Section V.2. The Fundamental Theorem (of Galois Theory)

Note. In this section, we define the "Galois group" of an arbitrary field extension. We prove (after several preliminary results) the Fundamental Theorem of Galois Theory. The Fundamental Theorem allows us to translate problems involving fields, polynomials, and extensions into group theoretical terms (again, showing the centrality of groups in modern algebra). Quoting Hungerford: "It was Galois' remarkable discovery that many questions about fields (especially about the roots of polynomials over a field) are in fact equivalent to certain group-theoretic questions in the automorphism group of the field."

Definition. Let F be a field. Let $\mathrm{Aut}(F)$ denote the set of all field automorphisms mapping $F \to F$. $\mathrm{Aut}(F)$ is a group under function composition (by Exercise V.2.1) called the *automorphism group* of F.

Definition/Definition IV.1.2. Let A and B be modules over a ring R. A function $f : A \to B$ is an *R-module homomorphism* provided that for all $a, c \in A$ and $r \in R$:

$$f(a+c) = f(a) + f(c) \text{ and } f(ra) = rf(a).$$

(Recall that a vector space is an R-module where R is a division ring with unity 1_R such that $1_R a = a$ for all $a \in A$.)

Note. Let E and F be extension fields of K. If $\sigma : E \to F$ is a nonzero homomorphism of fields, then $\sigma(1_E) = 1_F$ by Exercise III.1.15. If σ is also a K-module homomorphism then for each $k \in K$ we have

$$\sigma(k) = \sigma(k1_E) = k\sigma(1_E) = k1_E = k$$

(that is, σ fixes the elements of K). Conversely, if a homomorphism of fields $\sigma : E \to F$ fixes K elementwise then σ is nonzero and for any $u \in E$

$$\sigma(ku) = \sigma(k)\sigma(u) = k\sigma(u)$$

and so σ is a K-module homomorphism.

Definition V.2.1. Let E and F be extension fields of a field K. A nonzero map $\sigma : E \to F$ which is both a field and a K-module homomorphism is a *K-homomorphism*. Similarly if a field automorphism $\sigma \in \mathrm{Aut}(F)$ is a K-homomorphism (meaning that σ fixes K elementwise as noted above), then σ is a *K-automorphism* of F. The group of all K-automorphisms of F is the *Galois group* of F over K, denoted $\mathrm{Aut}_K(F)$.

Note. We can omit all this "K-module" talk by simply defining $\mathrm{Aut}_K(F)$ to be the set of all automorphisms of F which fix subfield K. This is how we are able to skip Chapter IV with little effect (and this is how Fraleigh deals with Galois theory without ever defining a module).

Example. Let K be any field and $F = K(x)$. Then F is an extension field of K (where we interpret K as the collection of constant rational functions in $K(x)$). For each $a \in K$, $a \neq 0$, define $\sigma_a : F \to F$ given by $f(x)/g(x) \mapsto f(ax)/g(ax)$. Then σ_a certainly fixes K. σ_a is a homomorphism by Corollary III.5.6. σ_a is onto since for any $f(x)/g(x) \in K(x)$, we have $f(x/a)/g(x/a) \in K(x)$ and $\sigma_a((f(x/a)/g(x/a)) = f(x)/g(x)$. Now $\sigma_a^{-1} = \sigma_{a^{-1}}$ and so σ is one to one by Theorem 0.3.1(i). So σ_a is an automorphism of $K(x)$ which fixes K; that is, $\sigma_a \in \mathrm{Aut}_K(F) = \mathrm{Aut}_K(K(x))$ for all $a \in K$, $a \neq 0$. Hence if K is infinite then $\mathrm{Aut}_K(F) = \mathrm{Aut}_K(K(x))$ is infinite. Similarly, for each $b \in K$, the map $\tau_b : F \to F$ given by $f(x)/g(x) \mapsto f(x+b)/g(x+b)$ is in $\mathrm{Aut}_K(F)$. If $a \neq 1_K$ and $b \neq 0$ then $\sigma_a\tau_b \neq \tau_b\sigma_a$ since

$$\sigma_a\tau_b(x) = \sigma_a(x+b) = (ax)+b = ax+b \text{ and } \tau_b\sigma_a(x) = \tau_b(ax) = a(x+b) = ax+ab.$$

Therefore $\mathrm{Aut}_K(F)$ is nonabelian.

Theorem V.2.2. Let F be an extension field of K and $K[x]$. If $u \in F$ is a root of f and $\sigma \in \mathrm{Aut}_K(F)$, then $\sigma(u) \in F$ is also a root of f.

Note. If u is algebraic over K and $f(u) = 0$ for irreducible $f \in K[x]$ of degree u, then by Theorem V.1.6(iv), $\{1_K, u, u^2, \ldots, u^{n-1}\}$ is a basis for $K(u)$. So any $\sigma \in \mathrm{Aut}_K(K(u))$ is completely determined by its action on u. We will use this property to restrict the number of elements of $\mathrm{Aut}_K(F)$ and to get some idea of the structure of $\mathrm{Aut}_K(F)$.

Example. If $F = K$, then $\mathrm{Aut}_K(F)$ only contains the identity isomorphism. The converse is false. Consider, for example, u the real root of $x^3 - 2$. Then $\mathbb{Q} \subset \mathbb{Q}(u) \subset \mathbb{R}$ (as fields). Then $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(u))$ consists only of the identity, since by Theorem V.2.2 the image of u must also be a root of x^3-2 but the other two roots of $x^3 - 2$ are complex and so u must be mapped to itself. Similarly, by Exercise V.2.2, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ contains only the identity.

Example. We now consider $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$. We have $\mathbb{C} = \mathbb{R}(i)$ where i is a root of x^2+1. By Theorem V.2.2, the only possible image of i by an element of $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ is either i itself (in which case the automorphism is the identity) or $-i$. It is easy to verify that the mapping $a+ib \mapsto a-ib$ is an automorphism of $\mathbb{C}$. So $|\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})| = 2$. Similarly $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})| = 2$.

Example. Let $F = \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. A basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1,\sqrt{2}\}$ by Theorem V.1.6(iv). Now x^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$, so a basis for $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$ is $\{1,\sqrt{3}\}$. But, as given by Theorem V.1.2, we know that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}),\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}),\mathbb{Q}] = 4$. In the proof of Theorem V.1.2—really, the proof of Theorem IV.2.16—it is shown that for fields $J \subset K \subset F$ with basis A of K over J and basis B of F over K, we have a basis of F over J of $AB = \{ab \mid a \in A, b \in B\}$. So the four elements of a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}$ is $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$. For more details, see Fraleigh's proof of his Theorem 31.4 on page 284 of the 7th edition of *A First Course in Abstract Algebra.* Next, by Theorem V.2.2, for $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ we must have $\sigma(1) = 1$, $\sigma(\sqrt{2}) \in \{-\sqrt{2},\sqrt{2}\}$, and $\sigma(\sqrt{3}) \in \{-\sqrt{3},\sqrt{3}\}$; notice that the behavior of σ on $\sqrt{2}$ and $\sqrt{3}$ determines its behavior on $\sqrt{6}$. Therefore $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$ consists of four $\mathbb{Q}$-automorphisms of $F = \mathbb{Q}(\sqrt{2},\sqrt{3})$. "It is readily verified that" $\mathrm{Aut}_{\mathbb{Q}}(F) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Note. The plan for Galois theory is to create a chain of extension fields (algebraic extensions, in practice) and to create a corresponding chain of automorphism groups. The first step in this direction is the following.

Theorem V.2.3. Let F be an extension field of K, E an intermediate field and H a subgroup of $\mathrm{Aut}_K(F)$. Then

(i) $H' = \{v \in F \mid \sigma(v) = v \text{ for all } \sigma \in H\}$ is an intermediate field of the extension;

(ii) $E' = \{\sigma \in \mathrm{Aut}_K(F) \mid \sigma(u) = u \text{ for all } u \in E\} = \mathrm{Aut}_E(F)$ is a subgroup of $\mathrm{Aut}_K(F)$.

Definition. Let F be an extension field of K and H a subgroup of $\mathrm{Aut}_K(F)$. The field $H' = \{v \in F \mid \sigma(v) = v \text{ for all } \sigma \in H\}$ is the *fixed field* of H in F. We use the prime notation to indicate fixed fields AND to indicate a Galois group $\mathrm{Aut}_K(F)$: $\mathrm{Aut}_K(F) = K'$ (notice that $F' = \mathrm{Aut}_F(F) = 1$, the trivial group consisting only of the identity permutation is called the *identity group*).

Definition V.2.4. Let F be an extension field of K such that the fixed field of the Galois group $\mathrm{Aut}_K(F)$ is K itself (and nothing else). Then F is a *Galois extension* of K, and F is said to be *Galois* over K.

Note. It follows from the definition that F is Galois over K if and only if for any $u \in F \setminus K$ there is some $\sigma \in \mathrm{Aut}_K(F)$ such that $\sigma(u) \neq u$.

Example. If $d \in \mathbb{Q}$ and $d \geq 0$, then $\mathbb{Q}(\sqrt{d})$ is Galois over $\mathbb{Q}$ (Exercise V.2.5(a)). $\mathbb{C}$ is Galois over $\mathbb{R}$ (Exercise V.2.5(b)). In Exercise V.2.2 it is shown that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ is the identity group. So $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ has fixed field $\mathbb{R}$ and hence $\mathbb{R}$ is not Galois over $\mathbb{Q}$.

Definition. If F is an extension field of K, and L, M are intermediate fields with $K \subset L \subset M \subset F$ then the dimension $[M : L]$ is the *relative dimension* of L and M. If H, J are subgroups of $\mathrm{Aut}_K(F)$ with $H < J$ then the index $[J : H]$ (the number of cosets of H in J) is the *relative index* of H and J.

Note. We now have the equipment to state the Fundamental Theorem of Galois Theory. However, we need several preliminary results before we have the equipment to *prove* it.

Theorem V.2.5. The Fundamental Theorem of Galois Theory.
If F is a finite dimensional Galois extension of K, then there is a one to one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group $\mathrm{Aut}_K(F)$ (given by $E \mapsto E' = \mathrm{Aut}_E(F)$) such that:

(i) the relative dimension of two intermediate fields is equal to the relative index of the corresponding subgroups; in particular, $\mathrm{Aut}_K(F)$ has order $[F : K]$;

(ii) F is Galois over every intermediate field E, but E is Galois over K if and only if the corresponding subgroup $E' = \mathrm{Aut}_E(F)$ is normal in $G = \mathrm{Aut}_K(F)$; in this case G/E' is (isomorphic to) the Galois group $\mathrm{Aut}_K(E)$ of E over K.

Note. The one to one correspondence—the “Galois correspondence”—assigns to each intermediate field E (that is, $K \subset E \subset F$) the Galois group $E' = \mathrm{Aut}_E(F)$ AND assigns to each subgroup $H < G = \mathrm{Aut}_K(F)$ the fixed field H'. These assignments of fields to groups and groups to fields are inverses of each other. Diagramatically we have:

$$\begin{array}{cccccc}
 & & & \textbf{Automorphism} & & \textbf{Fixed} \\
\textbf{Field} & & \textbf{Group} & \textbf{Group} & & \textbf{Field} \\
F & \longmapsto & 1 = \mathrm{Aut}_F(F) & 1 & \longmapsto & F \\
\cup & & \wedge & \wedge & & \cup \\
M & \longmapsto & M' = \mathrm{Aut}_M(F) & H & \longmapsto & H' \\
\cup & & \wedge & \wedge & & \cup \\
L & \longmapsto & L' = \mathrm{Aut}_L(F) & J & \longmapsto & J' \\
\cup & & \wedge & \wedge & & \cup \\
K & \longmapsto & K' = G = \mathrm{Aut}_K(F) & G = \mathrm{Aut}_K(F) & \longmapsto & K
\end{array}$$

The goal is to establish these mappings as inverses of each other (that is, to justify the one to one correspondence claims), as well as the relative dimension and normality claims of the Fundamental Theorem.

Lemma V.2.6. Let F be an extension field of K with intermediate fields L and M (say $K \subset L \subset M \subset F$). Let H and J be subgroups of $G = \mathrm{Aut}_K(F)$. Then:

(i) $F' = 1$ (the identity group) and $K' = G$;

(i′) $1' = F$;

(ii) $L \subset M$ implies $M' < L'$;

(ii′) $H < J$ implies $J' \subset H'$;

(iii) $L \subset L''$ and $H < H''$ (where $L'' = (L')'$ and $H'' = (H')'$);

(iv) $L' = L'''$ and $H' = H'''$.

Note. It is possible in Lemma V.2.6(iii) for L to be a proper subset of L''. For example, in Exercise V.2.2 we have $\text{Aut}_{\mathbb{Q}}(\mathbb{R})$ is the identity group. With $L = \mathbb{Q}$, we have $L' = \text{Aut}_{\mathbb{Q}}(\mathbb{R}) = 1$ (the identity group on $\mathbb{R}$) and so the fixed field of L' is $L'' = \mathbb{R}$. Also, H may be a proper subgroup of H'' in Lemma V.2.6(iii).

Note. By the definition of Galois extension, in terms of the prime notation, we have that F is Galois over K if and only if $G' = (\text{Aut}_K(F))'$. We always have $K' = \text{Aut}_K(F) = G$ (by definition of K'), so F is Galois over K if and only if $K = G' = K''$.

Definition. Let F be an extension field of K. Let X be either (i) an intermediate field, $K \subset X \subset F$, or (ii) a subgroup of the Galois group, $X < G = \text{Aut}_K(F)$. Then X is *closed* if $X = X''$.

Note. Subfield K of F is Galois over K if and only if K is closed.

Theorem V.2.7. If F is an extension field of K, then there is a one to one correspondence between the closed intermediate fields of the extension and the closed subgroups of the Galois group, given by $E \mapsto E' = \text{Aut}_E(F)$.

Note. Theorem V.2.7 only deals with closed fields and groups. This will be useful once we prove Lemma V.2.10. We now turn our attention to dimensions.

Lemma V.2.8. Let F be an extension field of K and L, M intermediate fields with $L \subset M$. If $M : L$ is finite, then $[L' : M'] \leq [M : L]$. In particular, if $[F : K]$ is finite, then $|\mathrm{Aut}_K(F)| \leq [F : K]$.

Lemma V.2.9. Let F be an extension field of K and let H, J be subgroups of the Galois group $\mathrm{Aut}_K(F)$ with $H < J$. If $[J : H]$ is finite, then $[H' : J'] \leq [J : H]$.

Lemma V.2.10. Let F be an extension field of K, L and M intermediate fields with $L \subset M$, and H, J subgroups of the Galois group $\mathrm{Aut}_K(F)$ with $H < J$.

(i) If L is closed and $[M : L]$ finite, then M is closed and $[L' : M'] = [M : L]$;

(ii) if H is closed and $[J : H]$ finite, then J is closed and $[H' : J'] = [J : H]$;

(iii) if F is a finite dimensional Galois extension of K, then all intermediate fields and and all subgroups of the Galois group are closed and $\mathrm{Aut}_K(F)$ has order $[F : K]$.

Note. We now turn our attention to the intermediate fields. To prove the Fundamental Theorem, we now focus our interest on when an intermediate fields has a corresponding group which is normal in the Galois group $\mathrm{Aut}_K(F)$.

Definition. Let $K \subset E \subset F$ be fields. Intermediate field E is *stable* (relative to K and F) if every $\sigma \in \mathrm{Aut}_K(F)$ maps E into itself. (Notice that $\sigma|_E \in \mathrm{Aut}_K(E)$.)

Note. We may have $\sigma \in \mathrm{Aut}_K(F)$ mapping E into itself (even onto E), but E may not be fixed *pointwise* by σ, so we are not saying that $(\mathrm{Aut}_K(F))' = E$.

Lemma V.2.11. Let F be an extension field of K.

(i) If E is a stable intermediate field of the extension, then $E' = \mathrm{Aut}_E(F)$ is a normal subgroup of the Galois group $\mathrm{Aut}_K(F)$;

(ii) if H is a normal subgroup of $\mathrm{Aut}_K(F)$, then the fixed field H' of H is a stable intermediate field of the extension.

Lemma V.2.12. If F is a Galois extension field of K and E is a stable intermediate field of the extension, then E is Galois over K.

Lemma V.2.13. If F is an extension field of K and E is an intermediate field of the extension such that E is algebraic and Galois over K, then E is stable (relative to F and K).

Definition. If $K \subset E \subset F$ be fields. Automorphism $\tau \in \mathrm{Aut}_K(E)$ is *extendible* to F if there exists $\sigma \in \mathrm{Aut}_K(F)$ such that the restriction of σ to E is τ, $\sigma|_E = \tau$.

Note. The automorphism in $\mathrm{Aut}_K(E)$ which are extendible to F form a subgroup of $\mathrm{Aut}_K(E)$. Recall that if E is stable, then $E' = \mathrm{Aut}_E(F)$ is a normal subgroup of $\mathrm{Aut}_K(F)$ by Lemma V.2.11(i). Consequently, the quotient group $\mathrm{Aut}_K(F)/\mathrm{Aut}_E(F)$ is defined.

Lemma V.2.14. Let F be an extension field of K and let E be a stable intermediate field of the extension. Then the quotient group $\mathrm{Aut}_K(F)/\mathrm{Aut}_E(F)$ is isomorphic to the group of all automorphisms in $\mathrm{Aut}_K(E)$ that are extendible to F.

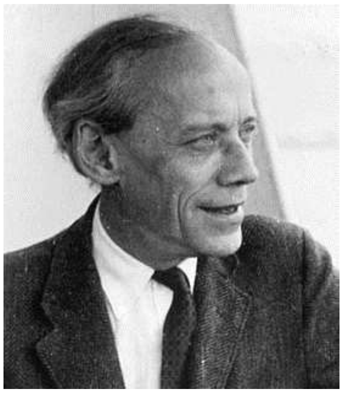
Note. *Now* we have the equipment to prove the Fundamental Theorem.

Theorem V.2.15. (Artin.)
Let F be a field, G a group of automorphisms of F, and K the fixed field of G in F. Then F is Galois over K. If G is finite, then F is a finite dimensional Galois extension of K with Galois group G.

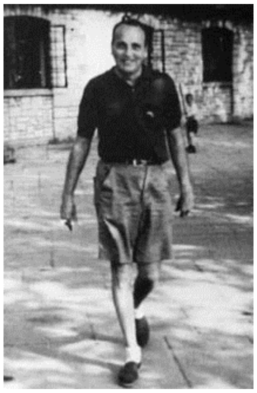
Note. Hungerford follows an approach to Galois theory originally due to Emil Artin. Artin's classical treatment appears in a 68 page work, *Galois Theory* in the *Notre Dame Mathematical Lectures*, Number 2 (1942). Dover Publications has the second (1944) edition of Artin's work in print and available today. You can likely also find a PDF copy online. For example, Project Euclid has an online PDF available at (accessed 3/9/2015):

`http://projecteuclid.org/euclid.ndml/1175197041#toc`

This version (and the Dover version) includes a section on applications by Arthur Milgram. Fraleigh follows Artin's approach to Galois theory in his 7th edition (see the comment on page 419 in the Historical Note). Hungerford also follows Artin's development, but as slightly modified by Irving Kaplansky in his 1969 *Fields and Rings* in the Chicago Lectures in Mathematics. A second (1972) edition is still in print (and you might find an online PDF copy of this as well); the 78 page Part I contains the results on Galois theory.



Emil Artin



Irving Kaplansky

(Images from the The MacTutor History of Mathematics Archive.)

Note. In the early 19th century, while exploring algebraic solutions of polynomial equations (that is, while looking for a quadratic-equation-type solution to a general nth degree polynomial equation), group theoretic ideas were introduced by Niels Henrik Abel (1802–1829) and Evaristé Galois (1811–1832). Abel proves that there is no algebraic way to solve (in general) a 5th or higher degree polynomial equation (this is Proposition V.9.8 in Hungerford). However, *some* 5th degree polynomial equations can be algebraically solved; for example, the equation $x^5 - x^3 = 0$ has solutions $x = 0$, $x = -1$, and $x = 1$. What Abel did not do, was to determine which equations are algebraically solvable and which are not. This was accomplished by Galois. In the opinion of your humble instructor, the *real* fundamental theorem of Galois' is given in Hungerford's Corollary V.9.7:

> Let F be a field of characteristic 0 and let $f \in F[x]$. Then the equation $f(x) = 0$ is solvable by radicals if and only if the Galois group of f is solvable.

In developing his ideas, Galois introduced the ideas of "substitution groups" (special cases of symmetry groups), normal subgroups, simple groups, and group isomorphisms. Unfortunately, Galois did not have time to publish his results because he died at the age of 20 in a pistol duel. Joseph Liouville (1809–1882) published part of Galois' work in 1846, though the importance of this work was not widely recognized at the time. In 1870, Camille Jordan (1838–1922) published *Traité des substitutions et des équations algébriques* in which Galois' theory of equations was presented and widely circulated. In fact, in Jordan's book he refers to commutative groups as "abelian," a term which is still in use. For additional information on Evaristé Galois, see `http://faculty.etsu.edu/gardnerr/Galois/Galois200.htm` and my YouTube video on Galois at `https://www.youtube.com/watch?v=64ZDFglF5eM` (accessed 3/3/2015).

Evaristé Galois (1811–1832)

This note is based in part on The MacTutor History of Mathematics Archive's *The Development of Group Theory* webpage at:

`http://www-history.mcs.st-andrews.ac.uk/HistTopics/`
`Development_group_theory.html`

and Chapter 31, "Galois Theory," of *Mathematical Thought from Ancient to Modern Times*, Volume 2, by Morris Kline, Oxford University Press (1972), 752–771.

Revised: 4/16/2018