2.1 Commuting Families

A commuting family is a space
where part of the family waits
until the rest of the family brings back the car.

Morally speaking, matrices should not commute. Setting aside moral problems, commuting matrices do occur in many natural settings, as we shall for instance see in Chap. 4. So, let us not wait for them to show up, but let us get into the driver's seat and start studying them. Given n pairwise commuting endomorphisms $\varphi_1, \dots, \varphi_n$ of a finite dimensional vector space V over a field K, we can form the *commuting family* $\mathscr{F} = K[\varphi_1, \dots \varphi_n]$, where a constant $a \in K$ is interpreted as $a \cdot \mathrm{id}_V$. Since $\mathscr{F}$ is a zero-dimensional commutative ring, we can revisit and utilize many methods of Computational Commutative Algebra. In particular, the Buchberger-Möller algorithm for Matrices 2.1.4 allows us to compute a presentation $\mathscr{F} \cong K[x_1, \dots, x_n]/\operatorname{Rel}_P(\Phi)$, where $\operatorname{Rel}_P(\Phi)$ is the ideal of algebraic relations of $\Phi = (\varphi_1, \dots, \varphi_n)$. A further excursion leads to the insight that we can restrict a commuting family to an invariant subspace U of V and that we can find a presentation of the restricted family by calculating the annihilator of U in $\mathscr{F}$. Finally, we have a short tour of the possible values of the dimension $\dim_K(\mathscr{F})$. Here we have to drive carefully, since we should not assume accidentally that this dimension equals $\dim_K(V)$, although it will do so in important special cases. In general, the dimension of $\mathscr{F}$ can be both larger and smaller than that of V. With the necessary patience and care, our commuting families will get going happily and safely.

Be careful! 80 % of people are caused by accidents.

In the following we let K be a field, let V be a finite dimensional K-vector space, and let $d = \dim_K(V)$. Assume that we are given a set of commuting endomorphisms of V, in other words a set $S = \{\varphi_i\}_{i \in \Sigma}$ in $\operatorname{End}_K(V)$ indexed by a set Σ and having the property that $\varphi_i \circ \varphi_j = \varphi_j \circ \varphi_i$ for all $i, j \in \Sigma$. Notice that also polynomial combinations of the elements of S commute. Thus the K-subalgebra $\mathscr{F}$ of $\operatorname{End}_K(V)$ generated by S, i.e. the K-algebra $\mathscr{F} = K[S]$, is a commutative ring. To define the K-algebra structure of $\mathscr{F}$, we identify an element $c \in K$ with the endomorphism $c\,\mathrm{id}_V$ in $\operatorname{End}_K(V)$.

Definition 2.1.1 Given a set of commuting endomorphisms S of the vector space V, we let $\mathscr{F} = K[S]$ be the commutative K-subalgebra of $\operatorname{End}_K(V)$ generated by S and call it the **family of commuting endomorphisms**, or simply the **commuting family**, generated by S.

Remark 2.1.2 Notice that the vector space V carries a natural structure of a module over the K-algebra $\mathscr{F}$ given by $\varphi \cdot v = \varphi(v)$ for all $\varphi \in \mathscr{F}$ and $v \in V$. We have $\operatorname{Ann}_{\mathscr{F}}(V) = \langle 0 \rangle$, i.e., the vector space V is a faithful $\mathscr{F}$-module, since a map $\varphi \in \mathscr{F}$ with $\varphi(v) = 0$ for all $v \in V$ is necessarily the zero map.

In this section we study general properties of commuting families. Later on, special commuting families and their properties will be examined. Since the family $\mathscr{F}$ is a vector subspace of $\mathrm{End}_K(V)$, it is a finite dimensional K-vector space. It follows that $\mathscr{F}$ is a zero-dimensional commutative K-algebra (see for instance [15], Proposition 3.7.1).

Given a system of K-algebra generators $\Phi = (\varphi_1, \dots, \varphi_n)$ of $\mathscr{F}$, we form the polynomial ring $P = K[x_1, \dots, x_n]$ and introduce the following ideal.

Definition 2.1.3 Let $\Phi = (\varphi_1, \dots, \varphi_n)$ be a system of K-algebra generators of $\mathscr{F}$, and let the K-algebra epimorphism $\pi : P \longrightarrow \mathscr{F}$ be defined by $\pi(x_i) = \varphi_i$ for every $i \in \{1, \dots, n\}$. Then the kernel of π is called the **ideal of algebraic relations** of Φ and denoted by $\mathrm{Rel}_P(\Phi)$.

Clearly, if Φ consists of a single endomorphism φ, the ideal of algebraic relations of Φ is the principal ideal generated by the minimal polynomial of φ.

Given the tuple Φ of endomorphisms of V, the ideal $\mathrm{Rel}_P(\Phi)$ can be computed effectively, as the following algorithms shows. In particular, given a matrix $A = (a_{ij}) \in \mathrm{Mat}_d(K)$, we order the entries according to the lexicographic ordering of their indices (i, j) and thereby transform (a.k.a. “flatten”) the matrix to a vector in K^{d^2}.

Algorithm 2.1.4 (The Buchberger-Möller Algorithm for Matrices)
Let $\Phi = (\varphi_1, \dots, \varphi_n)$ be a system of K-algebra generators of $\mathscr{F}$. For every $i \in \{1, \dots, n\}$, let $M_i \in \mathrm{Mat}_d(K)$ be a matrix representing φ_i with respect to a fixed K-basis of V, and let σ be a term ordering on $\mathbb{T}^n$. Consider the following sequence of instructions.

(1) *Let $G = \emptyset$, $\mathscr{O} = \emptyset$, $S = \emptyset$, $\mathscr{N} = \emptyset$, and $L = \{1\}$.*
(2) *If $L = \emptyset$, return the pair $(G, \mathscr{O})$ and stop. Otherwise let $t = \min_\sigma(L)$ and delete it from L.*
(3) *Compute $t(M_1, \dots, M_n)$ and reduce it against $\mathscr{N} = (N_1, \dots, N_k)$ to obtain*

$$R = t(M_1, \dots, M_n) - \textstyle\sum_{i=1}^k c_i N_i \quad \text{with } c_i \in K$$

(4) *If $R = 0$, append the polynomial $t - \sum_{i=1}^k c_i s_i$ to G, where s_i denotes the i-th element of S. Remove from L all multiples of t. Continue with Step (2).*
(5) *Otherwise, we have $R \neq 0$. Append R to $\mathscr{N}$ and $t - \sum_{i=1}^k c_i s_i$ to S. Append the term t to $\mathscr{O}$, and append to L those elements of $\{x_1 t, \dots, x_n t\}$ which are neither multiples of a term in L nor in $\mathrm{LT}_\sigma(G)$. Continue with Step (2).*

This is an algorithm which computes the reduced σ-Gröbner basis of $\mathrm{Rel}_P(\Phi)$ *and a list of terms* $\mathcal{O}$ *whose residue classes form a vector space basis of* $P/\mathrm{Rel}_P(\Phi)$.

The proof of this algorithm uses the theory of Gröbner bases. A sketch can be found in [16], Tutorial 91.j, and a complete proof is contained in [14], Theorem 4.1.7. Notice that the result of this algorithm does not depend on the choice of the basis of V. The following proposition shows the invariance of $\mathrm{Rel}_P(\Phi)$ with respect to field extensions.

Proposition 2.1.5 *Let $\Phi = (\varphi_1, \dots, \varphi_n)$ be a system of K-algebra generators of the family $\mathcal{F}$, let $L \supseteq K$ be a field extension, let $V_L = V \otimes_K L$. Then let $(\varphi_i)_L = \varphi_i \otimes_K L : V_L \longrightarrow V_L$ be the extension of φ_i for $i = 1, \dots, n$, and let $\Phi_L = ((\varphi_1)_L, \dots, (\varphi_n)_L)$. Then the ideal $\mathrm{Rel}_{L[x_1,\dots,x_n]}(\Phi_L)$ is the extension ideal of $\mathrm{Rel}_P(\Phi)$ to $L[x_1, \dots, x_n]$.*

Proof A K-basis B of V is also an L-basis of V_L, and the matrices which represent the endomorphisms φ_i with respect to B also represent $(\varphi_i)_L$. Now the claim follows by applying the above algorithm for Φ_L and noticing that all of its operations are performed over K. Hence the resulting polynomials will have coefficients in K. $\square$

In analogy to Definition 1.1.5, we define invariant subspaces for a commuting family as follows.

Definition 2.1.6 A K-vector subspace U of V is called an **invariant subspace** for the family $\mathcal{F}$ if we have $\varphi(U) \subseteq U$ for all $\varphi \in \mathcal{F}$.

Given an invariant subspace U for the family $\mathcal{F}$, we can consider the **restricted family** $\mathcal{F}_U = \{\varphi|_U \mid \varphi \in \mathcal{F}\}$. Then the vector space U carries the structure of an $\mathcal{F}_U$-module. As a consequence of the Buchberger-Möller Algorithm for Matrices we get the following algorithm for computing annihilators of invariant subspaces.

Algorithm 2.1.7 (The Annihilator of an Invariant Subspace)
Let $\Phi = (\varphi_1, \dots, \varphi_n)$ be a system of K-algebra generators of the family $\mathcal{F}$, let $U \subseteq V$ be an invariant subspace for $\mathcal{F}$, and let $\Phi_U = (\varphi_1|_U, \dots, \varphi_n|_U)$ be the corresponding system of generators of the restricted family. The following instructions compute $\mathrm{Ann}_{\mathcal{F}}(U)$.

(1) *Using the Buchberger-Möller Algorithm for Matrices, compute* $\mathrm{Rel}_P(\mathcal{F}_U)$.
(2) *Return $\pi(\mathrm{Rel}_P(\mathcal{F}_U))$, where $\pi : P \longrightarrow \mathcal{F}$ is given by $x_i \mapsto \varphi_i$ for every $i \in \{1, \dots, n\}$.*

Proof Step (1) computes a set of generators of the ideal in P whose members are the polynomials f such that $f(\varphi_1|_U, \dots, \varphi_n|_U) = 0$. Its image in $\mathscr{F}$, computed in Step (2), is clearly the annihilator of U. $\square$

Let us apply this algorithm to a concrete example.

Example 2.1.8 Let $K = \mathbb{Q}$, let $V = K^6$ and let $\varphi_1, \varphi_2 \in \mathrm{End}_K(V)$ be defined by the matrices

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

respectively. Since A_1 and A_2 commute, we have a commuting family $\mathscr{F} = K[\varphi_1, \varphi_2]$. It is easy to check that the vectors $u_1 = e_1 - e_3$, $u_2 = e_2 - e_4$, $u_3 = e_1 - e_5$, and $u_4 = e_2 - e_6$ are K-linearly independent. Let $U = \langle u_1, u_2, u_3, u_4 \rangle$. We calculate

$$\begin{array}{cccc} \varphi(u_1) = u_3 - u_1, & \varphi(u_2) = u_4 - u_2, & \varphi(u_3) = u_3 - u_1, & \varphi(u_4) = u_4 - u_2 \\ \varphi_2(u_1) = u_2, & \varphi_2(u_2) = 2u_1, & \varphi_2(u_3) = u_4, & \varphi_2(u_4) = 2u_3 \end{array}$$

and conclude that U is an invariant subspace for $\mathscr{F}$.

The matrices associated to $\varphi_1|_U$ and $\varphi_2|_U$ with respect to the basis (u_1, u_2, u_3, u_4) are

$$M_1 = \begin{pmatrix} -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Using the Buchberger-Möller Algorithm for Matrices 2.1.4 applied to the pair (M_1, M_2), we get the ideal $\mathrm{Rel}_P(\mathscr{F}_U) = \langle x_1^2, x_2^2 - 2 \rangle$. Consequently, we obtain $\mathrm{Ann}_{\mathscr{F}}(U) = \langle \varphi_1^2 \rangle$, since $\varphi_2^2 - \mathrm{id}_V = 0$ and $\varphi_1^2 \neq 0$.

Clearly, the **annihilator** in $\mathscr{F}$ can be defined for any vector subspace of V, not just an invariant one. The following remark explains how to compute it.

Remark 2.1.9 Let $(\psi_1, \dots, \psi_\delta)$ be a K-basis of $\mathscr{F}$, where $\delta = \dim_K(\mathscr{F})$, let U be a K-vector subspace of V, and let $(u_1, \dots, u_e)$ be a K-basis of V. Then we can calculate the annihilator $\mathrm{Ann}_{\mathscr{F}}(U) = \{u \in U \mid \varphi(u) = 0 \text{ for all } \varphi \in \mathscr{F}\}$ as follows.

Introduce new indeterminates $y_1, \dots, y_\delta$ and write down the linear system of equations

$$\psi_1(u_1)y_1 + \cdots + \psi_\delta(u_1)y_\delta = 0$$
$$\vdots$$
$$\psi_1(u_e)y_1 + \cdots + \psi_\delta(u_e)y_\delta = 0$$

Compute a K-basis $\{(c_{i1}, \dots, c_{i\delta}) \mid i = 1, \dots, \varepsilon\}$ of its solution space. Then the endomorphisms $c_{i1}\psi_1 + \cdots + c_{i\delta}\psi_\delta$ with $i \in \{1, \dots, \varepsilon\}$ form a K-basis of $\mathrm{Ann}_{\mathscr{F}}(U)$.

As a consequence of Algorithm 2.1.7, we get the following description of the restriction of the family $\mathscr{F}$ to an invariant subspace.

Corollary 2.1.10 *Let $U \subseteq V$ be an invariant subspace for $\mathscr{F}$. Then the restriction map $\varrho : \mathscr{F} \longrightarrow \mathscr{F}_U$ induces an isomorphism of K-algebras $\mathscr{F} / \mathrm{Ann}_{\mathscr{F}}(U) \cong \mathscr{F}_U$.*

Proof In Algorithm 2.1.7, we have the inclusion $\mathrm{Rel}(\mathscr{F}) \subseteq \mathrm{Rel}(\mathscr{F}_U)$, and therefore $\mathscr{F}_U \cong P/\mathrm{Rel}(\mathscr{F}_U) \cong (P/\mathrm{Rel}(\mathscr{F}))/(\mathrm{Rel}(\mathscr{F}_U)/\mathrm{Rel}(\mathscr{F})) \cong \mathscr{F}/\mathrm{Ann}_{\mathscr{F}}(U)$. □

Based on the Buchberger-Möller Algorithm for Matrices, we have an alternative to Algorithm 1.1.8 for computing the minimal polynomial of an element of $\mathscr{F}$.

Algorithm 2.1.11 (The Minimal Polynomial of a Family Member)
Let $\Phi = (\varphi_1, \dots, \varphi_n)$ be a system of K-algebra generators of the family $\mathscr{F}$, let $f(x_1, \dots, x_n) \in P$, and let $\psi = f(\varphi_1, \dots, \varphi_n)$. The following instructions compute the minimal polynomial of ψ.

(1) *In the ring $P[z]$ form the ideal $I_\psi = \langle z - f(x_1, \dots, x_n)\rangle + \mathrm{Rel}_P(\Phi) \cdot P[z]$ and compute $J_\psi = I_\psi \cap K[z]$.*
(2) *Return the monic generator of J_ψ.*

Proof By [15], Proposition 3.6.2, these instructions compute the monic generator of the kernel of the K-algebra homomorphism $K[z] \longrightarrow \mathscr{F}$ defined by $z \mapsto \psi$. This polynomial is exactly the minimal polynomial of ψ. □

Recall that a field K is called **perfect** if either its characteristic is 0 or its characteristic is $p > 0$ and we have $K = K^p$ (see also [15], Definition 3.7.7). It is known that finite fields are perfect (see [10], Sect. 4.4). Moreover, the **nilradical** of $\mathscr{F}$ is $\mathrm{Rad}_{\mathscr{F}}(0) = \{\psi \in \mathscr{F} \mid \psi^i = 0 \text{ for some } i \geq 1\}$, i.e., the set of nilpotent endomorphisms in $\mathscr{F}$. We can compute the nilradical of $\mathscr{F}$ as follows.

Remark 2.1.12 Let $\Phi = (\varphi_1, \dots, \varphi_n)$ be a system of K-algebra generators of $\mathscr{F}$. Using the Buchberger-Möller Algorithm for Matrices 2.1.4, we compute the ideal

$\mathrm{Rel}_P(\Phi)$. Then we use Algorithm 1.1.8 or Algorithm 2.1.11 to compute the minimal polynomial $\mu_{\varphi_i}(x_i)$ for every $i \in \{1, \dots, n\}$.

If K is a perfect field, we can use the algorithms in [15], 3.7.9 and 3.7.12 to compute the squarefree parts $f_i(x_i) = \mathrm{sqfree}(\mu_{\varphi_i}(x_i))$ for $i = 1, \dots, n$. Then the nilradical of $\mathscr{F}$ is given by $\mathrm{Rad}_{\mathscr{F}}(0) = \langle f_1(\varphi_1, \dots, \varphi_n), \dots, f_t(\varphi_1, \dots, \varphi_n)\rangle$. Later we will see an improvement of this method (see 5.4.2). If K is not perfect, we can use [13], Alg. 7 to compute the radical of $\mathrm{Rel}_P(\Phi)$ and get $\mathrm{Rad}_{\mathscr{F}}(0)$ as above.

In the last part of this section we study the dimension of a commuting family.

Definition 2.1.13 Let $\mathscr{F}$ be a family of commuting endomorphisms of V. The number $\dim_K(\mathscr{F})$ is called the **dimension** of the family $\mathscr{F}$.

The dimension of a commuting family can be larger than, equal to, or smaller than the dimension of V, as the following examples show.

Example 2.1.14 If $\varphi \in \mathrm{End}_K(V)$ and $\mathscr{F} = K[\varphi]$. Then the dimension of $\mathscr{F}$ is given by $\dim_K(\mathscr{F}) = \deg(\mu_\varphi(z))$. Thus it is smaller than or equal to d, with equality if and only if φ is commendable (see Theorem 1.5.8).

The maximal dimension of a commuting family was determined by J. Schur (see [26]) and N. Jacobson (see [12]) a long time ago: it coincides with $\lfloor d^2/4 \rfloor + 1$ for $d = \dim_K(V)$. In the next example $\dim_K(\mathscr{F})$ surpasses $\dim_K(V)$ maximally.

Example 2.1.15 Let $V = K^6$, and let $\mathscr{F}$ be the K-algebra generated by $\{\mathrm{id}_V\}$ and the set of all endomorphisms of V whose matrix with respect to the canonical basis of V is of the form $\left(\begin{smallmatrix} 0 & A \\ 0 & 0 \end{smallmatrix}\right)$ with a matrix A of size 3×3. The family $\mathscr{F}$ is commuting, since $\left(\begin{smallmatrix} 0 & A \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & A \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ for all matrices A, B of size 3×3. Here we have $\dim_K(V) = 6$ and $\dim_K(\mathscr{F}) = 10 = 6^2/4 + 1$, the maximal possible dimension.

The special case of a family generated by two commuting matrices was considered by Gerstenhaber (see [8]) who proved that in this case the sharp upper bound for the dimension of $\mathscr{F}$ is d. A sharp upper bound for the dimension of a family generated by three commuting matrices is apparently not known.

2.2 Kernels and Big Kernels of Ideals

A serious and good philosophical work
could be written consisting entirely of jokes.
(Ludwig Wittgenstein)

Dear Reader, although the notion of the kernel of an ideal may initially sound like a joke, let us assure you that it is a serious and philosophically sound idea. Let us meditate a bit.

http://www.springer.com/978-3-319-43599-2

Computational Linear and Commutative Algebra
Kreuzer, M.; Robbiano, L.
2016, XVIII, 321 p. 1 illus., Hardcover
ISBN: 978-3-319-43599-2