alternating** if $f(x_1, \ldots, x_n) = 0$ whenever there exists an index i, $1 \leqq i \leqq n-1$, such that $x_i = x_{i+1}$ (in other words, when two adjacent elements are equal).

Proposition 4.1. *Let f be an n-multilinear alternating map on E. Let $x_1, \ldots, x_n \in E$. Then*

$$f(\ldots, x_i, x_{i+1}, \ldots) = -f(\ldots, x_{i+1}, x_i, \ldots).$$

In other words, when we interchange two adjacent arguments of f, the value of f changes by a sign. If $x_i = x_j$ for $i \neq j$ then $f(x_1, \ldots, x_n) = 0$.

Proof. Restricting our attention to the factors in the i-th and j-th place, with $j = i + 1$, we may assume f is bilinear for the first statement. Then for all x, $y \in E$ we have

$$0 = f(x + y, x + y) = f(x, y) + f(y, x).$$

This proves what we want, namely $f(y, x) = -f(x, y)$. For the second assertion, we can interchange successively adjacent arguments of f until we obtain an n-tuple of elements of E having two equal adjacent arguments. This shows that when $x_i = x_j$, $i \neq j$, then $f(x_1, \ldots, x_n) = 0$.

Corollary 4.2. *Let f be an n-multilinear alternating map on E. Let $x_1, \ldots, x_n \in E$. Let $i \neq j$ and let $a \in R$. Then the value of f on $(x_1, \ldots, x_n)$ does not change if we replace x_i by $x_i + ax_j$ and leave all other components fixed.*

Proof. Obvious.

A multilinear alternating map taking its value in R is called a multilinear alternating **form**.

On repeated occasions we shall evaluate multilinear alternating maps on linear combinations of elements of E. Let

$$w_1 = a_{11}v_1 + \cdots + a_{1n}v_n,$$
$$\cdots$$
$$w_n = a_{n1}v_1 + \cdots + a_{nn}v_n.$$

Let f be n-multilinear alternating on E. Then

$$f(w_1, \ldots, w_n) = f(a_{11}v_1 + \cdots + a_{1n}v_n, \ldots, a_{n1}v_1 + \cdots + a_{nn}v_n).$$

We expand this by multilinearity, and get a sum of terms of type

$$a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} f(v_{\sigma(1)}, \ldots, v_{\sigma(n)}),$$

where σ ranges over arbitrary maps of $\{1, \ldots, n\}$ into itself. If σ is not a bijection (i.e. a permutation), then two arguments $v_{\sigma(i)}$ and $v_{\sigma(j)}$ are equal for $i \neq j$, and the term is equal to 0. Hence we may restrict our sum to permutations σ. Shuffling back the elements $(v_{\sigma(1)}, \ldots, v_{\sigma(n)})$ to their standard ordering and using Proposition 4.1, we see that we have obtained the following expansion:

Lemma 4.3. *If $w_1, \ldots, w_n$ are as above, then*

$$f(w_1, \ldots, w_n) = \sum_{\sigma} \epsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} f(v_1, \ldots, v_n)$$

where the sum is taken over all permutations σ of $\{1, \ldots, n\}$ and $\epsilon(\sigma)$ is the sign of the permutation.

For determinants, I shall follow Artin's treatment in *Galois Theory*.

By an $n \times n$ **determinant** we shall mean a mapping

$$\det : \mathrm{Mat}_n(R) \to R$$

also written

$$D : \mathrm{Mat}_n(R) \to R$$

which, when viewed as a function of the column vectors $A^1, \ldots, A^n$ of a matrix A, is multilinear alternating, and such that $D(I) = 1$. In this chapter, we use mostly the letter D to denote determinants.

We shall prove later that determinants exist. For the moment, we derive properties.

Theorem 4.4. (Cramer's Rule). *Let $A^1, \ldots, A^n$ be column vectors of dimension n. Let $x_1, \ldots, x_n \in R$ be such that*

$$x_1 A^1 + \cdots + x_n A^n = B$$

for some column vector B. Then for each i we have

$$x_i D(A^1, \ldots, A^n) = D(A^1, \ldots, B, \ldots, A^n),$$

where B in this last line occurs in the i-th place.

Proof. Say $i = 1$. We expand

$$D(B, A^2, \ldots, A^n) = \sum_{j=1}^{n} x_j D(A^j, A^2, \ldots, A^n),$$

and use Proposition 4.1 to get what we want (all terms on the right are equal to 0 except the one having x_1 in it).

Corollary 4.5. *Assume that R is a field. Then $A^1, \ldots, A^n$ are linearly dependent if and only if $D(A^1, \ldots, A^n) = 0$.*

Proof. Assume we have a relation

$$x_1 A^1 + \cdots + x_n A^n = 0$$

with $x_i \in R$. Then $x_i D(A) = 0$ for all i. If some $x_i \neq 0$ then $D(A) = 0$. Conversely, assume that $A^1, \ldots, A^n$ are linearly independent. Then we can express the unit vectors $e^1, \ldots, e^n$ as linear combinations

$$e^1 = b_{11} A^1 + \cdots + b_{1n} A^n,$$
$$\cdots$$
$$e^n = b_{n1} A^1 + \cdots + b_{nn} A^n$$

with $b_{ij} \in R$. But

$$1 = D(e^1, \ldots, e^n).$$

Using a previous lemma, we know that this can be expanded into a sum of terms involving $D(A^1, \ldots, A^n)$, and hence $D(A)$ cannot be 0.

Proposition 4.6. *If determinants exist, they are unique. If $A^1, \ldots, A^n$ are the column vectors of dimension n, of the matrix $A = (a_{ij})$, then*

$$D(A^1, \ldots, A^n) = \sum_{\sigma} \epsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n},$$

where the sum is taken over all permutations σ of $\{1, \ldots, n\}$, and $\epsilon(\sigma)$ is the sign of the permutation.

Proof. Let $e^1, \ldots, e^n$ be the unit vectors as usual. We can write

$$A^1 = a_{11}e^1 + \cdots + a_{n1}e^n,$$
$$\cdots$$
$$A^n = a_{1n}e^n + \cdots + a_{nn}e^n.$$

Therefore

$$D(A^1, \ldots, A^n) = \sum_{\sigma} \epsilon(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}$$

by the lemma. This proves that the value of the determinant is uniquely determined and is given by the expected formula.

Corollary 4.7. *Let $\varphi : R \to R'$ be a ring-homomorphism into a commutative ring. If A is a square matrix in R, define φA to be the matrix obtained by applying φ to each component of A. Then*

$$\varphi(D(A)) = D(\varphi A).$$

Proof. Apply φ to the expression of Proposition 4.6.

Proposition 4.8. *If A is a square matrix in R then*

$$D(A) = D({}^tA).$$

Proof. In a product

$$a_{\sigma(1),1} \cdots a_{\sigma(n),n}$$

each integer k from 1 to n occurs precisely once among the integers $\sigma(1), \ldots, \sigma(n)$. Hence we can rewrite this product in the form

$$a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)}.$$

Since $\epsilon(\sigma) = \epsilon(\sigma^{-1})$, we can rewrite the sum in Proposition 4.6 in the form

$$\sum_{\sigma} \epsilon(\sigma^{-1}) a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)}.$$

In this sum, each term corresponds to a permutation σ. However, as σ ranges over all permutations, so does σ^{-1}. Hence our sum is equal to

$$\sum_{\sigma} \epsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)},$$

which is none other than $D({}^tA)$, as was to be shown.

Corollary 4.9. *The determinant is multilinear and alternating with respect to the rows of a matrix.*

We shall now prove existence, and prove simultaneously one additional important property of determinants.

When $n = 1$, we define $D(a) = a$ for any $a \in R$.

Assume that we have proved the existence of determinants for all integers $< n$ ($n \geqq 2$). Let A be an $n \times n$ matrix in R, $A = (a_{ij})$. We let A_{ij} be the $(n-1) \times (n-1)$ matrix obtained from A by deleting the i-th row and j-th column. Let i be a fixed integer, $1 \leqq i \leqq n$. We define inductively

$$D(A) = (-1)^{i+1} a_{i1} D(A_{i1}) + \cdots + (-1)^{i+n} a_{in} D(A_{in}).$$

(This is known as the **expansion of D according to the i-th row**.) We shall prove that D satisfies the definition of a determinant.

Consider D as a function of the k-th column, and consider any term

$$(-1)^{i+j} a_{ij} D(A_{ij}).$$

If $j \neq k$ then a_{ij} does not depend on the k-th column, and $D(A_{ij})$ depends linearly on the k-th column. If $j = k$, then a_{ij} depends linearly on the k-th column, and $D(A_{ij})$ does not depend on the k-th column. In any case our term depends linearly on the k-th column. Since $D(A)$ is a sum of such terms, it depends linearly on the k-th column, and thus D is multilinear.

Next, suppose that two adjacent columns of A are equal, say $A^k = A^{k+1}$. Let j be an index $\neq k$ and $\neq k+1$. Then the matrix A_{ij} has two adjacent equal columns, and hence its determinant is equal to 0. Thus the term corresponding to an index $j \neq k$ or $k+1$ gives a zero contribution to $D(A)$. The other two terms can be written

$$(-1)^{i+k} a_{ik} D(A_{ik}) + (-1)^{i+k+1} a_{i,k+1} D(A_{i,k+1}).$$

The two matrices A_{ik} and $A_{i,k+1}$ are equal because of our assumption that the k-th column of A is equal to the $(k+1)$-th column. Similarly, $a_{ik} = a_{i,k+1}$.

Hence these two terms cancel since they occur with opposite signs. This proves that our form is alternating, and gives:

Proposition 4.10. *Determinants exist and satisfy the rule of expansion according to rows and columns.*

(For columns, we use the fact that $D(A) = D({}^tA)$.)

Example. We mention explicity one of the most important determinants. Let $x_1, \ldots, x_n$ be elements of a commutative ring. The **Vandermonde determinant** $V = V(x_1, \ldots, x_n)$ of these elements is defined to be

$$V = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix},$$

whose value can be determined explicitly to be

$$V = \prod_{i<j} (x_j - x_i).$$

If the ring is entire and $x_i \neq x_j$ for $i \neq j$, it follows that $V \neq 0$. The proof for the stated value is done by multiplying the next to the last row by x_1 and subtracting from the last row. Then repeat this step going up the rows, thus making the elements of the first column equal to 0, except for 1 in the upper left-hand corner. One can then expand according to the first column, and use the homogeneity property and induction to conclude the proof of the evaluation of V.

Theorem 4.11. *Let E be a module over R, and let $v_1, \ldots, v_n$ be elements of E. Let $A = (a_{ij})$ be a matrix in R, and let*

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

Let Δ be an n-multilinear alternating map on E. Then

$$\Delta(w_1, \ldots, w_n) = D(A)\,\Delta(v_1, \ldots, v_n).$$

Proof. We expand

$$\Delta(a_{11}v_1 + \cdots + a_{1n}v_n, \ldots, a_{n1}v_1 + \cdots + a_{nn}v_n),$$

and find precisely what we want, taking into account $D(A) = D({}^tA)$.

Let E, F be modules, and let $L_a^n(E, F)$ denote the set of n-multilinear alternating maps of E into F. If $F = R$, we also write $L_a^n(E, R) = L_a^n(E)$. It is clear that $L_a^n(E, F)$ is a module over R, i.e. is closed under addition and multiplication by elements of R.

Corollary 4.12. *Let E be a free module over R, and let $\{v_1, \ldots, v_n\}$ be a basis. Let F be any module, and let $w \in F$. There exists a unique n-multilinear alternating map*

$$\Delta_w : E \times \cdots \times E \to F$$

such that $\Delta_w(v_1, \ldots, v_n) = w$.

Proof. Without loss of generality, we may assume that $E = R^{(n)}$, and then, if $A^1, \ldots, A^n$ are column vectors, we define

$$\Delta_w(A^1, \ldots, A^n) = D(A)w.$$

Then Δ_w obviously has the required properties.

Corollary 4.13. *If E is free over R, and has a basis consisting of n elements, then $L_a^n(E)$ is free over R, and has a basis consisting of 1 element.*

Proof. We let Δ_1 be the multilinear alternating map taking the value 1 on a basis $\{v_1, \ldots, v_n\}$. Any element $\varphi \in L_a^n(E)$ can then be written in a unique way as $c\Delta_1$, with some $c \in R$, namely $c = \varphi(v_1, \ldots, v_n)$. This proves what we wanted.

Any two bases of $L_a^n(E)$ in the preceding corollary differ by a unit in R. In other words, if Δ is a basis of $L_a^n(E)$, then $\Delta = c\Delta_1 = \Delta_c$ for some $c \in R$, and c must be a unit. Our Δ_1 depends of course on the choice of a basis for E. When we consider $R^{(n)}$, our determinant D is precisely Δ_1, relative to the standard basis consisting of the unit vectors $e^1, \ldots, e^n$.

It is sometimes convenient terminology to say that any basis of $L_a^n(E)$ is a **determinant** on E. In that case, the corollary to Cramer's rule can be stated as follows.

Corollary 4.14. *Let R be a field. Let E be a vector space of dimension n. Let Δ be any determinant on E. Let $v_1, \ldots, v_n \in E$. In order that $\{v_1, \ldots, v_n\}$ be a basis of E it is necessary and sufficient that*

$$\Delta(v_1, \ldots, v_n) \neq 0.$$

Proposition 4.15. *Let A, B be $n \times n$ matrices in R. Then*

$$D(AB) = D(A)D(B).$$

Proof. This is actually a corollary of Theorem 4.11. We take $v_1, \ldots, v_n$ to be the unit vectors $e^1, \ldots, e^n$, and consider

$$AB\begin{pmatrix} e^1 \\ \vdots \\ e^n \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}.$$

We obtain

$$D(w_1, \ldots, w_n) = D(AB)D(e^1, \ldots, e^n).$$

On the other hand, by associativity, applying Theorem 4.11 twice,

$$D(w_1, \ldots, w_n) = D(A)D(B)D(e^1, \ldots, e^n).$$

Since $D(e^1, \ldots, e^n) = 1$, our proposition follows.

Let $A = (a_{ij})$ be an $n \times n$ matrix in R. We let

$$\tilde{A} = (b_{ij})$$

be the matrix such that

$$b_{ij} = (-1)^{i+j}D(A_{ji}).$$

(Note the reversal of indices!)

Proposition 4.16. *Let $d = D(A)$. Then $A\tilde{A} = \tilde{A}A = dI$. The determinant $D(A)$ is invertible in R if and only if A is invertible, and then*

$$A^{-1} = \frac{1}{d}\tilde{A}.$$

Proof. For any pair of indices i, k the ik-component of $A\tilde{A}$ is

$$a_{i1}b_{1k} + a_{i2}b_{2k} + \cdots + a_{in}b_{nk} = a_{i1}(-1)^{k+1}D(A_{k1}) + \cdots + a_{in}(-1)^{k+n}D(A_{kn}).$$

If $i = k$, then this sum is simply the expansion of the determinant according to the i-th row, and hence this sum is equal to d. If $i \neq k$, let $\bar{A}$ be the matrix obtained from A by replacing the k-th row by the i-th row, and leaving all other rows unchanged. If we delete the k-th row and the j-th column from $\bar{A}$, we obtain the same matrix as by deleting the k-th row and j-th column from A. Thus

$$\bar{A}_{kj} = A_{kj},$$

and hence our sum above can be written

$$a_{i1}(-1)^{k+1}D(\bar{A}_{k1}) + \cdots + a_{in}(-1)^{k+n}D(\bar{A}_{kn}).$$

This is the expansion of the determinant of $\bar{A}$ according to the i-th row. Hence $D(\bar{A}) = 0$, and our sum is 0. We have therefore proved that the ik-component of $A\tilde{A}$ is equal to d if $i = k$ (i.e. if it is a diagonal component), and is equal to 0 otherwise. This proves that $A\tilde{A} = dI$. On the other hand, we see at once from the definitions that ${}^t\tilde{A} = \widetilde{{}^tA}$. Then

$$ {}^t(\tilde{A}A) = {}^tA\,{}^t\tilde{A} = {}^tA\widetilde{{}^tA} = dI, $$

and consequently, $\tilde{A}A = dI$ also, since ${}^t(dI) = dI$. When d is a unit in R, then A is invertible, its inverse being $d^{-1}\tilde{A}$. Conversely, if A is invertible, and $AA^{-1} = I$, then $D(A)D(A^{-1}) = 1$, and hence $D(A)$ is invertible, as was to be shown.

Corollary 4.17. *Let F be any R-module, and let $w_1, \ldots, w_n$ be elements of F. Let $A = (a_{ij})$ be an $n \times n$ matrix in R. Let*

$$ \begin{aligned} a_{11}w_1 + \cdots + a_{1n}w_n &= v_1 \\ &\cdots \\ a_{n1}w_1 + \cdots + a_{nn}w_n &= v_n. \end{aligned} $$

Then one can solve explicitly

$$ \begin{pmatrix} D(A)w_1 \\ \vdots \\ D(A)w_n \end{pmatrix} = D(A)\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \tilde{A}\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}. $$

In particular, if $v_i = 0$ for all i, then $D(A)w_i = 0$ for all i. If $v_i = 0$ for all i and F is generated by $w_1, \ldots, w_n$, then $D(A)F = 0$.

Proof. This is immediate from the relation $\tilde{A}A = D(A)I$, using the remarks in §3 about applying matrices to column vectors whose components lie in the module.

Proposition 4.18. *Let E, F be free modules of dimension n over R. Let $f : E \to F$ be a linear map. Let $\mathfrak{B}$, $\mathfrak{B}'$ be bases of E, F respectively over R. Then f is an isomorphism if and only if the determinant of its associated matrix $M_{\mathfrak{B}}^{\mathfrak{B}'}(f)$ is a unit in R.*

Proof. Let $A = M_{\mathfrak{B}}^{\mathfrak{B}'}(f)$. By definition, f is an isomorphism if and only if there exists a linear map $g : F \to E$ such that $g \circ f = \mathrm{id}$ and $f \circ g = \mathrm{id}$. If f is an isomorphism, and $B = M_{\mathfrak{B}}^{\mathfrak{B}'}(g)$, then $AB = BA = I$. Taking the determinant of the product, we conclude that $D(A)$ is invertible in R. Conversely, if $D(A)$ is a unit, then we can define A^{-1} by Proposition 4.16. This A^{-1} is the associated matrix of a linear map $g : F \to E$ which is an inverse for f, as desired.

Finally, we shall define the determinant of an endomorphism.

Let E be a free module over R, and let $\mathfrak{B}$ be a basis. Let $f: E \to E$ be an endomorphism of E. Let

$$M = M_{\mathfrak{B}}^{\mathfrak{B}}(f).$$

If $\mathfrak{B}'$ is another basis of E, and $M' = M_{\mathfrak{B}'}^{\mathfrak{B}'}(f)$, then there exists an invertible matrix N such that

$$M' = NMN^{-1}.$$

Taking the determinant, we see that $D(M') = D(M)$. Hence the determinant does not depend on the choice of basis, and will be called the **determinant of the linear map** f. We shall give below a characterization of this determinant which does not depend on the choice of a basis.

Let E be any module. Then we can view $L_a^n(E)$ as a functor in the variable E (contravariant). In fact, we can view $L_a^n(E, F)$ as a functor of two variables, contravariant in the first, and covariant in the second. Indeed, suppose that

$$E' \xrightarrow{f} E$$

is a linear map. To each multilinear map $\varphi : E^{(n)} \to F$ we can associate the composite map $\varphi \circ f^{(n)}$,

$$E' \times \cdots \times E' \xrightarrow{f^{(n)}} E \times \cdots \times E \xrightarrow{\varphi} F$$

where $f^{(n)}$ is the product of f with itself n times. The map

$$L_a^n(f) : L_a^n(E, F) \to L_a^n(E', F)$$

given by

$$\varphi \mapsto \varphi \circ f^{(n)},$$

is obviously a linear map, which defines our functor. We shall sometimes write f^* instead of $L_a^n(f)$.

In particular, consider the case when $E = E'$ and $F = R$. We get an induced map

$$f^* : L_a^n(E) \to L_a^n(E).$$

Proposition 4.19. *Let E be a free module over R, of dimension n. Let $\{\Delta\}$ be a basis of $L_a^n(E)$. Let $f: E \to E$ be an endomorphism of E. Then*

$$f^*\Delta = D(f)\Delta.$$

Proof. This is an immediate consequence of Theorem 4.11. Namely, we let $\{v_1, \ldots, v_n\}$ be a basis of E, and then take A (or ${}^tA$) to be a matrix of f relative to this basis. By definition,

$$f^*\Delta(v_1, \ldots, v_n) = \Delta(f(v_1), \ldots, f(v_n)),$$

and by Theorem 4.11, this is equal to

$$D(A)\,\Delta(v_1, \ldots, v_n).$$

By Corollary 4.12, we conclude that $f^*\Delta = D(A)\Delta$ since both of these forms take on the same value on $(v_1, \ldots, v_n)$.

The above considerations have dealt with the determinant as a function on all endomorphisms of a free module. One can also view it multiplicatively, as a homomorphism.

$$\det : GL_n(R) \to R^*$$

from the group of invertible $n \times n$ matrices over R into the group of units of R. The kernel of this homomorphism, consisting of those matrices with determinant 1, is called the **special linear group**, and is denoted by $SL_n(R)$.

We now give an application of determinants to the situation of a free module and a submodule considered in Chapter III, Theorem 7.8.

Proposition 4.20. *Let R be a principal entire ring. Let F be a free module over R and let M be a finitely generated submodule. Let $\{e_1, \ldots, e_m, \ldots\}$ be a basis of F such that there exist non-zero elements $a_1, \ldots, a_m \in R$ such that:*

(i) *The elements $a_1e_1, \ldots, a_me_m$ form a basis of M over R.*
(ii) *We have $a_i \mid a_{i+1}$ for $i = 1, \ldots, m-1$.*

Let L_a^s be the set of all s-multilinear alternating forms on F. Let J_s be the ideal generated by all elements $f(y_1, \ldots, y_s)$, with $f \in L_a^s$ and $y_1, \ldots, y_s \in M$. Then

$$J_s = (a_1 \cdots a_s).$$

Proof. We first show that $J_s \subset (a_1 \cdots a_s)$. Indeed, an element $y \in M$ can be written in the form

$$y = c_1a_1e_1 + \cdots + c_ra_re_r.$$

Hence if $y_1, \ldots, y_s \in M$, and f is multilinear alternating on F, then $f(y_1, \ldots, y_s)$ is equal to a sum in terms of type

$$c_{i_1} \cdots c_{i_s} a_{i_1} \cdots a_{i_s} f(e_{i_1}, \ldots, e_{i_s}).$$

This is non-zero only when $e_{i_1}, \ldots, e_{i_s}$ are distinct, in which case the product $a_1 \cdots a_s$ divides this term, and hence J_s is contained in the stated ideal.

Conversely, we show that there exists an s-multilinear alternating form which gives precisely this product. We deduce this from determinants. We can write F as a direct sum

$$F = (e_1, \ldots, e_r) \oplus F_r$$

with some submodule F_r. Let f_i $(i = 1, \ldots, r)$ be the linear map $F \to R$ such that $f_i(e_j) = \delta_{ij}$, and such that f_i has value 0 on F_r. For $v_1, \ldots, v_s \in F$ we define

$$f(v_1, \ldots, v_s) = \det(f_i(v_j)).$$

Then f is multilinear alternating and takes on the value

$$f(e_2, \ldots, e_s) = 1,$$

as well as the value

$$f(a_1e_1, \ldots, a_se_s) = a_1 \cdots a_s.$$

This proves the proposition.

The uniqueness of Chapter III, Theorem 7.8 is now obvious, since first (a_1) is unique, then (a_1a_2) is unique and the quotient (a_2) is unique, and so forth by induction.

Remark. Compare the above theorem with Theorem 2.9 of Chapter XIX, in the theory of Fitting ideals, which gives a fancier context for the result.

§5. DUALITY

Let R be a commutative ring, and let E, F be modules over R. An ***R*-bilinear form** on $E \times F$ is a map

$$f: E \times F \to R$$

having the following properties: For each $x \in E$, the map

$$y \mapsto f(x, y)$$

is R-linear, and for each $y \in F$, the map

$$x \mapsto f(x, y)$$

is R-linear. We shall omit the prefix R- in the rest of this section, and write $\langle x, y \rangle_f$ or $\langle x, y \rangle$ instead of $f(x, y)$. If $x \in F$, we write $x \perp y$ if $\langle x, y \rangle = 0$. Similarly, if S is a subset of F, we define $x \perp S$ if $x \perp y$ for all $y \in S$. We then say that x is **perpendicular** to S. We let $S^\perp$ consist of all elements of E which are perpendicular to S. It is obviously a submodule of E. We define perpendicularity on the other side in the same way. We define the **kernel** of f on the left to be $F^\perp$ and the kernel on the right to be $E^\perp$. We say that f is **non-degenerate** on the left if its kernel on the left is 0. We say that f is **non-degenerate** on the right if its kernel on the right is 0. If E_0 is the kernel of f on the left, then we

get an induced bilinear map

$$E/E_0 \times F \to R$$

which is non-degenerate on the left, as one verifies trivially from the definitions. Similarly, if F_0 is the kernel of f on the right, we get an induced bilinear map

$$E/E_0 \times F/F_0 \to R$$

which is non-degenerate on either side. This map arises from the fact that the value $\langle x, y \rangle$ depends only on the coset of x modulo E_0 and the coset of y modulo F_0.

We shall denote by $L^2(E, F; R)$ the set of all bilinear maps of $E \times F$ into R. It is clear that this set is a module (i.e. an R-module), addition of maps being the usual one, and also multiplication of maps by elements of R.

The form f gives rise to a homomorphism

$$\varphi_f : E \to \mathrm{Hom}_R(F, R)$$

such that

$$\varphi_f(x)(y) = f(x, y) = \langle x, y \rangle,$$

for all $x \in E$ and $y \in F$. We shall call $\mathrm{Hom}_R(F, R)$ the **dual module** of F, and denote it by $F^\vee$. We have an *isomorphism*

$$\boxed{L^2(E, F; R) \leftrightarrow \mathrm{Hom}_R(E, \mathrm{Hom}_R(F, R))}$$

given by $f \mapsto \varphi_f$, its inverse being defined in the obvious way: If

$$\varphi : E \to \mathrm{Hom}_R(F, R)$$

is a homomorphism, we let f be such that

$$f(x, y) = \varphi(x)(y).$$

We shall say that f is **non-singular on the left** if φ_f is an isomorphism, in other words if our form can be used to identify E with the dual module of F. We define **non-singular on the right** in a similar way, and say that f is **non-singular** if it is non-singular on the left and on the right.

Warning: Non-degeneracy does not necessarily imply non-singularity.

We shall now obtain an *isomorphism*

$$\boxed{\mathrm{End}_R(E) \mapsto L^2(E, F; R)}$$

depending on a fixed non-singular bilinear map $f : E \times F \to R$.

Let $A \in \mathrm{End}_R(E)$ be a linear map of E into itself. Then the map

$$(x, y) \mapsto \langle Ax, y\rangle = \langle Ax, y\rangle_f$$

is bilinear, and in this way, we associate linearly with each $A \in \mathrm{End}_R(E)$ a bilinear map in $L^2(E, F; R)$.

Conversely, let $h : E \times F \to R$ be bilinear. Given $x \in E$, the map $h_x : F \to R$ such that $h_x(y) = h(x, y)$ is linear, and is in the dual space $F^\vee$. By assumption, there exists a unique element $x' \in E$ such that for all $y \in F$ we have

$$h(x, y) = \langle x', y\rangle.$$

It is clear that the association $x \mapsto x'$ is a linear map of E into itself. Thus with each bilinear map $E \times F \to R$ we have associated a linear map $E \to E$.

It is immediate that the mappings described in the last two paragraphs are inverse isomorphisms between $\mathrm{End}_R(E)$ and $L^2(E, F; R)$. We emphasize of course that they depend on our form f.

Of course, we could also have worked on the right, and thus we have a similar *isomorphism*

$$\boxed{L^2(E, F; R) \leftrightarrow \mathrm{End}_R(F)}$$

depending also on our fixed non-singular form f.

As an application, let $A : E \to E$ be linear, and let $(x, y) \mapsto \langle Ax, y\rangle$ be its associated bilinear map. There exists a unique linear map

$${}^tA : F \to F$$

such that

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

for all $x \in E$ and $y \in F$. We call ${}^tA$ the **transpose of A with respect to f.**

It is immediately clear that if, A, B are linear maps of E into itself, then for $c \in R$,

$${}^t(cA) = c\,{}^tA, \qquad {}^t(A + B) = {}^tA + {}^tB, \quad \text{and} \quad {}^t(AB) = {}^tB\,{}^tA.$$

More generally, let E, F be modules with non-singular bilinear forms denoted by $\langle\ ,\ \rangle_E$ and $\langle\ ,\ \rangle_F$ respectively. Let $A : E \to F$ be a linear map. Then by the non-singularity of $\langle\ ,\ \rangle_E$ there exists a unique linear map ${}^tA : F \to E$ such that

$$\langle Ax, y\rangle_F = \langle x, {}^tAy\rangle_E \text{ for all } x \in E \text{ and } y \in F.$$

We also call ${}^tA$ the **transpose** with respect to these forms.

Examples. For a nice classical example of a transpose, see Exercise 33. For the systematic study when a linear map is equal to its transpose, see the

spectral theorems of Chapter XV. Next I give another example of a transpose from analysis as follows. Let E be the (infinite dimensional) vector space of C^∞ functions on $\mathbf{R}$, having compact support, i.e. equal to 0 outside some finite interval. We define the scalar product

$$\langle f, g\rangle = \int_{-\infty}^{\infty} f(x)g(x)dx.$$

Let $D : E \to E$ be the derivative. Then one has the formula

$$\langle Df, g\rangle = -\langle f, Dg\rangle.$$

Thus one says that ${}^tD = -D$, even though the scalar product is not "non-singular", but much of the formalism of non-singular forms goes over. Also in analysis, one puts various norms on the spaces and one extends the bilinear form by continuity to the completions, thus leaving the domain of algebra to enter the domain of estimates (analysis). Then the spectral theorems become more complicated in such analytic contexts.

Let us assume that $E = F$. Let $f : E \times E \to R$ be bilinear. By an **automorphism of the pair (E,f)**, or simply of f, we shall mean a linear automorphism $A : E \to E$ such that

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

for all $x, y \in E$. The group of automorphisms of f is denoted by $\mathrm{Aut}(f)$.

Proposition 5.1. *Let $f : E \times E \to R$ be a non-singular bilinear form. Let $A : E \to E$ be a linear map. Then A is an automorphism of f if and only if ${}^tAA = \mathrm{id}$, and A is invertible.*

Proof. From the equality

$$\langle x, y\rangle = \langle Ax, Ay\rangle = \langle x, {}^tAAy\rangle$$

holding for all $x, y \in E$, we conclude that ${}^tAA = \mathrm{id}$ if A is an automorphism of f. The converse is equally clear.

Note. If E is free and finite dimensional, then the condition ${}^tAA = \mathrm{id}$ implies that A is invertible.

Let $f : E \times E \to R$ be a bilinear form. We say that f is **symmetric** if $f(x, y) = f(y, x)$ for all $x, y \in E$. The set of symmetric bilinear forms on E will be denoted by $L_s^2(E)$. Let us take a fixed symmetric non-singular bilinear form f on E, denoted by $(x, y) \mapsto \langle x, y\rangle$. An endomorphism $A : E \to E$ will be said to be **symmetric with respect** to f if ${}^tA = A$. It is clear that the set of symmetric endomorphisms of E is a module, which we shall denote by $\mathrm{Sym}(E)$.

Depending on our fixed symmetric non-singular f, we have an isomorphism

$$\boxed{L_s^2(E) \leftrightarrow \mathrm{Sym}(E)}$$

which we describe as follows. If g is symmetric bilinear on E, then there exists a unique linear map A such that

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

for all $x, y \in E$. Using the fact that both f, g are symmetric, we obtain

$$\langle Ax, y \rangle = \langle Ay, x \rangle = \langle y, {}^tAx \rangle = \langle {}^tAx, y \rangle.$$

Hence $A = {}^tA$. The association $g \mapsto A$ gives us a homomorphism from $L_s^2(E)$ into $\mathrm{Sym}(E)$. Conversely, given a symmetric endomorphism A of E, we can define a symmetric form by the rule $(x, y) \mapsto \langle Ax, y \rangle$, and the association of this form to A clearly gives a homomorphism of $\mathrm{Sym}(E)$ into $L_s^2(E)$ which is inverse to the preceding homomorphism. Hence $\mathrm{Sym}(E)$ and $L_s^2(E)$ are isomorphic.

We recall that a bilinear form $g : E \times E \to R$ is said to be **alternating** if $g(x, x) = 0$ for all $x \in E$, and consequently $g(x, y) = -g(y, x)$ for all $x, y \in E$. The set of bilinear alternating forms on E is a module, denoted by $L_a^2(E)$.

Let f be a fixed *symmetric* non-singular bilinear form on E. An endomorphism $A : E \to E$ will be said to be **skew-symmetric** or **alternating** with respect to f if ${}^tA = -A$, and also $\langle Ax, x \rangle = 0$ for all $x \in E$. If for all $a \in R$, $2a = 0$ implies $a = 0$, then this second condition $\langle Ax, x \rangle = 0$ is redundant, because $\langle Ax, x \rangle = -\langle Ax, x \rangle$ implies $\langle Ax, x \rangle = 0$. It is clear that the set of alternating endomorphisms of E is a module, denoted by $\mathrm{Alt}(E)$. *Depending on our fixed symmetric non-singular form f, we have an isomorphism*

$$\boxed{L_a^2(E) \leftrightarrow \mathrm{Alt}(E)}$$

described as usual. If g is an alternating bilinear form on E, its corresponding linear map A is the one such that

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

for all $x, y \in E$. One verifies trivially in a manner similar to the one used in the symmetric case that the correspondence $g \leftrightarrow A$ gives us our desired isomorphism.

Examples. Let k be a field and let E be a finite-dimensional vector space over k. Let $f : E \times E \to E$ be a bilinear map, denoted by $(x, y) \mapsto xy$. To each

$x \in E$, we associate the linear map $\lambda_x : E \mapsto E$ such that

$$\lambda_x(y) = xy.$$

Then the map obtained by taking the trace, namely

$$(x, y) \mapsto \operatorname{tr}(\lambda_{xy})$$

is a bilinear form on E. If $xy = yx$, then this bilinear form is symmetric.

Next, let E be the space of continuous functions on the interval $[0, 1]$. Let $K(s, t)$ be a continuous function of two real variables defined on the square $0 \leqq s \leqq 1$ and $0 \leqq t \leqq 1$. For $\varphi, \psi \in E$ we define

$$\langle \varphi, \psi \rangle = \iint \varphi(s) K(s, t) \psi(t)\, ds\, dt,$$

the double integral being taken on the square. Then we obtain a bilinear form on E. If $K(s, t) = K(t, s)$, then the bilinear form is symmetric. When we discuss matrices and bilinear forms in the next section, the reader will note the similarity between the preceding formula and the bilinear form defined by a matrix.

Thirdly, let U be an open subset of a real Banach space E (or a finite-dimensional Euclidean space, if the reader insists), and let $f : U \to \mathbf{R}$ be a map which is twice continuously differentiable. For each $x \in U$, the derivative $Df(x) : E \to \mathbf{R}$ is a continuous linear map, and the second derivative $D^2 f(x)$ can be viewed as a continuous symmetric bilinear map of $E \times E$ into $\mathbf{R}$.

§6. MATRICES AND BILINEAR FORMS

We shall investigate the relation between the concepts introduced above and matrices. Let $f : E \times F \to R$ be bilinear. Assume that E, F are free over R. Let $\mathfrak{B} = \{v_1, \ldots, v_m\}$ be a basis for E over R, and let $\mathfrak{B}' = \{w_1, \ldots, w_n\}$ be a basis for F over R. Let $g_{ij} = \langle v_i, w_j \rangle$. If

$$x = x_1 v_1 + \cdots + x_m v_m$$

and

$$y = y_1 w_1 + \cdots + y_n w_n$$

are elements of E and F respectively, with coordinates $x_i, y_j \in R$, then

$$\langle x, y \rangle = \sum_{i=1}^{m} \sum_{j=1}^{n} g_{ij} x_i y_j.$$

Let X, Y be the column vectors of coordinates for x, y respectively, with respect to our bases. Then

$$\langle x, y\rangle = {}^tXGY$$

where G is the matrix (g_{ij}). We could write $G = M_{\mathfrak{B}'}^{\mathfrak{B}}(f)$. We call G the **matrix associated with the form f relative to the bases $\mathfrak{B}$, $\mathfrak{B}'$.**

Conversely, given a matrix G (of size $m \times n$), we get a bilinear form from the map

$$(X, Y) \mapsto {}^tXGY.$$

In this way, we get a correspondence from bilinear forms to matrices and back, and it is clear that this correspondence induces an *isomorphism* (of R-modules)

$$\boxed{L^2(E, F; R) \leftrightarrow \mathrm{Mat}_{m \times n}(R)}$$

given by

$$f \mapsto M_{\mathfrak{B}'}^{\mathfrak{B}}(f).$$

The two maps between these two modules which we described above are clearly inverse to each other.

If we have bases $\mathfrak{B} = \{v_1, \ldots, v_n\}$ and $\mathfrak{B}' = \{w_1, \ldots, w_n\}$ such that $\langle v_i, w_j\rangle = \delta_{ij}$, then we say that these bases are **dual** to each other. In that case, if X is the coordinate vector of an element of E, and Y the coordinate vector of an element of F, then the bilinear map on X, Y has the value

$$X \cdot Y = x_1 y_1 + \cdots + x_n y_n$$

given by the usual dot product.

It is easy to derive in general how the matrix G changes when we change bases in E and F. However, we shall write down the explicit formula only when $E = F$ and $\mathfrak{B} = \mathfrak{B}'$. Thus we have a bilinear form $f : E \times E \to R$. Let $\mathfrak{C}$ be another basis of E and write $X_{\mathfrak{B}}$ and $X_{\mathfrak{C}}$ for the column vectors belonging to an element x of E, relative to the two bases. *Let C be the invertible matrix* $M_{\mathfrak{B}}^{\mathfrak{C}}(\mathrm{id})$, so that

$$X_{\mathfrak{B}} = CX_{\mathfrak{C}}.$$

Then our form is given by

$$\langle x, y\rangle = {}^tX_{\mathfrak{C}}\,{}^tCGCY_{\mathfrak{C}}.$$

We see that

$$M_{\mathfrak{C}}^{\mathfrak{C}}(f) = {}^tCM_{\mathfrak{B}}^{\mathfrak{B}}(f)C. \tag{1}$$

In other words, the matrix of the bilinear form changes by the *transpose*.

If F is free over R, with a basis $\{\eta_1, \ldots, \eta_n\}$, then $\mathrm{Hom}_R(F, R)$ is also free, and we have a dual basis $\{\eta_1', \ldots, \eta_n'\}$ such that

$$\eta_i'(\eta_j) = \delta_{ij}.$$

This has already been mentioned in Chapter III, Theorem 6.1.

Proposition 6.1. *Let E, F be free modules of dimension n over R and let $f: E \times F \to R$ be a bilinear form. Then the following conditions are equivalent:*

f is non-singular on the left.
f is non-singular on the right.
f is non-singular.
The determinant of the matrix of f relative to any bases is invertible in R.

Proof. Assume that f is non-singular on the left. Fix bases of E and F relative to which we write elements of these modules as column vectors, and giving rise to the matrix G for f. Then our form is given by

$$(X, Y) \mapsto {}^tXGY$$

where X, Y are column vectors with coefficients in R. By assumption the map

$$X \mapsto {}^tXG$$

gives an isomorphism between the module of column vectors, and the module of row vectors of length n over R. Hence G is invertible, and hence its determinant is a unit in R. The converse is equally clear, and if $\det(G)$ is a unit, we see that the map

$$Y \to GY$$

must also be an isomorphism between the module of column vectors and itself. This proves our assertion.

We shall now investigate how the transpose behaves in terms of matrices. Let E, F be free over R, of dimension n.

Let $f: E \times F \to R$ be a non-singular bilinear form, and assume given a basis $\mathfrak{B}$ of E and $\mathfrak{B}'$ of F. Let G be the matrix of f relative to these bases. Let $A: E \to E$ be a linear map. If $x \in E$, $y \in F$, let X, Y be their column vectors relative to $\mathfrak{B}$, $\mathfrak{B}'$. Let M be the matrix of A relative to $\mathfrak{B}$. Then for $x \in E$ and $y \in F$ we have

$$\langle Ax, y \rangle = {}^t(MX)GY = {}^tX{}^tMGY.$$

Let N be the matrix of ${}^tA$ relative to the basis $\mathfrak{B}'$. Then NY is the column vector of ${}^tAy$ relative to $\mathfrak{B}'$. Hence

$$\langle x, {}^tAy \rangle = {}^tXGNY.$$

From this we conclude that ${}^tMG = GN$, and since G is invertible, we can solve for N in terms of M. We get:

Proposition 6.2. *Let E, F be free over R, of dimension n. Let $f: E \times F \to R$ be a non-singular bilinear form. Let $\mathfrak{B}, \mathfrak{B}'$ be bases of E and F respectively over R, and let G be the matrix of f relative to these bases. Let $A: E \to E$ be a linear map, and let M be its matrix relative to $\mathfrak{B}$. Then the matrix of ${}^tA$ relative to $\mathfrak{B}'$ is*

$$(G^{-1}){}^tMG.$$

Corollary 6.3. *If G is the unit matrix, then the matrix of the transpose is equal to the transpose of the matrix.*

In terms of matrices and bases, we obtain the following characterization for a matrix to induce an automorphism of the form.

Corollary 6.4. *Let the notation be as in Proposition 6.2, and let $E = F$, $\mathfrak{B} = \mathfrak{B}'$. An $n \times n$ matrix M is the matrix of an automorphism of the form f (relative to our basis) if and only if*

$${}^tMGM = G.$$

If this condition is satisfied, then in particular, M is invertible.

Proof. We use the definitions, together with the formula given in Proposition 6.2. We note that M is invertible, for instance because its determinant is a unit in R.

A matrix M is said to be **symmetric** (resp. **alternating**) if ${}^tM = M$ (resp. ${}^tM = -M$ and the diagonal elements of M are 0).

Let $f: E \times E \to R$ be a bilinear form. We say that f is **symmetric** if $f(x, y) = f(y, x)$ for all $x, y \in E$. We say that f is **alternating** if $f(x, x) = 0$ for all $x \in E$.

Proposition 6.5. *Let E be a free module of dimension n over R, and let $\mathfrak{B}$ be a fixed basis. The map*

$$f \mapsto M_{\mathfrak{B}}^{\mathfrak{B}}(f)$$

induces an isomorphism between the module of symmetric bilinear forms on $E \times E$ (resp. the module of alternating forms on $E \times E$) and the module of symmetric $n \times n$ matrices over R (resp. the module of alternating $n \times n$ matrices over R).

Proof. Consider first the symmetric case. Assume that f is symmetric. In terms of coordinates, let $G = M_{\mathfrak{A}}^{\mathfrak{A}}(f)$. Our form is given by ${}^tXGY$ which must be equal to ${}^tYGX$ by symmetry. However, ${}^tXGY$ may be viewed as a 1×1 matrix, and is equal to its transpose, namely ${}^tY{}^tGX$. Thus

$$ {}^tYGX = {}^tY{}^tGX $$

for all vectors X, Y. It follows that $G = {}^tG$. Conversely, it is clear that any symmetric matrix defines a symmetric form.

As for the alternating case, replacing x by $x + y$ in the relation $\langle x, x\rangle = 0$ we obtain

$$ \langle x, y\rangle + \langle y, x\rangle = 0. $$

In terms of the coordinate vectors X, Y and the matrix G, this yields

$$ {}^tXGY + {}^tYGX = 0. $$

Taking the transpose of, say, the second of the 1×1 matrices entering in this relation, yields (for all X, Y):

$$ {}^tXGY + {}^tX{}^tGY = 0. $$

Hence $G + {}^tG = 0$. Furthermore, letting X be any one of the unit vectors

$$ {}^t(0, \ldots, 0, 1, 0, \ldots, 0) $$

and using the relation ${}^tXGX = 0$, we see that the diagonal elements of G must be equal to 0. Conversely, if G is an $n \times n$ matrix such that ${}^tG + G = 0$, and such that $g_{ii} = 0$ for $i = 1, \ldots, n$ then one verifies immediately that the map

$$ (X, Y) \mapsto {}^tXGY $$

defines an alternating form. This proves our proposition.

Of course, if as is usually the case, 2 is invertible in R, then our condition ${}^tM = -M$ implies that the diagonal elements of M must be 0. Thus in that case, showing that $G + {}^tG = 0$ implies that G is alternating.

§7. SESQUILINEAR DUALITY

There exist forms which are not quite bilinear, and for which the results described above hold almost without change, but which must be handled separately for the sake of clarity in the notation involved.

Let R have an automorphism of period 2. We write this automorphism as $a \mapsto \bar{a}$ (and think of complex conjugation).

Following Bourbaki, we say that a map

$$f: E \times F \to R$$

is a **sesquilinear form** if it is $\mathbf{Z}$-bilinear, and if for $x \in E$, $y \in F$, and $a \in R$ we have

$$f(ax, y) = af(x, y)$$

and

$$f(x, ay) = \bar{a}f(x, y).$$

(**Sesquilinear** means $1\frac{1}{2}$ times linear, so the terminology is rather good.)

Let E, E' be modules. A map $\varphi: E \to E'$ is said to be **anti-linear** (or **semi-linear**) if it is $\mathbf{Z}$-linear, and $\varphi(ax) = \bar{a}\varphi(x)$ for all $x \in E$. Thus we may say that a sesquilinear form is linear in its first variable, and anti-linear in its second variable. We let $\overline{\mathrm{Hom}}_R(E, E')$ denote the module of anti-linear maps of E into E'.

We shall now go systematically through the same remarks that we made previously for bilinear forms.

We define perpendicularity as before, and also the kernel on the right and on the left for any sesquilinear form f. These kernels are submodules, say E_0 and F_0, and we get an induced sesquilinear form

$$E/E_0 \times F/F_0 \to R,$$

which is non-degenerate on either side.

Let F be an R-module. We define its **anti-module** $\bar{F}$ to be the module whose additive group is the same as F, and such that the operation $R \times \bar{F} \to \bar{F}$ is given by

$$(a, y) \mapsto \bar{a}y.$$

Then $\bar{F}$ is a module. We have a natural isomorphism

$$\mathrm{Hom}_R(\bar{F}, R) \leftrightarrow \overline{\mathrm{Hom}}_R(F, R),$$

as R-modules.

The sesquilinear form $f: E \times F \to R$ induces a linear map

$$\varphi_f: E \to \mathrm{Hom}_R(\bar{F}, R).$$

We say that f is **non-singular on the left** if φ_f is an isomorphism. Similarly, we have a corresponding linear map

$$\varphi'_f: \bar{F} \to \mathrm{Hom}_R(E, R)$$

from $\bar{F}$ into the dual space of E, and we say that f is **non-singular on the right** if φ'_f is an isomorphism. We say that f is **non-singular** if it is non-singular on the left and on the right.

We observe that our sesquilinear form f can be viewed as a **bilinear** form

$$f : E \times \bar{F} \to R,$$

and that our notions of non-singularity are then compatible with those defined previously for bilinear forms.

If we have a fixed non-singular sesquilinear form on $E \times F$, then depending on this form, we obtain an isomorphism between the module of sesquilinear forms on $E \times F$ and the module of endomorphisms of E. We also obtain an anti-isomorphism between these modules and the module of endomorphisms of F. In particular, we can define the analogue of the transpose, which in the present case we shall call the adjoint. Thus, let $f : E \times F \to R$ be a non-singular sesquilinear form. Let $A : E \to E$ be a linear map. There exists a unique linear map

$$A^* : F \to F$$

such that

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

for all $x \in E$ and $y \in F$. Note that A^* is linear, not anti-linear. We call A^* the **adjoint** of A with respect to our form f. We have the rules

$$(cA)^* = \bar{c}A^*, \qquad (A + B)^* = A^* + B^*, \qquad (AB)^* = B^*A^*$$

for all linear maps A, B of E into itself, and $c \in R$.

Let us assume that $E = F$. Let $f : E \times E \to R$ be sesquilinear. By an **automorphism** of f we shall mean a linear automorphism $A : E \to E$ such that

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

just as we did for bilinear forms.

Proposition 7.1. *Let $f : E \times E \to R$ be a non-singular sesquilinear form. Let $A : E \to E$ be a linear map. Then A is an automorphism of f if and only if $A^*A = \mathrm{id}$, and A is invertible.*

The proof, and also the proofs of subsequent propositions, which are completely similar to those of the bilinear case, will be omitted.

A sesquilinear form $g : E \times E \to R$ is said to be **hermitian** if

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

for all $x, y \in E$. The set of hermitian forms on E will be denoted by $L_h^2(E)$. Let R_0 be the subring of R consisting of all elements fixed under our automorphism

$a \to \bar{a}$ (i.e. consisting of all elements $a \in R$ such that $a = \bar{a}$). Then $L_h^2(E)$ is an R_0-module.

Let us take a fixed hermitian non-singular form f on E, denoted by $(x, y) \mapsto \langle x, y \rangle$. An endomorphism $A : E \to E$ will be said to be **hermitian** with respect to f if $A^* = A$. It is clear that the set of hermitian endomorphisms is an R_0-module, which we shall denote by Herm(E). *Depending on our fixed hermitian non-singular form f, we have an R_0-isomorphism*

$$\boxed{L_h^2(E) \leftrightarrow \mathrm{Herm}(E)}$$

described in the usual way. A hermitian form g corresponds to a hermitian map A if and only if

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

for all $x, y \in E$.

We can now describe the relation between our concepts and matrices, just as we did with bilinear forms.

We start with a sesquilinear form $f : E \times F \to R$.

If E, F are free, and we have selected bases as before, then we can again associate a matrix G with the form, and in terms of coordinate vectors X, Y our sesquilinear form is given by

$$(X, Y) \mapsto {}^tXG\overline{Y},$$

where $\overline{Y}$ is obtained from Y by applying the automorphism to each component of Y.

If $E = F$ and we use the same basis on the right and on the left, then with the same notation as that used in formula (1), if f is sesquilinear, the formula now reads

$$M_{\mathfrak{C}}^{\mathfrak{C}}(f) = {}^tCM_{\mathfrak{B}}^{\mathfrak{B}}(f)\overline{C}. \tag{1S}$$

The automorphism appears.

Proposition 7.2. *Let E, F be free modules of dimension n over R, and let $f : E \times F \to R$ be a sesquilinear form. Then the following conditions are equivalent.*

f is non-singular on the left.
f is non-singular on the right.
f is non-singular.

The determinant of the matrix of f relative to any bases is invertible in R.

Proposition 7.3. *Let E, F be free over R, of dimension n. Let $f : E \times F \to R$ be a non-singular sesquilinear form. Let $\mathfrak{B}, \mathfrak{B}'$ be bases of E and F respectively over R, and let G be the matrix of f relative to these bases. Let $A : E \to E$ be a linear map, and let M be its matrix relative to $\mathfrak{B}$. Then the matrix of A^* relative to $\mathfrak{B}'$ is*

$$(\bar{G}^{-1})^t \bar{M} \bar{G}.$$

Corollary 7.4. *If G is the unit matrix, then the matrix of A^* is equal to ${}^t\bar{M}$.*

Corollary 7.5. *Let the notation be as in the proposition, and let $\mathfrak{B} = \mathfrak{B}'$ be a basis of E. An $n \times n$ matrix M is the matrix of an automorphism of f (relative to our basis) if and only if*

$${}^t M G \bar{M} = G.$$

A matrix M is said to be **hermitian** if ${}^t M = \bar{M}$.

Let R_0 be as before the subring of R consisting of all elements fixed under our automorphism $a \mapsto \bar{a}$ (i.e. consisting of all elements $a \in R$ such that $a = \bar{a}$).

Proposition 7.6. *Let E be a free module of dimension n over R, and let $\mathfrak{B}$ be a basis. The map*

$$f \mapsto M_{\mathfrak{B}}^{\mathfrak{B}}(f)$$

induces an R_0-isomorphism between the R_0-module of hermitian forms on E and the R_0-module of $n \times n$ hermitian matrices in R.

Remark. If we had assumed at the beginning that our automorphism $a \mapsto \bar{a}$ has period 2 or 1 (i.e. if we allow it to be the identity), then the results on bilinear and symmetric forms become special cases of the results of this section. However, the notational differences are sufficiently disturbing to warrant a repetition of the results as we have done.

Terminology

For some confusing reason, the group of automorphisms of a symmetric (resp. alternating, resp. hermitian) form on a vector space is called the **orthogonal** (resp. **symplectic**, resp. **unitary**) group of the form. The word orthogonal is especially unfortunate, because an orthogonal map preserves more than orthogonality: It also preserves the scalar product, i.e. length. Furthermore, the word symplectic is also unfortunate. It turns out that one can carry out a discussion of hermitian forms over certain division rings (having automorphisms of order 2), and their group of automorphisms have also been called symplectic, thereby creating genuine confusion with the use of the word relative to alternating forms.

In order to unify and improve the terminology, I have discussed the matter with several persons, and it seems that one could adopt the following conventions.

As said in the text, the group of automorphisms of any form f is denoted by $\mathrm{Aut}(f)$.

On the other hand, there is a standard form, described over the real numbers in terms of coordinates by

$$f(x, x) = x_1^2 + \cdots + x_n^2,$$

over the complex numbers by

$$f(x, x) = x_1\bar{x}_1 + \cdots + x_n\bar{x}_n,$$

and over the quaternions by the same formula as in the complex case. The group of automorphisms of this form would be called the **unitary group**, and be denoted by U_n. The points of this group in the reals (resp. complex, resp. quaternions) would be denoted by

$$U_n(\mathbf{R}), \qquad U_n(\mathbf{C}), \qquad U_n(\mathbf{K}),$$

and these three groups would be called the **real unitary group** (resp. **complex unitary group**, resp. **quaternion unitary group**). Similarly, the group of points of U_n in any subfield or subring k of the quaternions would be denoted by $U_n(k)$.

Finally, if f is the standard alternating form, whose matrix is

$$\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix},$$

one would denote its group of automorphisms by A_{2n}, and call it the **alternating form group**, or simply the alternating group, if there is no danger of confusion with the permutation group. The group of points of the alternating form group in a field k would then be denoted by $A_{2n}(k)$.

As usual, the subgroup of $\mathrm{Aut}(f)$ consisting of those elements whose determinant is 1 would be denoted by adding the letter S in front, and would still be called the **special group**. In the four standard cases, this yields

$$SU_n(\mathbf{R}), \qquad SU_n(\mathbf{C}), \qquad SU_n(\mathbf{K}), \qquad SA_{2n}(k).$$

§8. THE SIMPLICITY OF $SL_2(F)/\pm 1$

Let F be a field. Let n be a positive integer. By $GL_n(F)$ we mean the group of $n \times n$ invertible matrices over F. By $SL_n(F)$ we mean the subgroup of those matrices whose determinant is equal to 1. By $PGL_n(F)$ we mean the factor group of $GL_n(F)$ by the subgroup of scalar matrices (which are in the center).

Similarly for $PSL_n(F)$. In this section, we are interested in giving an application of matrices to the group theoretic structure of SL_2. The analogous statements for SL_n with $n \geqq 3$ will be proved in the next section.

The **standard Borel subgroup** B of GL_2 is the group of all matrices

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $a, b, d \in F$ and $ad \neq 0$. For the Borel subgroup of SL_2, we require in addition that $ad = 1$. By a **Borel subgroup** we mean a subgroup which is conjugate to the standard Borel subgroup (whether in GL_2 or SL_2). We let U be the group of matrices

$$u(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \quad \text{with } b \in F.$$

We let A be the group of diagonal matrices

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \quad \text{with } a, d \in F^*.$$

Let

$$s(a) = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \qquad \text{with } a \in F^*$$

and

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

For the rest of this section, we let

$$G = GL_2(F) \quad \text{or} \quad SL_2(F).$$

Lemma 8.1. *The matrices*

$$X(b) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad Y(c) = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

generate $SL_2(F)$.

Proof. Multiplying an arbitrary element of $SL_2(F)$ by matrices of the above type on the right and on the left corresponds to elementary row and column operations, that is adding a scalar multiple of a row to the other, etc. Thus a given matrix can always be brought into a form

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

by such multiplications. We want to express this matrix with $a \neq 1$ in the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix}.$$

Matrix multiplication will show that we can solve this equation, by selecting x arbitrarily $\neq 0$, then solving for b, c, and d successively so that

$$1 + bx = a, \quad c = \frac{-x}{1 + bx}, \quad d = \frac{-b}{1 + bc}.$$

Then one finds $1 + bc = (1 + xb)^{-1}$ and the two symmetric conditions

$$b + bcd + d = 0$$
$$c + bcx + x = 0,$$

so we get what we want, and thereby prove the lemma.

Let $\overline{U}$ be the group of lower matrices

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

Then we see that

$$wUw^{-1} = \overline{U}.$$

Also note the commutation relation

$$w\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}w^{-1} = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix},$$

so w normalizes A. Similarly,

$$wBw^{-1} = \overline{B}$$

is the group of lower triangular matrices.

We note that

$$B = AU = UA,$$

and also that A normalizes U.

There is a decomposition of G into disjoint subsets

$$G = B \cup BwB.$$

Indeed, view G as operating on the left of column vectors. The isotropy group of

$$e^1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

is obviously U. The orbit Be^1 consists of all column vectors whose second

component is 0. On the other hand,

$$we^1 = \begin{pmatrix} 0 \\ -1 \end{pmatrix},$$

and therefore the orbit Bwe^1 consists of all vectors whose second component is $\neq 0$, and whose first component is arbitrary. Since these two orbits of B and BwB cover the orbit Ge^1, it follows that the union of B and BwB is equal to G (because the isotropy group U is contained in B), and they are obviously disjoint. This decomposition is called the **Bruhat decomposition**.

Proposition 8.2. *The Borel subgroup B is a maximal proper subgroup.*

Proof. By the Bruhat decomposition, any element not in B lies in BwB, so the assertion follows since B, BwB cover G.

Theorem 8.3. *If F has at least four elements, then $SL_2(F)$ is equal to its own commutator group.*

Proof. We have the commutator relation (by matrix multiplication)

$$s(a)u(b)s(a)^{-1}u(b)^{-1} = u(ba^2 - b) = u(b(a^2 - 1)).$$

Let $G = SL_2(F)$ for this proof. We let G' be the commutator subgroup, and similarly let B' be the commutator subgroup of B. We prove the first assertion that $G = G'$. From the hypothesis that F has at least four elements, we can find an element $a \neq 0$ in F such that $a^2 \neq 1$, whence the commutator relation shows that $B' = U$. It follows that $G' \supset U$, and since G' is normal, we get

$$G' \supset wUw^{-1}.$$

From Lemma 8.1, we conclude that $G' = G$.

Let Z denote the center of G. It consists of $\pm I$, that is $\pm$ the identity 2×2 matrix if $G = SL_2(F)$; and Z is the subgroup of scalar matrices if $G = GL_2(F)$.

Theorem 8.4. *If F has at least four elements, then $SL_2(F)/Z$ is simple.*

The proof will result from two lemmas.

Lemma 8.5. *The intersection of all conjugates of B in G is equal to Z.*

Proof. We leave this to the reader, as a simple fact using conjugation with w.

Lemma 8.6. *Let $G = SL_2(F)$. If H is normal in G, then either $H \subset Z$ or $H \supset G'$.*

Proof. By the maximality of B we must have

$$HB = B \quad \text{or} \quad HB = G.$$

If $HB = B$ then $H \subset B$. Since H is normal, we conclude that H is contained in every conjugate of B, whence in the center by Lemma 8.5. On the other hand, suppose that $HB = G$. Write

$$w = hb$$

with $h \in H$ and $b \in B$. Then

$$wUw^{-1} = \overline{U} = hbUb^{-1}h^{-1} = hUh^{-1} \subset HU$$

because H is normal. Since $U \subset HU$ and $U, \overline{U}$ generate $SL_2(F)$, it follows that $HU = G$. Hence

$$G/H = HU/H \approx U/(U \cap H)$$

is abelian, whence $H \supset G'$, as was to be shown.

The simplicity of Theorem 8.4 is an immediate consequence of Lemma 8.6.

§9. THE GROUP $SL_n(F)$, $n \geqq 3$.

In this section we look at the case with $n \geqq 3$, and follow parts of Artin's *Geometric Algebra*, Chapter IV. (Artin even treats the case of a non-commutative division algebra as the group ring, but we omit this for simplicity.)

For $i, j = 1, \ldots, n$ and $i \neq j$ and $c \in F$, we let

$$E_{ij}(c) = \begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ 0 & & \ddots & \\ & c_{ij} & & \\ 0 & & 0 & 1 \end{pmatrix}$$

be the matrix which differs from the unit matrix by having c in the ij-component instead of 0. We call such $E_{ij}(c)$ an **elementary matrix**. Note that

$$\det E_{ij}(c) = 1.$$

If A is any $n \times n$ matrix, then multiplication $E_{ij}(c)A$ on the left adds c times the j-th row to the i-th row of A. Multiplication $AE_{ij}(c)$ on the right adds c times the i-th column to the j-th column. We shall mostly multiply on the left.

For fixed $i \neq j$ the map

$$c \mapsto E_{ij}(c)$$

is a homomorphism of F into the multiplicative group of $n \times n$ matrices $GL_n(F)$.

Proposition 9.1. *The group $SL_n(F)$ is generated by the elementary matrices. If $A \in GL_n(F)$, then A can be written in the form*

$$A = SD,$$

where $S \in SL_n(F)$ and D is a diagonal matrix of the form

$$D = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d \end{pmatrix}$$

so D has 1 on the diagonal except on the lower right corner, where the component is $d = \det(A)$.

Proof. Let $A \in GL_n(F)$. Since A is non-singular, the first component of some row is not zero, and by an elementary row operation, we can make $a_{11} \neq 0$. Adding a suitable multiple of the first row to the second row, we make $a_{21} \neq 0$, and then adding a suitable multiple of the second row to the first we make $a_{11} = 1$. Then we subtract multiples of the first row from the others to make $a_{i1} = 0$ for $i \neq 1$.

We now repeat the procedure with the second row and column, to make $a_{22} = 1$ and $a_{i2} = 0$ if $i > 2$. But then we can also make $a_{12} = 0$ by subtracting a suitable multiple of the second row from the first, so we can get $a_{i2} = 0$ for $i \neq 2$.

We repeat this procedure until we are stopped at $a_{nn} = d \neq 0$, and $a_{nj} = 0$ for $j \neq n$. Subtracting a suitable multiple of the last row from the preceding ones yields a matrix D of the form indicated in the statement of the theorem, and concludes the proof.

Theorem 9.2. *For $n \geqq 3$, $SL_n(F)$ is equal to its own commutator group.*

Proof. It suffices to prove that $E_{ij}(c)$ is a commutator. Using $n \geqq 3$, let $k \neq i, j$. Then by direct computation,

$$E_{ij}(c) = E_{ik}(c)E_{kj}(1)E_{ik}(-c)E_{kj}(-1)$$

expresses $E_{ij}(c)$ as a commutator. This proves the theorem.

We note that if a matrix M commutes with every element of $SL_n(F)$, then it must be a scalar matrix. Indeed, just the commutation with the elementary matrices

$$E_{ij}(1) = I + 1_{ij}$$

shows that M commutes with all matrices 1_{ij} (having 1 in the ij-component, 0 otherwise), so M commutes with all matrices, and is a scalar matrix. Taking the determinant shows that the center consists of $\boldsymbol{\mu}_n(F)I$, where $\boldsymbol{\mu}_n(F)$ is the group of n-th roots of unity in F.

We let Z be the center of $SL_n(F)$, so we have just seen that Z is the group of scalar matrices such that the scalar is an n-th root of unity. Then we define

$$PSL_n(F) = SL_n(F)/Z.$$

Theorem 9.3. *For $n \geqq 3$, $PSL_n(F)$ is simple.*

The rest of this section is devoted to the proof. We view $GL_n(F)$ as operating on the vector space $E = F^n$. If λ is a non-zero functional on E, we let

$$H_\lambda = \operatorname{Ker} \lambda,$$

and call H_λ (or simply H) the **hyperplane associated with** λ. Then $\dim H = n - 1$, and conversely, if H is a subspace of codimension 1, then E/H has dimension 1, and is the kernel of a functional.

An element $T \in GL_n(F)$ is called a **transvection** if it keeps every element of some hyperplane H fixed, and for all $x \in E$, we have

$$Tx = x + h \qquad \text{for some } h \in H.$$

Given any element $u \in H_\lambda$ we define a transvection T_u by

$$T_u x = x + \lambda(x)u.$$

Every transvection is of this type. If $u, v \in H_\lambda$, it is immediate that

$$T_{u+v} = T_u \circ T_v.$$

If T is a transvection and $A \in GL_n(F)$, then the conjugate ATA^{-1} is obviously a transvection.

The elementary matrices $E_{ij}(c)$ are transvections, and it will be useful to use them with this geometric interpretations, rather than formally as we did before. Indeed, let $e_1, \ldots, e_n$ be the standard unit vectors which form a basis of $F^{(n)}$. Then $E_{ij}(c)$ leaves e_k fixed if $k \neq j$, and the remaining vector e_j is moved by a multiple of e_i. We let H be the hyperplane generated by e_k with $k \neq j$, and thus see that $E_{ij}(c)$ is a transvection.

Lemma 9.4. *For $n \geqq 3$, the transvections $\neq I$ form a single conjugacy class in $SL_n(F)$.*

Proof. First, by picking a basis of a hyperplane $H = H_\lambda$ and using one more element to form a basis of $F^{(n)}$, one sees from the matrix of a transvection T that $\det T = 1$, i.e. transvections are in $SL_n(F)$.

Let T' be another transvection relative to a hyperplane H'. Say

$$Tx = x + \lambda(x)u \quad \text{and} \quad T'x = x + \lambda'(x)u'$$

with $u \in H$ and $u' \in H'$. Let z and z' be vectors such that $\lambda(z) = 1$ and $\lambda'(z') = 1$. Since a basis for H together with z is a basis for $F^{(n)}$, and similarly a basis for H' together with z' is a basis for $F^{(n)}$, there exists an element $A \in GL_n(F)$ such that

$$Au = u', \qquad AH = H', \qquad Az = z'.$$

It is then immediately verified that

$$ATA^{-1} = T',$$

so T, T' are conjugate in $GL_n(F)$. But in fact, using $n \geqq 3$, the hyperplanes H, H' contain vectors which are independent. We can change the image of a basis vector in H' which is independent of u' by some factor in F so as to make $\det A = 1$, so $A \in SL_n(F)$. This proves the lemma.

We now want to show that certain subgroups of $GL_n(F)$ are either contained in the center, or contain $SL_n(F)$. Let G be a subgroup of $GL_n(F)$. We say that G is **SL_n-invariant** if

$$AGA^{-1} \subset G \quad \text{for all } A \in SL_n(F).$$

Lemma 9.5. *Let $n \geqq 3$. Let G be SL_n-invariant, and suppose that G contains a transvection $T \neq I$. Then $SL_n(F) \subset G$.*

Proof. By Lemma 9.4, all transvections are conjugate, and the set of transvections contains the elementary matrices which generate $SL_n(F)$ by Proposition 9.1, so the lemma follows.

Theorem 9.6. *Let $n \geqq 3$. If G is a subgroup of $GL_n(F)$ which is SL_n-invariant and which is not contained in the center of $GL_n(F)$, then $SL_n(F) \subset G$.*

Proof. By the preceding lemma, it suffices to prove that G contains a transvection, and this is the key step in the proof of Theorem 9.3.

We start with an element $A \in G$ which moves some line. This is possible since G is not contained in the center. So there exists a vector $u \neq 0$ such that Au is not a scalar multiple of u, say $Au = v$. Then u, v are contained in some hyperplane $H = \operatorname{Ker} \lambda$. Let $T = T_u$ and let

$$B = ATA^{-1}T^{-1}.$$

Then

$$ATA^{-1} \neq T \quad \text{and} \quad B = ATA^{-1}T^{-1} \neq I.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$PGL_2(\mathbf{F}_3) \approx S_4 \quad \text{but} \quad SL_2(\mathbf{F}_3) \not\approx S_4; \quad PSL_2(\mathbf{F}_3) \approx A_4.$$

EXERCISES

1. Interpret the rank of a matrix A in terms of the dimensions of the image and kernel of the linear map L_A.

2. (a) Let A be an invertible matrix in a commutative ring R. Show that $({}^tA)^{-1} = {}^t(A^{-1})$.
   (b) Let f be a non-singular bilinear form on the module E over R. Let A be an R-automorphism of E. Show that $({}^tA)^{-1} = {}^t(A^{-1})$. Prove the same thing in the hermitian case, i.e. $(A^*)^{-1} = (A^{-1})^*$.

3. Let V, W be finite dimensional vector spaces over a field k. Suppose given non-degenerate bilinear forms on V and W respectively, denoted both by $\langle\ ,\ \rangle$. Let $L: V \to W$ be a surjective linear map and let ${}^tL$ be its transpose; that is, $\langle Lv, w\rangle = \langle v, {}^tLw\rangle$ for $v \in V$ and $w \in W$.
   (a) Show that ${}^tL$ is injective.
   (b) Assume in addition that if $v \in V$, $v \neq 0$ then $\langle v, v\rangle \neq 0$. Show that

$$V = \operatorname{Ker} L \oplus \operatorname{Im} {}^tL,$$

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

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

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

   If $b_1 = \cdots = b_r = 0$, one says the system is homogeneous. We call n the number of variables, and r the number of equations. A solution X of the homogeneous system is called **trivial** if $x_i = 0$, $i = 1, \ldots, n$.
   (a) Show that a homogeneous system of r linear equations in n unknowns with $n > r$ always has a non-trivial solution.
   (b) Let L be a system of homogeneous linear equations over a field k. Let k be a subfield of k'. If L has a non-trivial solution in k', show that it has a non-trivial solution in k.

5. Let M be an $n \times n$ matrix over a field k. Assume that $\operatorname{tr}(MX) = 0$ for all $n \times n$ matrices X in k. Show that $M = O$.

6. Let S be a set of $n \times n$ matrices over a field k. Show that there exists a column vector $X \neq 0$ of dimension n in k, such that $MX = X$ for all $M \in S$ if and only if there exists such a vector in some extension field k' of k.

7. Let $\mathbf{H}$ be the division ring over the reals generated by elements i, j, k such that $i^2 = j^2 = k^2 = -1$, and

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

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

$$a_0 + a_1 i + a_2 j + a_3 k \mapsto a_0 - a_1 i - a_2 j - a_3 k.$$

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

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

8. Let N be a strictly upper triangular $n \times n$ matrix, that is $N = (a_{ij})$ and $a_{ij} = 0$ if $i \geqq j$. Show that $N^n = 0$.

9. Let E be a vector space over k, of dimension n. Let $T: E \to E$ be a linear map such that T is nilpotent, that is $T^m = 0$ for some positive integer m. Show that there exists a basis of E over k such that the matrix of T with respect to this basis is strictly upper triangular.

10. If N is a nilpotent $n \times n$ matrix, show that $I + N$ is invertible.

11. Let R be the set of all upper triangular $n \times n$ matrices (a_{ij}) with a_{ij} in some field k, so $a_{ij} = 0$ if $i > j$. Let J be the set of all strictly upper triangular matrices. Show that J is a two-sided ideal in R. How would you describe the factor ring R/J?

12. Let G be the group of upper triangular matrices with non-zero diagonal elements. Let H be the subgroup consisting of those matrices whose diagonal element is 1. (Actually prove that H is a subgroup). How would you describe the factor group G/H?

13. Let R be the ring of $n \times n$ matrices over a field k. Let L be the subset of matrices which are 0 except on the first column.
    (a) Show that L is a left ideal.
    (b) Show that L is a minimal left ideal; that is, if $L' \subset L$ is a left ideal and $L' \neq 0$, then $L' = L$. (For more on this situation, see Chapter VII, §5.)

14. Let F be any field. Let D be the subgroup of diagonal matrices in $GL_n(F)$. Let N be the normalizer of D in $GL_n(F)$. Show that N/D is isomorphic to the symmetric group on n elements.

15. Let F be a finite field with q elements. Show that the order of $GL_n(F)$ is

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

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

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

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

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

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

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

17. Let F be a finite field with q elements. Show that the group of all upper triangular matrices with 1 on the diagonal is a Sylow subgroup of $GL_n(F)$ and of $SL_n(F)$.

18. The reduction map $\mathbf{Z} \to \mathbf{Z}/N\mathbf{Z}$, where N is a positive integer defines a homomorphism

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

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

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

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

where the product is taken over all primes dividing N.

20. Show that one has an exact sequence

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

In fact, show that

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

where G_N is the group of matrices

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

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

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

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

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

23. Let k be a field in which every quadratic polynomial has a root. Let B be the Borel subgroup of $GL_2(k)$. Show that G is the union of all the conjugates of B. (This cannot happen for finite groups!)

24. Let A, B be square matrices of the same size over a field k. Assume that B is non-singular. If t is a variable, show that $\det(A + tB)$ is a polynomial in t, whose leading coefficient is $\det(B)$, and whose constant term is $\det(A)$.

25. Let $a_{11}, \ldots, a_{1n}$ be elements from a principal ideal ring, and assume that they generate the unit ideal. Suppose $n > 1$. Show that there exists a matrix (a_{ij}) with this given first row, and whose determinant is equal to 1.

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

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

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

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

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

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

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

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

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

where T_a is translation by a.] Also show that

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

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

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

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

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

(a) Let A be an associative algebra over R. For $x, y \in A$, define $[x, y] = xy - yx$. Show that this makes A into a Lie algebra. Example: the algebra of R-endomorphisms of a module M, especially the algebra of matrices $\mathrm{Mat}_n(R)$.

(b) Let M be a module over R. For two derivations D_1, D_2 of M, define $[D_1, D_2] = D_1 D_2 - D_2 D_1$. Show that the set of derivations of M is a Lie subalgebra of $\mathrm{End}_R(M)$.

(c) Show that the map $x \mapsto \bar{E}_x$ is a Lie homomorphism of $\mathfrak{g}$ into the Lie algebra of derivations of $\mathfrak{g}$ into itself.

30. Given a set of polynomials $\{P_v(X_{ij})\}$ in the polynomial ring $R[X_{ij}]$ $(1 \leqq i, j \leqq n)$, a zero of this set in R is a matrix $x = (x_{ij})$ such that $x_{ij} \in R$ and $P_v(x_{ij}) = 0$ for all v. We use vector notation, and write $(X) = (X_{ij})$. We let $G(R)$ denote the set of zeros

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

As an example, the group of matrices satisfying the equation ${}^tXX = I_n$ is an algebraic group.

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

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

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

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

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

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

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

Non-commutative cocycles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Prove:

(a) The number of monomials of degree d is $\binom{n-1+d}{n-1}$, so this number is the dimension of $\mathrm{Pol}(n, d)$.

(b) Let $(D) = (D_1, \ldots, D_n)$ where D_i is the partial derivative with respect to the i-th variable. Then we can define $P(D)$ as usual. For $P, Q \in \mathrm{Pol}(n, d)$, define

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

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

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

(d) Let $\Delta = D_1^2 + \cdots + D_n^2$. Note that Δ: Pol$(n, d) \to$ Pol$(n, d-2)$ is a linear map. Prove that Δ is surjective.

(e) Define Har$(n, d) =$ KerΔ = vector space of **harmonic homogeneous polynomials** of degree d. Prove that

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

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

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

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

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

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

(g) Show that $[\Delta, S] = 4d + 2n$ on Pol(n, d). Here $[\Delta, S] = \Delta \circ S - S \circ \Delta$. Actually, $[\Delta, S] = 4E + 2n$, where E is the Euler operator $E = \sum X_i D_i$, which is, however, the degree operator on homogeneous polynomials.

(h) Prove that Pol$(n, d) =$ Har$(n, d) \oplus r^2\text{Pol}(n, d-2)$ and that the two summands are orthogonal. This is a classical theorem used in the theory of the Laplace operator.

(i) Let $(c_1, \ldots, c_n) \in k^n$ be such that $\sum c_i^2 = 0$. Let

$$H_c^d(X) = (c_1X_1 + \cdots + c_nX_n)^d.$$

Show that H_c^d is harmonic, i.e. lies in Har(n, d).

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

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

34. (Continuation of Exercise 33). Prove:

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

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

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

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

35. (Continuation of Exercise 34). Prove that the representation of $O(n) = U_n(\mathbf{R})$ on Har(n, d) is irreducible.
Readers will find a proof in the following:

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

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

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

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

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

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

$$\lambda\colon \mathrm{Har}(n,d) \to \mathbf{C}$$

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

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

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

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

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

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

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

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

CHAPTER XIV

Representation of One Endomorphism

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

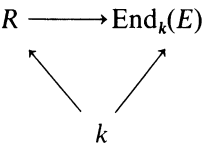
§1. REPRESENTATIONS

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

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

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

which makes the following diagram commutative:



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

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

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

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

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

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

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

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

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

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

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

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

$$x \mapsto xv$$

induces an isomorphism of R-modules,

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

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

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

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

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

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

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

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

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

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

This is always the case if k is a field.

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

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

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

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

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

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

occurring on the right in the matrix representing φ.

Furthermore, consider an exact sequence

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

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

$$\varphi'' : E'' \to E''$$

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

§2. DECOMPOSITION OVER ONE ENDOMORPHISM

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

$$k[t] \to k[A] \subset \mathrm{End}_k(E)$$

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

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

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

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

$$v, Av, A^2v, \ldots.$$

We called such a module **principal**, and if $R = k[t]$ we may write $E = Rv = (v)$.

If $q_A(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_0$ then the elements

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof. Exercise.

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

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

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

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

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

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

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

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

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

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

We contend that the elements

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

or equivalently,

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

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

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

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

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

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

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

$$M = B + N$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§3. THE CHARACTERISTIC POLYNOMIAL

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

$$k[t] \to k[A]$$

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

$$\det(tI_n - M)$$

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

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

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

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

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

where φP_M is obtained from P_M by applying φ to the coefficients of P_M.

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

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

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

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

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

Then

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

because

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

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

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

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

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

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

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

Proof. Suppose that we have

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

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

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

which shortens our relation, contradiction.

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

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

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

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

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

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

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

Thus the characteristic polynomial is multiplicative on direct sums.

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

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

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

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

single invariant q. Write

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Then

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

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

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

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

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

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

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

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

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

Proof. Clear.

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

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

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

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

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

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

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

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

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

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

meaning that the induced sequence

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

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

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

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

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

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

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

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

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

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

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

and

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

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

$$\mathbf{Z}[x_{ij}, y_1, \ldots, y_n] \to k$$

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

EXERCISES

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

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

   where each M_i is a square matrix, is equal to the product of the determinants of the matrices $M_1, \ldots, M_s$.
3. Let k be a commutative ring, and let M, M' be square $n \times n$ matrices in k. Show that the characteristic polynomials of MM' and $M'M$ are equal.
4. Show that the eigenvalues of the matrix

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

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

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

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

is the least common multiple of q, q'.

6. Let A be a nilpotent endomorphism of a finite dimensional vector space E over the field k. Show that $\operatorname{tr}(A) = 0$.

7. Let R be a principal entire ring. Let E be a free module over R, and let $E^\vee = \operatorname{Hom}_R(E, R)$ be its dual module. Then $E^\vee$ is free of dimension n. Let F be a submodule of E. Show that $E^\vee/F^\perp$ can be viewed as a submodule of $F^\vee$, and that its invariants are the same as the invariants of F in E.

8. Let E be a finite-dimensional vector space over a field k. Let $A \in \operatorname{Aut}_k(E)$. Show that the following conditions are equivalent:
   (a) $A = I + N$, with N nilpotent.
   (b) There exists a basis of E such that the matrix of A with respect to this basis has all its diagonal elements equal to 1 and all elements above the diagonal equal to 0.
   (c) All roots of the characteristic polynomial of A (in the algebraic closure of k) are equal to 1.

9. Let k be a field of characteristic 0, and let M be an $n \times n$ matrix in k. Show that M is nilpotent if and only if $\operatorname{tr}(M^v) = 0$ for $1 \leqq v \leqq n$.

10. Generalize Theorem 3.10 to rational functions (instead of polynomials), assuming that k is a field.

11. Let E be a finite-dimensional space over the field k. Let $\alpha \in k$. Let E_α be the subspace of E generated by all eigenvectors of a given endomorphism A of E, having α as an eigenvalue. Show that every non-zero element of E_α is an eigenvector of A having α as an eigenvalue.

12. Let E be finite dimensional over the field k. Let $A \in \operatorname{End}_k(E)$. Let v be an eigenvector for A. Let $B \in \operatorname{End}_k(E)$ be such that $AB = BA$. Show that Bv is also an eigenvector for A (if $Bv \neq 0$), with the same eigenvalue.

Diagonalizable endomorphisms

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

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

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

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

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

(c) If S is diagonalizable, and if F is a subspace of E such that $SF \subset F$, show that S is diagonalizable as an endomorphism of F, i.e. that F has a basis consisting of eigenvectors of S.

(d) Let S, T be endomorphisms of E, and assume that S, T commute. Assume that both S, T are diagonalizable. Show that they are simultaneously diagonalizable, i.e. there exists a basis of E consisting of eigenvectors for both S and T. [*Hint*: If λ is an eigenvalue of S, and E_λ is the subspace of E consisting of all vectors v such that $Sv = \lambda v$, then $TE_\lambda \subset E_\lambda$.]

14. Let E be a finite-dimensional vector space over an algebraically closed field k. Let $A \in \mathrm{End}_k(E)$. Show that A can be written in a unique way as a sum

$$A = S + N$$

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

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

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

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

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

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

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

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

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

17. Prove the normal basis theorem for finite extensions of a finite field.

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

19. Let (E, A) and (E', A') be pairs consisting of a finite-dimensional vector space over a field k, and a k-endomorphism. Show that these pairs are isomorphic if and only if their invariants are equal.

20. (a) How many non-conjugate elements of $GL_2(\mathbf{C})$ are there with characteristic polynomial $t^3(t+1)^2(t-1)$?
(b) How many with characteristic polynomial $t^3 - 1001t$?

21. Let V be a finite dimensional vector space over $\mathbf{Q}$ and let $A: V \to V$ be a $\mathbf{Q}$-linear map such that $A^5 = \mathrm{Id}$. Assume that if $v \in V$ is such that $Av = v$, then $v = 0$. Prove that $\dim V$ is divisible by 4.

22. Let V be a finite dimensional vector space over $\mathbf{R}$, and let $A: V \to V$ be an $\mathbf{R}$-linear map such that $A^2 = -\mathrm{Id}$. Show that $\dim V$ is even, and that V is a direct sum of 2-dimensional A-invariant subspaces.

23. Let E be a finite-dimensional vector space over an algebraically closed field k. Let A, B be k-endomorphisms of E which commute, i.e. $AB = BA$. Show that A and B have a common eigenvector. [*Hint*: Consider a subspace consisting of all vectors having a fixed element of k as eigenvalue.]

24. Let V be a finite dimensional vector space over a field k. Let A be an endomorphism of V. Let $\mathrm{Tr}(A^m)$ be the trace of A^m as an endomorphism of V. Show that the following power series in the variable t are equal:

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

Compare with Exercise 23 of Chapter XVIII.

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

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

Show that

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

and

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

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

26. Let $G = SL_n(\mathbf{C})$ and let K be the complex unitary group. Let A be the group of diagonal matrices with positive real components on the diagonal.
(a) Show that if $g \in \mathrm{Nor}_G(A)$ (normalizer of A in G), then $\mathbf{c}(g)$ (conjugation by g) permutes the diagonal components of A, thus giving rise to a homomorphism $\mathrm{Nor}_G(A) \to W$ to the group W of permutations of the diagonal coordinates.

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

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

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

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

CHAPTER XV

Structure of Bilinear Forms

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

§1. PRELIMINARIES, ORTHOGONAL SUMS

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

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

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

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

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

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

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

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

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

$$E = F \perp F'$$

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

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

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

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

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

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

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

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

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

with $v_i, w_i \in E_i$. Then

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$E = E_0 \oplus W'$$

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

§2. QUADRATIC MAPS

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

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

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

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

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

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

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

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

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

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

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

by

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

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

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

Proof. Obvious.

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

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

§3. SYMMETRIC FORMS, ORTHOGONAL BASES

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

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

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

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

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

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

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

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

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

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

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

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

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

$$E = E_0 \oplus W$$

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

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

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

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

Proof. Obvious.

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

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

with $x_i \in k$, then

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

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

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

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

§4. SYMMETRIC FORMS OVER ORDERED FIELDS

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

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

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

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

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

Then

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

Squaring both sides yields

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

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

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

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

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

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

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

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

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

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

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

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

$$|v \cdot w| \leqq |v|\,|w|$$

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

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

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

$$\mp 2ab\, v \cdot w \leqq 2|v|^2|w|^2.$$

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

From the Schwarz inequality, we deduce the triangle inequality

$$|v + w| \leqq |v| + |w|.$$

We leave it to the reader as a routine exercise.

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

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

Then v_1 has norm 1. Let

$$w_2 = v_2 - (v_2 \cdot v_1')v_1',$$

and then

$$v_2' = \frac{1}{|w_2|} w_2.$$

Inductively, we let

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

and then

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

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

§5. HERMITIAN FORMS

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

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

$$E \times E \to k$$

written

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

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

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

for all $x, y \in E$.

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

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

$$\langle v_1, v_1 \rangle, \ldots, \langle v_n, v_n \rangle$$

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

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

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

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

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

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

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

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

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

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

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

From this we conclude:

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

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

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

We have the **Schwarz inequality**, namely

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

whose proof comes again by expanding

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

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

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

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

Then we get at once the triangle inequality

$$|x + y| \leqq |x| + |y|,$$

and for $\alpha \in k$,

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

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

§6. THE SPECTRAL THEOREM (HERMITIAN CASE)

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

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

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

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

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

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

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

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

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

Proof. Let A be hermitian. Then

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof. Let ξ_1 be a non-zero eigenvector, with eigenvalue λ_1, and let E_1 be the subspace generated by ξ_1. Then A maps $E_1^{\perp}$ into itself, because

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

whence $AE_1^{\perp}$ is perpendicular to ξ_1.

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

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

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

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

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

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

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

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

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

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

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

Proof. Let $\xi_1 \neq 0$ be an eigenvector of U. It is immediately verified that the subspace of E orthogonal to ξ_1 is mapped into itself by U, using the relation $U^* = U^{-1}$, because if η is perpendicular to ξ_1, then

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

Thus we can finish the proof by induction as before.

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

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

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

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

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

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

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

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

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

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

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

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

§7. THE SPECTRAL THEOREM (SYMMETRIC CASE)

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

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

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

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

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

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

$$z = x + iy,$$

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

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

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

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

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

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

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

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

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

§8. ALTERNATING FORMS

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

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

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

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

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

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

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

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

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

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

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

complete the proof by induction.

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

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

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

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

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

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

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

is called the **standard alternating** matrix.

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

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

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

then

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

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

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

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

§9. THE PFAFFIAN

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

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

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

and hence

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

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

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

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

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

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

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

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

Let R be a commutative ring. We have a homomorphism

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

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

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

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

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

$$\mathrm{Pf}(CG^tC) = \det(C)\,\mathrm{Pf}(G).$$

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

$$\mathrm{Pf}(UT^tU) = \pm \det(U)\,\mathrm{Pf}(T),$$

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

§10. WITT'S THEOREM

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

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

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

Then select $a \in k$ such that

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

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

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

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

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

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

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

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

$$F = F_0 \perp U.$$

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

$$U \perp P_1 \perp \cdots \perp P_s.$$

Proof. Let

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

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

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

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

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

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

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

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

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

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

$$U \perp P_1 \perp \cdots \perp P_s \quad \text{and} \quad \sigma U \perp P_1' \perp \cdots \perp P_s'$$

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

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

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

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

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

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

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

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

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