ALGEBRA BOOT CAMP NOTES

ANDERS S. BUCH AND YI-ZHI HUANG

1. Sylow's theorems and product groups

Theorem 1.1 (Sylow I)**.** *Let G be a finite group, p a prime number, and $k \in \mathbb{N}$. If p^k divides $|G|$, then G contains a subgroup of order p^k.*

Definition 1.2. A subgroup $G' \leq G$ is called a Sylow p-subgroup if $|G'| = p^m$, where p^m is the largest power of the prime p that divides $|G|$.

It follows from Theorem 1.1 that every finite group G contains a Sylow p-subgroup for every prime p.

Theorem 1.3 (Sylow II)**.** *Let G be a finite group and p a prime number.*

(1) *Any two Sylow p-subgroups of G are conjugate.*

(2) *The number of Sylow p-subgroups divides the index of any Sylow p-subgroup and is congruent to 1 modulo p.*

(3) *Any subgroup of order p^k is contained in a Sylow p-subgroup.*

Application 1.4. Prove that a group of order 150 is not simple.

Proof. Let G be a group of order $150 = 2 \cdot 3 \cdot 5^2$. Let S be the set of Sylow 5-subgroups in G and $n_5 = |S|$. It follows from Theorem 1.3(2) that $n_5 \equiv 1 \pmod 5$ and $n_5 | 6$. This implies that $n_5 = 1$ or $n_5 = 6$.

Assume first that $n_5 = 1$. Then there is a unique Sylow 5-subgroup $H \leq G$. For $g \in G$, gHg^{-1} is also a Sylow 5-subgroup, so $gHg^{-1} = H$. It follows that H is a normal subgroup of G. Since $|H| = 25$, G contains a non-trivial proper normal subgroup, so G is not simple.

Assume next that $n_5 = 6$. Any element $g \in G$ defines a bijective map $\rho(g) : S \to S$ given by $\rho(g)(H) = gHg^{-1}$. Notice that $\rho(g_1 g_2)(H) = \rho(g_1)\rho(g_2)(H)$ for all $g_1, g_2 \in G$. If we identify the symmetric group S_6 with the set of bijective maps $S \to S$, then ρ is a group homomorphism $\rho : G \to S_6$. Let N be the kernel of ρ. Then $N \triangleleft G$ is a normal subgroup. It follows from Theorem 1.3(1) that N is a proper subgroup of G. Since $|G| = 150$ does not divide $|S_6| = 6! = 720$, it follows from Lagrange's Theorem that G is not isomorphic to a subgroup of S_6, so N is not the trivial subgroup of G. We deduce that N is a non-trivial proper normal subgroup of G, so again G is not simple. □

Exercise 1.5. Prove that a group of order 108 is not simple.

Given two groups H and K, the Cartesian product $H \times K$ is again a group with operation $(h_1, k_1) \cdot (h_2, k_2) = (h_1 h_2, k_1 k_2)$.

The commutator of two elements $h, k \in G$ is defined by $[h, k] = hkh^{-1}k^{-1}$. If H and K are subgroups of G, then $[H, K]$ denotes the commutator subgroup, defined as the subgroup of G generated by all commutators $[h, k]$ with $h \in H$ and $k \in K$.

Date: August 20, 2021.

Theorem 1.6. *Let H and K be subgroups of a group G and let $m : H \times K \to G$ be the multiplicative map defined by $m(h,k) = hk$.*

(1) *m is injective if and only if $H \cap K = \{1\}$.*

(2) *m is a group homomorphism if and only if all elements of H commute with all elements of K.*

(3) *If H is a normal subgroup of G, then HK is a subgroup of G and $[H,K] \leq H$.*

(4) *m is an isomorphism of groups if and only if $H \cap K = \{1\}$, $HK = G$, and both H and K are normal subgroups of G.*

Exercise 1.7. Prove Theorem 1.6.

Assume that $N \triangleleft G$ is a normal subgroup. Then each element $g \in G$ defines a group automorphism $\rho(g) : N \to N$ given by $\rho(g)(n) = gng^{-1}$. In fact, since $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ for $g_1, g_2 \in G$, $\rho : G \to \mathrm{Aut}(N)$ is a group homomorphism from G to the automorphism group of N. Notice that $\mathrm{Aut}(N)$ is typically much smaller than the group of all permutations of the elements of N.

Exercise 1.8. We have $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (Z/n\mathbb{Z})^\times$, that is, the automorphism group of the cyclic group $(\mathbb{Z}/n\mathbb{Z}, +)$ is the group of units in the commutative ring $\mathbb{Z}/n\mathbb{Z}$.

Exercise 1.9. Let G be a group of order 2015.
(a) Prove that G contains normal subgroups of orders 13, 31, and 155.
(b) Prove that G is isomorphic to a product of two groups of orders 13 and 155.

2. Polynomial rings

Let $\mathbb{F}$ be a field, and let $\mathbb{F}[x]$ denote the ring of polynomials in one variable with coefficients in $\mathbb{F}$.

Theorem 2.1. *$\mathbb{F}[x]$ is an Euclidean domain, that is, given $f(x), g(x) \in \mathbb{F}[x]$ where $g(x) \neq 0$, there exist $q(x), r(x) \in \mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$ and the degree of $r(x)$ is smaller than the degree of $g(x)$.*

The zero polynomial has negative degree by convention, so $r(x) = 0$ is allowed in Theorem 2.1.

Theorem 2.2. *$\mathbb{F}[x]$ is a principal ideal domain (PID).*

Proof. Given any non-zero ideal $I \subset \mathbb{F}[x]$, let $g(x) \in I$ be a non-zero element with the smallest possible degree. Then $I = \langle g(x) \rangle$. In fact, if $f(x) \in I$ is any element, we may write $f(x) = q(x)g(x) + r(x)$ as in Theorem 2.1. Since $r(x) \in I$ has degree smaller than the degree of $g(x)$, it follows that $r(x) = 0$, so $f(x) \in \langle g(x) \rangle$. $\square$

Exercise 2.3. Find ideals of $\mathbb{Z}[x]$ and of $\mathbb{F}[x,y]$ that are not principal.

Exercise 2.4. Let R be a commutative ring. Then $R[x]$ is a principal ideal domain if and only if R is a field.

Theorem 2.5. *Let $f(x) \in \mathbb{F}[x]$ be a polynomial of degree n. Then $f(x)$ has at most n distinct roots in $\mathbb{F}$.*

Proof. Given a root $a \in \mathbb{F}$ of $f(x)$, use Theorem 2.1 to write $f(x) = (x-a)q(x) + r$, where $q(x) \in \mathbb{F}[x]$ and r is a polynomial of degree at most 0, that is $r \in \mathbb{F}$. Since $r = f(a) = 0$, we obtain $f(x) = (x-a)q(x)$. Since the roots of $f(x)$ consist of a and the roots of $q(x)$, the result follows by induction on the degree of $f(x)$. $\square$

Exercise 2.6. Let $\mathbb{F}$ be a field with p elements and let $a_1, a_2, \ldots, a_{p-1}$ be the all the non-zero elements of $\mathbb{F}$. Then $a_1 a_2 \cdots a_{p-1} = -1$.

Exercise 2.7. Prove that the field $\mathbb{F}$ is finite if and only if the multiplicative group $\mathbb{F}^\times$ of non-zero elements in $\mathbb{F}$ is cyclic.

Exercise 2.8. Let $\mathbb{F}$ be a finite field of order q, with q odd. Show that the equation $x^2 + 1 = 0$ has a solution in $\mathbb{F}$ if and only if $q \equiv 1 \pmod 4$.

3. Generalized eigenspaces

Let $\mathbb{F}$ be a field. Given a vector space V over $\mathbb{F}$, let $\mathrm{End}(V)$ denote the set of all linear endomorphisms $\phi : V \to V$. Then $\mathrm{End}(V)$ is ring with operations defined by $(\phi + \psi)(v) = \phi(v) + \psi(v)$ and $(\phi\psi)(v) = \phi(\psi(v))$ for $\phi, \psi \in \mathrm{End}(V)$ and $v \in V$. $\mathrm{End}(V)$ is also an $\mathbb{F}$-vector space with scalar multiplication given by $(a\phi)(v) = a\,\phi(v)$ for $a \in \mathbb{F}$. Let $1_V \in \mathrm{End}(V)$ denote the identity function on V. Given a scalar $a \in \mathbb{F}$ we will occasionally denote the endomorphism $a\,1_V \in \mathrm{End}(V)$ simply by a.

Let V be an $\mathbb{F}$-vector space of finite dimension and fix an endomorphism $\phi \in \mathrm{End}(V)$. Relative to a basis $B = \{v_1, v_2, \ldots, v_n\}$ of V, ϕ is represented by the $n \times n$ matrix $A = (a_{ij})$ with entries defined by $\phi(v_j) = \sum_{i=1}^n a_{ij} v_i$. If $B' = \{v'_1, v'_2, \ldots, v'_n\}$ is a different basis of V, then the transition matrix $P = (p_{ij})$ from B to B' is defined by $v_j = \sum_{i=1}^n p_{ij} v'_i$, and ϕ is represented by $A' = PAP^{-1}$ relative to B'. Notice that $\det(A') = \det(A)$.

Definition 3.1. We set $\det(\phi) = \det(A)$ where A is any matrix representing ϕ.

Definition 3.2. The characteristic polynomial $\chi_\phi(x) \in \mathbb{F}[x]$ of ϕ is defined by $\chi_\phi(x) = \det(x\,1_V - \phi)$.

The polynomial $\chi_\phi(x)$ is monic and has degree equal to the dimension of V.

Definition 3.3. Let $\phi \in \mathrm{End}(V)$ and let $\lambda \in \mathbb{F}$. We say that λ is an eigenvalue for ϕ if there exists a non-zero vector $v \in V$ such that $\phi(v) = \lambda v$. In this case v is called an eigenvector with eigenvalue λ.

Let $\lambda \in \mathbb{F}$ be any scalar. Then the subspace $\mathrm{Ker}(\phi - \lambda) = \{v \in V \mid \phi(v) = \lambda v\}$ is called the eigenspace of ϕ with respect to λ. A larger generalized eigenspace is defined by

$$V_\lambda = V_\lambda(\phi) = \{v \in V \mid (\phi - \lambda)^N(v) = 0 \text{ for some } N \in \mathbb{N}\} = \bigcup_{N \in \mathbb{N}} \mathrm{Ker}((\phi - \lambda)^N)\,.$$

Exercise 3.4. We have $V_\lambda(\phi) = \mathrm{Ker}((\phi - \lambda)^{\dim V})$.

Any polynomial $f(x) = a_m x^m + \cdots + a_1 x + a_0$ in $\mathbb{F}[x]$ can be applied to $\phi \in \mathrm{End}(V)$ to obtain a new endomorphism

$$f(\phi) = a_m \phi^m + \cdots + a_1 \phi + a_0 1_V\,.$$

Notice that since $\mathrm{End}(V)$ is a vector space of dimension $n = (\dim V)^2$, it follows that $\{1_V, \phi, \phi^2, \ldots, \phi^n\}$ is a linearly dependent subset of $\mathrm{End}(V)$. It follows that there exists a non-zero polynomial $f(x) \in \mathbb{F}[x]$ such that $f(\phi) = 0$ in $\mathrm{End}(V)$. (We will see in Exercise 4.11 that in fact $\chi_\phi(\phi) = 0$.) Notice that $I = \{f(x) \in \mathbb{F}[x] \mid f(\phi) = 0\}$ is an ideal in $\mathbb{F}[x]$, so by Theorem 2.2 it is generated by a unique monic polynomial $p(x)$ called the minimal polynomial of ϕ.

Exercise 3.5. The following are equivalent.
(1) λ is an eigenvalue of ϕ.
(2) $\chi_\phi(\lambda) = 0$.
(3) $p(\lambda) = 0$ where $p(x)$ is the minimal polynomial of ϕ.
(4) $\operatorname{Ker}(\phi - \lambda) \neq 0$.
(5) $V_\lambda(\phi) \neq 0$.

Assume now that the minimal polynomial $p(x)$ of $\phi : V \to V$ can be written as a product of linear factors,

$$p(x) = \prod_{i=1}^{r} (x - \lambda_i)^{m_i} \,,$$

where $\lambda_1, \dots, \lambda_r \in \mathbb{F}$ are the (distinct) eigenvalues of ϕ and $m_1, \dots, m_r$ are positive integers. For example, this holds if the field $\mathbb{F}$ is algebraically closed. The following theorem demonstrates the utility of generalized eigenspaces.

Theorem 3.6. *Assume that the minimal polynomial of ϕ is a product of linear factors in $\mathbb{F}[x]$. Then we have $V = V_{\lambda_1}(\phi) \oplus \cdots \oplus V_{\lambda_r}(\phi)$.*

Proof. For $1 \leq i \leq r$ we define the polynomial

$$p_i(x) = \prod_{j \neq i} (x - \lambda_j)^{m_j} = \frac{p(x)}{(x - \lambda_i)^{m_i}} \,.$$

Using that $\mathbb{F}[x]$ is a PID, it follows that $\langle p_1, p_2, \dots, p_r \rangle = \langle 1 \rangle$ is the unit ideal in $\mathbb{F}[x]$. We may therefore choose $q_1, q_2, \dots, q_r \in \mathbb{F}[x]$ such that $q_1 p_1 + q_2 p_2 + \cdots + q_r p_r = 1$. Set $\phi_i = q_i(\phi) p_i(\phi) \in \operatorname{End}(V)$. Then we have $\phi_1 + \phi_2 + \cdots + \phi_r = 1_V$. For $i \neq j$ we have $\phi_i \phi_j = 0$, this follows because $p(x)$ divides $p_i(x) p_j(x)$. Notice also that $\phi_i = 1_V \phi_i = \phi_i^2$ for each i. These identities imply that $V = \phi_1(V) \oplus \cdots \oplus \phi_r(V)$.

It remains to show that $V_{\lambda_i} = \phi_i(V)$ for each i. One inclusion holds because $\phi_i(V) \subset \operatorname{Ker}((\phi - \lambda_i)^{m_i}) \subset V_{\lambda_i}$. For any $v \in V$, define the ideal $\operatorname{Ann}(v) = \{ f(x) \in \mathbb{F}[x] \mid f(\phi)(v) = 0 \}$ in $\mathbb{F}[x]$. Then $(x - \lambda_j)^{m_j} \in \operatorname{Ann}(\phi_j(v))$ for every j. Assume that $v \in V_{\lambda_i}$. Then we also have $(x - \lambda_i)^N \in \operatorname{Ann}(v) \subset \operatorname{Ann}(\phi_j(v))$ for some $N \in \mathbb{N}$. It follows that for $j \neq i$ we have $\operatorname{Ann}(\phi_j(v)) = \langle 1 \rangle$, and therefore $\phi_j(v) = 0$. We deduce that $v = 1_V(v) = \phi_1(v) + \cdots + \phi_r(v) = \phi_i(v) \in \phi_i(V)$, as required. $\square$

Exercise 3.7. Let V be any $\mathbb{F}$-vector space and let $\phi_1, \dots, \phi_r \in \operatorname{End}(V)$ satisfy $\phi_i \phi_j = \delta_{ij} \phi_i$ and $\phi_1 + \cdots + \phi_r = 1_V$. Then $V = \phi_1(V) \oplus \cdots \oplus \phi_r(V)$.

The endomorphism $\phi : V \to V$ is diagonalizable if V has a basis consisting of eigenvectors of ϕ.

Exercise 3.8. Assume that $\mathbb{F}$ is algebraically closed. Then the endomorphism $\phi : V \to V$ is diagonalizable if and only if $\operatorname{Ker}(\phi - \lambda) = V_\lambda(\phi)$ for each $\lambda \in \mathbb{F}$.

Exercise 3.9. Let $\phi, \psi \in \operatorname{End}(V)$ be commuting diagonalizable endomorphisms. Then V has a basis $\{v_1, \dots, v_n\}$ such that each vector v_i is an eigenvector of both ϕ and ψ.

4. Jordan canonical form

As in Section 3 we let V be an $\mathbb{F}$-vector space of finite dimension and fix an endomorphism $\phi \in \operatorname{End}(V)$.

Definition 4.1. An indecomposable Jordan set for ϕ with eigenvalue $\lambda \in \mathbb{F}$ is a set of non-zero vectors $\{v_1, v_2, \ldots, v_k\}$ in V such that $\phi(v_1) = \lambda v_1$ and $\phi(v_j) = \lambda v_j + v_{j-1}$ for $2 \leq j \leq k$. A Jordan basis for ϕ is a basis of V that is a disjoint union of indecomposable Jordan sets for ϕ.

Exercise 4.2. Let $P_n(\mathbb{C}) \subset \mathbb{C}[x]$ be the vector subspace of polynomials of degree at most n, and let $\frac{d}{dx} : P_n(\mathbb{C}) \to P_n(\mathbb{C})$ be the linear endomorphism that sends any polynomial to its derivative. Find a Jordan basis for $\frac{d}{dx}$.

Exercise 4.3. Any indecomposable Jordan set is linearly independent.

Exercise 4.4. Assume that ϕ has an indecomposable Jordan basis $\{v_1, \ldots, v_k\}$. Then the matrix of ϕ relative to this basis is the $k \times k$ Jordan block

$$J_{\lambda,k} \;=\; \begin{bmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & & 0 & 0 \\ 0 & 0 & \lambda & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & 1 & 0 \\ 0 & 0 & \cdots & 0 & \lambda & 1 \\ 0 & 0 & \cdots & 0 & 0 & \lambda \end{bmatrix}.$$

Exercise 4.5. The matrix of ϕ relative to any Jordan basis is a block matrix of the form

$$\begin{bmatrix} J_{\lambda_1,k_1} & 0 & \cdots & 0 \\ 0 & J_{\lambda_2,k_2} & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & J_{\lambda_\ell,k_\ell} \end{bmatrix}.$$

Exercise 4.6. A subset $B \subset V$ is a Jordan basis for ϕ if and only if it is a Jordan basis for $\phi - \lambda$, for any $\lambda \in \mathbb{F}$.

Theorem 4.7. *Assume that the minimal polynomial of ϕ is a product of linear factors in $\mathbb{F}[x]$. Then ϕ has a Jordan basis.*

Proof. It follows from Theorem 3.6 that $V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_r}$. Since $\phi(V_{\lambda_i}) \subset V_{\lambda_i}$, it is enough to show that each restricted endomorphism $\phi : V_{\lambda_i} \to V_{\lambda_i}$ has a Jordan basis. We may therefore assume that ϕ has a unique eigenvalue λ. By replacing ϕ with $\phi - \lambda$ and using Exercise 4.6, we may further assume that $\lambda = 0$.

Since 0 is an eigenvalue of ϕ, it follows that $\phi(V)$ is a proper subspace of V, so by induction on $\dim(V)$ there exists a Jordan basis for the restricted endomorphism $\phi : \phi(V) \to \phi(V)$. In other words, $\phi(V)$ has a basis of the form

$$\{\ v_1, \phi(v_1), \ldots, \phi^{k_1-1}(v_1)\ ,\ v_2, \phi(v_2), \ldots, \phi^{k_2-1}(v_2)\ ,\ \ldots\ ,\ v_\ell, \phi(v_\ell), \ldots, \phi^{k_\ell-1}(v_\ell)\ \}$$

such that $\phi^{k_i}(v_i) = 0$ for each i. Choose $u_1, \ldots, u_\ell \in V$ such that $v_i = \phi(u_i)$ for each i, and choose $w_1, \ldots, w_m \in V$ such that $\{\phi^{k_1-1}(v_1), \ldots, \phi^{k_\ell-1}(v_\ell), w_1, \ldots, w_m\}$ is a basis for $\mathrm{Ker}(\phi)$. We claim that

$$\{\ u_1, \phi(u_1), \ldots, \phi^{k_1}(u_1)\ ,\ \ldots\ ,\ u_\ell, \phi(u_\ell), \ldots, \phi^{k_\ell}(u_\ell)\ ,\ w_1, \ldots, w_m\ \}$$

is a basis for V, and hence a Jordan basis for ϕ. By applying ϕ to any vanishing linear combination of this set of vectors, we deduce that the set is linearly independent. On the other hand, the number of vectors is

$$(k_1 + \cdots + k_\ell) + (\ell + m) \;=\; \dim \phi(V) + \dim \mathrm{Ker}(\phi) \;=\; \dim(V)\,.$$

This completes the proof (which we learned from Mark Wildon's notes [4]). □

Corollary 4.8. *Let A be any square matrix with entries in an algebraically closed field $\mathbb{F}$. Then there exists an invertible matrix P with entries in $\mathbb{F}$ such that $P^{-1}AP$ is a Jordan block matrix as in Exercise 4.5.*

The matrix $P^{-1}AP$ is called the Jordan normal form of A. Notice that the columns of P form a Jordan basis for the linear map represented by A.

Exercise 4.9. Let λ be an eigenvalue of $\phi : V \to V$ and set $p_d = \dim \operatorname{Ker}((\phi-\lambda)^d)$ for $d \geq 0$. Then the number of Jordan blocks $J_{\lambda,k}$ in any Jordan normal form of ϕ is equal to $2p_k - p_{k-1} - p_{k+1}$. It follows that the Jordan normal form of any matrix is unique up to permutation of the Jordan blocks.

Exercise 4.10. Find the Jordan normal form of each of the complex matrices

$$\begin{bmatrix} 2 & 2 & 3 \\ 1 & 3 & 3 \\ -1 & -2 & -2 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 \\ -1 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

In addition, find Jordan bases for the associated linear maps $\mathbb{C}^n \to \mathbb{C}^n$.

Exercise 4.11 (Cayley-Hamilton Theorem)**.** Use Theorem 4.7 to prove that any endomorphism $\phi : V \to V$ of a finite dimensional vector space satisfies $\chi_\phi(\phi) = 0$. You may use that any field is a subfield of an algebraically closed field. Can you also deduce that $\chi_\phi(\phi) = 0$ if ϕ is a square matrix with entries in an arbitrary commutative ring?

Exercise 4.12. Explain how to find the minimal polynomial of an endomorphism $\phi : V \to V$ if a Jordan basis for ϕ is known.

Exercise 4.13. Assume that $\phi : V \to V$ satisfies $\phi^k = \phi$ for some $k \geq 2$. If $\mathbb{F} = \mathbb{C}$ then ϕ is diagonalizable. However, ϕ may fail to be diagonalizable if $\mathbb{F} = \mathbb{R}$ or $\mathbb{F}$ has positive characteristic.

Exercise 4.14. Let $\phi, \psi \in \operatorname{End}(V)$ satisfy $\phi\psi - \psi\phi = \psi$. If $\mathbb{F}$ has characteristic zero, then ψ is not invertible. If $\mathbb{F}$ has positive characteristic, then find an example where ψ is invertible.

Exercise 4.15. Let $\rho : \mathbb{Z}/m\mathbb{Z} \to \mathrm{GL}_n(\mathbb{C})$ be a group homomorphism, where $\mathrm{GL}_n(\mathbb{C})$ is the group of invertible $n \times n$ matrices with complex entries. Show that with respect to some basis of $\mathbb{C}^n$, every element of $\rho(\mathbb{Z}/m\mathbb{Z})$ is a diagonal matrix with m-th roots of unity on its diagonal.

Given an endomorphism $\phi : V \to V$ of a complex vector space $V \cong \mathbb{C}^n$, we define a new endomorphism $e^\phi = \exp(\phi) \in \operatorname{End}(V)$ by

$$e^\phi \;=\; 1_V + \phi + \frac{1}{2}\phi^2 + \frac{1}{6}\phi^3 + \cdots \;=\; \sum_{k \geq 0} \frac{1}{k!}\phi^k .$$

The following can be proved with analytic methods.

Theorem 4.16. *If $\phi, \psi \in \operatorname{End}(V)$ satisfy $\phi\psi = \psi\phi$, then $e^\phi e^\psi = e^\psi e^\phi = e^{\phi+\psi}$.*

Exercise 4.17. Compute $\exp(J_{\lambda,k})$ and find the Jordan normal form of $\exp(J_{\lambda,k})$.

The algebraic multiplicity of an eigenvalue λ of $\phi : V \to V$ is defined as the multiplicity of λ as a root of the characteristic polynomial $\chi_\phi(x)$. The geometric multiplicity of λ is the dimension of the eigenspace $\mathrm{Ker}(\phi - \lambda)$.

Exercise 4.18. The algebraic multiplicity of λ is equal to $\dim V_\lambda(\phi)$.

Exercise 4.19. Explain how to find the algebraic and geometric multiplicities of the eigenvalues of the endomorphism $\phi : V \to V$ if a Jordan basis for ϕ is known.

Exercise 4.20. Let $\phi : V \to V$ be an endomorphism of a complex vector space $V \cong \mathbb{C}^n$ and let $\lambda \in \mathbb{C}$ be an eigenvalue of ϕ. Then e^λ is an eigenvalue of e^ϕ. Furthermore, if all eigenvalues of ϕ are real, then the algebraic and geometric multiplicities of λ as an eigenvalue of ϕ are equal to the algebraic and geometric multiplicities of e^λ as an eigenvalue of e^ϕ.

5. Dual vector spaces

Given two vector spaces V and W over the field $\mathbb{F}$, let $\mathrm{Hom}(V, W) = \mathrm{Hom}_{\mathbb{F}}(V, W)$ denote the set of all $\mathbb{F}$-linear maps $\phi : V \to W$. This set is a vector space with operations $(\phi + \psi)(v) = \phi(v) + \psi(v)$ and $(a\phi)(v) = a\,\phi(v)$ for $\phi, \psi \in \mathrm{Hom}(V, W)$, $v \in V$, and $a \in \mathbb{F}$. Notice that $\mathrm{End}(V) = \mathrm{Hom}(V, V)$. The dual vector space of V is the space $V^\vee = \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$ of all linear maps $\alpha : V \to \mathbb{F}$. Any linear map $\phi : V \to W$ of has a dual map $\phi^\vee : W^\vee \to V^\vee$ defined by $\phi^\vee(\alpha)(v) = \alpha(\phi(v))$.

Exercise 5.1. Define a linear map $\iota : V \to V^{\vee\vee}$ by $\iota(v)(\alpha) = \alpha(v)$ for $v \in V$ and $\alpha \in V^\vee$. Show that ι is always injective, and that ι is an isomorphism of vector spaces if and only if V has finite dimension.

Given a basis $\{v_1, \ldots, v_n\}$ of a finite dimensional vector space V, we obtain a dual basis $\{v_1^\vee, \ldots, v_n^\vee\}$ of $V^\vee$ by defining $v_i^\vee : V \to \mathbb{F}$ to be the unique linear map satisfying $v_i^\vee(v_j) = \delta_{ij}$. Notice that this construction can be applied to a basis of V, but not to single elements.

Exercise 5.2. Let $\phi : V \to W$ be a linear map, and let $\{v_1, \ldots, v_n\}$ be a basis of V and $\{w_1, \ldots, w_m\}$ a basis of W. The matrix $A = (a_{ij})$ representing ϕ relative to these bases is given by $\phi(v_j) = \sum_{i=1}^m a_{ij} w_i$. Show that the transpose matrix A^T represents the dual map $\phi^\vee : W^\vee \to V^\vee$ relative to the dual bases $\{w_1^\vee, \ldots, w_m^\vee\}$ and $\{v_1^\vee, \ldots, v_n^\vee\}$. For this reason $\phi^\vee$ is sometimes called the transpose of ϕ.

6. Bilinear forms

A bilinear form on the $\mathbb{F}$-vector space V is a map $\omega : V \times V \to \mathbb{F}$ that is linear in each argument. In other words we have

$$\omega(av + v', w) = a\,\omega(v, w) + \omega(v', w) \quad \text{and} \quad \omega(v, bw + w') = b\,\omega(v, w) + \omega(v, w')$$

for all $v, v', w, w' \in V$ and $a, b \in \mathbb{F}$. The form ω is symmetric if $\omega(v, w) = \omega(w, v)$ for all $v, w \in V$. It is skew-symmetric if $\omega(v, w) = -\omega(w, v)$, and alternating if $\omega(v, v) = 0$ for all $v \in V$.

Example 6.1. (1) The standard symmetric bilinear form on $\mathbb{F}^n$ is the dot product, which is defined on column vectors x and y by $\omega(x, y) = x^T y = \sum_{i=1}^n x_i y_i$.
(2) The Lorentz metric on $\mathbb{R}^4$ is defined by $\omega(x, y) = x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4$. This form is symmetric but not positive definite.

(3) The cross product on $\mathbb{F}^2$ is defined by $\omega(x,y) = x_1y_2 - x_2y_1 = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$. This form is alternating.

Exercise 6.2. Any alternating bilinear form is also skew-symmetric. Is the converse implication true?

A bilinear form $\omega : V \times V \to \mathbb{F}$ defines an element in $\mathrm{Hom}(V, V^\vee)$ that we will also denote by ω. More precisely, we identify ω with the linear map $\omega : V \to V^\vee$ defined by $\omega(v)(w) = \omega(v,w)$. We will say that ω is non-degenerate if this linear map is injective. Equivalently, for each non-zero $v \in V$ there exists $w \in V$ such that $\omega(v,w) \neq 0$.

Exercise 6.3. The form $\omega : V \to V^\vee$ is symmetric if and only if $\omega = \omega^\vee \iota$, where $\iota : V \to V^{\vee\vee}$ is defined in Exercise 5.1. The form ω is skew-symmetric if and only if $\omega = -\omega^\vee \iota$.

Let $\omega : V \times V \to \mathbb{F}$ be a bilinear form. Relative to a basis $\{v_1, \dots, v_n\}$ of V, ω is represented by the $n \times n$ matrix $A = (a_{ij})$ defined by $a_{ij} = \omega(v_i, v_j)$.

Exercise 6.4. The form ω is symmetric if and only if $A = A^T$, skew-symmetric if and only if $A = -A^T$, and alternating if and only if $A = -A^T$ and all diagonal entries are zero. The form ω is non-degenerate if and only if A is invertible.

Exercise 6.5. The matrix representing a form $\omega : V \times V \to \mathbb{F}$ relative to a given basis of V is the transpose of the matrix representing the linear map $\omega : V \to V^\vee$ relative to the same basis and its dual basis of $V^\vee$.

Exercise 6.6. Let $B = \{v_1, \dots, v_n\}$ and $B' = \{v'_1, \dots, v'_n\}$ be two bases of an $\mathbb{F}$-vector space V, and let $P = (p_{ij})$ be the transition matrix from B to B', defined by $v_j = \sum_{i=1}^n p_{ij} v'_i$. If an endomorphism of V is represented by the matrix A relative to B and by A' relative to B', then $A = P^{-1} A' P$. If a bilinear form on V is represented by A relative to B and by A' relative to B', then $A = P^T A' P$.

Let $A, A' \in \mathrm{Mat}_n(\mathbb{F})$ be $n \times n$ matrices with entries in $\mathbb{F}$. We say that A and A' are similar if there exists an invertible matrix P such that $A = P^{-1} A' P$, and that A and A' are equivalent if there exists an invertible matrix P such that $A = P^T A' P$.

Exercise 6.7. Two matrices are similar if and only if they represent the same endomorphism $\phi : V \to V$ relative to two different bases of the vector space V. The matrices are equivalent if and only if they represent the same bilinear form $\omega : V \times V \to \mathbb{F}$ relative to two different bases.

Alternating bilinear forms are classified by the following theorem. It states that any alternating bilinear form can be represented by a block matrix of the form

$$\begin{bmatrix} 0 & I & 0 \\ -I & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} .$$

Theorem 6.8. *Let $\omega : V \times V \to \mathbb{F}$ be an alternating bilinear form on a finite dimensional vector space V. Then V has a basis $\{v_1, v_2, \dots, v_k, v'_1, v'_2, \dots, v'_k, w_1, \dots, w_m\}$ such that $\omega(v_i, v'_j) = \delta_{ij}$ and $\omega(v_i, v_j) = \omega(v'_i, v'_j) = \omega(u, w_l) = 0$ for all $1 \le i, j \le k$, $1 \le l \le m$, and $u \in V$.*

Proof. If $\omega = 0$, then the theorem is obvious. Otherwise choose $v, v' \in V$ such that $\omega(v, v') \neq 0$. By replacing v with $\omega(v, v')^{-1}v$, we may assume that $\omega(v, v') = 1$. Since ω is alternating we have $\omega(v, v) = \omega(v', v') = 0$, so v and v' are linearly independent. Let $W = \langle v, v' \rangle^{\perp} = \{w \in V \mid \omega(w, v) = \omega(w, v') = 0\}$. By induction on $\dim(V)$ there exists a basis of W of the form described in the theorem, and by adding v and v' to this basis we obtain the desired basis for V. □

Exercise 6.9. If a finite dimensional vector space V has an alternating nondegenerate bilinear form, then V has even dimension.

We next consider symmetric bilinear forms, which turn out to be most well behaved when the field $\mathbb{F}$ does not have characteristic 2. For the rest of this section we therefore assume that $\operatorname{char}(\mathbb{F}) \neq 2$.

Exercise 6.10 (Quadratic forms)**.** A set map $q : V \to \mathbb{F}$ is called a quadratic form if $q(\lambda v) = \lambda^2 q(v)$ for all $\lambda \in \mathbb{F}$ and $v \in V$, and if the function $\omega(v, w) = q(v + w) - q(v) - q(w)$ is a (symmetric) bilinear form on V. Show that there is a 1-1 correspondence between quadratic forms and symmetric bilinear forms on V.

The following classification states that every symmetric bilinear form can be represented by a diagonal matrix. However, the diagonal entries are in general not unique.

Theorem 6.11. *Let $\omega : V \times V \to \mathbb{F}$ be a symmetric bilinear form on a vector space V of finite dimension, and assume that $\operatorname{char}(\mathbb{F}) \neq 2$. Then there exists a basis $\{v_1, \dots, v_n\}$ of V and scalars $a_1, \dots, a_n \in \mathbb{F}$ such that $\omega(v_i, v_j) = a_i \delta_{ij}$ for all $1 \leq i, j \leq n$.*

Proof. If $\omega = 0$, then the theorem is obvious. Otherwise there exist $v, v' \in V$ such that $\omega(v, v') \neq 0$. Notice that if $\omega(v, v) = \omega(v', v') = 0$, then $\omega(v + v', v + v') = 2\omega(v, v') \neq 0$. We may therefore choose $v \in V$ such that $\omega(v, v) \neq 0$. The orthogonal complement $\langle v \rangle^{\perp} = \{w \in V \mid \omega(v, w) = 0\}$ has a basis of the form described in the theorem by induction on $\dim(V)$, and by adding the vector v we obtain the desired basis of V. □

The rank of a bilinear form $\omega : V \times V \to \mathbb{F}$ is the rank of the corresponding linear map $\omega : V \to V^{\vee}$. The following exercise states that, when $\mathbb{F}$ is algebraically closed, a bilinear form is determined by its rank up to isomorphism.

Exercise 6.12. Let $\omega : V \times V \to \mathbb{F}$ be a symmetric bilinear form on a vector space V of finite dimension, and assume that $\mathbb{F}$ is algebraically closed with $\operatorname{char}(\mathbb{F}) \neq 2$. Then V has a basis $\{v_1, \dots, v_n\}$ such that

$$\omega(v_i, v_j) = \begin{cases} 1 & \text{if } i = j \leq \operatorname{rank}(\omega); \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 6.13. Let V be as in Exercise 6.12 and let ω and ω' be symmetric bilinear forms on V of the same rank. Then there exists an isomorphism of vector spaces $\phi : V \xrightarrow{\cong} V$ such that $\omega'(v, w) = \omega(\phi(v), \phi(w))$ for all $v, w \in V$.

Exercise 6.14. Let $\omega : V \times V \to \mathbb{R}$ be a symmetric bilinear form on a real vector space V of finite dimension. Then there exists a basis $\{v_1, \dots, v_n\}$ and integers

$0 \leq k \leq l \leq n$ such that $\omega(v_i, v_j) = 0$ for $i \neq j$ and

$$\omega(v_i, v_i) = \begin{cases} 1 & \text{if } 1 \leq i \leq k, \\ -1 & \text{if } k < i \leq l, \text{ and} \\ 0 & \text{if } l < i \leq n. \end{cases}$$

A symmetric bilinear form $\omega : V \times V \to \mathbb{R}$ on a real vector space V is called positive definite if $\omega(v, v) > 0$ for all non-zero vectors $v \in V$. This implies that ω is non-degenerate.

Exercise 6.15. Show that the integers k and l of Exercise 6.14 depend only on the form ω and not on the chosen basis for V. In fact, if $V_+ \subset V$ is a subspace of maximal dimension such that ω restricts to a positive definite form on V_+, then $\dim(V_+) = k$. Similarly, $l - k = \dim(V_-)$ where $V_- \subset V$ is a maximal subspace such that ω restricts to a negative definite form on V_-.

The signature of the form ω from Exercise 6.14 is defined to be $k - (l - k)$, i.e. the number of basis vectors v_i with $\omega(v_i, v_i) > 0$ minus the number of basis vectors v_i with $\omega(v_i, v_i) < 0$. Exercise 6.14 and Exercise 6.15 show that a real symmetric bilinear form is determined up to isomorphism by its rank and signature.

Exercise 6.16. Determine whether the bilinear forms on $\mathbb{R}^3$ defined by $\omega(x, y) = 4x_1y_1 + x_2y_2 - x_3y_3$ and $\omega'(x, y) = x_1y_3 - x_2y_2 + x_3y_1$ are equivalent (represented by equivalent matrices).

7. Sesquilinear forms

Let V be a vector space over the complex numbers $\mathbb{C}$. A sesquilinear form on V is a map $\omega : V \times V \to \mathbb{C}$ that is antilinear in its first argument and linear in its second argument. More precisely we have

$$\omega(av + v', w) = \overline{a}\,\omega(v, w) + \omega(v', w) \quad \text{and} \quad \omega(v, bw + w') = b\,\omega(v, w) + \omega(v, w')$$

for $v, v', w, w' \in V$ and $a, b \in \mathbb{C}$, where $\overline{a}$ denotes the complex conjugate of a. The sesquilinear form ω is called Hermitian if $\omega(v, w) = \overline{\omega(w, v)}$ for all $v, w \in V$.

Given a basis $\{v_1, \dots, v_n\}$ of V, we can represent a sesquilinear form $\omega : V \times V \to \mathbb{C}$ by the matrix $A = (a_{ij})$, where $a_{ij} = \omega(v_i, v_j)$. The complex conjugate transpose of a complex matrix A is the matrix A^* obtained by replacing all entries in the transpose of A with their complex conjugates. The (i, j)-entry of A^* is equal to $\overline{a_{ji}}$. The matrix A is called Hermitian if $A^* = A$.

Exercise 7.1. A sesquilinear form $\omega : V \times V \to \mathbb{C}$ on a finite dimensional complex vector space is Hermitian if and only if it is represented by a Hermitian matrix.

Given any complex vector space V, we let $\overline{V}$ denote the complex conjugated vector space which is the same as V as an additive group, but with complex conjugated scalar multiplication. More precisely, set $\overline{V} = \{[v] \mid v \in V\}$ and define operations on this set by $[v] + [w] = [v + w]$ and $a[v] = [\overline{a}v]$, for $v, w \in V$ and $a \in \mathbb{C}$. For any $\mathbb{C}$-linear map $\phi : V \to W$ of complex vector spaces, we obtain a conjugate map $\overline{\phi} : \overline{V} \to \overline{W}$ by $\overline{\phi}([v]) = [\phi(v)]$. This map $\overline{\phi}$ is again a $\mathbb{C}$-linear map of complex vector spaces.

Exercise 7.2. A sesquilinear form $\omega : V \times V \to \mathbb{C}$ is the same as a $\mathbb{C}$-linear map $\omega : \overline{V} \to V^\vee$. The form ω is Hermitian if and only if $\overline{\omega} = \omega^\vee \iota$ in $\mathrm{Hom}_{\mathbb{C}}(V, \overline{V}^\vee)$.

The classification of Hermitian forms is exactly like that of symmetric bilinear real forms. In particular, a Hermitian bilinear form on a complex vector space of finite dimension is determined up to isomorphism by its rank and signature.

Exercise 7.3. Let $\omega : V \times V \to \mathbb{C}$ be a Hermitian form on a complex vector space V of finite dimension. Then there exists a basis $\{v_1, \dots, v_n\}$ and integers $0 \le k \le l \le n$ such that $\omega(v_i, v_j) = 0$ for $i \neq j$ and

$$\omega(v_i, v_i) = \begin{cases} 1 & \text{if } 1 \le i \le k, \\ -1 & \text{if } k < i \le l, \text{ and} \\ 0 & \text{if } l < i \le n. \end{cases}$$

The rank l and signature $2k - l$ of ω are independent of the chosen basis.

A Hermitian form $\omega : V \times V \to \mathbb{C}$ is called positive definite if $\omega(v, v) > 0$ for all non-zero vectors $v \in V$. In this case ω is also called an inner product on V. Given a fixed inner product ω we say that v is a unit vector if $\omega(v, v) = 1$, and v is perpendicular to w if $\omega(v, w) = 0$. An orthonormal basis of V is a basis consisting of unit vectors, such that any two distinct vectors from the basis are perpendicular. Similar terminology is used if ω is a positive definite symmetric bilinear form on a real vector space.

Exercise 7.4. Let $\omega : V \times V \to \mathbb{C}$ be a positive definite Hermitian form. Define $\omega_r : V \times V \to \mathbb{R}$ and $\omega_i : V \times V \to \mathbb{R}$ by $\omega(v, w) = \omega_r(v, w) + i\omega_i(v, w)$ for $v, w \in V$. Show that ω_r is a positive definite symmetric form on V considered as a real vector space, and that ω_i is a non-degenerate skew-symmetric real bilinear form.

8. Symmetric and Hermitian endomorphisms

Let V be a vector space over the field $\mathbb{F}$, and let $\phi : V \to V$ be an endomorphism. In this generality there is no natural definition of what it means for ϕ to be symmetric. However, if we are given a fixed basis $\{v_1, \dots, v_n\}$ of V and let $A = (a_{ij})$ be the matrix representing ϕ relative to this basis, then we might say that ϕ is symmetric relative to this basis if $A = A^T$ is a symmetric matrix. This is equivalent to the following definition if we use the form $\omega : V \times V \to \mathbb{F}$ defined by $\omega(v_i, v_j) = \delta_{ij}$.

Definition 8.1. The endomorphism $\phi \in \mathrm{End}(V)$ is symmetric relative to a bilinear form $\omega : V \times V \to \mathbb{F}$ if and only if we have $\omega(\phi(v), w) = \omega(v, \phi(w))$ for all $v, w \in V$.

We are mostly interested in endomorphisms that are symmetric relative to a non-degenerate symmetric form, but the definition makes sense in general.

Exercise 8.2. Let $A \in \mathrm{Mat}_n(\mathbb{F})$. The endomorphism on $\mathbb{F}^n$ given by multiplication by A is symmetric relative to the standard form on $\mathbb{F}^n$ if and only if $A = A^T$ is a symmetric matrix.

Exercise 8.3. Show by example that an endomorphism may be symmetric relative to one basis but non-symmetric relative to another.

Exercise 8.4. Consider the form ω as a linear map $\omega : V \to V^\vee$. Then $\phi \in \mathrm{End}(V)$ is symmetric relative to ω if and only if $\omega\phi = \phi^\vee\omega$ holds in $\mathrm{Hom}_{\mathbb{F}}(V, V^\vee)$.

Definition 8.5. Let V be a complex vector space and $\omega : V \times V \to \mathbb{C}$ a Hermitian form. An endomorphism $\phi \in \mathrm{End}(V)$ is called Hermitian relative to ω if we have $\omega(\phi(v), w) = \omega(v, \phi(w))$ for all $v, w \in V$.

Exercise 8.6. Let $V = \mathbb{C}^n$ and let $\omega : V \times V \to \mathbb{C}$ be the standard inner product defined by $\omega(v,w) = v^* w = \sum_i \overline{v_i} w_i$. Then an endomorphism $\phi : V \to V$ is Hermitian relative to ω if and only if it is represented by a Hermitian matrix relative to the standard basis of $\mathbb{C}^n$.

Theorem 8.7. *Let V be a complex vector space of finite dimension and let $\omega : V \times V \to \mathbb{C}$ be a positive definite Hermitian form. Assume that $\phi \in \mathrm{End}(V)$ is Hermitian relative to ω. Then V has an orthonormal basis consisting of eigenvectors of ϕ, and all eigenvalues of ϕ are real numbers.*

Proof. Since $\mathbb{C}$ is an algebraically closed field, we can find an eigenvalue $\lambda \in \mathbb{C}$ and a corresponding eigenvector $v \in V$ such that $\phi(v) = \lambda v$. By assumption $\omega(v,v)$ is a positive real number. Since $\lambda\omega(v,v) = \omega(v,\lambda v) = \omega(v,\phi(v)) = \omega(\phi(v),v) = \omega(\lambda v, v) = \overline{\lambda}\omega(v,v)$, it follows that $\lambda = \overline{\lambda}$ is a real number. By replacing v with $\omega(v,v)^{-1/2}v$, we may assume that v is a unit vector. Let $W = \{w \in V \mid \omega(v,w) = 0\}$ be the orthogonal complement of v. Since for each $w \in W$ we have $\omega(\phi(w),v) = \omega(w,\phi(v)) = \omega(w,\lambda v) = \lambda\omega(w,v) = 0$, we deduce that $\phi(W) \subset W$. Since the restricted endomorphism $\phi : W \to W$ is Hermitian relative to the restriction of ω to W, it follows by induction on $\dim(V)$ that W has an orthonormal basis consisting of eigenvectors of ϕ. The theorem follows because all vectors in this basis are perpendicular to v. □

A complex matrix $U \in \mathrm{Mat}_n(\mathbb{C})$ is called unitary if $U^*U = I$. Equivalently, the columns of U form an orthonormal basis of $\mathbb{C}^n$ with respect to the standard inner product.

Corollary 8.8. *Let $A \in \mathrm{Mat}_n(\mathbb{C})$ be a Hermitian matrix. Then there exists a unitary matrix U such that U^*AU is a diagonal matrix. In particular, A is diagonalizable. The eigenvalues of A are real numbers.*

Exercise 8.9. Let $A \in \mathrm{Mat}_n(\mathbb{R})$ be a symmetric real matrix. Then there exist an orthogonal matrix P such that P^TAP is a diagonal matrix.

Exercise 8.10. Let V be a real vector space of finite dimension and let $\omega : V \times V \to \mathbb{R}$ be a positive definite symmetric form. Assume that $\phi \in \mathrm{End}(V)$ is symmetric relative to ω. Then V has an orthonormal basis consisting of eigenvectors of ϕ.

Exercise 8.9 shows that all symmetric matrices with real entries are diagonalizable. However, this property does not generalize to symmetric matrices with entries in an arbitrary field.

Exercise 8.11. The complex matrix $A = \begin{bmatrix} i & 1 \\ 1 & -i \end{bmatrix}$ is symmetric but not diagonalizable.

Exercise 8.12. Let $\phi, \psi \in \mathrm{End}(V)$ be commuting endomorphisms of a finite dimensional complex vector space V, both of which are Hermitian relative to a positive definite Hermitian form ω on V. Then V has an orthonormal basis $\{v_1, \ldots, v_n\}$ such that each vector v_i is an eigenvector of both ϕ and ψ.

9. Normal endomorphisms

In this section we let V be a complex vector space of finite dimension, and we fix a positive definite Hermitian form $\omega : V \times V \to \mathbb{C}$. Then ω is non-degenerate in the sense that the corresponding $\mathbb{C}$-linear map $\omega : \overline{V} \to V^\vee$ is an isomorphism of vector spaces. In other words, for any $\alpha \in V^\vee$ there exists a unique vector $v \in V$ such that $\alpha(w) = \omega(v, w)$ for all $w \in V$.

Given any endomorphism $\phi \in \mathrm{End}(V)$ and a vector $v \in V$, we obtain an element $\alpha \in V^\vee$ by setting $\alpha(w) = \omega(v, \phi(w))$. Let $\phi^*(v) \in V$ denote the unique vector corresponding to α, that is $\phi^*(v)$ satisfies

$$\omega(\phi^*(v), w) = \omega(v, \phi(w))$$

for all w. This defines a $\mathbb{C}$-linear endomorphism $\phi^* : V \to V$ called the Hermitian transpose of ϕ relative to ω.

Exercise 9.1. Check that $\phi^* \in \mathrm{End}_{\mathbb{C}}(V)$. For $a \in \mathbb{C}$ we have $(a\phi)^* = \overline{a}\,\phi^*$.

Exercise 9.2. We have $\phi = \phi^*$ if and only if ϕ is Hermitian relative to ω.

Definition 9.3. An endomorphism $\phi \in \mathrm{End}(V)$ is called normal relative to ω if we have $\phi^*\phi = \phi\,\phi^*$.

Exercise 9.4. Let $\phi \in \mathrm{End}(V)$ be represented by $A \in \mathrm{Mat}_n(\mathbb{C})$ relative to an orthonormal basis of V. Then ϕ^* is represented by A^*, and ϕ is normal if and only if $A^*A = AA^*$.

The matrix $A \in \mathrm{Mat}_n(\mathbb{C})$ is called normal if $A^*A = AA^*$. Examples of normal matrices include Hermitian matrices ($A^* = A$), unitary matrices ($A^*A = I$), real symmetric matrices ($A^T = A^* = A$), real orthogonal matrices ($A^TA = A^*A = I$), and real skew-symmetric matrices ($A^T = A^* = -A$). The following theorem says that a complex matrix A is normal if and only if it is diagonalizable by a unitary matrix, i.e. there exists a unitary matrix U such that U^*AU is a diagonal matrix.

Theorem 9.5. *An endomorphism $\phi \in \mathrm{End}(V)$ is normal relative to ω if and only if V has an orthonormal basis consisting of eigenvectors of ϕ.*

Proof. Assume first that $\{v_1, \dots, v_n\}$ is an orthonormal basis of V consisting of eigenvectors of ϕ, and choose $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ such that $\phi(v_i) = \lambda_i v_i$ for each i. Since we have $\omega(\phi^*(v_i), v_j) = \omega(v_i, \phi(v_j)) = \delta_{ij}\lambda_j = \omega(\overline{\lambda_i} v_i, v_j)$ for all $1 \le i, j \le n$, it follows that $\phi^*(v_i) = \overline{\lambda_i}\, v_i$. This implies that $\phi(\phi^*(v_i)) = |\lambda_i|^2 v_i = \phi^*(\phi(v_i))$, so ϕ is normal.

Assume next that $\phi^*\phi = \phi\,\phi^*$. Set $\phi_1 = \frac{1}{2}(\phi + \phi^*)$ and $\phi_2 = \frac{1}{2i}(\phi - \phi^*)$. Then we have $\phi = \phi_1 + i\phi_2$, $\phi_1^* = \phi_1$, $\phi_2^* = \phi_2$, and $\phi_1\phi_2 = \phi_2\phi_1$. Since ϕ_1 and ϕ_2 are commuting Hermitian endomorphisms, it follows from Exercise 8.12 that there exists an orthonormal basis $\{v_1, \dots, v_n\}$ of V such that each v_i is an eigenvector of both ϕ_1 and ϕ_2. Write $\phi_1(v_i) = \mu_i v_i$ and $\phi_2(v_i) = \mu_i' v_i$ for each i. Then $\phi(v_i) = (\mu_i + i\mu_i')v_i$, so v_i is an eigenvector of ϕ, as required. □

Exercise 9.6. A complex $n \times n$ matrix is Hermitian if and only if it is normal and has real eigenvalues.

10. Direct sums and direct products of vector spaces

Suppose we are given an $\mathbb{F}$-vector space V_i for each element i in some set I. Let $\mathcal{V}$ be the disjoint union of all these vector spaces. Then the direct product $\prod_i V_i$ can be defined as the set of all functions $f : I \to \mathcal{V}$ for which $f(i) \in V_i$ for each i, and the direct sum $\bigoplus_i V_i$ is the set of functions $f \in \prod_i V_i$ for which $f(i) = 0$ for all but finitely many elements $i \in V$. If the index set I is finite, then

$\bigoplus_i V_i = \prod_i V_i$. For each $j \in I$ we have a natural projection $\rho_j : \prod_i V_i \to V_j$ defined by $\rho_j(f) = f(j)$, and we have a natural inclusion $\iota_j : V_j \to \bigoplus_i V_i$ given by $\iota_j(v_j)(j) = v_j$ and $\iota_j(v_j)(i) = 0$ for $i \neq j$.

More abstractly, direct products and direct sums can be defined as follows. Let P be any $\mathbb{F}$-vector space, and suppose we are given a linear map $\rho_i : P \to V_i$ for each $i \in I$. Then $(P, \{\rho_i\})$ is called a direct product of the family $\{V_i\}_{i\in I}$ if the following universal property is satisfied: If W is any $\mathbb{F}$-vector space and $h_i : W \to V_i$ is a linear map for each $i \in I$, then there exists a unique linear map $h : W \to P$ such that $h_i = \rho_i h$ for each $i \in I$.

Similarly, let S be any $\mathbb{F}$-vector space, and suppose we are given a linear map $\iota_i : V_i \to S$ for each $i \in I$. Then $(S, \{\iota_i\})$ is called a direct sum of $\{V_i\}_{i\in I}$ if the following universal property is satisfied: If W is any $\mathbb{F}$-vector space and $q_i : V_i \to W$ is a linear map for each $i \in I$, then there exists a unique linear map $q : S \to W$ such that $q_i = q\iota_i$ for each $i \in I$.

Exercise 10.1. Prove that $(\prod_i V_i, \{\rho_i\})$ is a direct product of the family of vector spaces $\{V_i\}_{i\in I}$ and $(\bigoplus_i V_i, \{\iota_i\})$ is a direct sum.

Exercise 10.2. Let P and P' be two direct products of the family $\{V_i\}_{i\in I}$, with projections $\rho_i : P \to V_i$ and $\rho'_i : P' \to V_i$. Then there is a unique isomorphism $\phi : P \xrightarrow{\cong} P'$ such that $\rho_i = \rho'_i \phi$ for each $i \in I$. Prove a similar statement saying that direct sums are unique up to unique isomorphism.

Exercise 10.3. Let V be a vector space and let $W_1, \dots, W_k$ be subspaces of V such that $W_1 + \cdots + W_k = V$. Assume that $W_1 \cap W_2 = 0$, $(W_1 + W_2) \cap W_3 = 0$, $\dots$, $(W_1 + \cdots + W_{k-1}) \cap W_k = 0$. Then V is isomorphic to $W_1 \oplus \cdots \oplus W_k$.

11. Tensor products

Assume first that V and W finite dimensional $\mathbb{F}$-vector spaces. In this case we can define the tensor product of V and W over $\mathbb{F}$ to be $V \otimes W = V \otimes_{\mathbb{F}} W = \mathrm{Hom}(V^\vee, W)$. For $v \in V$ and $w \in W$, define $v \otimes w \in V \otimes W$ by $(v \otimes w)(\alpha) = \alpha(v)w$.

Exercise 11.1. The map $V \times W \to V \otimes W$ given by $(v, w) \mapsto v \otimes w$ is $\mathbb{F}$-bilinear, that is, linear in each argument.

Exercise 11.2. If $\{v_1, \dots, v_n\}$ is a basis of V and $\{w_1, \dots, w_m\}$ is a basis of W, then $\{v_i \otimes w_j\}$ is a basis of $V \otimes W$.

More abstractly, a tensor product of V and W is defined as an $\mathbb{F}$-vector space T together with a bilinear map $\mu : V \times W \to T$ such that the following universal property holds: If M is any $\mathbb{F}$-vector space and $\nu : V \times W \to M$ is any bilinear map, then there exists a unique linear map $\phi : T \to M$ such that $\nu = \phi\mu$. If (T, μ) is a tensor product of V and W, then we write $v \otimes w = \mu(v, w)$ for $v \in V$ and $w \in W$. (This is the correct definition of the tensor product when the vector spaces are allowed to have infinite dimension, and it also applies to modules over a commutative ring.)

Exercise 11.3. Prove that $V \otimes W = \mathrm{Hom}(V^\vee, W)$ satisfies this universal property when V has finite dimension.

Exercise 11.4. If T and T' are both tensor products of V and W, with associated bilinear maps $\mu : V \times W \to T$ and $\mu' : V \times W \to T'$, then there exists a unique isomorphism $\phi : T \to T'$ such that $\mu' = \phi\mu$.

If S is any set, then let $\mathbb{F}(S)$ denote the $\mathbb{F}$-vector space with basis S. It consists of finite formal linear combinations of the elements in S. The tensor product of V and W can be constructed as follows. Let $\mathbb{F}(V \times W)$ be the (huge!) vector space with basis $\{[v, w] \mid v \in V \text{ and } w \in W\}$, and let $N \subset \mathbb{F}(V \times W)$ be the vector subspace spanned by all elements of the form

$$\begin{aligned} &[av, w] - a[v, w] && [v + v', w] - [v, w] - [v', w] \\ &[v, aw] - a[v, w] && [v, w + w'] - [v, w] - [v, w'] \end{aligned}$$

where $v, v' \in V$, $w, w' \in W$, and $a \in \mathbb{F}$. Then define $V \otimes W = \mathbb{F}(V \times W)/N$. Notice that the map $V \times W \to V \otimes W$ given by $(v, w) \mapsto [v, w] + N$ is bilinear.

Exercise 11.5. Prove that $V \otimes W = \mathbb{F}(V \times W)/N$ satisfies the universal property.

Exercise 11.6. Compute the dimensions of $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ and $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ as vector spaces over $\mathbb{R}$. Are these $\mathbb{R}$-vector spaces isomorphic?

Exercise 11.7 (Associativity)**.** Prove that $(V_1 \otimes V_2) \otimes V_3$ is canonically isomorphic to $V_1 \otimes (V_2 \otimes V_3)$. These tensor products satisfy the same universal property.

Exercise 11.8 (Commutativity)**.** $V \otimes W$ is canonically isomorphic to $W \otimes V$.

Exercise 11.9. Given linear maps $\phi : V \to V'$ and $\psi : W \to W'$, there is a unique linear map $\phi \otimes \psi : V \otimes W \to V' \otimes W'$ defined by $(\phi \otimes \psi)(v \otimes w) = \phi(v) \otimes \psi(w)$.

Exercise 11.10. Assume that $\phi : V \to V'$ is represented by the matrix A relative to given bases of V and V', and that $\psi : W \to W'$ is represented by the matrix B relative to given bases of W and W'. Then find the matrix representing $\phi \otimes \psi$ relative to the bases of $V \otimes W$ and $V' \otimes W'$ defined in Exercise 11.2.

Exercise 11.11. Let V be a vector space over $\mathbb{F}$ and let $v_1, v_2 \in V$. Show that $v_1 \otimes v_2 = v_2 \otimes v_1$ if and only if $\dim\langle v_1, v_2 \rangle \leq 1$.

Exercise 11.12. $\mathrm{Hom}(U \otimes V, W)$ is canonically isomorphic to $\mathrm{Hom}(U, \mathrm{Hom}(V, W))$.

12. Graded algebras

An $\mathbb{F}$-algebra (with unit) is a ring A together with a ring homomorphism $\mathbb{F} \to A$ such that $1 \in \mathbb{F}$ maps to the multiplicative unit in A, and the image of $\mathbb{F}$ lies in the center of A. When $\mathbb{F}$ is a field, we can identify $\mathbb{F}$ with a subring of A.

A grading of the $\mathbb{F}$-algebra by positive integers is a direct sum decomposition $A = \bigoplus_{n \geq 0} A_n$ as an $\mathbb{F}$-vector space, such that $A_n A_m \subset A_{n+m}$. In this case the elements of A_n are called homogeneous of degree n.

Let A be a graded $\mathbb{F}$-algebra and let $I \subset A$ be a 2-sided ideal. If we set $I_n = I \cap A_n$ for each n, then $\bigoplus_{n \geq 0} I_n \subset I$. We say that I is homogeneous if $I = \bigoplus_{n \geq 0} I_n$.

Example 12.1. The polynomial ring $S = \mathbb{F}[x_1, \ldots, x_k]$ is a (commutative) graded $\mathbb{F}$-algebra, $S = \bigoplus_{n \geq 0} S_n$, where $S_n \subset S$ is the vector subspace of homogeneous polynomials of total degree n. An ideal $I \subset S$ is homogeneous if and only if it is generated by homogeneous polynomials.

Exercise 12.2. The unit $1 \in A$ is homogeneous of degree 0.

Exercise 12.3. Any element $a \in A$ can be written as a sum of homogeneous elements $a = \sum a_n$, with $a_n \in A_n$. The ideal I is homogeneous if and only if $a \in I$ implies $a_n \in I_n$ for each n.

Exercise 12.4. If $I \subset A$ is any 2-sided ideal generated by homogeneous elements, then I is homogeneous.

Exercise 12.5. If $I \subset A$ is a homogeneous ideal, then A/I is again a graded algebra. We have $A/I = \bigoplus_{n\geq 0}(A/I)_n$ where $(A/I)_n = A_n/I_n$.

13. Tensor algebras

Let V be a vector space over $\mathbb{F}$. Define the n-th tensor power of V to be

$$T^n V \;=\; V^{\otimes n} \;=\; V \otimes V \otimes \cdots \otimes V \quad (n \text{ copies.})$$

The tensor algebra of V is the graded $\mathbb{F}$-algebra defined by

$$T(V) \;=\; \bigoplus_{n\geq 0} T^n V \;=\; \mathbb{F} \oplus V \oplus T^2 V \oplus T^3 V \oplus \cdots$$

Multiplication of homogeneous elements in $T(V)$ is defined by the bilinear maps

$$T^n V \times T^m V \;\to\; T^n V \otimes T^m V = T^{n+m} V\,.$$

Let $I_S \subset T(V)$ be the homogeneous ideal generated by all tensors of the form $v \otimes w - w \otimes v \in T^2 V$, with $v, w \in V$. The symmetric algebra of V is defined by $S(V) = T(V)/I_S$. In fact, $S(V)$ is a commutative graded $\mathbb{F}$-algebra, $S(V) = \bigoplus_{n\geq 0} S^n V$, where we set $S^n V = T^n V/(I_S)_n$. The vector space $S^n V$ is called the n-th symmetric power of V. Given $v_1, \dots, v_n \in V$, we let $v_1 \cdot v_2 \cdot \ldots \cdot v_n \in S^n V$ denote the image of $v_1 \otimes v_2 \otimes \cdots \otimes v_n \in T^n V$ under the map $T^n V \to S^n V$.

Let $I_\wedge \subset T(V)$ be the homogeneous ideal generated by all tensors of the form $v \otimes v \in T^2 V$, with $v \in V$. The exterior algebra of V is defined by $\bigwedge V = T(V)/I_\wedge$. This is a graded $\mathbb{F}$-algebra, $\bigwedge V = \bigoplus_{n\geq 0} \bigwedge^n V$, where we set $\bigwedge^n V = T^n V/(I_\wedge)_n$. The vector space $\bigwedge^n V$ is called the n-th exterior power of V. Given $v_1, v_2, \dots, v_n \in V$, we let $v_1 \wedge v_2 \wedge \cdots \wedge v_n \in \bigwedge^n V$ denote the image of $v_1 \otimes v_2 \otimes \cdots \otimes v_n \in T^n V$ under the map $T^n V \to \bigwedge^n V$.

Exercise 13.1. Formulate and prove universal properties of the maps $V^{\times n} \to T^n V$, $V^{\times n} \to S^n V$, and $V^{\times n} \to \bigwedge^n V$, where $V^{\times n} = V \times V \times \cdots \times V$ (n copies).

Exercise 13.2. Assume that $\{v_1, v_2, \dots, v_m\}$ is a basis of V. Then the tensor power $T^n V$ has basis $\{v_{i_1} \otimes v_{i_2} \otimes \cdots \otimes v_{i_n} \mid i_1, \dots, i_n \in [1, m]\}$, the symmetric power $S^n V$ has basis $\{v_{i_1} \cdot v_{i_2} \cdot \ldots \cdot v_{i_n} \mid 1 \leq i_1 \leq i_2 \leq \cdots \leq i_n \leq m\}$, and the alternating power $\bigwedge^n V$ has basis $\{v_{i_1} \wedge v_{i_2} \wedge \cdots \wedge v_{i_n} \mid 1 \leq i_1 < i_2 < \cdots < i_n \leq m\}$. Find the dimensions of $T^n V$, $S^n V$, $\bigwedge^n V$, and $\bigwedge V$.

Exercise 13.3. Find the $\mathbb{F}$-algebras $T(V)$, $S(V)$, and $\bigwedge(V)$ when $\dim(V) = 1$.

Exercise 13.4. If $\dim(V) = m$, then $S(V) \cong \mathbb{F}[x_1, \dots, x_m]$.

The symmetric group S_n acts on $T^n V$ by

$$\sigma.(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \ldots v_{\sigma^{-1}(n)}\,.$$

We say that $z \in T^n V$ is a symmetric tensor if $\sigma.z = z$ for all $\sigma \in S_n$, and that z is a skew-symmetric tensor if $\sigma.z = (-1)^\sigma z$ for all $\sigma \in S_n$. Here $(-1)^\sigma$ denotes the sign of the permutation σ. If $\operatorname{char}(\mathbb{F})$ does not divide $n!$ and $z \in T^n V$, we define

$$\begin{aligned} \operatorname{Sym}(z) &= \frac{1}{n!} \sum_{\sigma \in S_n} \sigma . z \\ \operatorname{Alt}(z) &= \frac{1}{n!} \sum_{\sigma \in S_n} (-1)^\sigma \sigma . z \,. \end{aligned}$$

Exercise 13.5. If $\operatorname{char}(\mathbb{F})$ does not divide $n!$, then Sym induces an isomorphism of $S^n V$ with the subspace of symmetric tensors in $T^n V$, and Alt induces an isomorphism of $\bigwedge^n V$ with the subspace of skew-symmetric tensors in $T^n V$.

Given a linear map $\phi : V \to W$ of vector spaces, we obtain induced linear maps $T^n(\phi) = \phi^{\otimes n} : T^n V \to T^n W$, $S^n(\phi) : S^n V \to S^n W$, and $\bigwedge^n(\phi) : \bigwedge^n V \to \bigwedge^n W$ defined by

$$\begin{aligned} T^n(\phi)(v_1 \otimes v_2 \otimes \cdots \otimes v_n) &= \phi(v_1) \otimes \phi(v_1) \otimes \cdots \otimes \phi(v_n) \,, \\ S^n(\phi)(v_1 \cdot v_2 \cdot \ldots \cdot v_n) &= \phi(v_1) \cdot \phi(v_1) \cdot \ldots \cdot \phi(v_n) \,, \text{ and} \\ \textstyle\bigwedge^n(\phi)(v_1 \wedge v_2 \wedge \cdots \wedge v_n) &= \phi(v_1) \wedge \phi(v_1) \wedge \cdots \wedge \phi(v_n) \,. \end{aligned}$$

Exercise 13.6. Use the universal properties from Exercise 13.1 to prove that these maps are well defined.

Exercise 13.7. Let $\phi \in \operatorname{End}(V)$ and set $n = \dim(V)$. Then $\dim \bigwedge^n V = 1$, and $\wedge^n \phi : \bigwedge^n V \to \bigwedge^n V$ is multiplication with the scalar $\det(\phi) \in \mathbb{F}$. This gives a coordinate-free definition of the determinant of ϕ.

Let $\mathbb{F} \subset \mathbb{K}$ be a field extension. If V is any $\mathbb{F}$-vector space, we obtain a $\mathbb{K}$-vector space as the tensor product $V_{\mathbb{K}} = V \otimes_{\mathbb{F}} \mathbb{K}$. Scalar multiplication with $a \in \mathbb{K}$ is given by the linear map $1_V \otimes a : V \otimes_{\mathbb{F}} \mathbb{K} \to V \otimes_{\mathbb{F}} \mathbb{K}$. If $\phi : V \to W$ is any $\mathbb{F}$-linear map of $\mathbb{F}$-vector spaces, then $\phi \otimes 1 : V_{\mathbb{K}} \to W_{\mathbb{K}}$ is a $\mathbb{K}$-linear map.

Exercise 13.8. Let $\{v_1, \ldots, v_n\}$ be a basis of the $\mathbb{F}$-vector space V. Then the set $\{v_1 \otimes 1, \ldots, v_n \otimes 1\}$ is a basis of the $\mathbb{K}$-vector space $V_{\mathbb{K}}$.

Exercise 13.9. Let $\phi : V \to W$ be a linear map of $\mathbb{F}$-vector spaces, and let $A \in \operatorname{Mat}(m \times n, \mathbb{F})$ be the matrix representing ϕ relative to given bases of V and W. Show that A also represents the $\mathbb{K}$-linear map $\phi \otimes 1 : V_{\mathbb{K}} \to W_{\mathbb{K}}$ relative to the bases of $V_{\mathbb{K}}$ and $W_{\mathbb{K}}$ defined in Exercise 13.8.

Let $\mathbb{F}(x)$ denote the field of rational functions in one variable over $\mathbb{F}$, that is, the field of fractions of the polynomial ring $\mathbb{F}[x]$.

Exercise 13.10. Let V be a finite dimensional $\mathbb{F}$-vector space, let $\phi \in \operatorname{End}_{\mathbb{F}}(V)$, and set $V_{\mathbb{F}(x)} = V \otimes_{\mathbb{F}} \mathbb{F}(x)$. Then the characteristic polynomial $\chi_\phi(x) \in \mathbb{F}[x]$ is the determinant of the endomorphism $x\, 1_{V_{\mathbb{K}(x)}} - \phi \otimes 1 \in \operatorname{End}_{\mathbb{F}(x)}(V_{\mathbb{F}(x)})$.

Exercise 13.11. Let V be an $\mathbb{F}$-vector space of dimension n and let $\phi \in \operatorname{End}(V)$. Define the trace $\operatorname{Tr}(\phi)$ to be (-1) times the coefficient of x^{n-1} in the characteristic polynomial $\chi_\phi(x)$. Show that if $A \in \operatorname{Mat}_n(\mathbb{F})$ is the matrix representing ϕ relative to any basis of V, then $\operatorname{Tr}(\phi)$ is the sum of the diagonal entries of A.

14. Representations

Let G be a group and let $\mathbb{F}$ be a field. A representation of G on an $\mathbb{F}$-vector space V is an action $G \times V \to V$ such that, for each $g \in G$ the map $\rho(g) : V \to V$ defined by $\rho(g)(v) = g.v$ is a linear endomorphism of V. Let $\mathrm{GL}(V) = \mathrm{GL}_{\mathbb{F}}(V) \subset \mathrm{End}_{\mathbb{F}}(V)$ denote the group of invertible endomorphisms of V.

Exercise 14.1. A representation of G on V is the same as a group homomorphism $\rho : G \to \mathrm{GL}(V)$.

The group algebra of G over $\mathbb{F}$ is defined as follows. Let $\mathbb{F}[G]$ be the vector space with basis G. The elements are functions $f : G \to \mathbb{F}$ with finite support, i.e. $f(g)$ is non-zero for only finitely many elements $g \in G$. Given $f, h \in \mathbb{F}[G]$, define a product $f \cdot h \in \mathbb{F}[G]$ by

$$(f \cdot h)(g) = \sum_{x \in G} f(x) h(x^{-1} g) = \sum_{xy = g} f(x) h(y) \,.$$

We can identify each element $g \in G$ with the function $G \to \mathbb{F}$ that sends g to 1 and sends all other elements of G to zero. With this convention we have $f = \sum_{g \in G} f(g) g$ for any $f \in \mathbb{F}[G]$, and for $g_1, g_2 \in G$ we have $g_1 \cdot g_2 = g_1 g_2$ as elements of $\mathbb{F}[G]$.

Exercise 14.2. A representation of G over $\mathbb{F}$ is the same as a left module of the group algebra $\mathbb{F}[G]$.

Let V be a representation of G over $\mathbb{F}$. Then V is called irreducible if it is non-zero and does not contain any non-trivial proper subrepresentations. Equivalently, V is a simple $\mathbb{F}[G]$-module. The representation V is called completely reducible if it is isomorphic to a direct sum of irreducible representations. Equivalently, V is a semisimple $\mathbb{F}[G]$-module. Finally, V is called decomposable if V is isomorphic to a direct sum $V_1 \oplus V_2$ of non-zero representations. Otherwise V is called indecomposable. Any irreducible representation is also indecomposable.

Exercise 14.3. Find a representation of the additive group $(\mathbb{Z}, +)$ that is indecomposable but not irreducible.

Exercise 14.4. Let V be a finite dimensional vector space over an algebraically closed field $\mathbb{F}$, and let $\phi \in \mathrm{End}_{\mathbb{F}}(V)$. Use the ring homomorphism $\mathbb{F}[x] \to \mathrm{End}(V)$ given by $x \mapsto \phi$ to consider V as a module over $\mathbb{F}[x]$. Then V is an indecomposable $\mathbb{F}[x]$-module if and only if ϕ has an indecomposable Jordan basis.

Theorem 14.5 (Maschke)**.** *Let G be a finite group and let V be a representation of G of finite dimension over $\mathbb{F}$. Assume that $\mathrm{char}(\mathbb{F})$ does not divide $|G|$. Then V is completely reducible.*

Let $\rho : G \to \mathrm{GL}_{\mathbb{F}}(V)$ be a representation of G on a finite dimensional vector space V. The character of this representation is the map $\chi_\rho : G \to \mathbb{F}$ defined by $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$, where $\mathrm{Tr}(\rho(g))$ is the trace of $\rho(g) \in \mathrm{End}_{\mathbb{F}}(V)$.

Theorem 14.6. *Let G be a finite group and let V and V' be finite dimensional representations of G over $\mathbb{C}$. Then V and V' are isomorphic as representations if and only if they have equal characters.*

Exercise 14.7. Consider the group algebra $\mathbb{C}[S_2]$ as a representation of the symmetric group S_2. Write this representation as a direct sum of irreducible representations of S_2, and find the characters of the irreducible summands.

Exercise 14.8. Repeat Exercise 14.7 for the symmetric group S_3.

15. Matrix groups

Let V be an $\mathbb{F}$-vector space and let $\omega : V \times V \to \mathbb{F}$ be a bilinear form. Then we can define a symmetry group of ω by

$$\mathrm{GL}_\omega(V) = \{\phi \in \mathrm{GL}(V) \mid \omega(\phi(v), \phi(w)) = \omega(v, w) \text{ for all } v, w \in V\}.$$

Here we could also replace $\mathrm{GL}(V)$ with the subgroup $\mathrm{SL}(V)$ of invertible endomorphisms of determinant 1. The following groups of matrices are variations over this theme.

$\mathrm{GL}(n, \mathbb{F}) = \{A \in \mathrm{Mat}_n(\mathbb{F}) \mid A \text{ is invertible}\}$: General linear group over $\mathbb{F}$.
$\mathrm{SL}(n, \mathbb{F}) = \{A \in \mathrm{GL}(n, \mathbb{F}) \mid \det(A) = 1\}$: Special linear group over $\mathbb{F}$.
$\mathrm{SO}(n, \mathbb{F}) = \{A \in \mathrm{SL}(n, \mathbb{F}) \mid A^T A = I\}$: Special orthogonal group over $\mathbb{F}$.
$\mathrm{Sp}(2n, \mathbb{F}) = \{A \in \mathrm{GL}(2n, \mathbb{F}) \mid A^T J A = J\}$: Symplectic group over $\mathbb{F}$.
Here we set $J = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$. One can show that $\mathrm{Sp}(2n, \mathbb{F}) \subset \mathrm{SL}(2n, \mathbb{F})$.

Exercise 15.1. $\mathrm{Sp}(2, \mathbb{F}) = \mathrm{SL}(2, \mathbb{F})$.

When the field $\mathbb{F}$ is the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$, the above matrix groups are Lie groups. A Lie group is a group G that is simultaneously a differentiable manifold, such that the product map $G \times G \to G$ and the inverse element map $G \to G$ are C^∞-functions. When studying representations of a Lie group G, one usually restricts to representations $\rho : G \to \mathrm{GL}(V)$, where V is a finite dimensional vector space over $\mathbb{R}$ or $\mathbb{C}$, and ρ is a C^∞ map of manifolds.

Similarly, when $\mathbb{F}$ is an algebraically closed field, then the matrix groups over $\mathbb{F}$ are linear algebraic groups, i.e. they are both groups and algebraic varieties. When studying representations of such a group G, one usually restricts to representations on a finite dimensional $\mathbb{F}$-vector space V, such that $\rho : G \to \mathrm{GL}(V)$ is a morphism of varieties, i.e. the $\dim(V)^2$ coordinate functions of the map $G \to \mathrm{GL}(V) \to \mathrm{End}(V)$ are rational functions in the coordinate functions on G.

Every Lie group contains a maximal compact subgroup which is unique up to conjugation. The most important compact Lie groups are:
$\mathrm{O}(n) = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid A^T A = I\}$: Orthogonal group.
$\mathrm{SO}(n) = \mathrm{O}(n) \cap \mathrm{SL}(n, \mathbb{R})$: Special orthogonal group.
$\mathrm{U}(n) = \{A \in \mathrm{GL}(n, \mathbb{C}) \mid A^* A = I\}$: Unitary group.
$\mathrm{SU}(n) = \mathrm{U}(n) \cap \mathrm{SL}(n, \mathbb{C})$: Special unitary group.
$\mathrm{Sp}(n) = \mathrm{U}(2n) \cap \mathrm{Sp}(2n, \mathbb{C})$: Symplectic group.

Exercise 15.2. The group $\mathrm{SO}(n)$ has index 2 in $\mathrm{O}(n)$.

Exercise 15.3. There is a short exact sequence $1 \to \mathrm{SU}(n) \to U(n) \to U(1) \to 1$.

Notice that $U(1)$ is the unit circle in the complex plane. A compact Lie group is called a torus if it is isomorphic to $U(1)^n = U(1) \times \cdots \times U(1)$ for some n. Every compact Lie group contains a maximal torus T that is unique up to conjugation. Maximal tori of the compact Lie groups of matrices listed above can be obtained as their subgroups of diagonal matrices.

Similarly, an algebraic group over the algebraically closed field $\mathbb{F}$ is called an (algebraic) torus if it is isomorphic to $(\mathbb{F}^\times)^n$ for some n, where $\mathbb{F}^\times$ is the multiplicative group of units in $\mathbb{F}$. For example, $\mathbb{C}^\times$ is the complement of the origin in the complex plane, which is homotopy equivalent to the unit circle $U(1)$. Every linear algebraic group G contains a maximal torus T and a Borel subgroup B such that $T \subset B \subset G$, again unique up to conjugation. A Borel subgroup means a maximal Zariski-closed connected solvable subgroup. If G is any of the matrix groups $\mathrm{GL}(n, \mathbb{F})$, $\mathrm{SL}(n, \mathbb{F})$, $\mathrm{SO}(n, \mathbb{F})$, or $\mathrm{Sp}(2n, \mathbb{F})$, then the subgroup of diagonal matrices in G is a maximal torus, and the subgroup of upper triangular matrices is a Borel subgroup.

If a group G acts on a set X, then the orbit of an element $x \in X$ is the subset $G.x = \{g.x \mid g \in G\}$, and the stabilizer of x is the subgroup $G_x = \{g \in G \mid g.x = x\}$. If $S \subset G$ is any subset, we write $g.S = \{g.x \mid x \in S\}$ for any element $g \in G$. This defines an action of G on the power set $\mathcal{P}(X)$ of all subsets of X. The stabilizer of S is $G_S = \{g \in G \mid g.S = S\}$. The pointwise stabilizer of S is the subgroup $\bigcap_{x \in S} G_x = \{g \in G \mid g.x = x \ \forall x \in S\}$.

Exercise 15.4. The group $G = \mathrm{GL}(2, \mathbb{C})$ acts on $\mathbb{C}^2$ by matrix multiplication.
(1) Determine the number of orbits for this action, and describe each orbit.
(2) Find the stabilizer and the pointwise stabilizer of $S = \{(x, y) \in \mathbb{C}^2 \mid x = y\}$.
(3) Show that the stabilizer of S is a Borel subgroup of G.

Exercise 15.5. The group $\mathrm{GL}(2, \mathbb{R})$ acts on the vector space of 2×2 symmetric real matrices by $A.S = ASA^T$ for $A \in \mathrm{GL}(2, \mathbb{R})$ and $S \in \mathrm{Mat}_2(\mathbb{R})$ symmetric.
(1) Show that each orbit under this action has a representative which is a diagonal matrix with entries being -1, 0, or 1.
(2) Find a representative for each orbit under this action.

Exercise 15.6. Let S be the set of all 2-dimensional subspaces of $\mathbb{R}^4$. Then $\mathrm{GL}(4, \mathbb{R})$ acts naturally on S. Fix $W \in S$ and let $H = \{g \in \mathrm{GL}(4, \mathbb{R}) \mid g(W) = W\}$ be the stabilizer of W. Show that the action of H on S has exactly three orbits.

References

[1] J. Brundan and A. Kleshchev, *A graduate course in algebra*, book in preparation, 2017.
[2] N. Jacobson, *Basic algebra. I*, second ed., W. H. Freeman and Company, New York, 1985. MR 780184
[3] ———, *Basic algebra. II*, second ed., W. H. Freeman and Company, New York, 1989. MR 1009787
[4] M. Wildon, *A short proof of the existence of Jordan normal form*, notes, 2007.