FIELD EXTENSIONS AND K-HOMOMORPHISMS

Let F be a field containing K. Then F is a K-algebra. If E is another field containing K we let $\mathrm{Alg}_K(F, E)$ denote the set of morphisms of K-algebras from F to E.

Note that if $\sigma \in \mathrm{Alg}_K(F, E)$ then $\sigma \neq 0$ since $\sigma(1) = 1$. Since F is a field, it follows that σ is monic.

(1) F is a **purely transcendental** extension of K with transcendence degree n if and only for every field E containing K, there there exist $u_1, \ldots, u_n \in F$ (not unique) such that there is a one-to-one correspondence between $\mathrm{Alg}_K(F, E)$ and the cartesian power E^n given by $\sigma \mapsto (\sigma(u_1), \ldots, \sigma(u_n))$.

(2) Let $u_1, \ldots, u_n \in F$. Then $u_1, \ldots, u_n$ are **algebraically independent** if and only the sub-K-algebra of F generated by $u_1, \ldots, u_n$ is a purely transcendental extension of K with transcendence degree n.

(3) F is an **algebraic** extension of K if and only if for every $u \in F$ and every field E containing K, there exist at most finitely many $e \in E$ such that there is a K-homomorphism $\sigma\colon F \to E$ with $\sigma(u) = e$.

(4) F is a **purely inseparable** extension of K if for every field E containing K there is at most one K-homomorphism from F into E.

(5) F is a finite dimensional **separable** extension of K if $\dim_K F = n < \infty$ and there exists a field E containing K such that there are n K-homomorphisms from F to E.

(6) More generally, F is a separable extension of K if F is algebraic over K and every finite dimensional subfield of F is separable over K.

(7) If F is a field with dimension n over K, then F is a **Galois** extension of K if $\mathrm{Alg}_K(F, F)$ contains n homomorphisms. In this case, we write $\mathrm{Gal}(F/K) = \mathrm{Alg}_K(F, F)$.

(8) F is a **normal** extension of K with for every field E containing K and $\sigma \in \mathrm{Alg}_K(F, E)$, $\sigma(F) \subseteq F$.

Proposition [Hungerford, Lemma 7.5, p 291]. Let E and F be fields containing E. $\mathrm{Hom}_K(F, E)$ is a vector space with dimension $\dim_K F$ over E. If $\sigma_1, \ldots, \sigma_n$ are distinct non-trivial mappings in $\mathrm{Alg}_K(F, E)$, then $\sigma_1 \ldots, \sigma_n$ are linearly independent elements of $\mathrm{Hom}_K(F, E)$. Consequently, $n \leq \dim_K F$.

Definition. The **separable degree** of F over K is

$$[F\colon K]_s = \sup_E |\operatorname{Alg}_K(F, E)|,$$

where the supremum is taken over all fields E containing K. (In fact, it suffices to consider any extension E of F which is normal over K.)

We write $[F\colon K] = \dim_K F$. Thus the preceding Proposition can be rephrased as asserting that $[F\colon K]_s \leq [F\colon K]$. Clearly if $[F\colon K] < \infty$ then F is separable over K if and only if $[F\colon K]_s = [F\colon K]$.

Lemma. (1) If $K \subseteq F \subseteq F_1$ with F_1 algebraic over K and $\sigma \in \operatorname{Alg}_K(F, E)$ for some field E containing K, then σ extends to a K-homomorphism $\sigma_1\colon F_1 \to E_1$ for some field E_1 containing E.

(2) If F_1 above is normal over K then σ extends to a K-automorphism of F_1.

Corollary. If $K \subseteq F \subseteq F_1$ (with F_1 algebraic over K), then $[F_1\colon K]_s = [F_1\colon F]_s\,[F\colon K]_s$.

Proposition. (1) If $f \in K[X]$ is an irreducible polynomial and u, v are roots of f in some extension field F of K, then there exists an extension E of F and a K-homomorphism $\sigma\colon F \to E$ such that $\sigma(u) = v$.

(2) If f is a polynomial in $K[X]$ with distinct roots and F is a normal extension of K in which f has a root, then f is irreducible if and only if $\operatorname{Aut}_K F$ acts transitively on the roots of f.

PROOF: (1) $K[u] \approx K[X]/(f) \approx K[v]$. By a previous Corollary, a K-homomorphism $K[u] \to K[v]$ extends to a K-homomorphism from F into some field E. ☑

Proposition. Let F be an algebraic extension of K.

(1) F is separable over K if and only if the minimal polynomial in $K[X]$ for every element $u \in F$ has distinct roots (in some possibly larger extension of K).

(2) F is normal over K if and only if for every $u \in F$, the minimal polynomial in $K[X]$ for u splits completely in $F[X]$.

(3) F is a galois extension of K if and only if the minimal polynomial over K for every $u \in F$ splits completely into distinct linear factors over K.

PROOF: (1) It suffices to deal with the case where $[F\colon K]$ is finite. In this case it is easy to see that there is a maximal subfield F' of F which is separable over K. If

$F' \subsetneq F$ let $u \in F$ with $u \notin F'$. The minimal polynomial g for u over F' is a factor of the minimal polynomial for u over K, hence has distinct roots. By the preceding proposition, for each of these roots there is a F'-homomorphism σ defined on $F'[u]$ with taking u to the specified root. Thus $[F'[u]\colon F']_s \geq \deg g = [F'[u]\colon F']$. Then $[F'[u]\colon K]_s = [F'[u]\colon F']_s\,[F'\colon K]_s \geq [F'[u]\colon F']\,[F'\colon K] = [F'[u]\colon K]$, so that $F'[u]$ is separable over K, contradicting the maximality of F'. Thus $F' = F$.

(2) If E is a field containing F and $\sigma \in \mathrm{Alg}_K(F, E)$ and $u \in F$, then $\sigma(u)$ is a root of the minimal polynomial for u over K. But this root must belong to F, since by hypothesis this polynomial splits completely in $F[X]$. Hence $\sigma(F) \subseteq F$, thus showing that F/K is normal.

Corollary. If F is a galois extension of K then for every $u \in F$ with $u \notin K$ there exists $\sigma \in \mathrm{Alg}_K(F, F)$ with $\sigma(u) \neq u$.

PROOF: If F is separable over K and $u \notin K$, then the minimal polynomial for u over K has more than one root so there exists $\sigma\colon F \to E$ with $\sigma(u) \neq u$ for some extension field E of F. If F/K is normal, we may take $E = F$. ☑

Corollary. If F is a normal [separable/galois] extension of K and $K \subseteq L \subseteq F$, then F is a normal [separable/galois] extension of L.

Notation. (1) If G is a group and X is a set/module/ring/field/K-algebra which G acts on, then we write

$$X^G = \{x \in X \mid (\forall \sigma \in G)\, \sigma x = x\}.$$

(X^G is the subobject of X **fixed** by G.)

If $x \in X$ then the **stabilizer** (or **isotropy subgroup**) of x is $G_x = \{\sigma \in G \mid \sigma x = x\}$. The **orbit** of x is $Gx = \{\sigma x \mid \sigma \in G\}$. Notice that distinct orbits are disjoint and that $Gx = Gy$ if and only if $y \in Gx$. We say that G acts **transitively** on X if X itself is the orbit of one (and therefore all) of its elements, i. e. if for all $x, y \in X$ there exists at least one $\sigma \in G$ with $y = \sigma x$.

If G acts on X then G acts on the set of subobjects of X in the obvious way, i. e. for $\sigma \in G$, $\sigma(Y) = \{\sigma(y) \mid y \in Y\}$. If Y is a subobject of X then we say that Y is **invariant** under G if $\sigma Y \subseteq Y$ for all $g \in G$. (Because the elements of G have inverses, it is easy to see that if $\sigma(Y) \subseteq Y$ then $\sigma(Y) = Y$. Clearly a subobject which is fixed under G is invariant, but not necessarily conversely.

If Y is a subobject of X then we will write $G_Y = \{\sigma \in G \mid (\forall y \in Y)\, \sigma(y) = y\}$. In other words, G_Y is the largest subgroup of G which fixes Y. (This is not standard notation.)

We will write $G_{\{Y\}} = \{\sigma \in G \mid \sigma(Y) = Y\}$. Thus $G_{\{Y\}}$ is the largest subgroup of G under which Y is invariant and is the stabilizer of Y under the action of G on the set of subobjects of X. Clearly $G_{\{Y\}} \subseteq G_Y$.

Proposition. Let G act on a set X and let $x \in X$. If $\sigma, \sigma' \in G$ then $\sigma x = \sigma' x$ if and only if σ and σ' are in the same left coset modulo G_x. Thus there is a one-to-one correspondence between the elements in the orbit Gx and the space of left cosets G/G_x.

Proposition. (1) For $Y \subseteq X$ and $\tau \in G$,

$$G_{\tau Y} = \tau^{-1}(G_Y)\tau.$$

(2) If Y is invariant under G then G_Y is a normal subgroup of G.

(3) If $Y = X^{G_Y}$ then Y is invariant under G if and only if G_Y is a normal subgroup of G.

PROOF: (1) If $\sigma \in G$ then $\sigma \in G_{\tau Y}$ and and only if for all $y \in Y$, $\sigma(\tau y) = \tau y$, or equivalently $\tau^{-1}\sigma\tau y = y$, i. e. if and only if $\tau^{-1}\sigma\tau \in G_Y$.

(2) For $\tau \in G$, if $\tau Y = Y$ then $\tau^{-1} G_Y \tau = G_{\tau Y} = G_Y$. Thus if $\tau Y = Y$ for all τ, then G_Y is a normal subgroup of G.

(3) Conversely, suppose that $Y = X^{G_Y}$ and G_Y is a normal subgroup of G. Then for all $\tau \in G$, $G_{\tau Y} = G_Y$. Thus if $y \in \tau Y$ then for all $\sigma \in G_Y$, $\sigma(y) = y$, so that $y \in X^{G_Y} = Y$. Thus $\tau Y \subseteq Y$ for all $\tau \in G$, showing that Y is invariant under G. ☑

Lemma. A finite subgroup of the multiplicative group of a field is cyclic.

Lemma. If V is a vector field over an infinite field K, then V is not a (set-theoretic) union of a finite number of proper subspaces.

PROOF: Suppose that $V = V_1 \cup \cdots \cup V_n$ with $V_i \subsetneq V$. We may assume WLOG V is not a union of any proper subset of $\{V_1, \ldots, V_n\}$. Thus we may choose $x \in V_1$ with $x \notin V_2 \cup \cdots \cup V_n$ and $y \in V_2$ with $y \notin V_1$. Then for any $k \neq 0 \in K$, $kx + y \notin V_1 \cup V_2$ (WHY?) so $kx + y \in V_i$ for $i \geq 3$. Since K is infinite and there are only finitely many V_i, it follows that there exist $k, k' \in K$ such that $kx + y, k'x + y \in V_i$ for some $i \geq 3$. But it then follows that $x \in V_i$, a CONTRADICTION. ☑

Lemma. If there are only a finite number of fields E with $K \subseteq E \subseteq F$, then $F = K(u)$ for some $u \in F$.

PROOF: If K is finite then F must also be finite and so the set of non-trivial elements of F is a cyclic group under multiplication and we can choose u to be a generator of this group.

If K is infinite then by the preceding lemma, there exists $u \in F$ with $u \notin \bigcup E$, where the union is taken over the proper subfields of F containing K. Then $K(u)$ must be all of F. ☑

Lemma. If $K \subseteq F \subseteq E$ and $\sigma_1, \ldots, \sigma_n \in \mathrm{Alg}_K(F, E)$ are such that no σ_i fixes F, then there exists $u \in F$ such that $\sigma_i(u) \neq u$ for all i.

PROOF: If K is finite, we may assume that F is finite and choose u to be a generator for its multiplicative group. If K is infinite then, for each i, let $F_i = \{f \in F \mid \sigma_i(f) = f\}$. By hypothesis, each F_i is a proper subfield of F. By a previous lemma, F cannot be a union of this set of proper subfields. Thus there exists $u \in F$ with $\sigma_i(u) \neq u$ for all i. ☑

Lemma. Let F be a finite separable extension of K and $K \subseteq L \subseteq F$. Let E be a normal extension of K containing F. If the only $\sigma \in \mathrm{Alg}_K(F, E)$ which fixes L is the inclusion $F \hookrightarrow E$, then $L = F$.

PROOF: Since F is separable over K, the number of maps in $\mathrm{Alg}_K(F, E)$ is $[F\colon K]$. Now if $\sigma \neq \sigma' \in \mathrm{Alg}_K(F, E)$ then $\sigma^{-1}\sigma'$ does not fix F, and hence by hypothesis does not fix L. I. e. σ and σ' have different restrictions to L. Thus there are at least $[F\colon K]$ distinct K-homomorphisms from L to E so that $[L\colon K] \geq [L\colon K]_s \geq [F\colon K] \geq [L\colon K]$. It follows that $F = L$. ☑

Theorem of the Primitive Element. (1) If F is a finite separable extension of K then $F = K(u)$ for some $u \in F$.

(2) If F is a separable extension of K and there exists n such that for every $u \in F$, $[K[u]\colon K] \leq n$, then $[F\colon K]$ is finite. In fact, $[F\colon K] \leq n$.

PROOF: (1) Let E be a normal extension of K containing F. By a previous lemma there exists $u \in F$ such that $\sigma(u) \neq u$ for every $\sigma \in \mathrm{Alg}_K(F, E)$ which does not fix F. Thus $K(u)$ is not fixed by any σ which does not fix F. By the preceding lemma, $K(u) = F$.

(2) Choose $u \in F$ such that $[K[u]\colon K]$ is maximal. If $K[u] \neq F$ then there exists $v \in F$ with $K[u] \subsetneq K[u, v]$. But by (1) $K[u, v] = K[w]$ for some w, so this yields a contradiction to the maximality of $K[u]$. Thus $F = K[u]$ and $[F\colon K] \leq n$. ☑

More Notation. If F is a galois extension of K and L a subfield of F containing K, then we will see below that F is a galois extension of L. $\mathrm{Gal}(F/L)$ can be identified as a subgroup of $\mathrm{Gal}(F/K)$, namely

$$\mathrm{Gal}(F/L) = \{\sigma \in \mathrm{Gal}(F/K) \mid (\forall \ell \in L)\, \sigma(\ell) = \ell\}.$$

In other words, $\mathrm{Gal}(F/L)$ is the set of elements in $\mathrm{Gal}(F/K)$ which **fix** L. (Hungerford uses the notation L' for this subgroup.)

Theorem. Let H be a finite group acting faithfully on a field F and let $u \in F$. Let H_u be the stabilizer of u, i.e. $H_u = \{\sigma \in H \mid \sigma(u) = u\}$. Let

$$g(x) = \prod_{H/H_u} (X - \sigma(u)),$$

where the product is taken over a set of representatives σ for the space of left cosets H/H_u. Then

(1) g has distinct roots and is the minimal polynomial for u over F^H.
(2) F is a galois extension of F^H.
(3) $[F\colon F^H] = |H|$.
(4) $\mathrm{Gal}(F/F^H) = H$.
(5) If $F = K(u)$ for some subfield K of F^H, then the coefficients of g generate F^H over K.

PROOF: Since H acts faithfully on F and fixes F^H, we will think of H as a subgroup of $\mathrm{Aut}_{F^H}(F)$.

(1) Restated, one sees that $g(x) = \prod(X - \sigma(u))$, where the $\sigma(u)$ (which constitute the roots of g) range over the orbit of u under H. Thus g has distinct roots. Furthermore, each $\tau \in H$ permutes the orbit of u, so $\tau(g(X)) = \prod(X - \tau\sigma(u)) = g(X)$ so that $g \in F^H[X]$. And g must be irreducible as a polynomial in $F^H[X]$ since H acts transitively on its roots. Since $g(u) = 0$, g is thus the minimal polynomial for u over F^H.

(2) From (1) we see that the minimal polynomial in $F^H[X]$ for every element $u \in F$ has distinct roots and splits completely in $F[X]$. Thus F is a galois extension of F^H.

(3) By (1), for any $u \in F$, the minimal polynomial for u over F^H has degree at most $|H|$, so $[F^H[u]\colon F^H] \leq |H|$. Since F/F^H is separable, it follows that

$[F\colon F^H] \le |H|$ (see the theorem of the primitive element). On the other hand, the elements of H are distinct F^H-homomorphism of F so $|H| \le [F\colon F^H]_s = [F\colon F^H]$.

(4) $H \subseteq \mathrm{Gal}(F/F^H)$ and $|\mathrm{Gal}(F/F^H)| \le [F\colon F^H]_s = [F\colon F^H] = |H|$.

(5) Suppose that $F = K(u)$ and let g as above be the minimal polynomial for u over F^H. Then $F = F^H(u)$ so by (3), $\deg g = |H|$. Let L be the K-subalgebra of F generated by the coefficients of g. (L is in fact a field, since it's an integral domain with finite dimension over K.) Then $g \in L[X]$ and $g(u) = 0$, so $[F\colon L] = [K[u]\colon L] \le \deg g = [F\colon F^H]$. Since $L \subseteq F^H$ by (1), it follows that $F^H = L$. ☑

Theorem. Let F be a galois extension of K.

(1) If H is a subgroup of $\mathrm{Gal}(F/K)$ then $\mathrm{Gal}(F/F^H) = H$.

(2) If $K \subseteq L \subseteq F$ then $F^{\mathrm{Gal}(F/L)} = L$.

(3) If H is a subgroup of $\mathrm{Gal}(F/K)$ then H is a normal subgroup if and only if F^H is a normal extension of K. In this case, $\mathrm{Gal}(F^H/K) \approx \mathrm{Gal}(F/K) \,/\, \mathrm{Gal}(F/F^H)$.

PROOF: (1) See the preceding proposition.

(2) F is a galois extension of L. Now suppose that $u \in F$ and $u \notin L$. Then there exists a L-homomorphism $\sigma\colon F \to F$ such that $\sigma(u) \ne u$. Then $\sigma \in \mathrm{Gal}(F/L)$, so $u \notin F^{\mathrm{Gal}(F/L)}$. Thus $F^{\mathrm{Gal}(F/L)} \subseteq L$. But the converse inclusion is trivial.

(3) See a previous proposition. ☑

Hilbert Theorem 90 [Hungerford, p. 292]. If F is a galois extension of K and $\mathrm{Gal}(F/K)$ is cyclic generated by σ, then an element $u \in F$ has norm 1 if and only if $u = v/\sigma(v)$ for some $v \in F$.

Corollary. If K contains a primitive d^{th} root of unity and F is a galois extension of K degree d such that $\mathrm{Gal}(F/K)$ is cyclic, then F is generated over K by a d^{th} root of some element of K.

PROOF: let $\zeta \in K$ be a primitive d^{th} root of unity. Then ζ has norm 1 so by the Hilbert Theorem 90, $\zeta = v/\sigma(v)$ for some $v \in F$. Then $\sigma(v) = \zeta^{-1}v$ and so $\sigma(v^d) = \zeta^{-d}v^d = v^d$. Since σ generates $\mathrm{Gal}(F/K)$, thus $v^d \in K$. Furthermore, since $\sigma^i(v) = \zeta^{-i}v \ne v$ for $0 < i < d$, $\mathrm{Gal}(F/K[v]) = \{1\}$. Thus $F = K[v]$. ☑

For a little bit of historical backgroud, see Scientific American, April, 1982, pp. 136–49, *The Short Life of Evariste Galois.*