UNIVERSITY OF WYOMING
$F[\alpha] \cong F[t]/(f(t))$
$\frac{1}{3+2\sqrt{2}} = 3-2\sqrt{2}$

Math 4520—Fall 2024
Algebra III
Fields
Department of Mathematics

A Taste of Galois Theory

Evariste Galois (1811-1832) observed a very beautiful connection between field theory and group theory. Our priority is to see the beauty of this connection, which we will illustrate using a few examples. Detailed proofs of the main results are not our highest priority, which (because of time constraints) will be kept to a minimum.

Recall that a *group* is a set G with a single binary operation (which we will call multiplication) satisfying three axioms:

(IDENTITY) There exists $\iota \in G$ satisfying $g\iota = \iota g = g$ for all $g \in G$.
(ASSOCIATIVITY) For all $g, h, k \in G$, we have $(gh)k = g(hk)$.
(INVERSES) For every $g \in G$, there exists $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = \iota$.

The order of a group G, denoted by $|G|$, is simply the number of elements in G. A subset $H \subseteq G$ is a *subgroup of* G (denoted by $H \leqslant G$) if H is also a group, using the same operation as in G (restricted, however, to the elements of H). Note that a subset of G is a subgroup iff it contains the identity element, and is closed under multiplication and the the taking of inverses. If G is a finite group ($|G| < \infty$) then by Lagrange's Theorem, every subgroup $H \leqslant G$ has order $|H|$ dividing $|G|$.

For our interests, the foremost examples of a group are permutation groups, and automorphism groups of fields.

Permutation Groups. Given a set Ω, a *permutation of* Ω is a bijection from Ω to itself. The set of all permutations of Ω forms a group under composition, called the *symmetric group of* Ω. This group is denoted $\operatorname{Sym}\Omega$. A *permutation group on* Ω is a subgroup of $\operatorname{Sym}\Omega$.

If Ω is finite, we often choose to label its elements using the first n positive integers: $\Omega = \{1, 2, \ldots, n\}$. We also abbreviate $S_n := \operatorname{Sym}\{1, 2, \ldots, n\}$. Permutations of $1, 2, \ldots, n$ are written in cycle notation, e.g. $\sigma = (1\,5\,4)(2\,6) \in S_6$ is the permutation

$$\sigma \,:\, 1 \mapsto 5 \mapsto 4 \mapsto 1; \quad 2 \mapsto 6 \mapsto 2; \quad 3 \mapsto 3.$$

In this case $\sigma^{-1} = (1\,4\,5)(2\,6)$; and if $\tau = (2\,3\,6\,4) \in S_6$ then

$$\sigma\tau = (1\,5\,4)(2\,6)(2\,3\,6\,4) = (1\,5\,4\,6)(2\,3), \qquad \tau\sigma = (2\,3\,6\,4)(1\,5\,4)(2\,6) = (1\,5\,2\,4)(3\,6).$$

(Following the Andersen-Feil textbook, we use 'right-to-left' composition of permutations. Many other textbooks, however, follow the convention of 'left-to-right' composition.) The fact that σ and τ do not commute ($\sigma\tau \neq \tau\sigma$) is evidence that S_6 is *nonabelian*. Note that $|S_n| = n!$; for example there are $3! = 6$ permutations of $\{1,2,3\}$:

$$\begin{aligned} S_3 = \langle (1\,2\,3),\,(1\,2)\rangle &= \{\iota,\,(1\,2\,3),\,(1\,3\,2),\,(1\,2),\,(1\,3),\,(2\,3)\};\\ \langle (1\,2\,3)\rangle &= \{\iota,\,(1\,2\,3),\,(1\,3\,2)\};\\ \langle (1\,2)\rangle &= \{\iota,\,(1\,2)\};\\ \langle (1\,3)\rangle &= \{\iota,\,(1\,3)\};\\ \langle (2\,3)\rangle &= \{\iota,\,(2\,3)\};\\ \langle \iota\rangle &= \{\iota\} \end{aligned}$$

where $\iota = ()$ is the identity permutation $x \mapsto x$ for all $x \in \{1,2,3\}$; and $\langle g_1, g_2, \ldots, g_k\rangle$ is the *subgroup of G generated by* $g_1, g_2, \ldots, g_k \in G$, i.e. the set of all group elements expressible as products of the generators $g_1, g_2, \ldots, g_n$ and their inverses.

Automorphism Groups of Fields. Let F be a field. An *automorphism of F* is a bijection $\sigma : F \to F$ such that

$$\sigma(a+b) = \sigma(a) + \sigma(b) \quad\text{and}\quad \sigma(ab) = \sigma(a)\sigma(b)$$

for all $a, b \in F$. The set of all automorphisms of F is a group under composition, denoted by $\operatorname{Aut} F$. We may view $\operatorname{Aut} F$ as a subgroup of $\operatorname{Sym} F$. For example, we have seen that $\operatorname{Aut}\mathbb{Q} = \{\iota\}$ and $\operatorname{Aut}\mathbb{R} = \{\iota\}$ where $\iota(x) = x$ for all x (the identity automorphism); also $\operatorname{Aut}\mathbb{C}$ contains at least two automorphisms ι, τ where $\tau(z) = \overline{z}$, the complex conjugate of z. (Actually $\operatorname{Aut}\mathbb{C}$ is very large; we will not take time here to digress on automorphisms of $\mathbb{C}$.) Also

$$\operatorname{Aut}\mathbb{F}_{p^r} = \langle \sigma \rangle = \{\iota, \sigma, \sigma^2, \ldots, \sigma^{r-1}\},$$

a cyclic group of order r generated by $\sigma : a \mapsto a^p$; thus $\sigma^j(a) = a^{p^j}$.

Permuting Roots of Polynomials. There is an important connection between the two classes of groups described above. Consider a polynomial (let's assume it's monic) with rational coefficients:

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_2t^2 + a_1t + a_0 \in \mathbb{Q}[t].$$

Suppose that α is a root of $f(t)$ in some extension field $E \supseteq \mathbb{Q}$, and let $\sigma \in \operatorname{Aut} E$. Recall that $\sigma(a) = a$ for all $a \in \mathbb{Q}$, so that

$$\begin{aligned} f(\sigma(\alpha)) &= \sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_2\sigma(\alpha)^2 + a_1\sigma(\alpha) + a_0 \\ &= \sigma(\alpha^n) + a_{n-1}\sigma(\alpha^{n-1}) + \cdots + a_2\sigma(\alpha^2) + a_1\sigma(\alpha) + a_0 \\ &= \sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \cdots + \sigma(a_2\alpha^2) + \sigma(a_1\alpha) + a_0 \\ &= \sigma\big(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_2\alpha^2 + a_1\alpha + a_0\big) \\ &= \sigma(0) \\ &= 0, \end{aligned}$$

i.e. $\sigma(\alpha)$ is also a root of $f(t)$. In other words, σ takes roots of $f(t)$ to roots of $f(t)$; and since σ is bijective, σ permutes the roots of $f(t)$. A slight generalization of this argument gives the following:

Theorem 1. Let $E \supseteq F$ be an extension field, and let $f(t) \in F[t]$. Let σ be any automorphism of F such that $\sigma(a) = a$ for all $a \in F$. Then σ permutes the roots (if any) of $f(t)$ in E.

Now suppose that $E \supseteq F$ is an extension in which $f(t)$ splits into linear factors as

$$f(t) = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n), \quad \alpha_j \in E.$$

(For this we can take $E = \overline{F}$, the algebraic closure of F. However, a smaller extension of F is always enough: we could get by with a finite extension $F[\alpha_1, \ldots \alpha_n] \supseteq F$.) In this case, if $\sigma \in \operatorname{Aut} E$ fixes every element of F, then σ permutes $\alpha_1, \ldots, \alpha_n$; essentially this gives and element of S_n.

A familiar special case is the following: Let $f(t) \in \mathbb{R}[t]$. Then complex conjugation permutes the complex roots of $f(t)$; in particular, for every root $\alpha \in \mathbb{C}$ of $f(t)$, either

- $\alpha \in \mathbb{R}$, in which case $t - \alpha$ is a real linear factor of $f(t)$; or
- we obtain a pair of complex conjugate roots $\{\alpha, \overline{\alpha}\}$. In this case $f(t)$ has an irreducible real quadratic factor $(t-\alpha)(t-\overline{\alpha}) = t^2 - bt + c \in \mathbb{R}[t]$ where $b = \alpha + \overline{\alpha}$ and $c = \alpha\overline{\alpha}$.

From Theorem 1 we obtain

Corollary 2. Let $E \supseteq \mathbb{Q}$ be an extension of degree n. Then $|\operatorname{Aut} E| \leqslant n$.

To prove Corollary 2, we require $\alpha \in E$ such that $\mathbb{Q}[\alpha] = E$. Such an element exists by another result (the Theorem of the Primitive Element) that we will not take time to prove now. Let $f(t)$ be the minimal polynomial of α over $\mathbb{Q}$. We may factor

$$f(t) = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)$$

where $\alpha_1 = \alpha$; without loss of generality $\alpha_1, \ldots, \alpha_k \in F$ where $1 \leqslant k \leqslant n$. If $\sigma \in \operatorname{Aut} F$ then by Theorem 1, $\sigma(\alpha) \in F$ is a root of $f(t)$, so $\sigma(\alpha) = \alpha_j$ for some $j \in \{1, 2, \ldots, k\}$. Each choice of j determines a unique automorphism of F given by

$$\sigma_j\big(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}\big) \;=\; a_0 + a_1\alpha_j + a_2\alpha_j^2 + \cdots + a_{n-1}\alpha_j^{n-1}$$

so $\operatorname{Aut} F = \{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ of order $k \leqslant n$. This proves Corollary 2.

Separability and Simple Extensions

When working with a finite field extension $E \supseteq F$, it is useful (as seen in Corollary 2) to have a single element $\alpha \in E$ such that $E = F[\alpha]$, i.e. $\alpha \in E$ is algebraic of degree n over F. So it is natural to ask: can we always assume that such an element exists? Fortunately for us, the answer is: yes, usually. Actually, in most cases we find that such an element α is hard to avoid: typically, almost every element of E has the properties required! For example, if $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ then $E = \mathbb{Q}[\alpha]$ where

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \quad a, b, c, d \in \mathbb{Q}$$

as long as no more than one of b, c, d is zero; so a 'randomly chosen' element $\alpha \in E$ works; in particular, a relatively simple choice is $\alpha = \sqrt{2} + \sqrt{3}$.

An extension $E \supseteq F$ is *simple* if $E = F(\alpha)$ for some $\alpha \in E$. The extension $E \supseteq F$ is *separable* if every element $\alpha \in E$ is a simple root of its minimal polynomial over F. We will use

Theorem 3 (Theorem of the Primitive Element). Every finite separable extension $E \supseteq F$ is simple: there exists $\alpha \in E$ such that $E = F[\alpha]$.

The proof of Theorem 3 is omitted. Recall that separability holds automatically in characteristic zero; also for finite fields (details will be found in another handout 'Some Consequences of Field Characteristic') which covers almost all extensions we study in this course. So on first exposure to this material, you should feel free to *ignore all references to separability.* A more complete version of Corollary 2 is the following:

Corollary 4. Let $E \supseteq F$ be a separable extension of degree $[E : F] = n$, and consider $G \leqslant \operatorname{Aut} E$ consisting of all $\sigma \in \operatorname{Aut} E$ such that $\sigma(a) = a$ for all $a \in F$. Then $|G| \leqslant n$.

Of course if F is the prime subfield of E (i.e. $\mathbb{Q}$ or $\mathbb{F}_p$) then every automorphism fixes every element of F, so the additional hypothesis holds automatically, and $|\operatorname{Aut} E| \leqslant n$ in this case.

We are most interested in those extensions $E \supseteq F$ attaining the upper bound of Corollary 3; these are *Galois extensions*. Before indicating which extensions have this property, we consider some examples.

Example 1: A Cyclic Extension of Degree 3

Let $f(t) = t^3 + t^2 - 2t - 1 \in \mathbb{Q}[t]$. We have seen that $f(t)$ is irreducible over $\mathbb{Q}$. Let $\alpha \in \mathbb{C}$ be a root of $f(t)$, so that

$$\begin{aligned} \alpha^3 &= 1 + 2\alpha - \alpha^2, && \\ \alpha^4 &= \alpha + 2\alpha^2 - \alpha^3 &&= -1 - \alpha + 3\alpha^2, \\ \alpha^5 &= -\alpha - \alpha^2 + 3\alpha^3 &&= 3 + 5\alpha - 4\alpha^2, \\ \alpha^6 &= 3\alpha + 5\alpha^2 - 4\alpha^3 &&= -4 - 5\alpha + 9\alpha^2, \end{aligned}$$

etc. It is straightforward to verify that $\beta = \alpha^2 - 2$ is also a root of $f(t)$:

$$\begin{aligned} f(\beta) &= \beta^3 + \beta^2 - 2\beta - 1 \\ &= (\alpha^2-2)^3 + (\alpha^2-2)^2 - 2(\alpha^2-2) - 1 \\ &= (\alpha^6-6\alpha^4+12\alpha^2-8) + (\alpha^4-4\alpha^2+4) - 2(\alpha^2-2) - 1 \\ &= \alpha^6 - 5\alpha^4 + 6\alpha^2 - 1 \\ &= 0 \end{aligned}$$

using the relations above. Now it is not hard to find a third root of $f(t)$: exactly the same reasoning shows that another root must be given by

$$\begin{aligned} \gamma &= \beta^2 - 2 \\ &= (\alpha^2 - 2)^2 - 2 \\ &= \alpha^4 - 4\alpha^2 + 2 \\ &= 1 - \alpha - \alpha^2. \end{aligned}$$

Alternatively, given that α and $\beta = \alpha^2 - 2$ are roots of $f(t)$, we could have used the fact that the three roots of $f(t)$ satisfy

$$\alpha{+}\beta{+}\gamma = -1; \qquad \alpha\beta{+}\alpha\gamma{+}\beta\gamma = -2; \qquad \alpha\beta\gamma = 1$$

to solve for $\gamma = -1 - \alpha - \beta = 1 - \alpha - \alpha^2$. Of course the same reasoning could be applied again: since γ is a root of $f(t)$, so is

$$\begin{aligned} \gamma^2 - 2 &= (1 - \alpha - \alpha^2)^2 - 2 \\ &= -1 - 2\alpha - \alpha^2 + 2\alpha^3 + \alpha^4 \\ &= -1 - 2\alpha - \alpha^2 + 2(1{+}2\alpha{-}\alpha^2) + (-1{-}\alpha{+}3\alpha^2) \\ &= \alpha. \end{aligned}$$

This should not be a surprise; since there are only three roots, eventually the map $x \mapsto x^2 - 2$ had to bring us back to the same root we started with.

The field $E = \mathbb{Q}[\alpha]$ has three automorphisms: $\operatorname{Aut} E = \{\iota, \sigma, \sigma^2\}$ where $\sigma : E \to E$ is defined by

$$\begin{aligned} \sigma\big(a + b\alpha + c\alpha^2\big) &= a + b\beta + c\beta^2 \\ &= (a{-}2b{+}3c) - c\alpha + (b{-}c)\alpha^2 \end{aligned}$$

for all $a, b, c \in \mathbb{Q}$. The map σ cyclically permutes $\alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$. In cycle notation we may write this as the 3-cycle $(\alpha\,\beta\,\gamma)$ (although most textbooks reserve the cycle notation for permutations of $1, 2, \ldots, n$ only). The fact that σ is an automorphism of E follows from our work above. To see that these are the *only* automorphisms of E, suppose that $\rho : E \to E$ is an automorphism. By Theorem 1, $\rho(\alpha) \in \{\alpha, \beta, \gamma\}$. If $\rho(\alpha) = \alpha$ then

$$\rho(a + b\alpha + c\alpha^2) = a + b\rho(\alpha) + c\rho(\alpha)^2 = a + b\alpha + c\alpha^2$$

so $\rho = \iota$, the identity automorphism. If $\rho(\alpha) = \beta$, then

$$\rho(a + b\alpha + c\alpha^2) = a + b\rho(\alpha) + c\rho(\alpha)^2 = a + b\beta + c\beta^2$$

so $\rho = \sigma$. Similarly, if $\rho(\alpha) = \gamma$, then $\rho = \sigma^2$.

The only subfields of E are $\mathbb{Q}$ and E itself; this is because for any intermediate field K we have

$$[E : K][K : \mathbb{Q}] = [E : \mathbb{Q}] = 3$$

so either $[E : K] = 1$ or $[K : \mathbb{Q}] = 1$. The subfields of E are in one-to-one correspondence with the subgroups of $G = \operatorname{Aut} E = \langle\sigma\rangle$:

$$\begin{tikzcd}
E \arrow[d, Rrightarrow, no head, "3"'] \arrow[dr, leftrightarrow] & G \arrow[d, Rrightarrow, no head, "3"] \arrow[dl, leftrightarrow] \\
\mathbb{Q} & \langle\iota\rangle
\end{tikzcd}$$

In general the correspondence takes a subgroup $H \leqslant G$ to its *fixed field* $\operatorname{Fix} H = \{a \in E : \sigma(a) = a \text{ for all } \sigma \in H\}$. Going in the other direction, we map a subfield $K \subseteq E$ to the subgroup $G_K = \{\sigma \in G : \sigma(a) = a \text{ for all } a \in K\}$. This correspondence reverses inclusion: if $K_1 \supseteq K_2$ are subfields of E, then $H_1 \leqslant H_2$ for the corresponding subgroups of G. Moreover in this case, the extension degree coincides with the subgroup index:

$$[K_1 : K_2] = [H_2 : H_1].$$

Even more is true: double lines on the right, which indicate normality of subgroups, correspond to double lines on the left, representing normality of field extensions (which we have not defined yet). Further definitions and results, are postponed until after another example of a field extension.

Example 2: A Noncyclic Extension of Degree 3

Let $f(t) = t^3 - 2 \in \mathbb{Q}[t]$. Again, this is irreducible over $\mathbb{Q}$. Let $\theta = \sqrt[3]{2}$, the unique real root of $f(t)$; and $K = \mathbb{Q}[\theta]$, a cubic extension of $\mathbb{Q}$. Then $f(t)$ factors into irreducible factors in $K[t]$ as

$$f(t) = t^3 - 2 = (t - \theta)(t^2 + \theta t + \theta^2).$$

Note that the discriminant of the quadratic factor is $-3\theta^2 < 0$; and since $K \subset \mathbb{R}$, this means that the quadratic factor is in fact irreducible over K. Any automorphism of K must map $\theta \mapsto \theta$ (since θ is the only root of $f(t)$ in K) so it must map $a+b\theta+c\theta^2 \mapsto a+b\theta+c\theta^2$ for all $a, b, c \in \mathbb{Q}$; and this is the identity automorphism of K. So $\operatorname{Aut} K = \{\iota\}$, in contrast to what happened in Example 1 above.

The defect of K is that it is not large enough to contain all the roots of $f(t)$: it is not a splitting field for $f(t)$. A *splitting field* for a polynomial $f(t)$ is an extension field over which $f(t)$ splits into linear factors.

A splitting field for our polynomial $f(t)$ is given by the larger extension $E = K[\omega] = \mathbb{Q}[\theta, \omega]$ where $\omega = e^{2\pi i/3} = \frac{1}{2}\big(-1 + i\sqrt{3}\big)$. In $E[t]$ we have

$$f(t) = (t - \theta)(t - \omega\theta)(t - \omega^2\theta).$$

Now $G = \operatorname{Aut} E$ contains an automorphism τ given by complex conjugation. Here

$$\tau(\omega) = \overline{\omega} = \omega^2 = -1 - \omega$$

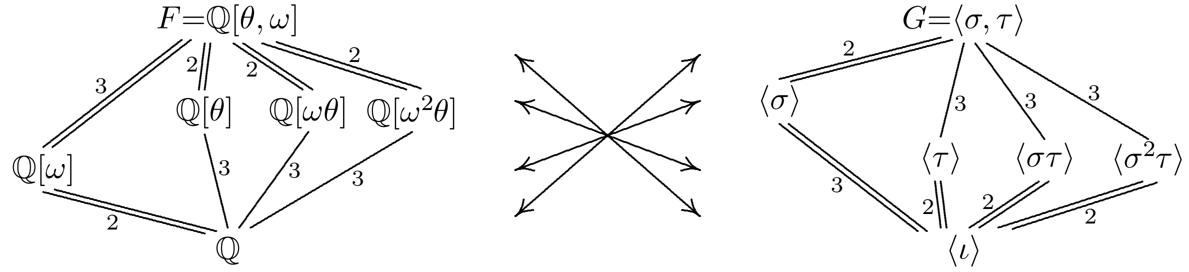
since the minimal polynomial of ω over $\mathbb{Q}$ is $t^2 + t + 1$. Since $\theta \in \mathbb{R}$ we have $\tau(\theta) = \theta$. By Theorem 1 there is also an automorphism $\sigma : E \to E$ taking θ to $\omega\theta$. We may assume that σ takes $\omega\theta$ to the third root $\omega^2\theta$; otherwise replace σ by $\sigma\tau$. Now in cycle notation the three roots of $f(t)$ are permuted by σ and τ as

$$\sigma = (\theta\ \ \omega\theta\ \ \omega^2\theta); \qquad \tau = (\omega\theta\ \ \omega^2\theta).$$

These two permutations behave just like $(1\,2\,3)$ and $(2\,3)$ which generate S_3. We obtain

$$G = \operatorname{Aut} F = \langle \sigma, \tau \rangle \cong S_3.$$

Just as $G \cong S_3$ has six subgroups, F has exactly six subfields and a one-to-one correspondence between subgroups of G and subfields of F is shown by


$F{=}\mathbb{Q}[\theta,\omega]$
$\mathbb{Q}[\theta]$
$\mathbb{Q}[\omega\theta]$
$\mathbb{Q}[\omega^2\theta]$
$\mathbb{Q}[\omega]$
$\mathbb{Q}$
3
2
2
2
2
3
3
3
$G{=}\langle\sigma,\tau\rangle$
$\langle\sigma\rangle$
$\langle\tau\rangle$
$\langle\sigma\tau\rangle$
$\langle\sigma^2\tau\rangle$
$\langle\iota\rangle$
2
3
3
3
3
2
2
2

The Fundamental Theorem of Galois Theory

As intimated by our examples, the Fundamental Theorem of Galois Theory gives a bijective correspondence between the intermediate fields of a field extension $E \supseteq F$, and the group of automorphisms of the field extension. This correspondence is most readily described if the extension satisfies three conditions:

- We assume $n = [E : F]$ is finite, and in particular the extension $E \supseteq F$ is algebraic. While much of the theory generalizes to extensions of infinite degree, we will not concern ourselves with these complications.

- The extension $E \supseteq F$ is *separable*. This means that every element $a \in E$ is a simple root of its minimal polynomial over F. Recall that this condition automatically holds for fields of characteristic zero; it also holds whenever E and F are finite. Typically, we implicitly assume the extension is separable, and not worry about it.
- The extension $E \supseteq F$ is *normal*. This means that for every $a \in E$, the minimal polynomial of a over F splits into linear factors over E. In other words, every polynomial $f(t) \in F[t]$ of degree k, irreducible in $F[t]$ but having a root in E, actually has k (distinct) roots in E. Equivalently, E is the splitting field of some irreducible polynomial $f(t) \in F[t]$, i.e. $E = F[\alpha_1, \alpha_2, \ldots, \alpha_n]$ where $f(t) = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)$ in $E[t]$. As we saw in Example 2, if this condition is not fulfilled, then the remedy is to further extend E to a finite extension which is normal.

An extension $E \supseteq F$ satisfying the three conditions above (i.e. a finite normal separable extension) is called a *Galois extension*.

An automorphism $\sigma \in \operatorname{Aut} E$ such that $\sigma(a) = a$ for all $a \in F$ is called an *F-automorphism of E*. The set of all F-automorphisms of E form a subgroup of $\operatorname{Aut} E$ denoted by $G(E/F) \leqslant \operatorname{Aut} E$. Corollary 4 has a more complete version, given by

Theorem 5. Let $E \supseteq F$ be a separable extension of degree $n = [E : F]$. Then $|G(E/F)| \leqslant n$; and equality holds iff the extension $E \supseteq F$ is normal (and hence Galois).

Let us abbreviate $G = G(E/F)$. We assume equality holds in Theorem 5. In this case, $G = G(E/F)$ is called the *Galois group* of the extension $E \supseteq F$. To every intermediate field K, $E \supseteq K \supseteq F$, we associate the group $G(E/K)$ of all K-automorphisms of E; and to every subgroup $H \leqslant G$ we associate the intermediate subfield $\operatorname{Fix} H = \{a \in E : \sigma(a) = a$ for all $\sigma \in H\}$. By the *Fundamental Theorem of Galois Theory*, we have a bijective correspondence, called the *Galois correspondence*:

$$\left\{\begin{matrix}\text{intermediate fields} \\ \text{between } E \text{ and } F\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{subgroups of} \\ G = G(E/F)\end{matrix}\right\}$$

given by

$$K \longmapsto G(E/K)$$

$$\operatorname{Fix}(H) \longleftarrow\!\shortmid H$$

Given subgroups $H_1, H_2 \leqslant G$ and corresponding intermediate subfields K_1, K_2, we have

$$H_1 \leqslant H_2 \;\Leftrightarrow\; K_1 \supseteq K_2,$$

i.e. the Galois correspondence is order-reversing. Assuming containment as in the previous line, index of subgroups equals degree of extension:

$$[H_2 : H_1] = [K_1 : K_2]$$

and normality is preserved: H_1 is normal in H_2, iff K_1 is a normal extension of K_2. Moreover in the latter case of normality,

$$G(K_1/K_2) \cong H_2/H_1\,.$$

Example 3: Quadratic Extensions

Unlike cubic extensions, which are not necessarily Galois (as we noted in the previous examples), quadratic separable extensions of fields are always Galois. So if $E \supseteq F \supseteq \mathbb{Q}$ is a tower of fields with $[E : F] = 2$, then there is necessarily an automorphism $\tau \in \operatorname{Aut} E$ of order two (τ^2 is the identity) such that $\tau(a) = a$ for all $a \in F$, and $G(E/F) = \langle\tau\rangle = \{\iota, \tau\}$. This corresponds to the fact (from group theory) that subgroups of index 2 are necessarily normal.

Example 4: Finite Fields

Let $q = p^r$ where $r \geqslant 1$ and p is prime. There is a unique field $\mathbb{F}_q$ of order q, and the extension $\mathbb{F}_q \supseteq \mathbb{F}_p$ is Galois. Its Galois group is

$$G = G(\mathbb{F}_q/\mathbb{F}_p) = \langle\sigma\rangle = \{\iota, \sigma, \sigma^2, \ldots, \sigma^{r-1}\}$$

where $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ is given by $\sigma(a) = a^p$, so that $\sigma^j(a) = a^{p^j}$. Since G is cyclic, the extension $\mathbb{F}_q \supseteq \mathbb{F}_p$ is called *cyclic.*

Abel's Theorem

Niels Abel (1802-1829) used Galois Theory to answer one of the most classical problems of mathematics: For which polynomials $f(t)$ can one express the roots of the polynomial in terms of the coefficients using only the elementary field operations of addition and subtraction, multiplication an division, and powers or roots? While this was known to

be possible for polynomials of degree at most 4, the case of degree 5 remained elusive until Abel's Theorem showed that in general, such a solution does not exist. For example, consider the irreducible polynomials[1]

$$\begin{aligned} f_1(t) &= t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1 \\ f_2(t) &= t^5 - 5t + 12 \\ f_3(t) &= t^5 - 2 \\ f_4(t) &= t^5 + 20t + 16 \\ f_5(t) &= t^5 - 4t + 2 \end{aligned}$$

Of these five examples, the first three have roots expressible in terms of basic field operations including radicals. The corresponding Galois groups, as subgroups of S_5, are isomorphic to

$$\begin{aligned} \langle(1\,2\,3\,4\,5)\rangle &\text{ (a cyclic group of order 5);} \\ \langle(1\,2\,3\,4\,5),\ (2\,5)(3\,4)\rangle &\text{ (a dihedral group of order 10);} \\ \langle(1\,2\,3\,4\,5),\ (1\,2\,4\,3)\rangle &\text{ (a Frobenius group of order 20);} \\ \langle(1\,2\,3\,4\,5),\ (1\,2\,3)\rangle &\cong A_5 \text{ (the alternating group of order 60);} \\ \langle(1\,2\,3\,4\,5),\ (1\,2)\rangle &\cong S_5 \text{ (the symmetric group of order 120)} \end{aligned}$$

respectively. The first three of these groups are solvable, whereas the last two are nonsolvable; this accounts for the statements above concerning roots of the corresponding polynomials. By the earliest results of Galois theory, every irreducible $f(t) \in \mathbb{Q}[t]$ of degree 5 has a Galois group G containing a 5-cycle; and the five examples above illustrate all possible cases for G that can arise.

[1] See D. J. H. Garling, *A Course in Galois Theory,* Cambridge Univ. Press, 1986.