I.L. Higher degree

We now turn to the calculation of Galois groups for polynomials of arbitrary degree, starting with a "general" result — quite literally. That is, we shall calculate the Galois group of the *generic polynomial*

(I.L.1) $$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^n t_n \in K[x],$$

where $K = F(t_1, \ldots, t_n)$ is the fraction field of the polynomial ring $F[t_1, \ldots, t_n]$ over some field F. We've already demonstrated that, for $n \leq 4$ and $\mathrm{char}(F) \neq 2, 3$, this is solvable by radicals.

Let L/K be a splitting field extension for f, with $G = \mathrm{Gal}_K(f) = \mathrm{Aut}(L/K)$. Over L, we have $f(x) = \prod_{i=1}^n (x - y_i)$, with $t_j = e_j(\{y_i\})$, and $L = K(y_1, \ldots, y_n) = F(y_1, \ldots, y_n)$. We are now in the setting of Theorem I.G.29 and its proof, which together with Galois's Theorem yields at once the

I.L.2. ABEL-RUFFINI THEOREM (Abel, 1824). *The general equation* (I.L.1) *of the n^{th} degree is separable and irreducible in $F(t_1, \ldots, t_n)[x]$, with Galois group $\mathfrak{S}_n$. Hence for* $\mathrm{char}(F) = 0$ *and $n \geq 5$, it is insoluble by radicals.*

Thus one way to get an "explicit" polynomial not solvable in radicals over its "field of definition" K is to take $n \geq 5$, replace the $\{t_i\}$ in (I.L.1) by algebraically independent transcendentals[37] $\{\gamma_i\} \subset \mathbb{C}$, and set $K = \mathbb{Q}(\{\gamma_i\})$. But this is not really different from the generic polynomial — a harder problem is whether we can "specialize" the $\{t_i\}$ to elements of F to get a polynomial in $F[x]$ that still behaves (over $F[x]$) like the generic polynomial does (over $K[x]$), in the sense of being irreducible with Galois group $\mathfrak{S}_n$. For instance:

- for $F = \mathbb{C}$, we can never do this, because $\mathbb{C}$ is algebraically closed!
- for $F = \mathbb{R}$ (and $n > 2$), again impossible!
- for $F = \mathbb{Q}$, on the other hand, this was proved by Hilbert using his "irreducibility theorem", and we will give an explicit construction of such polynomials below for n prime.

[37] We will say exactly what this means, how to generate them, and why $F(\gamma_1, \ldots, \gamma_n) \cong F(t_1, \ldots, t_n)$ when we discuss transcendental extensions.

If you accept Hilbert's result, then there exists (for each n) a Galois extension $L/\mathbb{Q}$ with $\mathrm{Aut}(L/\mathbb{Q}) \cong \mathfrak{S}_n$, and then every subgroup — indeed, every finite group G — is realized as the Galois group of an extension L/M of number fields. Taking the minimal polynomial μ_α over M of a primitive element $\alpha \in L$ realizes G as the Galois group $\mathrm{Gal}_M(\mu_\alpha)$.

A much more difficult problem is the question of whether any finite group is the Galois group $\mathrm{Gal}_{\mathbb{Q}}(g)$ of a polynomial over $\mathbb{Q}$: this is the celebrated **inverse Galois problem**. It turns out that any finite abelian group A is a quotient group of some $\mathbb{Z}_m^*$, cf. I.L.21. Since these latter groups arise as $\mathrm{Aut}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ in view of the discussion of cyclotomic polynomials below, this realizes A as the Galois group of an (abelian) extension of $\mathbb{Q}$ (and thus as the Galois group of the minimal polynomial of a primitive element).

What about nonabelian groups? Hilbert showed that, in addition to $\mathfrak{S}_n$, all alternating groups $\mathfrak{A}_n$ are Galois groups/$\mathbb{Q}$; and half a century later, Shafarevich proved this for solvable groups. Currently the inverse Galois problem is still open for (at least) some simple groups of Lie type and one of the sporadic simple groups.

In the rest of this section we consider various approaches computing Galois groups, including reducing a polynomial modulo a prime, as well as methods specific to polynomials of prime degree, and finally concluding with a treatment of cyclotomic polynomials and applications thereof.

Polynomials of prime degree.

Let $p \geq 5$ be prime. Recall the statement of I.G.20:[38]

Given $f \in \mathbb{Q}[x]$ irreducible of degree p,

with exactly $p-2$ roots in $\mathbb{R}$, we have $\mathrm{Gal}_{\mathbb{Q}}(f) \cong \mathfrak{S}_p$.

It remains to actually *construct* such polynomials for every p! The construction that follows is attributed by **[Jacobson]** to Brauer.

[38]The reason for taking $n = p$ was that the proof relied on the fact that transitive subgroups of $\mathfrak{S}_p$ containing a transposition are the whole group.

So let $n_1 < n_2 < \cdots < n_{p-2}$ be even integers, and $m \geq \frac{1}{2}\sum_{\ell=1}^{p-2} n_\ell^2$ a positive even integer, and consider

$$g(x) := (x^2 + m)(x - n_1)\cdots(x - n_{p-2}) \in \mathbb{Q}[x]. \tag{I.L.3}$$

I.L.4. THEOREM. *$f := g - 2$ is irreducible, with Galois group $\mathfrak{S}_p$.*

PROOF. First note that g has $p-2$ real roots, hence $p-3$ relative extrema (as a function on $\mathbb{R}$), with half of these maxima. For $\ell \in \mathbb{Z}$ odd (which includes values between adjacent n_i), evidently $|g(\ell)| > 2$; and so the relative extrema have $|\cdot| > 2$ as well. It follows that f has $\frac{p-3}{2}$ positive relative maxima between n_1 and n_{p-2}, hence at least $p-2$ real roots, $p-3$ of which lie in (n_1, n_{p-2}).

Writing $f = x^p + a_1 x^{p-1} + \cdots + a_p = g - 2$, we see that $a_1, \ldots, a_p$ are even. Clearly 4 divides the constant term of g, so does *not* divide a_p; hence by Eisenstein, f is irreducible.

Factoring $f(x) = \prod_{i=1}^{k}(x - r_i)$ in $\mathbb{C}[x]$ and comparing with (I.L.3), we evidently have (from coefficients of x^{p-1} and x^{p-2}) that

$$\textstyle\sum_{i=1}^{p} r_i = \sum_{\ell=1}^{p-2} n_\ell \quad \text{and} \quad \sum_{i<j} r_i r_j = m + \sum_{k<\ell} n_k n_\ell,$$

whence

$$\begin{aligned}\textstyle\sum_i r_i^2 = (\sum_i r_i)^2 - 2\sum_{i<j} r_i r_j &= \textstyle(\sum_\ell n_\ell)^2 - 2(\sum_{k<\ell} n_k n_\ell + m)\\ &= \textstyle\sum_\ell n_\ell^2 + 2\sum_{k<\ell} n_k n_\ell - 2\sum_{k<\ell} n_k n_\ell - 2m\\ &= \textstyle\sum_\ell n_\ell^2 - 2m \leq 0\end{aligned}$$

by our assumption on m. As also $\prod_i r_i = a_p \neq 0$, some r_i must be non-real, say r_1; and since $f \in \mathbb{Q}[x]$, its conjugate $\bar{r}_1$ must also be a root, say r_2. Then $r_3, \ldots, r_p$ are the real roots, and I.G.20 completes the proof. □

This yields a plethora of explicit polynomials over $\mathbb{Q}$ not solvable by radicals. For instance, taking $n_1 = -2$, $n_2 = 0$, $n_3 = 2$, and $m = 4$ produces $f(x) = (x^2 + 4)x(x^2 - 4) - 2 = x^5 - 16x - 2$.

It is also of interest to classify the possible Galois groups for polynomials which *are* solvable by radicals. For prime degree, there is a nice result. Let X denote $\mathbb{Z}_p$ viewed as a set, and consider the groups

$$W_p := \{\omega_{a,b} \mid a \in \mathbb{Z}_p^*,\ b \in \mathbb{Z}_p\} \leq \mathfrak{S}_{\mathrm{X}} \cong \mathfrak{S}_p \tag{I.L.5}$$

of affine transformations $\omega_{a,b}(x) := ax + b$ of X. Writing $\sigma := \omega_{1,1}$, the cyclic subgroup $\mathbb{Z}_p \cong \langle\sigma\rangle \trianglelefteq W_p$ is the kernel of the homomorphism $W_p \twoheadrightarrow \mathbb{Z}_p^*$ given by $\omega_{a,b} \mapsto a$.

I.L.6. THEOREM. *Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p, which is solvable by radicals. Then $G := \mathrm{Gal}_{\mathbb{Q}}(f)$ is isomorphic to a subgroup of W_p containing $\mathbb{Z}_p$. More precisely, there is a (cyclic) subgroup $C \leq \mathbb{Z}_p^*$ such that $G \cong \{\omega_{a,b} \mid a \in C,\ b \in \mathbb{Z}_p\}$.*[39]

PROOF. Since f is irreducible, we know (identifying X with $\mathcal{R}_f$) that G is a transitive subgroup of $\mathfrak{S}_{\mathrm{X}}$. For any nontrivial normal subgroup $\{1\} \neq H \trianglelefteq G$, if we partition X into (disjoint) orbits $H(x)$, then I claim these orbits have the same order. Indeed, given $x, y \in$ X, there exists (by transitivity) $g \in G$ with $y = gx$; and then $x' \in H(x) \implies gx' \in gH(x) = gHg^{-1}(gx) = H(y)$. So $gH(x) \subset H(y)$, and conversely $g^{-1}H(y) = H(x)$, whence $\ell_g\colon H(x) \to H(y)$ is a bijection, and $|H(x)| = |H(y)|$. It follows that $|H(x)|$ divides $|\mathrm{X}| = p$; and since $|H(x)| \neq 1$ (remember that $|H| \neq 1$), the only option is to have $H(x) = \mathrm{X}$. Thus H acts transitively on X.

We also know that G is solvable. Then it has a normal series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_{m-1} \triangleright G_m = \{1\}$ with cyclic quotients. By the last paragraph, G_1 is a transitive subgroup of $\mathfrak{S}_{\mathrm{X}}$; and by induction we get that all the G_j ($j < m$) are transitive as well. Since G_{m-1} is also cyclic, it must be isomorphic to $\mathbb{Z}_p$, generated by a (cyclic) permutation of X. Reordering the identification of X with $\mathbb{Z}_p$ if necessary, we have $G_{m-1} = \langle\sigma\rangle$ in the notation after (I.L.5).

Now suppose inductively that (under this identification) we have $G_j \leq W_p$ (with $j < m$); obviously $\sigma \in G_j$. Given $\tau \in G_{j-1}$, normality yields $\tau\sigma\tau^{-1} \in G_j$, whence $\tau\sigma\tau^{-1}$ is some ω_{a_0,b_0} of order p (like σ), which must permute X cyclically. This means that $x = \omega_{a_0,b_0}(x) =$

---

[39]This can also be phrased in terms of short-exact sequences, namely $0 \to \mathbb{Z}_p \to W_p \to \mathbb{Z}_p^* \to 1$ and $0 \to \mathbb{Z}_p \to G \to C \to 1$.

$a_0x + b_0$ can have no solutions in $\mathbb{Z}_p$. But this is only possible if $a_0 = 1$ and $b_0 \neq 0$. So we have

$$\begin{aligned}\tau(k) &= \tau\sigma(k-1) = \tau\sigma\tau^{-1}(\tau(k-1)) = \omega_{1,b_0}(\tau(k-1)) \\ &= \tau(k-1) + b_0 = \cdots = \tau(k-2) + 2b_0 = \cdots \\ &= \tau(0) + kb_0,\end{aligned}$$

which means that $\tau = \omega_{b_0,\tau(0)}$. In particular, τ belongs to W_p; and since $\tau \in G_{j-1}$ was arbitrary, $G_{j-1} \leq W_p$. Downward induction on j now yields that $G \leq W_p$. □

Reduction mod p.

Given a monic polynomial $f \in \mathbb{Z}[x]$ of degree n, we may consider its images $f_p \in \mathbb{Z}_p[x] = \mathbb{Z}[x]/(p)$. How might $\mathrm{Gal}_{\mathbb{Q}}(f)$ be related to $\mathrm{Gal}_{\mathbb{Z}_p}(f_p)$?

It is reasonable to assume that f has no repeated roots, since otherwise it would just have a repeated irreducible factor. (As usual, we shall write $\mathcal{R}$ for the roots of f in a splitting field.) As the discriminant of a polynomial of degree n is a universal polynomial in its coefficients (cf. (I.K.5)ff), the image of $\Delta_f \in \mathbb{Z}$ under the reduction map $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_p$ is Δ_{f_p}. So if $p \nmid \Delta_f$, we have $\Delta_{f_p} \neq 0$ in $\mathbb{Z}_p$, and f_p does not have multiple roots. Henceforth we shall work with such a choice of p.

I.L.7. THEOREM. *Suppose f_p factors as a product of irreducibles of degrees n_i, $\sum_{i=1}^{s} n_i = n$. Then $\mathrm{Gal}_{\mathbb{Q}}(f)$ (viewed as a subgroup of $\mathfrak{S}_{\mathcal{R}_f}$) contains a permutation $\sigma_p \in \mathfrak{S}_{\mathcal{R}_f}$ with cycle-structure $n_1, \ldots, n_s$.*

The idea of the proof is as follows:

- Let $E/\mathbb{Q}$ and $E_p/\mathbb{Z}_p$ be SFEs for f resp. f_p, and $D := \mathbb{Z}[\mathcal{R}_f]$. Fix a ring homomorphism $\psi \colon D \to E_p = \mathbb{Z}_p[\mathcal{R}_{f_p}]$. (We will show that this exists below.)
- Then any other such homomorphism ψ' will differ from ψ by an element $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$ on the right: that is, $\psi' = \psi\sigma$.
- Given $\pi \in \mathrm{Aut}(E_p/\mathbb{Z}_p)$, $\pi\psi \colon D \to E_p$ is a ring homomorphism. So there exists $\sigma_\pi \in \mathrm{Aut}(E/\mathbb{Q})$ such that $\pi\psi = \psi\sigma_\pi$. Sending $\pi \mapsto$

σ_π produces a group homomorphism $\mathrm{Aut}(E_p/\mathbb{Z}_p) \to \mathrm{Aut}(E/\mathbb{Q})$, from permutations of $\mathcal{R}_{f_p}$ to permutations of $\mathcal{R}_f$.

- $|E_p| < \infty \implies \mathrm{Aut}(E_p/\mathbb{Z}_p) = \langle \phi_p \rangle$ is cyclic,[40] acting transitively on the root sets of the irreducible factors $f_{p,i}$ (of degree n_i) of f_p.
- $\sigma_p := \sigma_{\phi_p}$ has the same cycle-structure as ϕ_p.

To carry this plan out carefully, we begin with two lemmas. Given a field F, an ***F*-valued character** of a monoid or group is simply a (multiplicative) homomorphism into F^* (sending $1 \mapsto 1$).

I.L.8. LEMMA (Dedekind Independence Theorem). *Distinct characters of a monoid into a field are linearly independent over that field.*

PROOF. Let $\mathbb{H}$ be a monoid, F a field, and $\chi_i \colon \mathbb{H} \to F^*$ ($1 \le i \le m$) distinct characters. The claim is that if

$$a_1\chi_1(h) + \cdots + a_n\chi_m(h) = 0 \quad (\forall h \in \mathbb{H}) \tag{I.L.9}$$

then all $a_i = 0$. For $m = 1$, this is clear since $a\chi(h) = 0$ $(\forall h) \implies 0 = a\chi(1) = a$.

Supposing inductively that the claim holds for $m-1$ characters, we can then assume all $a_i \neq 0$. Since $\chi_1 \neq \chi_m$, they must disagree on some a_0. Plugging $a_0 h$ into (I.L.9) yields

$$a_1\chi_1(a_0)\chi_1(h) + \cdots + a_m\chi_m(a_0)\chi_m(h) = 0,$$

while multiplying (I.L.9) by $\chi_m(a_0)$ yields

$$a_1\chi_m(a_0)\chi_1(h) + \cdots + a_m\chi_m(a_0)\chi_m(h) = 0.$$

Subtracting these two equations yields

$$\sum_{i=1}^{m-1} a_i(\chi_i(a_0) - \chi_m(a_0))\chi_i(h) = 0 \;\; (\forall h \in \mathbb{H}). \tag{I.L.10}$$

Applying the inductive hypothesis, we get in particular that the coefficient $a_1(\chi_1(a_0) - \chi_m(a_0))$ of $\chi_1(h)$ in (I.L.10) is zero. Since $\chi_1(a_0) \neq \chi_m(a_0)$, this gives $a_1 = 0$, a contradiction. $\square$

[40] See I.H.3. Recall that ϕ (here ϕ_p) denotes the Frobenius map $(\cdot) \mapsto (\cdot)^p$.

(If this argument seemed familiar, it is because it generalizes a paragraph from the proof of I.J.11.)

I.L.11. LEMMA. (i) *A homomorphism* $\psi\colon D \to E_p$ *exists.*
(ii) *Any such homomorphism gives a bijection* $\mathcal{R}_f \overset{\cong}{\to} \mathcal{R}_{f_p}$.
(iii) *If* ψ, ψ' *are two such, then* $\psi' = \psi\sigma$ *for some* $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$.

PROOF. (i): Writing $\mathcal{R}_f = \{r_1, \ldots, r_n\}$, we have $f(x) = \prod_{i=1}^{n}(x - r_i)$ in $D[x]$. The subset

$$D' := \mathbb{Z}\langle \underline{r}^{\underline{e}} \mid \underline{e} \in (\mathbb{N}_{<n})^n \rangle \subset D = \mathbb{Z}[\{r_1, \ldots, r_n\}]$$

contains r_i^n, since this may be expressed as a $\mathbb{Z}$-linear combination of $1, r_i, r_i^2, \ldots, r_i^{n-1}$ using $f(r_i) = 0$. So $r_i D' \subset D'$, whence $D' \subset D$ is a subring containing $\mathcal{R}_f$, hence equals D. In other words, D is finitely generated as a $\mathbb{Z}$-module; and it is also free (since $\mathrm{char}(E) = 0$). By the structure theorem, we have $D = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_N$ for some $u_j \in D$. That is, there is no $\mathbb{Z}$-linear relation on the $\{u_i\}$, hence no $\mathbb{Q}$-linear relation on them either, making $\mathbb{Q}u_1 \oplus \cdots \oplus \mathbb{Q}u_N$ a subring of E.

But any "intermediate ring" R in an algebraic field extension L/K is always a *field*. [This is simply because, for any $\alpha \in R$, $K[\alpha]$ is a finite-dimensional K-vector space; and multiplication $\mu_\alpha\colon K[\alpha] \to K[\alpha]$ by α is an endomorphism thereof, which is injective because $K[\alpha]$ is a domain. So it is also surjective, and there is a $\beta \in K[\alpha] \subset R$ such that $1 = \mu_\alpha(\beta) = \alpha\beta$.] So $\mathbb{Q}u_1 \oplus \cdots \oplus \mathbb{Q}u_N$ is a subfield of E containing $\mathcal{R}_f$, and we conclude that $E = \mathbb{Q}u_1 \oplus \cdots \oplus \mathbb{Q}u_N$, with $N = [E{:}\mathbb{Q}]$.

Now consider the ideal $pD = \oplus_{i=1}^{N}\mathbb{Z}(pu_i) \subset D$; clearly $|D/pD| = p^N$. Let $M \subsetneq D$ be a maximal ideal containing pD; then $M/pD \subsetneq D/pD$ is also a maximal ideal, and D/M a field of characteristic p with $|D/M| = p^m$ ($m \leq N$). The quotient map $\nu\colon D \twoheadrightarrow D/M$ sends $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_p$; and writing $\bar{r}_i := \nu(r_i)$, we clearly have $D/M = \mathbb{Z}_p[\bar{r}_1, \ldots, \bar{r}_n]$ (as the images of generators over $\mathbb{Z}$ become generators over $\mathbb{Z}_p$). The induced map $D[x] \twoheadrightarrow (D/M)[x]$ sends $f(x) = \prod_{i=1}^{n}(x - r_i)$ to $f_p(x) = \prod_{i=1}^{n}(x - \bar{r}_i)$. Evidently D/M is a splitting field for f_p (why?), and composing $D \twoheadrightarrow D/M$ with the resulting isomorphism $D/M \overset{\cong}{\to} E_p$ yields a ψ, proving (i).

<u>(ii)</u>: Let $\psi \colon D \to E_p$ be given. Since any ring homomorphism sends $1 \mapsto 1$, it must restrict to the quotient map $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_p$. So $f_p(x) = \psi(f(x)) = \prod_{i=1}^{n}(x - \psi(r_i)) \implies \psi$ maps $\mathcal{R}_f \overset{\cong}{\to} \mathcal{R}_{f_p}$.

<u>(iii)</u>: Any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(f) = \mathrm{Aut}(E/\mathbb{Q})$ restricts to a permutation (= set automorphism) of $\mathcal{R}_f$ (= generators of D over $\mathbb{Z}$) hence to a ring automorphism of D. So $\psi\sigma := \psi \circ \sigma \in \mathrm{Hom}(D, E_p)$. Moreover, distinct σ, σ' yield distinct $\psi\sigma$ and $\psi\sigma'$; altogether, we get $N = [E{:}\mathbb{Q}] = |\mathrm{Gal}_{\mathbb{Q}}(f)|$ distinct homomorphisms $\psi_j = \psi\sigma_j \colon D \to E_p$ $(1 \leq j \leq N)$ in this way.

I claim that these are *all* of the homomorphisms from D to E_p. Indeed, if ψ_{N+1} is another, then the linear system

$$\sum_{j=1}^{N+1} x_j \psi_j(u_i) = 0 \qquad (1 \leq i \leq N)$$

must have a nonzero solution $\underline{x} = (a_1, \ldots, a_{N+1}) \in E_p^{N+1}$. Given any $y = \sum_{i=1}^{N} m_i u_i \in \oplus_{i=1}^{N} \mathbb{Z} u_i = D$,

$$\psi_j(y) = \sum_{i=1}^{N} \bar{m}_i \psi_j(u_i) \qquad \implies$$

$$\sum_{j=1}^{N+1} a_j \psi_j(y) = \sum_{i=1}^{N} \sum_{j=1}^{N+1} \bar{m}_i a_j \psi_j(u_i) = \sum_{i=1}^{N} \bar{m}_i \sum_{j=1}^{N+1} a_j \psi_j(u_i) = 0.$$

But then we have $N+1$ distinct characters $D \setminus \{0\} \to E_p$ with a nontrivial linear dependency, contradicting I.L.17. $\square$

We can now prove the main theorem on "reduction mod p" as a means for computing Galois groups.

PROOF OF I.L.7. Consider the Frobenius (p^{th} power) map $\phi_p \in \mathrm{Aut}(E_p/\mathbb{Z}_p)$. If $\psi \in \mathrm{Hom}(D, E_p)$, then $\phi_p\psi \in \mathrm{Hom}(D, E_p)$. By I.L.11(iii), there exists $\sigma_{\phi_p} \in \mathrm{Gal}_{\mathbb{Q}}(f)$ such that $\phi_p\psi = \psi\sigma_{\phi_p}$. By

I.L.11(ii), we therefore have

$$\sigma_{\phi_p}|_{\mathcal{R}_f} = (\psi|_{\mathcal{R}_f})^{-1} \circ (\phi_p|_{\mathcal{R}_{f_p}}) \circ (\psi|_{\mathcal{R}_f}).$$

That is, ψ identifies the oribits of ϕ_p in $\mathcal{R}_{f_p}$ with the orbits of σ_{ϕ_p} in $\mathcal{R}_f$, equating their cycle-structures. Since ϕ_p is the (cyclic) generator of $\text{Gal}_{\mathbb{Z}_p}(f_p)$, it acts transitively on the roots of each factor $f_{p,i}$ of f in $\mathbb{Z}_p[x]$, with each $\mathcal{R}_{f_{p,i}}$ becoming an $n_i = \deg(f_{p,i})$-cycle for ϕ_p. □

Notice that the Theorem I.L.7 says nothing about f being irreducible, so we don't need to check that to apply it. It does say that f and f_p should not have a repeated root; but this is easier to check for f_p, and implies the same for f if it is true for any p.

I.L.12. EXAMPLE (Jacobson). Consider

$$f(x) = x^6 + 26x^5 + 21x^4 + 12x^3 - 37x^2 - 29x - 15.$$

Reducing mod 2 yields $f_2(x) = x^6 + x^4 + x^2 + x + 1$, which has $f_2' = 1$ hence no multiple roots. In fact, it is also irreducible (brute force), and so f is irreducible, and $G := \text{Gal}_{\mathbb{Q}}(f)$ contains a 6-cycle (in particular, is transitive).

Two more reductions yield $f_3(x) = x(x^5+x^4-x+1)$ and $f_5(x) = x(x-1)(x+1)(x+2)(x^2+2)$ (with irreducible factors shown), so that G contains a 5-cycle and a transposition. In fact, a transitive subgroup of $\mathfrak{S}_n$ containing an $(n-1)$-cycle and a transposition is $\mathfrak{S}_n$ (Exercise), and so $G \cong \mathfrak{S}_6$.

Evidently the technique is great for putting a "floor" under G, so to speak; but when G is not $\mathfrak{S}_n$ we need to use other techniques to put a "ceiling" on G.

I.L.13. EXAMPLES. Using reduction modulo p, Theorem I.L.6, and the other techniques at our disposal, we will now demonstrate that all five of the (isomorphism classes of) transitive subgroups of $\mathfrak{S}_5$ do in fact occur as Galois groups of irreducible quintic polynomials/$\mathbb{Q}$. These were $\mathfrak{S}_5$, $\mathfrak{A}_5$, W_5, D_5, and $\mathbb{Z}_5$, with orders 120, 60, 20, 10, and

5. (Of course, we have seen $\mathfrak{S}_5$ in I.G.19 and once more as a consequence of I.L.4; but we will use a simpler polynomial this time.) We will write G for $\mathrm{Gal}_{\mathbb{Q}}(f)$ in each case.

(A) $\underline{f(x) = x^5 - x - 1}$: We know from I.H.10 that its reduction modulo 5 is irreducible, so f is irreducible and G contains a 5-cycle. On the other hand, $f_2 = (x^2+x+1)(x^3+x^2+1)$ means that $\sigma_2 \in G$ has cycle-structure $(\cdots)(\cdot\cdot)$ hence order 6. So $30 \big| |G| \implies |G| = 30, 60,$ or 120; but 30 was not in our list above and is actually not the order of *any* subgroup of $\mathfrak{S}_5$. So G is $\mathfrak{A}_5$ or $\mathfrak{S}_5$.

When $n = 5$, the formula from HW for the discriminant of a polynomial of the form $x^n + px + q$ specializes to $\Delta = 4^4p^5 + 5^5q^4$. For this f, we get $\Delta = 5^5 - 4^4 = 2869 = 19 \cdot 151$. Since $\sqrt{\Delta} \notin \mathbb{Q}$, by I.K.3 we must have $G \cong \mathfrak{S}_5$.[41]

(B) $\underline{f(x) = x^5 + 20x + 16}$: One checks that $f_3 = x^5 - x + 1$ is irreducible in $\mathbb{Z}_3[x]$; so f is irreducible and G has a 5-cycle σ_3. Moreover, $f_7 = x^5 - x + 2 = (x+2)(x+3)(x^3 + 2x^2 - 2x - 2)$ yields a 3-cycle $\sigma_7 \in G$. So $15 \big| |G|$ and we are again deciding between $\mathfrak{S}_5$ and $\mathfrak{A}_5$. But the discriminant $\Delta = 2^{16}5^6$ is a rational square, so $G \cong \mathfrak{A}_5$.

(C) $\underline{f(x) = x^5 - 2}$: This is solvable by radicals: extend first to $\mathbb{Q}(\zeta_5)$, then to $E = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$. So by I.L.6, we have $G \leq W_5$. But since E contains fields $\mathbb{Q}(\sqrt[5]{2})$ and $\mathbb{Q}(\zeta_5)$ with (coprime) degrees 4 and 5 over $\mathbb{Q}$, $20 \big| |G|$. Conclude that $G \cong W_5$.

(D) $\underline{f(x) = x^5 - 5x + 12}$: The discriminant $\Delta = 2^{12}5^6$ is a square $(\implies G \cong \mathfrak{A}_5, D_5, \text{ or } \mathbb{Z}_5)$, and $f_3 = x(x^2+x-1)(x^2-x-1)$ shows that σ_3 has cycle-structure $(\cdot\cdot)(\cdot\cdot)(\cdot)$ $(\implies G \ncong \mathbb{Z}_5)$. But how to distinguish $\mathfrak{A}_5$ and D_5? If the answer is $\mathfrak{A}_5$, then we should get a 3-cycle by reducing modulo another prime. But if the answer is D_5, how do we show this?

Well, if you could explicitly "solve $f = \prod_i (x - r_i)$ by radicals", that would do it; but this appears to be quite hard. Another approach

[41] Alternatively to this paragraph, you can just observe that σ_2 is an odd permutation.

is this: define a polynomial $g(x) := \prod_{i<j}(x - (r_i + r_j))$ of degree 10. For f of the form $x^5 + px + q$, you can show (by symmetric function algebra) that $g = x^{10} - 3px^6 - 11qx^5 - 4p^2x^2 + 4pqx - q^2$. Now the idea is that if $G \cong \mathfrak{A}_5$, then this is irreducible; while if $G \cong D_5$, then it splits into two irreducible quintics. (The reason is this: imagine a pentagon with vertices at the roots r_i; if it is D_5 acting on these roots, then the 5 edges are permuted and the 5 interior diagonals are permuted, but edges and diagonals do not mingle.) And it so happens that here[42]

$$\begin{aligned} g(x) &= x^{10} + 15x^6 - 132x^5 - 100x^2 - 240x - 144 \\ &= (x^5 - 5x^3 - 10x^2 + 30x - 36)(x^5 + 5x^3 + 10x^2 + 10x + 4). \end{aligned}$$

So we get $G \cong D_5$.

(E) $\underline{f(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1}$: I am going to cheat a little, since I know where this one came from: it is the minimal polynomial of $\zeta_{11} + \bar{\zeta}_{11}$. Its splitting field is the "real subfield" of $\mathbb{Q}(\zeta_{11})$, invariant under complex conjugation.

There is a subtle issue here in general: if you have a subfield L of $\mathbb{C}$ on which complex conjugation gives an automorphism ρ, the order-2 subgroup $\langle\rho\rangle \leq \mathrm{Aut}(L/\mathbb{Q})$ may or may not be normal. For cyclotomic fields, it's normal, and so these fixed fields are splitting fields for minimal polynomials of primitive elements in them. Moreover, since here $E = \mathrm{Inv}(\langle\rho\rangle) \subset \mathbb{Q}(\zeta_{11})$, we have $G = \mathrm{Aut}(E/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\zeta_{11})/\mathbb{Q})/\langle\rho\rangle \cong \mathbb{Z}_{11}^*/\langle -1\rangle \cong \mathbb{Z}_{10}/\langle 5\rangle \cong \mathbb{Z}_5$.

Cyclotomic polynomials.

So far we have only introduced the polynomials Φ_p for p prime; we'll now discuss the more general kind. We begin with the following simple but useful[43]

[42]See Jensen and Yui, J. Number Theory 15 (1982), 347-375.

[43]We only need (ii) here. But when (i) holds, it implies (ii) (i.e. for $R = K$), so is stronger. It was also used in the solution to HW 4 #5.

I.L.14. PROPOSITION. (i) *Let L/K be a field extension, and $f, g \in K[x]$ monic. Then the monic gcd of f and g in $L[x]$ belongs to $K[x]$, and is their monic gcd there.*

(ii) *Let R be a subring of a field L, and $f, g \in R[x]$ monic, with $g \mid f$ in $L[x]$. Then $g \mid f$ in $R[x]$.*

PROOF. (i) Write h_K, h_L for the 2 monic gcds. Both belong to $L[x]$, in which h_L is a *greatest* common divisor; so $h_K \mid h_L$ (in $L[x]$). On the other hand, there exist $F, G \in K[x]$ such that $h_K = Ff + Gg$, and then $h_L \mid f, g \implies h_L \mid h_K$ (in $L[x]$). Since they are both monic, they are equal.

(ii) Write $f = \sum_{i=0}^{m+n} a_i x^i$, $g = \sum_{j=0}^{n} b_j x^j$, and $h = \frac{f}{g} = \sum_{k=0}^{m} c_k x^k$, where $a_i, b_j \in R$ and $c_k \in L$, and $a_{m+n}, b_n, c_m = 1$. Assume (by downward induction on ℓ) that $c_k \in R$ for $k > \ell$. Then

$$c_\ell = a_{n+\ell} - c_{\ell+1} b_{n-1} - \cdots - c_m b_{n+\ell-m} \in R$$

furnishes the inductive step. □

Let $L = \mathbb{Q}(\zeta_m)$, and define the $\boldsymbol{m}^{\textbf{th}}$ **cyclotomic polynomial**

$$\Phi_m(x) := \prod_{\substack{1 \le j \le m-1 \\ \gcd(j,m)=1}} (x - \zeta_m^j). \tag{I.L.15}$$

Its roots are the primitive m^{th} roots of 1, and it belongs *a priori* to $L[x]$. But considering a handful of examples, e.g.

$$\Phi_1 = x - 1, \;\; \Phi_4 = x^2 + 1, \;\; \Phi_6 = x^2 - x + 1, \;\; \Phi_8 = x^4 + 1,$$
$$\Phi_9 = x^6 + x^3 + 1, \;\; \Phi_{10} = x^4 - x^3 + x^2 - x + 1$$

they certainly appear to be nicer than that.

Indeed, as the m^{th} roots of 1 comprise primitive d^{th} roots of 1 for the divisors $d \mid m$, we have in $L[x]$

$$x^m - 1 = \prod_{d \mid m} \Phi_d(x). \tag{I.L.16}$$

Inductively assuming that the $\{\Phi_d(x)\}_{d<m}$ belong to $\mathbb{Z}[x]$ (clear for $d = 1$), and taking $R = \mathbb{Z}$, $f = x^m - 1$, and[44] $g = \prod_{d\|m} \Phi_d(x)$ in I.L.14(ii), we conclude that

$$\Phi_m(x) \in \mathbb{Z}[x]$$

for all m. As for the Φ_p, we have more generally

I.L.17. THEOREM. *Φ_m is irreducible in $\mathbb{Q}[x]$ for every m.*

PROOF. Suppose $\Phi_m = fg$, with f irreducible monic and both factors of positive degree; by Gauss's Lemma we may assume $f, g \in \mathbb{Z}[x]$. Let $\zeta \in L$ be a root of f, and consider a prime $p \nmid m$. Then ζ^p is a root of either f or g. I claim that ζ^p is a root of f.

If it is a root of g, then ζ is a root of $G(x) := g(x^p)$, and $f = m_\zeta \mid G$ yields $G = fh$ in $\mathbb{Z}[x]$. Reduce this mod p, writing $\bar{G} = \bar{f}\bar{h}$ in $\mathbb{Z}_p[x]$; since $\overline{G(x)} = \overline{g(x^p)} = \overline{g(x)}^p$, we have $\bar{f}\bar{h} = \bar{g}^p$. Let $\bar{q} \mid \bar{f}$ be an irreducible factor; then $\bar{q} \mid \bar{g}^p \implies \bar{q} \mid \bar{g} \implies \bar{q}^2 \mid \bar{f}\bar{g} \implies \overline{\Phi}_m$ has a repeated root. This is impossible since the gcd of $x^m - 1$ and $(x^m - 1)' = mx^{m-1}$ is 1. Claim is proved.

Now let η be any root of f, and θ any root of g. Both are primitive m^{th} roots of 1; and so $\theta = \eta^r$ for some r coprime to m, which we may write in the form $r = p_1 \cdots p_k$, for some primes $p_i \nmid m$. Iterating the above argument, $\theta = ((\eta^{p_1})^{p_2 \cdots})^{p_k}$ must be a root of f. But then Φ_m has a repeated root, a contradiction. $\square$

By I.L.17, Φ_m is the minimal polynomial of ζ_m over $\mathbb{Q}$. Writing $m = \prod_{i=1}^s p_i^{e_i}$, with $\{p_i\}$ distinct primes, the degree of the SFE is therefore

$$[\mathbb{Q}(\zeta_m){:}\mathbb{Q}] = \deg(\Phi_m) = \varphi(m) = \textstyle\prod_{i=1}^s p_i^{e_i - 1}(p_i - 1). \qquad \text{(I.L.18)}$$

Moreover, the roots $\mathcal{R}_{x^m-1}$ form a copy of $\mathbb{Z}_m$; and so by I.G.26 together with the transitivity of the action on $\mathcal{R}_{\Phi_m}$ implied by I.L.17,

(I.L.19)

$$\mathrm{Gal}_{\mathbb{Q}}(\Phi_m) \cong \mathrm{Aut}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong \mathrm{Gal}_{\mathbb{Q}}(x^m - 1) \cong \mathrm{Aut}(\mathbb{Z}_m) \cong \mathbb{Z}_m^*.$$

[44]The notation $d \| m$ means "d is a proper divisor of m", i.e. they are not equal (more generally, not associate).

As one application of the more general cyclotomic polynomials, we finish off the story about constructible n-gons.

I.L.20. THEOREM (Gauss-Wantzel). *A regular n-gon is constructible if and only if $n = 2^e p_2 \cdots p_s$ with $e \in \mathbb{N}$ and p_i distinct Fermat primes.*

PROOF. Recall that ζ_n is a constructible number $\iff$ $\mathbb{Q}(\zeta_n)$ is contained in a square-root tower over $\mathbb{Q}$. If n is *not* of the form shown, then (I.L.18) is not a power of 2 (since Fermat primes are the only ones with $p-1$ a power of 2), and so by the Tower Law such a square-root tower can't exist.

If n *is* of the indicated form, then by (I.L.18) $|G| = 2^t$; and appealing to [**Algebra I**, II.L.8], we obtain a normal series with $\mathbb{Z}_2$-quotients inside G. Applying the Galois correspondence, we see that $\mathbb{Q}(\zeta_n)$ is *itself* a square-root tower. □

Another application is to the inverse Galois problem for finite abelian groups, i.e. products of cyclic groups $\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_k}$. To exhibit them as quotients of a cyclotomic Galois group (I.L.19) it is enough to find distinct primes $p_1, \cdots, p_k$ with $a_i \mid (p_i - 1)$, and take $m = \prod p_i$. (Why? Use the Chinese Remainder Theorem.) The next result says this is always possible:

I.L.21. THEOREM. *For each $n \in \mathbb{Z}_{>1}$ there are infinitely many primes p with $n \mid p-1$.*

PROOF. Suppose to the contrary that $\{p_1, \ldots, p_N\}$ is a complete list. As Φ_n is monic, there exists $a \in \mathbb{N}$ sufficiently large that $M := \Phi_n(y) > 1$, where $y = anp_1 \cdots p_N$. Let p be a prime dividing M.

Since the constant term $\Phi_n(0) = \pm 1$, and each p_i divides the other terms, $p_i \nmid M$ ($\forall i$). So p is not in our list. Also $p \nmid n$: otherwise, $p \mid y \implies p \nmid M$, a contradiction.

Now $p \mid \Phi_n(y) \implies p \mid y^n - 1 \implies y^n \underset{(p)}{\equiv} 1$. We can't have $y^d \underset{(p)}{\equiv} 1$ for $d \| n$, since then $p \mid y^d - 1 \implies y$ is a repeated root of $x^n - 1$ over $\mathbb{Z}_p$ (impossible). But then y has order n in $\mathbb{Z}_p$ and Lagrange $\implies$ $n \mid p-1$. This contradicts our finite list. □

Finally we should mention the following generalization of the cyclicity of $\mathbb{Z}_p^*$, since it is relevant to deciding when (I.L.19) is cyclic.

I.L.22. THEOREM. *For each odd prime p and positive integer e, $\mathbb{Z}_{p^e}^*$ is cyclic.*

PROOF. Write $G = \mathbb{Z}_{p^e}$ and $J := \{a \in G \mid a^p = 1\}$. Given $a \in J$, $a^p \underset{(p)}{\equiv} a \implies a \underset{(p)}{\equiv} 1$. There are then two possibilities: $a = 1 + zp^{e-1}$, which indeed gives p elements in J; and $a = 1 + yp^{f-1} + zp^f$ with $1 < f < e$ and $0 < y < p$. If the last one happened, we'd have $1 \underset{(p^{f+1})}{\equiv} a^p \underset{(p^{f+1})}{\equiv} 1 + yp^f \implies y \underset{(p)}{\equiv} 0$, a contradiction. So $|J| = p$.

Now apply the p-primary version of the structure theorem together with $|G| = p^{e-1}(p-1)$ to decompose G as in internal direct product of $H := \{g \in G \mid g^{p^{e-1}} = 1\}$ and $K := \{g \in G \mid g^{p-1} = 1\}$, with $|H| = p^{e-1}$ and $|K| = p-1$, and to write $H \cong \times_{i=1}^k \mathbb{Z}_{p^{e_i}}$ ($\sum e_i = e-1$). But then $H \cap J = \mathbb{Z}_p^k$, which gives $k = 1$. So H is cyclic.

For K, let $a \in G$ be a generator mod p (i.e. of $\mathbb{Z}_p^*$) and put $b := a^{p^{e-1}} \in G$. Since $b \underset{(p)}{\equiv} a$ (Fermat), its powers $b, b^2, \ldots, b^{p-1}$ must be distinct in G. But since $b^{p-1} = a^{|G|} = 1$, these b^i lie in K; and so $K = \langle b \rangle \cong \mathbb{Z}_{p-1}$ is also cyclic. Conclude that $G \cong \mathbb{Z}_{p^{e-1}} \times \mathbb{Z}_{p-1} \cong \mathbb{Z}_{p^{e-1}(p-1)}$. □

This result (which immediately implies $\mathbb{Z}_{2p^e}^*$ is also cyclic) is perhaps surprising, since of course $\mathbb{Z}_{p^e}^*$ is *not* a finite field. It does not hold for $p = 2$: $\mathbb{Z}_{2^e}^*$ fails to be cyclic for $e > 2$ (cf. [**Jacobson**]).

Incidentally, while it's great to know that these groups are cyclic, it isn't necessarily obvious what a generator is. It is a conjecture of Artin (open since 1927) that every non-square positive integer is a generator of $\mathbb{Z}_p^*$ for infinitely many p. It isn't known for any integer, but predicts for instance that 2 is a generator of $\approx 37\%$ of $\mathbb{Z}_p^*$'s.