One special case of this theorem is when E is *finitely generated* over F, that is, $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, for some (not necessarily algebraically independent) elements $\alpha_1, \ldots, \alpha_n$ of E. It is clear that we may renumber $\alpha_1, \ldots, \alpha_n$ so that $\alpha_1, \ldots, \alpha_m$ are independent transcendentals and $\alpha_{m+1}, \ldots, \alpha_n$ are algebraic over $F(\alpha_1, \ldots, \alpha_m)$ (so E is a finite extension of the latter field). In this case E is called a *function field in m variables* over F. Such fields play a fundamental role in algebraic geometry as fields of functions on m-dimensional surfaces. For instance, when $F = \mathbb{C}$ and $m = 1$, these fields arise in analysis as fields of meromorphic functions on compact Riemann surfaces.

Note that if S_1 and S_2 are transcendence bases for E/F it is not necessarily the case that $F(S_1) = F(S_2)$. For example, if t is transcendental over $\mathbb{Q}$, $\{t\}$ and $\{t^2\}$ are both transcendence bases for $\mathbb{Q}(t)/\mathbb{Q}$ but (as we shall see shortly) $\mathbb{Q}(t^2)$ is a proper subfield of $\mathbb{Q}(t)$.

We now see that if $x_1, x_2, \ldots, x_n$ are indeterminates over F and

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n) \tag{14.28}$$

is the general polynomial of degree n, then the set of n elementary symmetric functions $s_1, s_2, \ldots, s_n$ in the x_i's are also independent transcendentals over F. This is because $x_1, \ldots, x_n$ is a transcendence base for $E = F(x_1, \ldots, x_n)$ over F (so the transcendence degree is n) and E is algebraic over $F(s_1, \ldots, s_n)$ (of degree $n!$). The theorem forces $s_1, \ldots, s_n$ to be a transcendence base for this extension as well (in particular, they are independent transcendentals). The general polynomial of degree n over F may therefore equivalently be defined by taking $a_1, \ldots, a_n$ to be any independent transcendentals (or indeterminates) and letting

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \tag{14.29}$$

where the roots of f are denoted by $x_1, \ldots, x_n$ (and $s_i = (-1)^i a_i$).

Definition. An extension E/F is called *purely transcendental* if it has a transcendence base S such that $E = F(S)$.

In the preceding discussion, both $F(x_1, \ldots, x_n)$ and $F(s_1, \ldots, s_n)$ are purely transcendental over F. As an exercise (following) one can show that $\mathbb{Q}(t, \sqrt{t^3 - t}\,)$ is not a purely transcendental extension of $\mathbb{Q}$ even though it contains no elements that are algebraic over $\mathbb{Q}$ other than those in $\mathbb{Q}$ itself (i.e., the process of decomposing a general extension into a purely transcendental extension followed by an algebraic extension cannot generally be reversed so that the algebraic piece occurs first).

If E is a purely transcendental extension of F of transcendence degree $n = 1$ or 2 and L is an intermediate field, $F \subseteq L \subseteq E$ with the same transcendence degree, then L is again a purely transcendental extension of F (Lüroth ($n = 1$), Castelnuovo ($n = 2$)). This result is not true if the transcendence degree is ≥ 3, however, although examples where L fails to be purely transcendental are difficult to construct. For extensions of transcendence degree 1 the intermediate fields are described by the following theorem.

Theorem. Let t be transcendental over F.

(1) (Lüroth) If $F \subseteq K \subseteq F(t)$, then $K = F(r)$, for some $r \in F(t)$. In particular, every nontrivial extension of F contained in $F(t)$ is purely transcendental over F.

(2) If $P = P(t)$, $Q = Q(t)$ are nonzero relatively prime polynomials in $F[t]$ which are not both constant,

$$[F(t) : F(P/Q)] = \max(\deg P, \deg Q).$$

Proof: The proof of (2) is outlined in Exercise 18 of Section 13.2.

By part (2) of this theorem we see that $F(P/Q) = F(t)$ if and only if P, Q are nonzero relatively prime polynomials of degree ≤ 1 (not both constant). Thus $F(r) = F(t)$ if and only if $r = \dfrac{at+b}{ct+d}$, where $a, b, c, d \in F$ and $ad - bc \neq 0$ (called a *fractional linear transformation of* t). For *any* $r \in F(t) - F$ the map $t \mapsto r$ extends to an embedding of $F(t)$ into itself which is the identity on F. This embedding is surjective (i.e., is an automorphism of $F(t)$) precisely for the fractional linear transformations. Furthermore, the map

$$GL_2(F) \to \mathrm{Aut}(F(t)/F) \quad \text{defined by} \quad A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \sigma_A,$$

where σ_A denotes the automorphism of $F(t)$ defined by mapping t to $(at+b)\big/(ct+d)$, is a surjective homomorphism with kernel consisting of the scalar matrices. Thus

$$\mathrm{Aut}(F(t)/F) \cong PGL_2(F)$$

where $PGL_2(F) = GL_2(F)/\{\lambda I \mid \lambda \in F^\times\}$ gives the group of automorphisms of this transcendental extension (cf. Exercise 8 of Section 1).

When $\mathbb{F}$ is a finite field of order q, $\mathrm{Aut}(\mathbb{F}(t)/\mathbb{F}) \cong PGL_2(\mathbb{F})$ is a finite group of order $q(q-1)(q+1)$. By Corollary 11 if K is the fixed field of $\mathrm{Aut}(\mathbb{F}(t)/\mathbb{F})$, then $\mathbb{F}(t)$ is Galois over K with Galois group equal to $\mathrm{Aut}(\mathbb{F}(t)/\mathbb{F})$. In particular, the fixed field of $\mathrm{Aut}(\mathbb{F}(t)/\mathbb{F})$ is not $\mathbb{F}$ in this case.

This also provides further examples of the Galois correspondence which can be written out completely for small values of q. For instance, if $q = |\mathbb{F}| = 2$, $PGL_2(\mathbb{F})$ is nonabelian of order 6, hence is isomorphic to S_3, and has the following lattice of subgroups:

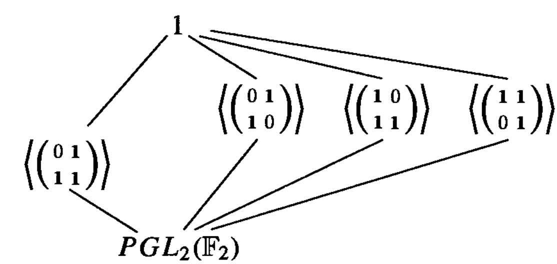

Fig. 5

The field $\mathbb{F}(t)$ is of degree 6 over the fixed field K of $\mathrm{Aut}(\mathbb{F}(t)/\mathbb{F})$ and the lattice of subfields $K \subseteq L \subseteq \mathbb{F}(t)$ is dual to the lattice of subgroups of S_3. The fixed field of a cyclic subgroup $\langle \sigma \rangle$ is easily found (via the preceding theorem) by finding a rational function r in t which is fixed by σ such that $[\mathbb{F}(t) : \mathbb{F}(r)] = |\sigma|$. For example, if $\sigma : t \mapsto 1/(1+t)$, then σ has order 3. The rational function

$$r = t + \sigma(t) + \sigma^2(t) = \frac{t^3+t+1}{t(t+1)}$$

is fixed by σ and $[\mathbb{F}(t) : \mathbb{F}(r)] = 3$ (by part (2) of the theorem). Since $\mathbb{F}(r)$ is contained in the fixed field of $\langle \sigma \rangle$ and the degree of $\mathbb{F}(t)$ over the fixed field is 3, $\mathbb{F}(r)$ is the fixed field of $\langle \sigma \rangle$. In this way one can explicitly describe the lattice of all subfields of $\mathbb{F}(t)$ containing K shown in Figure 6.

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{F}_2(t) \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\mathbb{F}_2\left(\frac{t^3+t+1}{t^2+t}\right) \arrow[dr] & \mathbb{F}_2\left(\frac{t^2+1}{t}\right) \arrow[d] & \mathbb{F}_2(t^2+t) \arrow[dl] & \mathbb{F}_2\left(\frac{t^2}{t+1}\right) \arrow[dll] \\
 & \mathbb{F}_2\left(\frac{(t^3+t+1)(t^3+t^2+1)}{(t^2+t)^2}\right) & &
\end{tikzcd}$$

Fig. 6

Purely transcendental extensions of $\mathbb{Q}$ play an important role in the problem of realizing finite groups as Galois groups over $\mathbb{Q}$. We describe a deep result of Hilbert which is fundamental to this area of research. If $a_1, a_2, \ldots, a_n$ are independent indeterminates over a field F, we may evaluate (or *specialize*) $a_1, \ldots, a_n$ at any elements of F, i.e., substitute values in F for the "variables" $a_1, a_2, \ldots, a_n$. If E is a Galois extension of $F(a_1, \ldots, a_n)$, then E is obtained as a splitting field of a polynomial whose coefficients lie in $F[a_1, \ldots, a_n]$. Any specialization of $a_1, \ldots, a_n$ into F maps this polynomial into one whose coefficients lie in F. The specialization of E is the splitting field of the resulting specialized polynomial.

Theorem. (Hilbert) Let $x_1, x_2, \ldots, x_n$ be independent transcendentals over $\mathbb{Q}$, let $E = \mathbb{Q}(x_1, \ldots, x_n)$ and let G be a finite group of automorphisms of E with fixed field K. If K is a purely transcendental extension of $\mathbb{Q}$ with transcendence basis $a_1, a_2, \ldots, a_n$, then there are infinitely many specializations of $a_1, \ldots, a_n$ in $\mathbb{Q}$ such that E specializes to a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to G.

Hilbert's Theorem gives a sufficient condition for the specialized extension not to collapse. In general, the Galois group of the specialized extension is a subgroup of G (cf. Proposition 19) and may be a proper subgroup of G. It is also known that the fixed field K need not always be a purely transcendental extension of $\mathbb{Q}$. An example of this occurs when G is the cyclic group of order 47.

This theorem can be used to give another proof of Proposition 42:

Corollary. S_n is a Galois group over $\mathbb{Q}$, for all n.

Proof of the Corollary: We have already proved that the fixed field of S_n acting in the obvious fashion on $\mathbb{Q}(x_1, \dots, x_n)$ is purely transcendental over $\mathbb{Q}$ (with the elementary symmetric functions as a transcendence base), so Hilbert's Theorem immediately implies the corollary.

The hypothesis that K be purely transcendental over $\mathbb{Q}$ is crucial to the proof of Hilbert's Theorem. Every finite group is isomorphic to a subgroup of S_n and so acts on $\mathbb{Q}(x_1, \dots, x_n)$ for some n. It is not known, however, even for the subgroup A_n of S_n whether its fixed field under the obvious action is a purely transcendental extension of $\mathbb{Q}$ (although it is known by other means that A_n is a Galois group over $\mathbb{Q}$ for all n). Thus there are a number of important open problems in this area of research.

One should also notice that Hilbert's Theorem does not work when the base field $\mathbb{Q}$ is replaced by an arbitrary field F (suppose F were algebraically closed, for instance). In particular, as noted earlier, the general polynomial $f(x)$ in Section 6 has Galois group S_n over $F(a_1, \dots, a_n)$ for any F, but when F is a finite field, the specialized extension obtained from its splitting field is always cyclic.

We next expand on the theory of inseparable extensions described in Section 13.5. Let p be a prime and let F be a field of characteristic p.

Definition. An algebraic extension E/F is called *purely inseparable* if for each $\alpha \in E$ the minimal polynomial of α over F has only one distinct root.

It is easy to see that the following are equivalent:

(1) E/F is purely inseparable
(2) if $\alpha \in E$ is separable over F, then $\alpha \in F$
(3) if $\alpha \in E$, then $\alpha^{p^n} \in F$ for some n (depending on α), and $m_{\alpha,F}(x) = x^{p^n} - \alpha^{p^n}$.

The following easy proposition describes composites of separable and purely inseparable extensions.

Proposition. If E_1 and E_2 are subfields of E which are both separable (or both purely inseparable) extensions of F, then their composite $E_1 E_2$ is separable (purely inseparable, respectively) over F.

Proof: Exercise.

One immediate consequence of this is the following result.