Proposition. Let E/F be an algebraic extension. Then there is a unique field E_{sep} with $F \subseteq E_{sep} \subseteq E$ such that E_{sep} is separable over F and E is purely inseparable over E_{sep}. The field E_{sep} is the set of elements of E which are separable over F.

The degree of E_{sep}/F is called the *separable degree* of E/F and the degree of E/E_{sep} is called the *inseparable degree* of E/F (often denoted as $[E : F]_s$ and $[E : F]_i$ respectively). The product of these two degrees is the (ordinary) degree. The propositions immediately give the following corollary.

Corollary. Separable degrees (respectively inseparable degrees) are multiplicative.

When E is generated over F by the root of an irreducible polynomial $p(x) \in F[x]$ the separable and inseparable degrees of the extension E/F are the same as the separable and inseparable degrees of the polynomial $p(x)$ defined in Section 13.5.

The proposition asserts that any algebraic extension may be decomposed into a separable extension followed by a purely inseparable one. Exercise 3 at the end of this section outlines an example illustrating that this decomposition cannot generally be reversed, namely an extension which is not a separable extension of a purely inseparable extension. We shall shortly state conditions on an extension under which the decomposition into separable and purely inseparable subextensions may be reversed.

We now know that an arbitrary extension E/F can be decomposed into a purely transcendental extension $F(S)$ of F followed by a separable extension E_1 of $F(S)$ followed by a purely inseparable extension E/E_1. In certain instances the inseparability in the algebraic extension at the "top" may be removed by a judicious choice of transcendence base:

Proposition. If E is a finitely generated extension of a perfect field F, then there is a transcendence base T of E/F such that E is a separable (algebraic) extension of $F(T)$.

A transcendence base T as described in the proposition is called a *separating transcendence base*. Exercise 4 at the end of this section illustrates this with a nontrivial example.

Recall that an extension E/F is *normal* if it is the splitting field of some (possibly infinite) set of polynomials in $F[x]$ (in particular, normal extensions are algebraic but not necessarily finite or separable). We previously used the synonymous term splitting field and the term normal is reintroduced here in the context of arbitrary algebraic extensions since it is used frequently in the literature, often in the context of embeddings of a field into an algebraic closure. Although the following set of equivalences can be gleaned from the preceding sections, the reader should write out a complete proof, checking that the arguments work for both infinite and inseparable extensions:

Proposition. Let E/F be an arbitrary algebraic extension and let Ω be an algebraic closure of E. The following are equivalent:

(1) E/F is a normal extension (i.e., is the splitting field over F of some set of polynomials in $F[x]$)

(2) whenever $\sigma : E \to \Omega$ is an embedding such that $\sigma|_F$ is the identity, $\sigma(E) = E$
(3) whenever an irreducible polynomial $f(x) \in F[x]$ has one root in E, it has all its roots in E.

In general, any embedding of a normal extension E/F into an algebraic closure of E which extends the identity embedding of F is an automorphism of E, i.e., is an element of $\mathrm{Aut}(E/F)$. Moreover, the number of such automorphisms equals the separable degree of E/F, provided the latter is finite:

if E/F is a normal extension and $[E : F]_s$ is finite, $\quad |\mathrm{Aut}(E/F)| = [E : F]_s$.

If $[E : F]_s$ is infinite we shall see shortly that $|\mathrm{Aut}(E/F)|$ is also infinite but need not be of the same cardinality.

If E/F is a normal extension whose separable degree is finite, let E_0 be the fixed field of $\mathrm{Aut}(E/F)$. By Corollary 11, E/E_0 is a (separable) Galois extension whose degree equals $|\mathrm{Aut}(E/F)|$. It follows that E_0/F must be purely inseparable (of degree equal to $[E : F]_i$), i.e., the separable and purely inseparable pieces of the extension may be reversed for normal extensions. More precisely, we easily obtain the following proposition.

Proposition. If E/F is normal with $[E : F]_s < \infty$, then $E = E_{sep}E_{pi}$, where E_{pi} is a purely inseparable extension of F (E_{pi} consists of all purely inseparable elements of E over F) and $E_{sep} \cap E_{pi} = F$.

Finally, we mention how Galois Theory generalizes to infinite extensions.

Definition. An extension E/F is called *Galois* if it is algebraic, normal and separable. In this case $\mathrm{Aut}(E/F)$ is called the *Galois group* of the extension and is denoted by $\mathrm{Gal}(E/F)$.

For infinite extensions there need not be a bijection between the set of all subgroups of the Galois group and the set of all subfields of E containing F, as the following example illustrates.

Let E be the subfield of $\mathbb{R}$ obtained by adjoining to $\mathbb{Q}$ all square roots of positive rational numbers. One easily sees that E may also be described as the splitting field of the set of polynomials $x^2 - p$, where p runs over all primes in $\mathbb{Z}^+$. Note that E is a (countably) infinite Galois extension of $\mathbb{Q}$. Since every automorphism σ of E is determined by its action on the square roots of the primes and σ either fixes or negates each of these, σ^2 is the identity automorphism. It follows that $\mathrm{Aut}(E)$ is an infinite elementary abelian 2-group. Thus $\mathrm{Aut}(E)$ is an infinite dimensional vector space over $\mathbb{F}_2$. By an exercise in the section on dual spaces (Section 11.3) the number of nonzero homomorphisms of $\mathrm{Aut}(E)$ into $\mathbb{F}_2$ is uncountable, whence their kernels (which are subspaces of co-dimension 1) are uncountable in number (and distinct). Thus $\mathrm{Aut}(E)$ has *uncountably* many subgroups of index 2, whereas $\mathbb{Q}$ has only a *countable* number of quadratic extensions.

The basic problem is that many (most) subgroups of $\mathrm{Gal}(E/F)$ do not correspond (in a bijective fashion) to subfields of E containing F. In order to pick out the "right"

set of subgroups of $\mathrm{Gal}(E/F)$ we must introduce a topology on this group (called the Krull topology). The axioms for the collection of (topologically) closed subsets of a topological space are precisely the bookkeeping devices which single out the relevant subgroups (these are listed in Section 15.2). Galois theory for finite extensions force certain subgroups of finite index to be closed sets and these in turn determine the topology on the entire group (as we might expect since every extension of F inside E is a composite of finite extensions). Moreover, the Galois group of E/F is the inverse limit of the collection of finite groups $\mathrm{Gal}(K/F)$, where K runs over all finite Galois extensions of F contained in E (cf. Exercise 10, Section 7.6).

Theorem. (Krull) Let E/F be a Galois extension with Galois group G. Topologize G by taking as a base for the closed sets the subgroups of G which are the fixing subgroups of the finite extensions of F in E, together with all left and right cosets of these subgroups. Then with this ("Krull") topology the closed subgroups of G correspond bijectively with the subfields of E containing F and the corresponding lattices are dual. Closed normal subgroups of G correspond to normal extensions of F in E.

One important area of current research is to describe (as a topological group) the Galois group of certain field extensions such as $\overline{F}/F$, where $\overline{F}$ is the algebraic closure of F. Little is known about the latter group when $F = \mathbb{Q}$ (in particular, its normal subgroups of finite index, i.e., which finite groups occur as Galois groups over $\mathbb{Q}$, are not known). If E is the algebraic closure of the finite field $\mathbb{F}_p$, the Galois group of this extension is the topologically cyclic group $\widehat{\mathbb{Z}}$ with the Frobenius automorphism as a topological generator. The group $\widehat{\mathbb{Z}}$ is an uncountable group (in particular, is not isomorphic to $\mathbb{Z}$) with the property that every closed subgroup of finite index is normal with cyclic quotient. Note that $\widehat{\mathbb{Z}}$ must also have nontrivial infinite closed subgroups (unlike $\mathbb{Z}$) since E contains proper subfields which are infinite over $\mathbb{F}_p$ (such as the composite of all extensions of $\mathbb{F}_p$ of q-power degree, for any prime q — this Galois extension of $\mathbb{F}_p$ has Galois group $\mathbb{Z}_q$, the q-adic integers, as described in Exercise 11 of Section 7.6).

EXERCISES

1. Prove that every purely inseparable extension is normal.
2. Let p be a prime and let $K = \mathbb{F}_p(x, y)$ with x and y independent transcendentals over $\mathbb{F}_p$. Let $F = \mathbb{F}_p(x^p - x, y^p - x)$.
   (a) Prove that $[K : F] = p^2$ and the separable degree and inseparable degree of K/F are both equal to p.
   (b) Prove that there is a subfield E of K containing F which is purely inseparable over F of degree p (so then K is a separable extension of E of degree p). [Let $s = x^p - x \in F$ and $t = y^p - x \in F$ and consider $s - t$.]
3. Let p be an odd prime, let s and t be independent transcendentals over $\mathbb{F}_p$, and let F be the field $\mathbb{F}_p(s, t)$. Let β be a root of $x^2 - sx + t = 0$ and let α be a root of $x^p - \beta = 0$ (in some algebraic closure of F). Set $E = F(\beta)$ and $K = F(\alpha)$.
   (a) Prove that E is a Galois extension of F of degree 2 and that K is a purely inseparable extension of E of degree p.