Linear Galois Theory

Michael Francis

October 10, 2018

Abstract

In this expository essay, we develop the fundamental correspondence of Galois theory while paying careful attention to the division of labour between field theory and elementary linear algebra. The goal is to make plain which parts of the theory only rely on dimension counting arguments and which rely in an essential way on, for example, the construction of splitting fields. We then set up a different Galois correspondence, more linear algebraic in nature than the usual one, in which the role of groups is replaced by rings of linear transformations and which is applicable to *arbitrary* finite-dimensional field extensions, instead of merely to Galois extensions. The usual group-theoretic Galois correspondence can be recovered from this ring-theoretic one.

Introduction

To the student of Galois theory, the path from the basic setup to the fundamental correspondence theorem may oftentimes feel rather murky. Certain needed facts are trivial consequences of the definitions, while other, cosmetically similar, facts seem to require more intricate arguments. Moreover, while one can certainly tell *that* linear algebraic methods (dimensional comparisons, linear independence, etc) are driving a large part of the argument, it is less clear where to draw the line separating the part of the proof which just relies on linear algebraic techniques from the part of the proof which is, in an essential sense, field-theoretic or group-theoretic.

We hope that this expository note can serve as a remedy to the above plight. In the development of the basic theory which follows, we push the linear algebraic arguments as far as it is natural for them to go and in this way obtain, we believe, an exposition in which one can easily identify which parts of the argument are coming from where. In order to achieve this development, we involve one tool which is not standard fare for a first course in Galois theory, namely the Jacobson density theorem. The latter will act as a surrogate for Artin's lemma used in many standard proofs, e.g. the one in [3].

The structure of this document is as follows. In Section 1, we demonstrate how one can, without ever defining a splitting field or even considering any rings of polynomials, formulate and prove the fundamental correspondence of Galois theory. In Section 2, we show how the use of Artin's lemma can be replaced by that of the Jacobson density theorem and how, in

doing this, one may obtain a ring-theoretic form (Theorem 12) of the fundamental correspondence which is, moreover, applicable to all finite-dimensional field extensions, rather than just to the Galois ones. The correspondence is as follows: given a field E, there is a 1-1 correspondence between subfields F of E such that $[E : F] < \infty$ and rings R of additive group endomorphisms of E such that $E \subseteq R$ (as multiplication operators) and $\dim_E(R) < \infty$. The correspondence simply associates to each F the ring $\mathscr{L}_F(E)$ of F-linear transformations of E. In Section 3, we illustrate the ring-theoretic correspondence theorem with some simple examples.

1 The usual Galois correspondence

The utility of dimension counting strategies in Galois theory mostly traces back to a pair of results commonly known as *Dedekind's lemma* and *Artin's Lemma*. Dedekind's lemma, as we aim to bring out below, is little more than an instance of the fact that eigenvectors with distinct eigenvalues are linearly independent. Recall that a *character* of a group G is a homomorphism from G to the multiplicative group of nonzero elements of some field.

Lemma 1 (Dedekind's lemma)**.** *For any group G and field E, the set of E-valued characters of G is linearly independent in the vector space E^G of E-valued functions on G.*

A natural way to show that a collection of vectors $v_1, \ldots, v_n$ is linearly independent is to exhibit operators $\Delta_1, \ldots, \Delta_n$ such that $\Delta_i(v_j) \neq 0$ if and only if $i = j$. In the case where $v_1, \ldots, v_n$ are eigenvectors of an operator T with distinct eigenvalues $\lambda_1, \ldots, \lambda_n$, this can be achieved by taking $\Delta_i = \prod_{j \neq i}(T - \lambda_j \cdot \mathrm{id})$. Along the same lines, we have

Proof of Dedekind's lemma. For each $g \in G$, let $T_g : E^G \to E^G$ be the translation operator $(T_g f)(x) = f(gx)$. Observe that, if $\varphi : G \to E$ is a character, then φ is an eigenvector of T_g with eigenvalue $\varphi(g)$. If $\varphi_1, \ldots, \varphi_n$ are distinct characters, then, for all $i \neq j$, there exists $g_{ij} \in G$ such that $\varphi_i(g_{ij}) \neq \varphi_j(g_{ij})$. Putting $\Delta_i = \prod_{j \neq i}(T_{g_{ij}} - \varphi_j(g_{ij}) \cdot \mathrm{id})$, we find that $\Delta_i(\varphi_j) \neq 0$ if and only if $i = j$, whence $\varphi_1, \ldots, \varphi_n$ are independent. □

Since a field imbedding $K \hookrightarrow E$ is, in particular, an E-valued character for the multiplicative group $K^\times$, one has the following important corollary in field theory.

Corollary 2. *For any fields K and E, the set $\mathrm{Imb}(K, E)$ of field imbeddings $K \hookrightarrow E$ is E-linearly independent in E^K. In particular, $\mathrm{Aut}(E)$ is linearly independent in E^E.*

Corollary 2 tells us that the size of a collection of E-valued imbeddings or automorphisms is bounded by the dimension of any finite-dimensional E-vector space containing the collection. The following proposition is trivial.

Proposition 3. *Let $F \subseteq K \subseteq E$ be a tower of fields and write $\mathrm{Imb}_F(K, E)$ for the set of $\varphi \in \mathrm{Imb}(K, E)$ such that $\varphi\big|_F = \mathrm{id}_F$. Then,*

1. *$\mathrm{Imb}_F(K, E) \subseteq \mathscr{L}_F(K, E)$, the set of F-linear maps from K to E.*

2. $\mathscr{L}_F(K,E)$ *is an* E*-subspace of* E^K *with dimension* $[K:F]$.

In particular, if E/F *is some field extension, we have*

3. $\mathrm{Aut}_F(E) \subseteq \mathscr{L}_F(E)$

4. $\mathscr{L}_F(E)$ *is an* E*-subspace of* E^E *with dimension* $[E:F]$.

Combining the above proposition with Corollary 2, we immediately have

Corollary 4. *For any tower of fields* $F \subseteq K \subseteq E$*, one has* $|\mathrm{Imb}_F(K,E)| \leq [K:F]$*. In particular, for any field extension* E/F*, one has* $|\mathrm{Aut}_F(E)| \leq [E:F]$.

Note that the statement "E/F is Galois and $F \subseteq K \subseteq E$ implies E/K is Galois" is a triviality once it is known the Galois extensions are the splitting fields of separable polynomials. However, if we insist on staying in the world of basic linear algebra, there is still an easy and rather informative proof. We take the following definition.

Definition 5. A finite-dimensional field extension E/F is called a **Galois extension** if $|\mathrm{Aut}_F(E)| = [E:F]$, i.e. there are as many automorphisms as permitted by Corollary 4.

In order to show that a Galois extension is also Galois over any intermediate field, we use a natural generalization of the orbit-stabilizer theorem applicable to subsets instead of individual points. Specifically, suppose that a group G acts on a set X and let S be a subset of X. Define the *stabilizer subgroup* $\mathrm{Stab}(S)$ to consist of all $g \in G$ such that $gx = x$ for all $x \in S$ and the *orbit* $\mathrm{Orb}(S)$ to be the set of all imbeddings $S \hookrightarrow X$ arising as $x \mapsto gx$ for some $g \in G$. Then, the map $G/\mathrm{Stab}(S) \to \mathrm{Orb}(S)$ sending a left-coset $g\mathrm{Stab}(S)$ to the imbedding $x \mapsto gx : S \to X$ is a well-defined bijection. So, with these definitions, we get $|G| = |\mathrm{Stab}(S)| \cdot |\mathrm{Orb}(S)|$ as usual.

Proposition 6. *Let* $F \subseteq K \subseteq E$ *be a tower of finite-dimensional field extensions. If* E/F *is Galois, then so is* E/K*. In fact, we have*

1. $|\mathrm{Aut}_K(E)| = [E:K]$

2. $|\mathrm{Imb}_F(K,E)| = [E:F]$

3. *Every element of* $\mathrm{Imb}_F(K,E)$ *occurs as* $\varphi\big|_K$ *for some* $\varphi \in \mathrm{Aut}_F(E)$.

Proof. Applying the orbit-stabilizer theorem discussed above with $G = \mathrm{Aut}_F(E)$, $X = E$ and $S = K$ gives $|\mathrm{Aut}_F(E)| = |\mathrm{Aut}_K(E)| \cdot |\{\varphi\big|_K : \varphi \in \mathrm{Aut}_F(E)\}|$. By assumption, $|\mathrm{Aut}_F(E)| = [E:F]$. By Corollary 4, $|\mathrm{Aut}_K(E)| \leq [E:K]$. We have $\{\varphi\big|_K : \varphi \in \mathrm{Aut}_F(E)\} \subseteq \mathrm{Imb}_F(K,E)$ and, by Corollary 4, $|\mathrm{Imb}_F(K,E)| \leq [K:F]$. The desired conclusions follow. □

As a corollary, we can prove half of the fundamental correspondence theorem.

Corollary 7. *Let* E/F *be a finite-dimensional Galois extension. Then, for any field* K *with* $E \subseteq K \subseteq E$*, one has* $E^{\mathrm{Aut}_K(E)} = K$.

Proof. Let $H = \mathrm{Aut}_K(E)$ and $K' = E^H$. It's easy to see that $K' \supseteq K$ and $\mathrm{Aut}_{K'}(E) = H$. The preceding proposition gives $[E : K] = |H| = [E : K']$, whence $K = K'$. □

In view of the above, to get the full correspondence theorem, it just remains to check that going from groups to subfields and back also gives the identity. To achieve this, it is standard to make of use of Artin's lemma, stated below.

Lemma 8 (Artin's Lemma)**.** *Let H be a finite group of automorphisms of a field E. Then, E is a finite-dimensional extension of F^H with $[E : F^H] \leq |H|$.*[1]

Artin's lemma is also, essentially, a linear algebraic result. See [3], pp. 236 for a proof in this vein. In the next section, we shall see that the role of Artin's lemma can be filled by the Jacobson density theorem which is, in the author's view, an even more linear algebraic tool.

Corollary 9. *Let H be a finite group of automorphisms of a field E. Then,* $\mathrm{Aut}_{E^H}(E) = H$.

Proof. Let $F = E^H$. By Lemma 8 (Artin's lemma), E is finite-dimensional over F and $[E : F] \leq |H|$. Let $H' = \mathrm{Aut}_F(E)$. By Lemma 1 (Dedekind's lemma), $|H'| \leq [E : F]$. Obviously, $H' \supseteq H$, and so we have $|H| \leq |H'| \leq [E : F] \leq |H|$ whence, all quantities being equal, $H = H'$, as needed. □

Together, Corollary 7 and Corollary 9 give the fundamental correspondence.

Theorem 10 (Fundamental correspondence of Galois theory)**.** *Let E/F be a finite-dimensional Galois extension with Galois group $G = \mathrm{Aut}_F(E)$. Then, the maps $K \mapsto \mathrm{Aut}_K(E)$ and $H \mapsto E^H$ communicating between intermediate extensions $F \subseteq K \subseteq E$ and subgroups $H \subseteq G$ are mutually inverse.*

Note that, throughout this section, we have not really done any field theory. We have not discussed splitting fields, nor indeed considered any rings of polynomials. Nothing but basic linear algebra has transpired, and yet the fundamental correspondence of Galois has been established.

2 The ring-theoretic correspondence

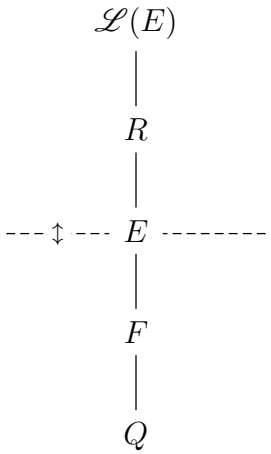
Given a field E, we write $\mathscr{L}(E)$ for the ring of additive group homomorphisms $E \to E$. Notice that $E \subseteq \mathscr{L}(E)$ as the multiplication operators M_a, $a \in E$ which send $x \mapsto ax$. We shall establish a 1-1 correspondence between:

- fields F contained in E such that E is finite-dimensional over F,
- rings $R \subseteq \mathscr{L}(E)$ containing E such that R is finite-dimensional over E.

The correspondence sends a field F to $\mathscr{L}_F(E)$, the ring of F-linear transformations. Note that $\mathscr{L}_E(E) = E$ and $\mathscr{L}_Q(E) = \mathscr{L}(E)$, where Q is the prime field of E. In the other direction, we use the map $R \mapsto E^R$ provided by the following easy lemma.

[1] In fact, $[E : F^H] = |H|$.

Figure 1: Schematic of the ring-theoretic correspondence. Note both the fields and the rings sit in a single poset one may think of the correspondence as a sort of reflection through E.



Lemma 11. *Let E be a field and consider a subring $R \subseteq \mathscr{L}(E)$ such that $E \subseteq R$. Then, $E^R = \{T \in \mathscr{L}(E) : TS = ST \text{ for all } S \in R\}$ is a subfield of E.*

Proof. Since $E \subseteq R$, each element of E^R is an E-linear map of E and so $E^R \subseteq E$. Clearly E^R is closed under addition and multiplication and $1 \in E^R$. If $a \neq 0$ is in E^R and $T \in R$, then multiplying $TM_a = M_aT$ on both sides by $M_{a^{-1}}$ shows that $a^{-1} \in E^R$ too. □

Put differently, E^R is the largest subfield $F \subseteq E$ satisfying $R \subseteq \mathscr{L}_F(E)$. We now state the ring-theoretic form of the fundamental Galois correspondence which we aim to prove.

Theorem 12 (Ring-theoretic correspondence theorem)**.** *Let E be a field. Then, $F \mapsto \mathscr{L}_F(E)$ and $R \mapsto E^R$ define mutually inverse bijections between subfields F of E such that $[E : F] < \infty$ and subrings $R \subseteq \mathscr{L}(E)$ with $E \subseteq R$ such that $\dim_E(R) < \infty$. Moreover, this bijection preserves the aforementioned dimensions.*

Remark 13. (a) It is well-known that the centre of $\mathscr{L}_F(V)$ is F whenever V is a vector space on a field F. So, one direction of this fundamental correspondence is trivial; we have $E^{\mathscr{L}_F(E)} = F$ for any field extension E/F (finite-dimensional or not).

(b) The "moreover" part of Theorem 12 follows from the first half of the theorem; once we know that each R is $\mathscr{L}_F(E)$ for some F, then $\dim_E(R) = \frac{\dim_F(R)}{[E:F]} = \frac{[E:F]^2}{[E:F]} = [E : F]$.

(c) Both of the assignments $F \mapsto \mathscr{L}_F(E)$ and $R \mapsto E^R$ are the result of forming the commutator subring inside of $\mathscr{L}(E)$. If the theory of central simple algebras is available, then the above theorem may be viewed as a corollary of the double centralizer theorem. See [4], Page 115 for details.

As noted in (a) above, to prove Theorem 12 we just need to show that going from subrings to subfields and back gives the identity. In the interest of sticking as close as possible to the main thoroughfare of linear algebra, we shall check this using the *Jacobson density theorem*. Specializing the statement for the present context, this amounts to the following theorem.

Theorem 14 (Jacobson density theorem)**.** *Let E be a field and $R \subseteq \mathscr{L}(E)$ a ring of transformations of E such that $E \subseteq R \subseteq \mathscr{L}(E)$. Let F be the subfield $E^R \subseteq E$ of Lemma 11. Then, R is* dense *in $\mathscr{L}_F(E)$ in the sense that, for any $S \in \mathscr{L}_F(E)$ and any finite F-dimensional subspace V of E, there exists $T \in R$ such that $T = S$ on V.*

In the interest of keeping this document self-contained, we include a proof of the above, following the one given in [2] on Page 420.

Proof. The nontrivial part of the argument is contained in the following claim.

Claim. *For any finite, F-independent set $e_1, \ldots, e_n \in E$, there exists $T \in R$ such that $T(e_1) \neq 0$ and $T(e_i) = 0$ for $i > 1$.*

We prove the claim by induction on n. When $n = 1$, we may take $T = 1$ (since $E \subseteq R$).

When $n = 2$, suppose for contradiction that $Te_2 = 0$ implies $Te_1 = 0$, $T \in R$. Then, we get a well-defined map $\theta : E \to E$ by the definition $\theta(Te_2) = Te_1$, $T \in R$. Of course, taking $T = xe_2^{-1}$ where $x \in E$ is arbitrary, it is clear that θ is just $x \mapsto e_1 e_2^{-1} x$. On the other hand, notice that θ commutes with R by the calculation $\theta(TSe_2) = TSe_1 = T\theta(Se_2)$, $T, S \in R$. Thus, $\theta = e_1 e_2^{-1} \in F$, contradicting the F-independence of $\{e_1, e_2\}$.

Generally, take $n > 2$ and assume the claim for $n - 1$. Let $W = \mathrm{span}_F\{e_3, \ldots . e_n\}$ and let I_W be the left ideal in R consisting of elements which annihilate W. By the inductive hypothesis, $I_W e_2 \neq 0$ and so, since $E \subseteq R$, actually $I_W e_2 = R$. Suppose for contradiction that $Te_2 = \ldots = Te_n = 0$ implies $Te_1 = 0$. Then, we get a well-defined map $\theta : E \to E$ by the definition $\theta(Te_2) = Te_1$, $T \in I_W$. Again, note that θ commutes with R by the calculation $\theta(TSe_2) = TSe_1 = T\theta(Se_2)$, $T \in R, S \in I_W$ (using that I_W is a left ideal), and so $\theta \in F$. But now, for any $T \in I_W$, we have $Te_1 = \theta Te_2 = T\theta e_2$ i.e. the images of e_1 and θe_2 are the same under any element of I_W. Since, by the induction hypothesis, any element of $E \setminus W$ is not killed by some element of I_W, we must conclude that $e_1 = \theta e_2 \pmod W$, contradicting that $e_1 \notin \mathrm{span}_F\{e_2, \ldots, e_n\}$. This completes the proof of the claim.

To recover the full statement, let $e_1, \ldots, e_n$ be an F-basis for V. By the above lemma, there are $T_1, \ldots, T_n \in R$ such that $T_i(e_j) \neq 0$ if and only if $i = j$. Since $E \subseteq R$, we can replace T_i with $T_i(e_i)^{-1} T_i$ and get $T_i(e_j) = \delta_{ij}$ (the Dirac delta). Put $T = \sum_{i=1}^n S(e_i) T_i$. $\square$

The ring-theoretic correspondence theorem that we are aiming for is a straightforward consequence of the Jacobson density theorem.

Proof of Theorem 12. As noted in Remark 13, we only need to show that, if $R \subseteq \mathscr{L}(E)$ is a ring such that $E \subseteq R$ and $\dim_E(R) < \infty$, then $R = \mathscr{L}_F(E)$, where $F = E^R$. Indeed, by the simple linear algebraic lemma given below, there exists a finite set $Y \subseteq E$ such each T in R is determined by its restriction to Y. Take any $S \in \mathscr{L}_F(E)$. By the Jacobson density theorem, there exists, for any $x \in E$, a $T_x \in R$ such that $T_x = S$ on $Y \cup \{x\}$. On the

other hand, since elements of R are determined by their values on Y, all these $T_x \in R$ must actually be equal, and equal to S, so that $S \in R$. □

Lemma 15. *Let X be a set, E a field and denote by E^X the vector space of E-valued functions on X. Then, for any n-dimensional subspace $V \subseteq E^X$, there exists an n-element set $Y \subseteq X$ such that $f \mapsto f|_Y$ defines a vector space isomorphism from V to $E^Y \cong E^n$.*

Proof. We show by induction on n that, if $f_1, \ldots, f_n \in E^X$ are linearly independent functions, then an n-element set $Y \subseteq E$ can be chosen so that $f_1|_Y, \ldots, f_n|_Y$ are a basis for E^Y. If $n = 1$, we just know f_1 is not identically zero. Put $Y = \{x\}$ for some point $x \in X$ on which f_1 is not zero. Now suppose that the claim holds for some $n \geq 1$ and consider $n+1$ linearly independent functions $f_1, \ldots, f_n, f \in E^X$. By hypothesis, there is an n-element set $Y \subseteq X$ such that $f_1|_Y, \ldots, f_n|_Y$ are a basis for E^Y. Thus, there are unique $c_i \in E$ such that $f|_Y = \sum_{i=1}^n c_i f_i|_Y$. On the other hand, f does not actually belong to the span of $f_1, \ldots, f_n$, so there is some $z \in X$ with $f(z) \neq \sum_{i=1}^n c_i f_i(z)$. Then, it is easy to see that the restrictions of $f, f_1, \ldots, f_n$ to $Y \cup \{z\}$ are linearly independent. □

Let us now explain how this ring-theoretic Galois correspondence can be used to recover the usual group-theoretic one. The basic point is that every finite group of automorphisms of a field determines a unique ring of the type encountered in Theorem 12.

Definition 16. Let H be a finite group of automorphisms of a field E. Denote by $E \rtimes H$ the subring of $\mathscr{L}(E)$ generated by E and H, where E is embedded in $\mathscr{L}(E)$ as the collection of multiplication operators M_a, $a \in E$.

The basic features of this of the ring $E \rtimes H$ are tabulated in the following proposition.

Proposition 17. *Let $H = \{1 = \varphi_1, \ldots, \varphi_n\}$ be a finite group of automorphisms of a field E. Then, the following hold.*

(i) $\varphi M_a \varphi^{-1} = M_{\varphi(a)}$ *for all* $a \in E$, $\varphi \in \mathrm{Aut}(E)$

(ii) $E \rtimes H = \{\sum_{i=1}^n M_{a_i}\varphi_i : a_1, \ldots, a_n \in E\}$, *where* M_a *denotes multiplication by* $a \in E$

(iii) $\dim_E(E \rtimes H) = n$

(iv) $(E \rtimes H) \cap \mathrm{Aut}(E) = H$

(v) $E^{E \rtimes H} = E^H$

(vi) $E \rtimes H = \mathscr{L}_{E^H}(E)$.

Proof. (i) is a calculation. For (ii), note that "$\supseteq$" is obvious and the relation (i) implies "$\subseteq$". (iii) is a consequence of (ii). For (iv), we obviously have "$\supseteq$" and, on the other hand, $\mathrm{Aut}(E)$ is E-independent in $\mathscr{L}(E)$ (Corollary 2 of Dedekind's lemma) and so, by (iii), $E \rtimes H$ cannot contain any additional automorphisms. For (v), the left hand side is all the elements of E (embedded in $\mathscr{L}(E)$ as multiplication operators) which commute with E and H, whereas the right hand side is the elements of E commuting with H and so, since E commutes with itself, we are done. Finally, (vi) follows from (v) and Theorem 12. □

Remark 18. The relation (i) justifies the notation $E \rtimes H$, which is intended as a nod to the *crossed-product* construction, commonplace in operator theory.

It is now easy to use our ring-theoretic correspondence Theorem 12 to give an alternate proof of Corollary 9, the statement of which is repeated below.

"Let H be a finite group of automorphisms of a field E. Then, $\mathrm{Aut}_{E^H}(E) = H$."

Together with Corollary 7, this facilitates an alternate proof of the fundamental correspondence theorem of Galois theory which avoids any use of Artin's lemma.

Alternate proof of Corollary 9. Let H be a finite group of automorphisms of some field E and put $R = E \rtimes H$, as in Definition 16 above. Then,

$$\begin{aligned} \mathrm{Aut}_{E^H}(E) &= \mathrm{Aut}_{E^R}(E) && \text{Proposition 17 (v)} \\ &= \mathscr{L}_{E^R}(E) \cap \mathrm{Aut}(E) \\ &= R \cap \mathrm{Aut}(E) && \text{Proposition 17 (vi)} \\ &= H && \text{Proposition 17 (iv)} \end{aligned}$$

as desired. The second line uses the rather obvious fact that $\mathrm{Aut}_F(E) = \mathscr{L}_F(E) \cap \mathrm{Aut}(E)$, valid for any subfield F of E. □

When E/F is a Galois extension, we know that the Galois group $H = \mathrm{Aut}_F(E)$ is an E-basis for $\mathscr{L}_F(E) = E \rtimes H$. If E is only finite-dimensional over F, and not necessarily Galois, we still have an easy, but less canonical, way to produce an E-basis for $\mathscr{L}_F(E)$.

Lemma 19. *Let E be a finite-dimensional field extension of F and fix an F-basis $u_1, \ldots, u_n$ for E. Then, the corresponding coordinate projections $P_1, \ldots, P_n \in \mathscr{L}_F(E)$ are an E-basis for $\mathscr{L}_F(E)$.*

Proof. Since $\dim_E(\mathscr{L}_F(E)) = n$, we just need to check the P_i are E-independent. Suppose that $a_1, \ldots, a_n \in E$ are such that $\sum_{i=1}^n M_{a_i} P_i = 0$. Applying this equation to u_i gives $a_i u_i = 0$ whence $a_i = 0$. □

3 Computations

We conclude by illustrating the ring-theoretic correspondence in some simple cases. Consider a simple extension $E = Q(\alpha)$ of a field Q where α has minimum polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Recall that $1, \alpha, \ldots, \alpha^{n-1}$ is a Q-basis for E and, with respect to this basis, we may identify $\mathscr{L}_Q(E)$ with $M_n(Q)$. Under this identification, the copy of E in $\mathscr{L}_Q(E)$ is generated by the diagonal copy of Q and the so-called *companion matrix*.

$$C_p = \begin{bmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{n-1} \end{bmatrix}$$

In this situation, there are finitely-many fields between Q and $E = Q(\alpha)$. Indeed, a classic theorem due to Steinitz asserts that an extension has a primitive element precisely when there are a finite number of intermediate field extensions (see Theorem 4.28 in [3]). We pause to make note of the following corollary of Theorem 12.

Corollary 20. *Let $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ be a monic irreducible polynomial over a field Q. Then, only finitely many subrings $R \subseteq M_n(Q)$ contain both the diagonal copy of Q and the companion matrix C_p described above.*

Proof. Such rings are in bijection with subextensions of $Q(\alpha)$ over Q, where α has minimum polynomial p. □

Suppose now that F is an intermediate field between $E = Q(\alpha)$ and Q with $[E : F] = k$ and $[F : Q] = d$, so that $n = dk$. Since $E = F(\alpha)$ too and the minimum polynomial of α over F has degree k, we have that $1, \alpha, \ldots, \alpha^{k-1}$ is an F-basis for E. Thus, by Lemma 19, the corresponding projections $P_1, P_\alpha \ldots, P_{\alpha^{k-1}}$ are an E-basis for $\mathscr{L}_F(E)$.

Let us now restrict attention to the case where $Q = \mathbb{Q}$ and $\alpha = \sqrt[n]{a}$ for some $a \in \mathbb{Q}$, $a > 0$. Assume also that $p(x) = x^n - a$ is irreducible, and therefore equals the minimum polynomial of α (for instance, this happens when a is a prime number, by Eisenstein's criterion). In this case, the powers of the companion matrix

$$C_{x^n-a} = \begin{bmatrix} 0 & 0 & 0 & \cdots & a \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

are easily calculated and one obtains that, under the identification of $\mathscr{L}(E)$ with $M_n(\mathbb{Q})$, the copy of $E = \mathbb{Q}(\alpha)$ in $\mathscr{L}(E)$ is given by

$$E = \left\{ \begin{bmatrix} b_0 & ab_{n-1} & ab_{n-2} & \cdots & ab_1 \\ b_1 & b_0 & ab_{n-1} & \cdots & ab_2 \\ b_2 & b_1 & b_0 & \cdots & ab_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & b_{n-2} & b_{n-3} & \cdots & b_0 \end{bmatrix} : b_0, \ldots, b_{n-1} \in \mathbb{Q} \right\}.$$

The intermediate fields F between $\mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[n]{a})$ are also easy to describe; they are just the various fields $F = \mathbb{Q}(\sqrt[d]{a})$ where d is a positive divisor of n (see [1], Exercise 4, pp. 626). Indeed, $d \mapsto \mathbb{Q}(\sqrt[d]{a})$ is an order isomorphism from positive divisors of n to such intermediate fields. As noted above, a natural F-basis for E is $\{1, \alpha, \ldots, \alpha^{k-1}\}$, where $k = n/d$, and, by Corollary 19, the corresponding projections $P_1, P_\alpha, \ldots, P_{\alpha^{k-1}}$ are an E-basis for $\mathscr{L}_F(E)$. Furthermore, since $\alpha^k = \sqrt[d]{a} \in F$, it is easy to see that a $\mathbb{Q}$-basis for the

F-span of each α^i, $0 \leq i \leq k-1$ is $\alpha^i, \alpha^{i+k}, \alpha^{i+2k}, \ldots, \alpha^{i+n-k}$. Thus, under the identification of $\mathscr{L}(E)$ with $M_n(\mathbb{Q})$, the projections $P_1, P_\alpha, \ldots, P_{\alpha^{k-1}}$ are given by the diagonal matrices

$$\begin{aligned} P_1 &= \operatorname{diag}(\underbrace{1,0,\ldots,0}, \underbrace{1,0,\ldots,0}, \ldots, \underbrace{1,0,\ldots,0}) \\ P_\alpha &= \operatorname{diag}(\underbrace{0,1,\ldots,0}, \underbrace{0,1,\ldots,0}, \ldots, \underbrace{0,1,\ldots,0}) \\ &\vdots \\ P_{\alpha^{k-1}} &= \operatorname{diag}(\underbrace{0,0,\ldots,1}, \underbrace{0,0,\ldots,1}, \ldots, \underbrace{0,0,\ldots,1}) \end{aligned}$$

where each brace encloses k coordinates. So, following Lemma 19, the subring $\mathscr{L}_F(E)$ of $M_n(\mathbb{Q})$ which is associated to the subfield $F = \mathbb{Q}(\sqrt[d]{a})$ of $E = \mathbb{Q}(\sqrt[n]{a})$ by the correspondence of Theorem 12 is given by $\mathscr{L}_F(E) = \operatorname{span}_E(P_1, P_\alpha, \ldots, P_{\alpha^{k-1}})$.

In particular, let us take $a = 2$ and $n = 6$ so that $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[6]{2})$. The proper subfields of E are exactly $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt{2})$. According to the description of $\mathscr{L}_F(E)$ just given, under the identification of $\mathscr{L}(E) = \mathscr{L}_\mathbb{Q}(E)$ with $M_6(\mathbb{Q})$, the subrings R and S of $M_6(\mathbb{Q})$ associated to, respectively, $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt{2})$ are the following.

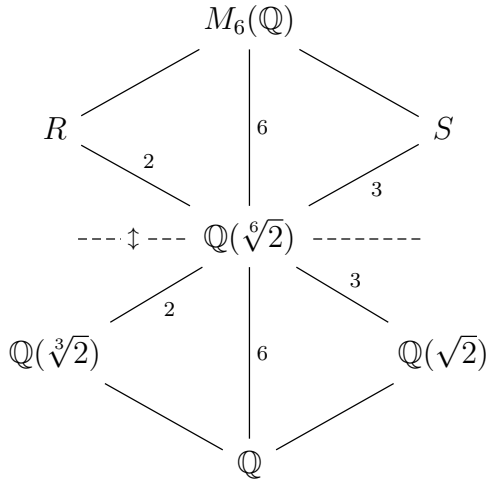
$$R = \left\{ \begin{bmatrix} a_0 & 2b_5 & 2a_4 & 2b_3 & 2a_2 & 2b_1 \\ a_1 & b_0 & 2a_5 & 2b_4 & 2a_3 & 2b_2 \\ a_2 & b_1 & a_0 & 2b_5 & 2a_4 & 2b_3 \\ a_3 & b_2 & a_1 & b_0 & 2a_5 & 2b_4 \\ a_4 & b_3 & a_2 & b_1 & a_0 & 2b_5 \\ a_5 & b_4 & a_3 & b_2 & a_1 & b_0 \end{bmatrix} : a_i, b_i \in \mathbb{Q} \right\}$$

$$S = \left\{ \begin{bmatrix} a_0 & 2b_5 & 2c_4 & 2a_3 & 2b_2 & 2c_1 \\ a_1 & b_0 & 2c_5 & 2a_4 & 2b_3 & 2c_2 \\ a_2 & b_1 & c_0 & 2a_5 & 2b_4 & 2c_3 \\ a_3 & b_2 & c_1 & a_0 & 2b_5 & 2c_4 \\ a_4 & b_3 & c_2 & a_1 & b_0 & 2c_5 \\ a_5 & b_4 & c_3 & a_2 & b_1 & c_0 \end{bmatrix} : a_i, b_i, c_i \in \mathbb{Q} \right\}$$

The relationships between the various rings and fields at stake are summarized in Figure 3 below. Note that $H = \operatorname{Aut}(\mathbb{Q}(\sqrt[6]{2}))$ is a 2-element group, the nontrivial automorphism being the one sending $\sqrt[6]{2} \mapsto -\sqrt[6]{2}$. The fixed field of H is $\mathbb{Q}(\sqrt[3]{2})$, of which $\mathbb{Q}(\sqrt[6]{2})$ is a Galois (in fact quadratic) extension. We may alternatively describe the ring R as $\mathbb{Q}(\sqrt[6]{2}) \rtimes H$, in the notation of Definition 16.

The subfield $\mathbb{Q}(\sqrt{2})$ of $\mathbb{Q}(\sqrt[6]{2})$, on the other hand, is *not* the fixed field of any group of automorphisms of $\mathbb{Q}(\sqrt[6]{2})$. Nonetheless, we are still able to describe $\mathbb{Q}(\sqrt{2})$ as the "fixed field" for the ring S which, this time, does not contain *any* nontrivial field automorphisms and so, as an object, is rather divorced from the world of Galois groups.

Figure 2: Subfields of $\mathbb{Q}(\sqrt[6]{2})$ correspond to ring extensions of $\mathbb{Q}(\sqrt[6]{2})$ in $M_6(\mathbb{Q})$.



References

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[2] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[3] Nathan Jacobson. *Basic Algebra I*. W. H. Freeman and Company, New York, second edition, 1985.

[4] Anthony W. Knapp. *Advanced Algebra*. Cornerstones. Birkhäuser Boston, 2007.