I.G. Automorphisms and fixed fields

Begin with a field L and its group $\mathrm{Aut}(L)$ of automorphisms. To each subfield $K \subset L$ we can associate the subgroup

$$\mathrm{Aut}(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(k) = k \ (\forall k \in K)\} \leq \mathrm{Aut}(L)$$

of automorphisms over K, which we will denote sometimes by the shorthand notation "$\Gamma(K)$". Similarly, to each subgroup (or even sub*set*) $G \leq \mathrm{Aut}(L)$ we may associate the subfield

$$\mathrm{Inv}(G) := \{\ell \in L \mid \sigma(\ell) = \ell \ (\forall g \in G)\} \subseteq L$$

of elements invariant under G, or "$\Phi(G)$" for short.[21]

One notices immediately that both of these operations are *contravariant* in the sense of reversing inclusions:

$$\text{(I.G.1)} \qquad \begin{cases} G_1 \supseteq G_2 \implies \mathrm{Inv}(G_1) \subseteq \mathrm{Inv}(G_2) \\ K_1 \supseteq K_2 \implies \mathrm{Aut}(L/K_1) \subseteq \mathrm{Aut}(L/K_2) \end{cases}$$

That is, a larger set of automorphisms leaves a smaller field invariant, and a larger subfield has a smaller group of automorphisms fixing it. Yes, that's nice, but how are the two operations *related?*

I know what you really want to hear is "they produce a bijection between subfields of L and subgroups of $\mathrm{Aut}(L)$, and are inverse to each other." We will eventually reach such a statement, but you will have to settle for a weaker, preliminary result at this stage:

I.G.2. PROPOSITION. *Let $\mathcal{A} \subseteq \mathrm{Aut}(L)$ be a subset, $\langle \mathcal{A} \rangle$ the subgroup it generates, and $K \subset L$ a subfield. Then:*

(i) $\Gamma\Phi(\mathcal{A}) \supseteq \mathcal{A}$.
(ii) $\Phi\Gamma(K) \supseteq K$.
(iii) $\Phi\Gamma\Phi(\mathcal{A}) = \Phi(\mathcal{A})$.
(iv) $\Gamma\Phi\Gamma(K) = \Gamma(K)$.
(v) $\Phi(\langle \mathcal{A} \rangle) = \Phi(\mathcal{A})$.

We can read (i) as saying that $\mathcal{A}$ is among the automorphisms fixing its fixed field (though there may be more), and (ii) as saying that

[21] This is also called the "fixed field" of G, hence the "Φ".

K is invariant by the automorphisms fixing it (though they may fix a larger subfield). Even better, (iii) and (iv) suggest that on subfields arising as fixed fields, and subgroups arising as "Galois groups",[22] we do get something like a bijection. On the other hand, (v) asserts that, if we don't restrict at least to sub*groups*, we definitely *don't* get a bijection.

PROOF. (i) and (ii) are clear (see the above paragraph). For (iii), take $K = \Phi(\mathcal{A})$ and apply (ii) to get "$\supseteq$"; and apply Φ to (i) (and use (I.G.1)) to get "$\subseteq$". For (iv), use a symmetric argument.

Finally, by (i), $\Gamma\Phi(\mathcal{A})$ is a group containing $\mathcal{A}$, hence contains $\langle\mathcal{A}\rangle$ (the minimal such group). Applying Φ (and (I.G.1) and (iii)) to $\mathcal{A} \subset \langle\mathcal{A}\rangle \subset \Gamma\Phi(\mathcal{A})$ gives $\Phi(\mathcal{A}) \supset \Phi(\langle\mathcal{A}\rangle) \supset \Phi\Gamma\Phi(\mathcal{A}) = \Phi(\mathcal{A})$, hence the equality in (v). $\square$

Now given a subgroup $G = \{\sigma_1, \ldots, \sigma_{|G|}\} \leq \mathrm{Aut}(L)$ and an element $\lambda \in L$, consider the *orbit vector*

$$\lambda^G := (\sigma_1(\lambda), \ldots, \sigma_{|G|}(\lambda)) \in L^{|G|},$$

where by $L^{|G|}$ we simply mean the L-vector space of dimension $|G|$.

I.G.3. LEMMA. *Set $K := \mathrm{Inv}(G)$, and let $\Lambda \subset L$ be a subset. Then the following are equivalent:*

(a) *Λ is linearly independent over K.*
(b) *$\{\lambda^G\}_{\lambda\in\Lambda}$ is linearly independent over K.*
(c) *$\{\lambda^G\}_{\lambda\in\Lambda}$ is linearly independent over L.*

PROOF. (c) $\Longrightarrow$ (b): This is obvious.

(b) $\Longrightarrow$ (a): If (a) fails, there exist $\lambda_1, \ldots, \lambda_r \in \Lambda$ such that $\sum_{i=1}^r k_i\lambda_i = 0$ with all $k_i \in K^*$. Since K is fixed by G, $\sum_{i=1}^r k_i\sigma_j(\lambda_i) = 0$ for each $\sigma_j \in G$. Thus $\sum_{i=1}^r k_i\lambda_i^G = 0$ and (b) fails.

(a) $\Longrightarrow$ (c): If (c) fails, let $\sum_{i=1}^r \ell_i\lambda_i^G = 0$ be a nontrivial relation ($\lambda_i \in \Lambda$, $\ell_i \in L^*$) with minimal $r\,(> 1)$. That is, for each $\sigma \in G$, we have

[22] in **[Jacobson]**'s more general sense

$\sum_{i=1}^{r} \ell_i \sigma(\lambda_i) = 0$. Fixing any $g \in G$, we replace σ by $g^{-1}\sigma$ and apply g to get $\sum_{i=1}^{r} g(\ell_i)\sigma(\lambda_i) = 0$, so that

$$\begin{aligned} 0 &= \ell_r \textstyle\sum_{i=1}^{r} g(\ell_i)\sigma(\lambda_i) \; - \; g(\ell_r)\sum_{i=1}^{r} \ell_i \sigma(\lambda_i) \\ &= \textstyle\sum_{i=1}^{r-1} (g(\ell_i)\ell_r - g(\ell_r)\ell_i)\sigma(\lambda_i). \end{aligned}$$

By minimality of r, each coefficient in the last sum must be 0: so $g(\ell_i)\ell_r = g(\ell_r)\ell_i \implies g(\ell_i/\ell_r) = \ell_i/\ell_r$. Since g was arbitrary, $\ell_i/\ell_r \in \mathrm{Inv}(G) = K$. The $\sigma = \mathrm{id}$ component of $\sum_{i=1}^{r} \frac{\ell_i}{\ell_r} \lambda_i^G = 0$ now reads $\sum_{i=1}^{r} \frac{\ell_i}{\ell_r} \lambda_i = 0$, so that (a) fails. □

From this Lemma we now deduce our first big advance towards the Galois correspondence:

I.G.4. THEOREM. *Assume $G \leq \mathrm{Aut}(L)$ is finite. Then $L/\mathrm{Inv}(G)$ is Galois, $G = \mathrm{Aut}(L/\mathrm{Inv}(G))$ $(= \Gamma\Phi(G))$, and $|G| = [L{:}\mathrm{Inv}(G)]$.*

PROOF. Set $K = \mathrm{Inv}(G)$.

Let $\Lambda \subset L$ be a subset which is linearly independent over K; in particular, we may take $|\Lambda| = [L{:}K]$. By the Lemma, the orbit vectors $\{\lambda^G\}_{\lambda \in \Lambda} \subset L^{|G|}$ are linearly independent over L. Since $\dim_L(L^{|G|}) = |G|$, we must have $|\Lambda| \leq |G|$ hence $[L{:}K] \leq |G|$.

On the other hand, by I.G.2(i) $G \leq \mathrm{Aut}(L/K)$, and by I.F.21 $|\mathrm{Aut}(L/K)| \leq [L{:}K]$ hence $|G| \leq [L{:}K]$. Conclude that $|G| = [L{:}K]$, forcing $G = \mathrm{Aut}(L/K)$, and by I.F.21 again, that L/K is Galois. □

Suppose now we are given any field extension L/K. The following is then immediate from I.G.4:

I.G.5. COROLLARY. *Let $G \leq \mathrm{Aut}(L/K)$ be a finite subgroup, and put $M := \mathrm{Inv}(G)$. Then L/M is finite and normal (and separable).*

(Of course, M/K could still be a mess — in particular, non-normal.)

In contrast to the last Theorem and Corollary, if we start with a subfield instead of a subgroup, we arrive at the following:

I.G.6. PROPOSITION. *Let $K \subset L$ be a subfield with $[L{:}K]$ finite, and put $G := \mathrm{Aut}(L/K)$. Then L/K is Galois $\iff$ $K = \mathrm{Inv}(G)$ $(\iff |G| = [L{:}K])$. Otherwise, $K \subsetneq \mathrm{Inv}(G)$ (and $|G| < [L{:}K]$).*

PROOF. The statements about $|G|$ and $[L{:}K]$ are from I.F.21; in particular, $|G| < \infty$. So I.G.4 applies, and $|G| = [L{:}\mathrm{Inv}(G)]$. Also, we know that $K \subseteq \mathrm{Inv}(G)$ from I.G.2(ii).

So if L/K is Galois, then $|G| = [L{:}K] \implies [L{:}\mathrm{Inv}(G)] = [L{:}K]$ forces $\mathrm{Inv}(G) = K$. If L/K is not Galois, then $|G| < [L{:}K] \implies [L{:}\mathrm{Inv}(G)] < [L{:}K] \implies [\mathrm{Inv}(G){:}K] > 1 \implies \mathrm{Inv}(G) \supsetneq K$. □

Here are some examples from **[Jacobson]**:

I.G.7. EXAMPLE. Assuming $\mathrm{char}(K) \neq 2$, and that $a \in K$ has no square root in K, we consider the quadratic extension $L := K[x]/(x^2 - a)$. Writing u for the image of x, sending $u \mapsto -u$ induces a nontrivial automorphism of L/K, namely[23] $\sigma(k_1 + k_2 u) := k_1 - k_2 u$. Between this and id_L, we can't have any more, since $|\mathrm{Aut}(L/K)| \leq [L{:}K] = 2$. (To see there are two, you could also use the fact that L/K is a splitting field hence Galois.) So $\mathrm{Aut}(L/K) \cong \mathbb{Z}_2$.

I.G.8. EXAMPLE. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since this is a splitting field for $(x^2 - 2)(x^2 - 3)$ (hence Galois), and has degree $[L{:}K] = 4$, we must have $|\mathrm{Aut}(L/K)| = 4$. Alternatively, you can construct the 4 automorphisms and deduce L/K is Galois from that. In fact, $\mathrm{Aut}(L/K)$ is the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$, with $\sigma_{(m,n)}$ sending $\sqrt{2} \mapsto (-1)^m \sqrt{2}$ and $\sqrt{3} \mapsto (-1)^n \sqrt{3}$.

I.G.9. EXAMPLE. Consider an imperfect field K of characteristic p, and $\alpha \in K \setminus \phi(K)$. Then $f(x) := x^p - \alpha$ is irreducible and inseparable, becoming (by I.E.9) a p^{th} power $(x - u)^p$ in a splitting field $L = K(u) := K[x]/(f(x))$. Since an automorphism of L/K must send any root of f to another root, it sends $u \mapsto u$ hence is the identity. So $\mathrm{Aut}(L/K) = \{\mathrm{id}_L\}$ is trivial, which also implies L/K is not Galois, but we already knew that.

I.G.10. EXAMPLE. For a transcendental extension, look at $L = K(t)$, the rational function field in the indeterminate t. Any automorphism must send t to another generator $u = f(t)/g(t)$ of L (where

[23]Or you can just invoke the general result I.C.21(i).

$f, g \in K[t]$ are coprime). Since $F(t) := f(t) - ug(t)$ is irreducible over $K[u]$ hence (by Gauss) $K(u)$, $K(t) = K(u)[t]/(F(t))$ has degree $d := \max(\deg(f), \deg(g))$ over $K(u)$, which means u is a generator (i.e. $K(u) = K(t)$) iff $d = 1$. Conclude that $u = (at+b)/(ct+d)$, with $ad - bc \neq 0$ so that f and g are indeed coprime.

In other words, the automorphisms are pullback maps along "fractional linear transformations", and we have $\mathrm{Aut}(L/K) \cong \mathrm{PSL}_2(K)$: to each $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}_2(K)$, we associate σ_M sending $t \mapsto \sigma_M(t) := \frac{at+b}{ct+d}$, and then any rational expression $R(t) \in L$ has $\sigma_M(R(t)) = R(\sigma_M(t))$.

Galois groups.

The first three examples above concern groups of automorphisms of splitting field extensions. These are closely related to (algebraically consistent) permutations of roots of the corresponding polynomial, whose investigation was the original purpose of Galois's theory. Here are some things we already know regarding automorphisms of a SFE L/K for f:

- Any such automorphism sends roots of f to roots of f: for any root α, $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$.
- If an automorphism of an SFE L/K for f fixes all the roots of f, then it is the identity, since L is generated by these roots.
- If g is (over K) an irreducible factor of f, and α and β are two roots of g, then there exists an automorphsim sending $\alpha \mapsto \beta$ (cf. I.C.21).

These are clearly at the heart of the whole story, so the following seems almost overdue:

I.G.11. Definition. The **Galois group** of a polynomial $f \in K[x]$ is[24]

$$\mathrm{Gal}_K(f) := \mathrm{Aut}(L/K),$$

where L/K is a splitting field extension for f.

[24]This is well-defined, since (by I.C.19) splitting fields are unique up to isomorphism.

In this context, I.G.6 translates[25] to the statement

$$\text{(I.G.12)}\qquad \begin{cases} \text{(i) } |\mathrm{Gal}_K(f)| = [L{:}K] \\ \text{(ii) } K = \mathrm{Inv}(\mathrm{Gal}_K(f)) \subset L \end{cases} \iff f \text{ separable.}$$

If f is inseparable, then both (i) and (ii) fail: $|\mathrm{Gal}_K(f)| < [L{:}K]$, and $\mathrm{Inv}(\mathrm{Gal}_K(f))$ is bigger than K. On the other hand, if K is perfect, then *(i) and (ii) are true for any polynomial*.

As for permutations of roots, we may interpret I.G.12 as saying that $|\mathrm{Gal}_K(f)| = [L{:}K]$ if there are enough roots to permute: the roots in *irreducible factors* of f must be distinct. On the other hand, even if f is both irreducible and separable (of degree n), we cannot expect that all $n!$ possible permutations of the roots are realized by $\mathrm{Gal}_K(f)$: only the permutations "preserving algebraic relations" amongst the roots *should* be allowed. Here are some specific computations that begin to clarify the various possibilities; for the first three, $K = \mathbb{Q}$.

I.G.13. EXAMPLE. $f(x) = x^4 + x^3 + x^2 + x + 1$, $L/K = \mathbb{Q}(\zeta_5)/\mathbb{Q}$: since $[L{:}K] = 4$, we have $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_4$ or V_4. Let σ be an automorphism sending the root $\zeta_5 \mapsto \zeta_5^2$. Since L is generated by ζ_5, this determines σ. Clearly, this must also send $\zeta_5^j \mapsto \zeta_5^{2j}$ in order to be a field homomorphism — an instance of what is meant by "preserving algebraic relations". Finally, we have $\sigma^2(\zeta_5) = \zeta_5^4 \implies \sigma \neq \mathrm{id}_L \implies \mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_4$.

I.G.14. EXAMPLE. $f(x) = (x^2-2)(x^2-3)$, $L/K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$: from I.G.8, we have $\mathrm{Gal}_{\mathbb{Q}}(f) \cong V_4$.

I.G.15. EXAMPLE. $f(x) = x^3 - 2$, $L/K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$: since $[L{:}K] = 6$, $\mathrm{Gal}_{\mathbb{Q}}(f)$ must be a group of order 6; and since there are three roots, it must be a subgroup of $\mathfrak{S}_3$. So it *is* $\mathfrak{S}_3$. To see this more explicitly: consider the intermediate fields $M_j = \mathbb{Q}(\zeta_3^j \sqrt[3]{2})$, over each of which $L = M(\zeta_3)$ is a SFE for $x^2 + x + 1$. By I.C.21, we have (for

[25] Since SFEs for a polynomial are already finite and normal, we can read "L/K is Galois" as "L/K (equiv. f) is separable." Of course, (i) and (ii) are equivalent; I am just placing a different emphasis here.

each j) an automorphism σ_j fixing M_j and sending $\zeta_3 \mapsto \zeta_3^2$; evidently this fixes one root of x^3-2 and swaps the other two. For the cyclic permutations, take $M = \mathbb{Q}(\zeta_3)$, over which f remains irreducible, and argue in the same way.

I.G.16. EXAMPLE. $f(x) = x^p - \alpha$ irreducible ($\alpha \in K \setminus \phi(K)$), $\mathrm{char}(K) = p$, $L = K(\sqrt[p]{\alpha})$: since f is $(x - \sqrt[p]{\alpha})^p$ in $L[x]$, $\mathrm{Gal}_K(f) = \{1\}$. Note that our setup, by requiring $\phi(K) \neq K$ (hence K imperfect), means K cannot be a finite field or algebraically closed.

Let's formalize our observations: given $f \in K[x]$ of degree n, with splitting field extension L/K, write

$$\mathcal{R}_f := \{r \in L \mid f(r) = 0\}$$

for its roots in L. Obviously $|\mathcal{R}_f| \leq n$, with equality if (say) f is irreducible and separable.

I.G.17. THEOREM. (i) *Restricting automorphisms to $\mathcal{R}_f$ induces an injective group homomorphism*

$$\Theta \colon \mathrm{Gal}_K(f) \hookrightarrow \mathfrak{S}_{\mathcal{R}_f},$$

or equivalently, a group action of $\mathrm{Gal}_K(f)$ *on $\mathcal{R}_f$. In particular, we have* $|\mathrm{Gal}_K(f)| \leq n!$.

(ii) *If f is irreducible, then this action is transitive. In particular, if f is irreducible and separable, then* $|\mathrm{Gal}_K(f)| \geq n$.

(iii) *If $|\mathcal{R}_f| = n$ and* $\mathrm{Gal}_K(f)$ *acts transitively, then f is irreducible.*

PROOF. (i) We know that $\sigma \in \mathrm{Gal}_K(f)$ acts on the roots. Since $L = K(\mathcal{R}_f)$ is generated over K by the roots, if that action is trivial, σ is too. So $\ker(\Theta) = \{\mathrm{id}_L\}$.

(ii) is again I.C.21, which gives at least $|\mathcal{R}_f|$ automorphisms.

(iii) Given $\alpha \in \mathcal{R}_f$ with $m_\alpha \in K[x]$; by assumption, for each $\beta \in \mathcal{R}_f$, there exists a $\sigma \in \mathrm{Gal}_K(f)$ with $\sigma(\alpha) = \beta$. Hence $m_\alpha(\beta) = m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0$. Conclude that m_α has $|\mathcal{R}_f| = n$ distinct roots, which together with irreducibility of m_α and $m_\alpha | f$ makes $m_\alpha \sim f$ hence f irreducible. $\square$

I.G.18. EXAMPLE. Let $K = \mathbb{Q}$. What are the possible Galois groups of an *irreducible* polynomial of degree $n = 3$, 4, or 5? Clearly it has order between n and $n!$, and dividing $n!$. But the real key is the transitivity of the action: we say that a subgroup of $\mathfrak{S}_n$ is *transitive* if the "tautological" action on $\{1, \ldots, n\}$ is transitive. Imposing this constraint leaves us with the lists of possibilities (up to conjugation/isomorphism):

- in $\mathfrak{S}_3$: $\mathbb{Z}_3$ and $\mathfrak{S}_3$;
- in $\mathfrak{S}_4$: $\mathbb{Z}_4$, V_4, D_4, $\mathfrak{A}_4$, and $\mathfrak{S}_4$;
- in $\mathfrak{S}_5$: $\mathbb{Z}_5$, D_5, W_5, $\mathfrak{A}_5$, $\mathfrak{S}_5$. (Here W_5 is an extension of $\mathbb{Z}_4$ by $\mathbb{Z}_5$.)

Here V_4 is tricky: its realization $\{\mathbf{1}, (12), (34), (12)(34)\}$ as a subgroup of $\mathfrak{S}_4$ is *not* transitive — this corresponds to our reducible polynomial from I.G.14 — while $\{\mathbf{1}, (12)(34), (13)(24), (14)(23)\}$ is.

So where is our cubic with Galois group $\mathbb{Z}_3$? It's the polynomial from our first example, $f(x) = x^3 - 3x - 1$ from I.A.2. If θ is a root, we showed there that $\mathcal{R}_f \subset \mathbb{Q}(\theta)$. So $L = \mathbb{Q}(\theta)$ is cubic, whence $|\mathrm{Gal}_K(f)| = 3$.

We will be in a position later to show that all the groups listed above do occur; for now, we just do one example.

I.G.19. EXAMPLE. Consider $f(x) = x^5 - 4x + 2$, which is irreducible over $K = \mathbb{Q}$ by Eisenstein. Since $f'(x) = 5x^4 - 4$ has 2 real zeroes, f has no more than 3; and $f(-2) = -22$, $f(0) = 2$, $f(1) = -1$ show (by the IVT) that indeed f has exactly 3 real roots. We may conclude at once that $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathfrak{S}_5$, due to the fabulous

I.G.20. PROPOSITION. *If $f \in \mathbb{Q}[x]$ is irreducible of prime degree p, with exactly $p - 2$ real roots, then* $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathfrak{S}_p$.

I.G.21. LEMMA. (i) *If $G \leq \mathfrak{S}_{\mathrm{X}}$ is a group action on a finite set* X, *then*

$$x \sim y \iff \{x = y \ \text{ or } \ G \ni (x\, y)\}$$

defines an equivalence relation.

(ii) *If G acts transitively on* X, *then* (*denoting the equivalence class of x by $\mathcal{E}_x$*) *for all $x, y \in \mathrm{X}$, we have $|\mathcal{E}_x| = |\mathcal{E}_y|$.*

(iii) *If G acts transitively and contains a transposition, and $|X|$ is prime, then $G = \mathfrak{S}_X$.*

PROOF. (i) We only need to check transitivity, which follows from $(x\,y)(y\,z)(x\,y) = (x\,z)$.

(ii) Let $\sigma(x) = y$. Then $\sigma(x\,x')\sigma^{-1} = (y\,\sigma(x')) \implies \sigma(\mathcal{E}_x) \subseteq \mathcal{E}_y$ (and vice-versa).

(iii) If there is a transposition, then for some (hence every) x, $e := |\mathcal{E}_x| > 1$. Clearly (by (ii)) e must divide $|X|$, whence $e = p$. That is, X is a single equivalence class, and so G must contain all transpositions (which generate $\mathfrak{S}_X$). $\square$

PROOF OF I.G.20. Let $L \subset \mathbb{C}$ be the SFE for $f \in \mathbb{Q}[x]$. Since f is irreducible, $\mathrm{Gal}_{\mathbb{Q}}(f)$ acts transitively on $\mathcal{R}_f = \{r_1, \ldots, r_{p-2}, \alpha, \bar{\alpha}\}$. (Any nonreal root of a real polynomial has a complex-conjugate root.) Evidently L is closed under complex conjugation, which therefore gives an element $\rho \in \mathrm{Gal}_{\mathbb{Q}}(f)$ acting on $\mathcal{R}_f$ through a transposition. Now apply I.G.21(iii). $\square$

The Galois Correspondence.

I will state a slightly more general result than **[Jacobson]**. Suppose we have any finite extension L/K. Let $G := \mathrm{Aut}(L/K)$ and $K_0 := \mathrm{Inv}(G)$; by I.F.21 and I.G.4, $G = \mathrm{Aut}(L/K_0)$. (If we start with L/K Galois, then $K = K_0$ by I.G.6.)

I.G.22. FUNDAMENTAL THEOREM OF GALOIS THEORY. (i) *Taking fixed fields and automorphism groups induces a bijection:*

$$\begin{tikzcd} \boxed{\begin{matrix}\textit{subgroups}\\ H \leq G\end{matrix}} \arrow[r, bend left, "\mathrm{Inv}(\cdot)"] & \boxed{\begin{matrix}\textit{subfields } M \subset L\\ \textit{containing } K_0\end{matrix}} \arrow[l, bend left, "\mathrm{Aut}(L/\cdot)"] \end{tikzcd}$$

(ii) $H_1 \geq H_2 \iff \mathrm{Inv}(H_1) \subseteq \mathrm{Inv}(H_2)$.

(iii) $|H| = [L{:}\mathrm{Inv}(H)]$, *and* $[G{:}H] = [\mathrm{Inv}(H){:}K_0]$.

(iv) $H \trianglelefteq G \iff \mathrm{Inv}(H)/K_0$ *is a normal extension.*

(v) *In the situation of* (iv), $G/H \cong \mathrm{Aut}(\mathrm{Inv}(H)/K_0)$.

I.G.23. REMARK. (a) There are lots of little things to unpack here, but (besides the sought-for bijection) the part that stands out is the link between normal subgroups and normal "intermediate-to-bottom" field extensions. (Remember that "top-to-intermediate" extensions $L/\mathrm{Inv}(H)$ are always normal; in particular, L/K_0 is normal since $K_0 = \mathrm{Inv}(G)$.) Note that since (i) asserts that (between L and K_0) every intermediate field is "Inv" of something, we can turn (iv) around to say: if M/K_0 is normal, then $\mathrm{Aut}(L/M) \trianglelefteq \mathrm{Aut}(L/K_0)$, and also $\mathrm{Aut}(M/K_0) \cong \mathrm{Aut}(L/K_0)/\mathrm{Aut}(L/M)$.

(b) In the proof, we will need to use I.F.3 in the following form, which is worth stating separately: *given a Galois extension L/M, all automorphisms of M extend to automorphisms of L.* To see this, take "K, M, L" in I.F.3 to be the present M, L, L. Then one extracts the following statement (equivalent to concluding merely that $r \geq 1$): "Let L/M be a Galois extension, and fix an injective map $\jmath \colon M \hookrightarrow L$. Then there exists an automorphism $\tilde{\jmath} \colon L \xrightarrow{\cong} L$ with $\tilde{\jmath}|_M = \jmath$." So given the embedding $\imath \colon M \hookrightarrow L$ and an automorphism $\sigma_M \colon M \xrightarrow{\cong} M$, we simply need to take $\jmath := \imath \circ \sigma_M$, and the output $\tilde{\jmath}$ is our desired automorphism of L extending σ_M.

I.G.24. EXAMPLE. Continuing Example I.G.15, with $f(x) = x^3 - 2$, we have $K_0 = \mathbb{Q}$ and $G = \mathfrak{S}_3$, in which we can label elements by how they permute the roots $\alpha_j = \zeta_3^j \sqrt[3]{2}$. The non-normal subgroups $H_1 := \langle (23) \rangle$, $H_2 := \langle (13) \rangle$, and $H_3 := \langle (12) \rangle$ correspond to the subfields M_j, which are not normal over $\mathbb{Q}$. The normal subgroup $H := \langle (123) \rangle$ corresponds to M, which is normal/$\mathbb{Q}$; and the quotients match: $G/H \cong \mathbb{Z}_2 \cong \mathrm{Aut}(M/\mathbb{Q})$.

PROOF. (i) Given $H \leq G$, $|H| \leq |G| \leq [L{:}K] < \infty \implies H = \mathrm{Aut}(L/\mathrm{Inv}(H))$ by I.G.4. From this we see that $\mathrm{Inv}(\cdot)$ is 1-to-1 and $\mathrm{Aut}(L/\cdot)$ is onto.

Also by I.G.4, L/K_0 is Galois. Given an intermediate field $K_0 \subset M \subset L$, by I.F.2 and I.F.12 L/M is separable and normal, hence Galois. By I.G.6 it now follows that $M = \mathrm{Inv}(\mathrm{Aut}(L/M))$, hence that $\mathrm{Aut}(L/\cdot)$ is 1-to-1 and $\mathrm{Inv}(\cdot)$ is onto. (Clearly they are also inverses.)

(ii) We already know " $\Longrightarrow$ ", and " $\Longleftarrow$ " follows from the comparable result for $\mathrm{Aut}(L/\cdot)$ combined with (i).

(iii) From (i), $\mathrm{Aut}(L/\mathrm{Inv}(H)) \cong H$; since $L/\mathrm{Inv}(H)$ is Galois, this gives $[L{:}\mathrm{Inv}(H)] = |\mathrm{Aut}(L/\mathrm{Inv}(H))| = |H|$. The second equality follows from this by the Tower Law.

(iv) Given $L \supset M \supset K_0$ and $\sigma \in G$, we have $L \supset \sigma(M) \supset K_0$. Now

$$\begin{aligned}
\tau \in \mathrm{Aut}(L/\sigma(M)) &\iff \tau\sigma(\mu) = \sigma(\mu) \ \ (\forall \mu \in M) \\
&\iff \sigma^{-1}\tau\sigma(\mu) = \mu \ \ (\forall \mu \in M) \\
&\iff \sigma^{-1}\tau\sigma \in \mathrm{Aut}(L/M) \\
&\iff \tau \in \sigma\mathrm{Aut}(L/M)\sigma^{-1};
\end{aligned}$$

from which we conclude

$$\sigma\mathrm{Aut}(L/M)\sigma^{-1} = \mathrm{Aut}(L/\sigma(M)). \tag{I.G.25}$$

So $\mathrm{Inv}(H)/K_0$ is normal

$$\begin{aligned}
&\underset{\text{I.F.14}}{\iff} \sigma(\mathrm{Inv}(H)) = \mathrm{Inv}(H) \ \ (\forall \sigma \in G) \\
&\underset{\text{(i)}}{\iff} \mathrm{Aut}(L/\sigma(\mathrm{Inv}(H))) = \mathrm{Aut}(L/\mathrm{Inv}(H)) \ \ (\forall \sigma \in G) \\
&\underset{\text{(I.G.25)}}{\iff} \sigma\mathrm{Aut}(L/\mathrm{Inv}(H))\sigma^{-1} = \mathrm{Aut}(L/\mathrm{Inv}(H)) \ \ (\forall \sigma \in G) \\
&\iff \mathrm{Aut}(L/\mathrm{Inv}(H)) \trianglelefteq G.
\end{aligned}$$

(v) Write $M := \mathrm{Inv}(H)$. If $H \trianglelefteq G$, then M/K_0 is normal by (iv). So for each $\sigma \in G$, we have $\sigma M = M$ hence $\sigma|_M \in \mathrm{Aut}(M/K_0)$. That is, restricting automorphisms from L to M induces a homomorphism $\psi\colon G \to \mathrm{Aut}(M/K_0)$. By Remark I.G.23(b), all automorphisms of M extend to automorphisms of L, and so ψ is surjective. Moreover, the kernel of ψ consists precisely of automorphisms fixing M pointwise, i.e. $\ker(\psi) \cong \mathrm{Aut}(L/M)$. So we conclude (by the fundemental theorem of group homomorphisms) that $G/\mathrm{Aut}(L/M) \cong \mathrm{Aut}(M/K_0)$. $\square$

A few applications.

(a) Constructible p-gons. The polynomials $x^n - 1$ are of interest for various reasons — they are products of cyclotomic ones (which played a role in our discussion of Fermat's last theorem), and their splitting fields are related to the constructibility problem for regular n-gons. They also have a fatal flaw which we can exploit.

I.G.26. PROPOSITION. *Let $f \in K[x]$ be a polynomial whose roots $\mathcal{R}_f$ are closed under multiplication and inversion. Then $\Theta\colon \mathrm{Gal}_K(f) \hookrightarrow \mathfrak{S}_{\mathcal{R}_f}$ factors through* $\mathrm{Aut}(\mathcal{R}_f)$ (*where we mean* group *automorphisms*).

PROOF. $\Theta(\sigma)$ respects multiplication (and identity, hence inversion), since σ is a field automorphism after all. $\square$

I.G.27. EXAMPLE. Take $K = \mathbb{Q}$, $f(x) = x^{17} - 1$, and $L = \mathbb{Q}(\zeta_{17})$; the roots are nothing but the powers of ζ_{17}, and so form a cyclic group: $\mathcal{R}_f \cong \mathbb{Z}_{17}$. By the Proposition, $\mathrm{Gal}_{\mathbb{Q}}(f)$ is a subgroup of $\mathrm{Aut}(\mathcal{R}_f) = \mathrm{Aut}(\mathbb{Z}_{17}) \cong \mathbb{Z}_{17}^*$, which (as the multiplicative group of a finite field) is isomorphic to $\mathbb{Z}_{16}$ by [**Algebra I**, III.G.18]. Moreover, since $f(x)/(x-1) = \sum_{j=0}^{16} x^j$ is irreducible, $|\mathrm{Gal}_{\mathbb{Q}}(f)| = [L{:}K] = 16$. This forces $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathbb{Z}_{17}^*$, an isomorphism realized by $\sigma_j(\zeta_{17}) := \zeta_{17}^j$ for $j \in \mathbb{Z}_{17}^*$.

Since 3 generates $\mathbb{Z}_{17}^*$, we set $\eta := \sigma_3$ and consider the sequence of subgroups

$$\mathrm{Aut}(L/K) = \langle \eta \rangle \geq \langle \eta^2 \rangle \geq \langle \eta^4 \rangle \geq \langle \eta^8 \rangle \geq \{1\}$$

with successive quotients $\mathbb{Z}_2$. Taking Inv and applying the FTGT[26] produces a sequence of field extensions

$$K \subset K_1 \subset K_2 \subset K_3 \subset L$$

of degree 2. Since quadratic extensions (in characteristic $\neq 2$, cf. I.C.7) are always obtained by adjoining a square-root, L is a square-root tower. By I.B.4, it follows that $\mathcal{R}_f$ (and hence a regular 17-gon) is constructible.

[26] An abbreviation for "Fundamental Theorem of Galois Theory". Specifically, I am using I.G.22(iii) here.

This is a better proof than the one at the end of §I.B, *because it generalizes* to all Fermat primes $p = 2^{2^s} + 1$. Taking $f(x) = x^p - 1$, $\Phi_p(x) = (x^p - 1)/(x-1)$ is irreducible, $\mathcal{R}_f \cong \mathbb{Z}_p$ consists of the p^{th} roots of unity, and $\text{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \text{Aut}(\mathcal{R}_f) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{2^{2^s}}$, whence $\mathbb{Q}(\zeta_p)$ is a square-root tower by the same arguments as above. Together with I.B.9, this yields the

I.G.28. THEOREM. *A regular p-gon, p prime, is constructible if and only if p is a Fermat prime.*

(b) Symmetric rational functions. Let F be a field, and $L := F(x_1, \ldots, x_n)$ the field of rational expressions over F in n indeterminates. Write $\sigma(\pi) \in \text{Aut}(L/F)$ for the automorphism induced by a permutation $\pi \in \mathfrak{S}_n$. This gives an embedding $\mathfrak{S}_n \hookrightarrow \text{Aut}(L/F)$, and we write $K_0 := \text{Inv}(\mathfrak{S}_n) = F(x_1, \ldots, x_n)^{\mathfrak{S}_n}$ for the field of *symmetric* rational expressions.[27]

There is a another field that comes to mind: $K := F(e_1, \ldots, e_n)$, where $e_k := e_k(x_1, \ldots, x_n)$ is the k^{th} *elementary symmetric polynomial*. Recall from [**Algebra I**, III.G.27-28] that this is $(-1)^k$ times the coefficient of x^{n-k} in $g(x) = \prod_{i=1}^n (x - x_i)$. What we are going to do now is prove the surjectivity part of [**Algebra I**, III.G.29], i.e. that the $\{e_k\}$ generate K_0/F, in a completely different way:

I.G.29. THEOREM. $F(e_1, \ldots, e_n) = F(x_1, \ldots, x_n)^{\mathfrak{S}_n}$.

PROOF. Clearly $K \subset K_0$, as every $\sigma(\pi)$ fixes K. Conversely, consider $\sigma \in \text{Aut}(L/K)$. Working in $L[x]$, $\sigma(g(x)) = g(x) \implies 0 = \sigma(0) = \sigma(g(x_i)) = \sigma(g)(\sigma(x_i)) = g(\sigma(x_i)) \implies \sigma(x_i) = x_j$ for some $j \implies \sigma = \sigma(\pi)$ for some $\pi \in \mathfrak{S}_n$. So we have $\text{Aut}(L/K) = \text{Aut}(L/K_0) = \mathfrak{S}_n$. To conclude that $K = K_0$, we need that L/K is Galois. But L/K is a SFE for $g = \sum_{k=0}^n (-1)^k e_k x^{n-k} \in K[x]$,which is separable because it has distinct roots $x_1, \ldots, x_n \in L$; so L/K is Galois by I.F.22. $\square$

[27]For those interested in algebraic geometry, you can think of this as the function field of $(\mathbb{P}^1_F)^n/\mathfrak{S}_n$ (or any resolution thereof).

(c) Degrees of normal closures. Here is a question about the numerology of degrees of field extensions. It's a bit silly, but gives a first glimpse of how we can learn a lot about field theory by applying group theory. Suppose $[L{:}K] = p$ is prime and L/K is *non-normal*; then *is* $[L^c{:}K]$ *a power of* p*?* Since L^c/K is normal, we can apply the Galois correspondence to $L^c \supset L \supset K$ to obtain $\{1\} \leq H \leq G$, where

- $H = \text{Aut}(L^c/L)$ and $G = \text{Aut}(L^c/K)$,
- $H \ntrianglelefteq G$ (since L/K isn't normal), and
- $[G{:}H] = [\text{Inv}(H){:}K] = [L{:}K] = p$.

Suppose $[L^c{:}K] = p^k$. Then G is a p-group with a non-normal subgroup H of index p. By [**Algebra I**, II.H.8], we know that G has nontrivial center, hence (by Cauchy) that $C(G)$ contains a subgroup J of order p. If $J \nleq H$, then $G = JH$ and $H \trianglelefteq G$, a contradiction; while if $J \leq H$, then $H/J \ntrianglelefteq G/J$ (by the First Isomorphism Thm.) and we continue the argument, which reaches a contradiction by induction. Conclude that $[L^c{:}K]$ is *never* a power of p!

(d) The theorem on natural irrationalities. Finally, we turn to an important technical result which answers the question of what happens to the Galois group of a polynomial $f \in K[x]$ when we perform an arbitrary field extension M/K. That is, how can we compare $\text{Gal}_K(f)$ and $\text{Gal}_M(f)$? If f has a splitting field extension L/K containing M, then of course

$$\text{Gal}_M(f) = \text{Aut}(L/M) \leq \text{Aut}(L/K) = \text{Gal}_K(f).$$

But in general, M is not an intermediate field like this. The next theorem says that this essentially doesn't matter, which will be crucial when we study solubility by radicals. The name "natural irrationalities" comes from the view that extensions of $\mathbb{Q}$ by radicals are somehow more "natural" than other extensions; our theorem doesn't deal specifically with such extensions, but it generalizes results of Lagrange and Abel which did.

I.G.30. THEOREM. *Given* $f \in K[x]$ *and* M/K *an extension,* $\text{Gal}_M(f)$ *is isomorphic to a subgroup of* $\text{Gal}_K(f)$*.*

More precisely, let L' be a splitting field for f over M, with roots $\mathcal{R}_f \subset L'$ (and $L' = M(\mathcal{R}_f)$), so that $L = K(\mathcal{R}_f)/K$ is a splitting field for f over K. Set $M_0 := \mathrm{Inv}(\mathrm{Gal}_M(f)) \subset L'$. Then sending $\sigma \mapsto \sigma|_L$ induces an isomorphism

$$\begin{array}{ccc} \mathrm{Aut}(L'/M) \overset{\cong}{\to} \mathrm{Aut}(L/M_0 \cap L) \leq & \mathrm{Aut}(L/K). \\ \| & \| \\ \mathrm{Gal}_M(f) & \mathrm{Gal}_K(f) \end{array}$$

PROOF. Here is a diagram of the situation:

$$\begin{array}{ccccc} L' & \supset & M_0 & \supset & M \\ \cup & & \cup & & \cup \\ L & \supset & M_0 \cap L & \supset & K \end{array}$$

First, given $\sigma \in \mathrm{Aut}(L'/M)$, σ fixes M_0 hence K, and permutes the roots in $\mathcal{R}_f$. So it sends $L \to L$ while fixing $M_0 \cap L$; that is, $\sigma|_L$ does indeed lie in $\mathrm{Aut}(L/M_0 \cap L)$. If $\sigma|_L = \mathrm{id}_L$, then σ fixes $\mathcal{R}_f$ (and M), hence is $\mathrm{id}_{L'}$; so $\sigma \mapsto \sigma|_L$ is injective.

Let $V := \mathrm{Inv}(\mathrm{Aut}(L'/M)|_L) \subseteq L$. I claim that the obvious inclusion $V \supseteq M_0 \cap L$ is an equality. Indeed, given $x \in L \setminus (M_0 \cap L)$, then as $M_0 = \mathrm{Inv}(\mathrm{Aut}(L'/M))$, there exists a $\sigma \in \mathrm{Aut}(L'/M)$ such that $\sigma(x) \neq x$; thus $x \notin V$. So $V = M_0 \cap L$, which yields $\mathrm{Aut}(L'/M)|_L = \mathrm{Aut}(L/\mathrm{Inv}(\mathrm{Aut}(L'/M)|_L)) = \mathrm{Aut}(L/M_0 \cap L)$ (by applying I.G.4 with $G = \mathrm{Aut}(L'/M)|_L$). That is, $\sigma \mapsto \sigma|_L$ is onto. $\square$

I.G.31. REMARK. Assuming f is separable cuts down on the complexity of notation a bit, since then $M = M_0$. In that case the result says that L'/M and $L/(M \cap L)$ are "Galois-equivalent extensions".

I.G.32. EXAMPLE. Take $K = \mathbb{Q}$, and $L \subset \mathbb{C}$ a number field normal over $\mathbb{Q}$; then $L/\mathbb{Q}$ is a SFE for some $f \in \mathbb{Q}[x]$. Assume $L \not\subset \mathbb{R}$. Taking $M = \mathbb{R}$, $L' = \mathbb{C}$ is a splitting field for f over $\mathbb{R}$, and I.G.30 gives an embedding of $\mathbb{Z}_2 \cong \langle \rho \rangle = \mathrm{Aut}(\mathbb{R}/\mathbb{C})$ into $\mathrm{Aut}(L/\mathbb{Q})$, where ρ is complex conjugation. (This is of course obvious by other means but illustrates the result.) Note that one may *not* get such an embedding if $L/\mathbb{Q}$ isn't normal.