# Outline of Galois Theory Development

1. Field extension $F \hookrightarrow E$ as vector space over $F$. $|E : F|$ equals dimension as vector space. If $F \hookrightarrow K \hookrightarrow E$ then $|E : F| = |E : K||K : F|$.

2. Element $a \in E$ is algebraic over $F$ if and only if $|F(a) : F|$ is finite. Minimum polynomial $f(X) \in F[X]$ for algebraic $a \in E$. $f(X)$ is irreducible, $F(a) = F[a] \cong F[X]/(f(X))$, $|F[a] : F| = \deg f(X)$, a basis is $\{1, a, a^2, \ldots, a^{d-1}\}$, where $d = \deg f(X)$. The set of elements $a \in E$ which are algebraic over $F$ is a subfield of $E$.

3. Existence of Splitting Fields for a polynomial or family of polynomials $\mathcal{F} \subset F[X]$. Existence of Algebraic Closure. Characterizations of Algebraic Closure: A field $E$ is algebraically closed if every non-constant polynomial in $E[X]$ factors as a product of linear polynomials. (Equivalently, every non-constant polynomial in $E[X]$ has a root in $E$.) A field $E$ is an algebraic closure of a subfield $F$ if $E$ is algebraic over $F$ and every non-constant polynomial in $F[X]$ factors as a product of linear polynomials in $E[X]$. Such an $E$ is algebraically closed.

4. Uniqueness of Splitting Fields.
MAIN LEMMA: $h : F \to L'$ extends to $h' : F[a] \to L'$ if and only if $hf(X)$ has roots in $L'$, where $f(X)$ is the minimum polynomial for $a$ over $F$ and $hf(X)$ is the image of $f(X)$ under the map $F[X] \to L'[X]$ induced by $h$. The number of distinct extensions of $h$, $h' : F[a] \to L'$, equals the number of distinct roots of $hf(X)$ in $L'$, and $h'$ is determined by the value $h'(a) = a'$, where $a'$ is a root of $hf(X)$ in $L'$.
CONSEQUENCE: If $F \hookrightarrow L$ is a splitting field of $\mathcal{F} \subset F[X]$, $h : F \to F'$ a field homomorphism, and $F' \hookrightarrow L'$ an extension which contains a splitting field of $h\mathcal{F} \subset F'[X]$, then $h$ extends to $h' : L \to L'$. In particular, any two splitting fields of $\mathcal{F}$ are isomorphic over $F$.

5. COROLLARY OF MAIN LEMMA: If $|E : F|$ is finite, the number of distinct extensions $h' : E \to L$ of $h : F \to L$ is always less than or equal to $|E : F|$.

6. Normal (Algebraic) Extensions $F \hookrightarrow E$. Three characterizations:
   (i) $E$ is a splitting field of a family of polynomials over $F$.
   (ii) If $h : E \to \hat{F}$ is any embedding into the algebraic closure of $F$ with $h = \mathrm{id}$ on $F$, then $h(E) = E$. (WLOG, $F \subset E \subset \hat{F}$.)
   (iii) If an irreducible polynomial $g(X) \in F[X]$ has a root in $E$ then $g(X)$ factors into a product of linear factors in $E[X]$. That is, all roots of $g(X)$ in $\hat{F}$ are in $E$.

7. The derivative $f'(X)$ and algebraic properties. Especially $\gcd(f, f') = 1$ if and only if $f(X)$ has no multiple roots. Consequently, if $\mathrm{char}(F) = 0$ or if $F$ is a finite field then every irreducible polynomial of degree $d$ in $F[X]$ has $d$ distinct roots in the algebraic closure $\hat{F}$.

8. Separable (Algebraic) Extensions $F \hookrightarrow E$. Three characterizations:
   (i) Every element $a \in E$ is the root of a polynomial with no multiple roots. That is, every element of $E$ is 'separable' over $F$.
   (ii) $E$ is generated over $F$ by separable elements.
   (iii) If $E' \subset E$ and $|E' : F|$ is finite, then $|E' : F|$ equals the number of distinct embeddings $h' : E' \to \hat{F}$ with $h' = \mathrm{id}$ on $F$. (So if $|E : F|$ is finite, then $|E : F|$ equals the number of distinct embeddings $E \to \hat{F}$ over $F$).

   NOTE: It follows from these considerations, especially (**??**), that given $F \hookrightarrow K \hookrightarrow E$, $K/F$ and $E/K$ both separable implies $E/F$ separable. Also, the set of elements in any $E$ which are separable over $F$ forms a subfield of $E$.

9. Theorem of the Primitive Element for finite separable extensions $E/F$. Namely, $E = F[a]$, for some $a \in E$. There are many proofs. E.g., start with $F[u, v]$, then look at elements $a = u + cv$ with $c \in F$. If $f(X)$ and $g(X)$ are the minimal polynomials for $u$ and $v$ over F, choose $c$ so that $f(a - cX)$ and $g(X)$ have exactly one common root, namely $v$. Then $\gcd(f(a - cX), g(X)) \in F[a][X]$ must be $X - v$, hence $v$ is in $F[a]$, so also $u$ is in $F[a]$, and $F[u, v] = F[a]$. (This proof works for infinite $F$. If $F$ is finite so is $E$, and $E^*$ is a cyclic multiplicative group, so $E = F[a]$ is clear.)

10. Define $E/F$ to be a Galois extension if and only if $E$ is separable AND normal over F. (This is the 'right' definition, because the conditions separable and normal are easily understood in terms of individual generators of $E$ over $F$ and the roots of their minimal polynomials.)

11. COROLLARY: A finite extension $E/F$ is Galois if and only if $|E : F|$ equals the number of automorphisms $g : E \to E$ with $g = \mathrm{id}$ on $F$. (The proof just combines characterization (**??**) of Normal with characterization (**??**) of Separable.)

12. Define the Galois Group $\mathrm{Gal}(E/F)$ to be the group of automorphisms $g : E \to E$ which fix all elements of $F$. For finite Galois extensions, $|\mathrm{Gal}(E/F)| = |E : F|$, by item 11.

13. If $f(X)$ is a separable, irreducible polynomial of degree $n$, then the Galois group of its splitting field is a transitive subgroup of the symmetric group $S_n$ of all permutations of the roots of $f(X)$. The order of the group is divisible by $n$.

14. Define the Fundamental Correspondences

$$\{H \leq G\} \leftrightarrow \{\text{intermediate fields } L \text{ of } E/F\},$$

where $G = \mathrm{Gal}(E/F)$. $H \mapsto E^H$, the subfield of $E$ fixed by all elements of $H$. $L \mapsto \mathrm{Gal}(E/L)$, the subgroup of $G$ fixing all elements of $L$.

15. State and prove the Fundamental Theorem for Finite Galois Extensions.

The direction $L \mapsto \mathrm{Gal}(E/L) = H \mapsto E^H = L$ is 'easy', and just uses the definitions and the fact from 12 that $|\mathrm{Gal}(E/L)| = |E : L|$. The direction $H \mapsto E^H = L \mapsto \mathrm{Gal}(E/L) = H$ requires more. The sticking point is why is $|E : E^H| \leq |H|$? But if $E = L[a]$ then the product $\prod(X - ha)$, $h \in H$, is a polynomial with coefficients in $E^H = L$ which has $a$ as a root and has degree $|H|$. So $|L[a] : L| \leq |H|$. By the Theorem of the Primitive Element, the assumption $E = L[a]$ is justified here. If $g : E \to E$ is an automorphism over $F$ and $L \subset E$ is an intermediate field, corresponding to subgroup $H \subset G$, then it is a trivial 'group action' fact that the subgroup of $G$ corresponding to the field $gL \subset E$ is the conjugate subgroup $gHg^{-1}$ of $H$. So $H$ is normal in $G$ if and only if $L$ is normal over $F$. In this case, $\mathrm{Gal}(L/F) = G/H$ follows easily, since there is a map $G \to \mathrm{Gal}(L/F)$, which is onto and has kernel $H$.

16. Two miscellaneous results:
    (i) An algebraic extension $F \hookrightarrow E$ is primitive, that is, $E = F[a]$, if and only if there are only finitely many intermediate fields $L$, with $F \subset L \subset E$.
    (ii) If $H$ is a finite group of automorphisms of a field $E$ and $E^H$ is the fixed field, then the extension $E/E^H$ is finite, normal, separable, and $|E : E^H| = |H|$.

(Result (**??**) is closely related to the trickier part of the Fundamental Theorem in 15. In that situation though, one knew $E/E^H$ was finite, normal, separable, because one started with a finite Galois extension $E/F$. But, here, all this must be proved.)

17. Two results about composite extensions:
    (i) If $K/F$ is a finite Galois extension and $L/F$ is any extension, then $KL$ is Galois over $L$ with $\mathrm{Gal}(KL/L) = \mathrm{Gal}(K/K \cap L) \subset \mathrm{Gal}(K/F)$.
    (ii) If $K/F$ and $L/F$ are two finite Galois extensions then $KL/F$ is Galois and

$$\mathrm{Gal}(KL/F) \subset \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F),$$

specifically, the subgroup $\{(u, v) \mid u : K \to K \text{ and } v : L \to L \text{ with } u = v \text{ on } K \cap L\}$.

(In part (**??**), interpret $KL$ and $K \cap L$ as subfields of $\hat{L}$, the algebraic closure of $L$. Specifically, $\hat{L}$ contains a unique isomorphic copy of $K$, since $K$ is the splitting field of some polynomial in $F[X]$. In part (**??**), interpret both $K$ and $L$ as subfields of $\hat{F}$.)

18. Artin's proof that $\mathbb{C} = \mathbb{R}[i]$ is algebraically closed. First, every element of $\mathbb{C}$ has square roots, so $\mathbb{C}$ has no quadratic extensions. Suppose $E/\mathbb{C}$ is some finite algebraic extension, which WLOG can be assumed normal over $\mathbb{R}$. If $|E : \mathbb{R}|$ is divisble by an odd prime, the fixed field of a Sylow 2-subgroup of $\mathrm{Gal}(E/\mathbb{R})$ would have odd degree over $\mathbb{R}$. Any element of this field would have minimal polynomial over $\mathbb{R}$ of odd degree. But every odd degree polynomial over $\mathbb{R}$ has a root in $\mathbb{R}$, hence can't be irreducible. Thus, $|E : \mathbb{C}| = 2^n$, for some $n$. But then if $n > 0$, $\mathrm{Gal}(E/\mathbb{C})$ would contain a normal subgroup of index 2, corresponding to a proper quadratic extension of $\mathbb{C}$.

19. EXAMPLE: Roots of Unity.

    The roots of $X^n - 1 = 0$ that lie in a field extension $E$ of $F$ form a multiplicative subgroup of $E$, hence form a cyclic group. If $\mathrm{char}(F) = p$ does not divide $n$, there are $n$ roots in the splitting field. Thus, the Galois group is a subgroup of $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, hence is abelian of order dividing $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$. The splitting field is generated over $F$ by any primitive $n$th root of 1, say $z$, and a Galois automorphism is determined by the image of $z$, which is some power $z^j$ with $(n, j) = 1$. The automorphism must fix $F$, so perhaps only a proper subgroup of such $j$ in $(\mathbb{Z}/n\mathbb{Z})^*$ give Galois group elements. In $\mathbb{Z}[X]$, there is a factorization $X^n - 1 = \prod_d F_d(X)$, where $d$ runs over all divisors of $n$, and the $F_d(X)$ are defined inductively. The roots of $F_n(X)$ are precisely the primitive $n$th roots of 1, so $\deg F_n(X) = \phi(n)$. It is proved that all $F_n(X)$ are irreducible in $\mathbb{Q}[X]$, hence the splitting field of $X^n - 1$ over $\mathbb{Q}$ has degree $\phi(n)$ and Galois group $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^*$. (If $n = mp^i$, with $(m, p) = 1$, $p = \mathrm{char}(F)$, then $X^n - 1 = (X^m - 1)^q$, $q = p^i$, so the splitting fields of $X^n - 1$ and $X^m - 1$ coincide.)

20. EXAMPLE: $n$th roots.

    Assume the $n$th roots of 1 are in $F$, say $z, z^2, \ldots, z^n = 1$. We also assume $\mathrm{char}(F) = 0$ or $(n, p) = 1$, where $p = \mathrm{char}(F)$. If $a \in F$, the polynomial $X^n - a$ has roots $b, zb, \ldots, z^{(n-1)}b$, hence the splitting field is generated over $F$ by one $n$th root $b$ of $a$. A Galois automorphism is determined by the image of $b$, which is some $z^j b$. Thus the Galois group is a subgroup of $\mathbb{Z}/n\mathbb{Z}$, hence is cyclic.

21. EXAMPLE: $X^p - X + a$, where $\mathrm{char}(F) = p$, and $a \in F$.

    If $b$ is one root then all the roots are given by $b, b + 1, b + 2, \cdots, b + (p - 1)$. A Galois automorphism is determined by the image of $b$, which is some $b + j$. Since $p$ is prime, either all roots are in $F$ or the Galois group is cyclic of order $p$.

22. EXAMPLE: Finite fields.

    For each prime $p$ and positive integer $n$, there is exactly one field $F_q$ with $q = p^n$ elements, namely, the splitting field of $X^q - X$ over $F_p$. The Galois group over the prime field $F_p = \mathbb{Z}/p\mathbb{Z}$ is cyclic of order $n$, generated by the Frobenius automorphism $x \mapsto x^p$. $F(p^d) \subset F(p^n)$ if and only if $d$ divides $n$. Also, any extension $E/F$ where both $F$ and $E$ are finite fields is Galois, that is, normal and separable, with cyclic Galois group generated by some power of the Frobenius automorphism. Adjoining a single root of any irreducible polynomial of degree $n$ over $\mathbb{Z}/p\mathbb{Z}$ gives the field $F_q$, where $q = p^n$. Since the cyclic Galois group acts transitively on the $n$ roots, it must act as an $n$-cycle on these roots. A product of distinct irreducible polynomials of degree $n_1, n_2, \ldots, n_r$ will also have a cyclic Galois group, which is generated by a product of disjoint $n_j$ cycles. The degree of the splitting field will be $\mathrm{lcm}(n_1, n_2, \ldots, n_r)$. Since $F^*$ is a finite cyclic group for any finite field $F$, the splitting field of $X^m - 1$, $(m, p) = 1$, is the field $F_q$, $q = p^n$, where n is least so that $m$ divides $p^n - 1$. The polynomial $X^q - X$, $q = p^n$, is the product of all monic irreducible polynomials of degrees $d$ which divide $n$.

23. EXAMPLE: Iterated radical extensions. Suppose

$$F = F_0 \hookrightarrow F_1 \hookrightarrow \cdots \hookrightarrow F_m = E$$

    is a sequence of extensions such that $E$ is normal over $F$ and each extension $F_i \hookrightarrow F_{i+1}$ is one of three types:

    (i) splitting field of $X^n - 1$ with char = 0 or char = $p$ and $(n, p) = 1$,
    (ii) splitting field of $X^n - a$, where $a \in F_i$ and the $n$th roots of 1 are in $F_i$, with char = 0 or char = $p$ and $(n, p) = 1$,

(iii) splitting field of $X^p - X + a$, where $a \in F_i$ and char $= p$.

Then $\mathrm{Gal}(E/F)$ is a solvable group.

This is rather easy from The Fundamental Theorem, Examples 19, 20, 21 above, and the definition of (finite) solvable group. But this implies the amazing result that certain polynomials $f(X) \in F[X]$, e.g. quintics with group $S_5$, cannot have a root in any field $K$ obtained from $F$ by a sequence of extensions of the above types, hence there cannot be formulas for the roots as iterated radicals. (Namely, if $K$ is obtained from $F$ by a sequence of extensions of the above types, then the normal closure $E$ of $K$ can also be so obtained, because at each stage the normal closure over $F$ can be obtained by further extensions of exactly the same type. For example if $n$th roots of a are adjoined at some point to a field which is assumed inductively to be normal over $F$, then also adjoin successively the $n$th roots of all conjugates of a to give the next normal closure. The Galois group of $f(X)$ would then be a quotient group of $\mathrm{Gal}(E/F)$, hence solvable.)

24. EXAMPLE: There is a converse to Example 23. Suppose a separable polynomial $f(X)$ in $F[X]$ has a solvable Galois group, $G$. Then the roots of $f(X)$ are in a field $E$ obtained from $F$ by a sequence of extensions as in Example 23. Namely, if $E$ is the splitting field of $f(X)$ over $F$ and $F'$ is the extension obtained by adjoining all $|G|$-th roots of unity to $F$, let $E' = EF'$ be the composite. Then $E'/F'$ is Galois and has solvable group, say $G' \subset G$. There is a composition series for $G'$ with each successive quotient group cyclic of prime order, say $p_i$, where $p_i$ divides $|G|$. Hence, either $p_i = p = \mathrm{char}(F)$, or the $p_i$-th roots of 1 are in $F'$. The Fundamental Theorem produces a corresponding sequence of cyclic Galois extensions. The desired converse to Example 23 then follows by dealing with the cyclic cases, as in the next three paragraphs.

25. LINEAR INDEPENDENCE OF CHARACTERS: If $G$ is a group and $h_1, \ldots, h_n : G \to E^*$ are distinct homomorphisms from $G$ to the multiplicative group of a field $E$, then $\{h_1, \ldots, h_n\}$ are linearly independent as functions $G \to E$. The proof uses a little sleight of hand to reduce the length of any linear dependence relation. Note if $G = E^*$, then automorphisms $E \to E$ can be interpreted as characters of $E^*$.

26. EXAMPLE: $E/F$ Galois, with cyclic group of order $n$, where the $n$th roots of 1 are in $F$ and where char $= 0$ or char $= p$ with $(n, p) = 1$. Then $E = F[\sqrt[n]{a}]$, for some $a \in F$. (Let $\mathrm{Gal}(E/F) = \{1, s, s^2, \ldots, s^{n-1}\}$ and let $z \in F$ be a primitive $n$th root of 1. Use linear independence of the characters $\{s^j\}$ of $E^*$ to find $b \in E$ so that the element given by

$$r = b + zs(b) + z^2 s^2(b) + \cdots + z^{n-1} s^{n-1}(b)$$

is not 0. Then $zs(r) = r$, so $r$ has $n$ distinct conjugates in $E$ and $s(r^n) = r^n$. It follows that $r^n = a \in F$ and $E = F[r]$.)

27. EXAMPLE: $E/F$ Galois, with cyclic group of order $p = \mathrm{char}(F)$. Again let $\mathrm{Gal}(E/F) = \{1, s, \ldots, s^{p-1}\}$ and choose $t \in E$ with $t + s(t) + \ldots + s^{p-1}(t) = \mathrm{Tr}(t) \neq 0$, which can be done since the characters are linearly independent. Note $\mathrm{Tr}(t) \in F$ since $s(\mathrm{Tr}(t)) = \mathrm{Tr}(t)$. Now set

$$r = -\frac{1}{\mathrm{Tr}(t)}(s(t) + 2s^2(t) + \cdots + (p-1)s^{p-1}(t)).$$

Then $s(r) - r = 1$, so $r$ has $p$ distinct conjugates in $E$ and $s(r^p - r) = (r+1)^p - (r+1) = r^p - r$, so this element is in $F$. Thus, $r$ is a root of $X^p - X + a$, for some $a \in F$, and $E = F[r]$.

28. Norms and Traces. Let $E/F$ be a finite separable extension, $s_1, \ldots, s_n$ the distinct embeddings $E \to \hat{F}$, the algebraic closure of $F$, with $s_i = \mathrm{id}$ on $F$. So $n = |E : F|$. For $r \in E$, define the norm $\mathrm{N}_{E/F}(r) = \prod_i s_i(r)$, and define the trace $\mathrm{Tr}_{E/F}(r) = \sum_i s_i(r)$. Here are some properties of norms and traces:

- If $X^d - a_1 X^{d-1} + \cdots + (-1)^d a_d$ is the minimal polynomial for $r$ over $F$ then $\mathrm{N}(r) = a_d^{n/d}$ and $\mathrm{Tr}(r) = (n/d)a_1$. In particular, $\mathrm{N}(r)$ and $\mathrm{Tr}(r)$ are functions $E \to F$.
- $\mathrm{N}(rs) = \mathrm{N}(r)\,\mathrm{N}(s)$, $\mathrm{Tr}(r+s) = \mathrm{Tr}(r) + \mathrm{Tr}(s)$, and $\mathrm{Tr}(cr) = c\,\mathrm{Tr}(r)$ for $c \in F$.

- Both trace and norm are transitive for a double extension $F \hookrightarrow E \hookrightarrow K$, that is, $\mathrm{N}_{K/F}(r) = \mathrm{N}_{E/F}(\mathrm{N}_{K/E}(r))$, and similarly for the trace.
- The $F$-linear map $E \to E$ given by multiplication by $r$ has trace $\mathrm{Tr}(r)$ and det $\mathrm{N}(r)$.

29. Hilbert Theorem 90. If $E/F$ is a cyclic Galois extension with Galois group generated by $s : E \to E$, and if $x \in E$ has norm $\mathrm{N}(x) = 1$, then $x = b/s(b)$ for some $b \in E$. If $y \in E$ has trace $\mathrm{Tr}(y) = 0$, then $y = c - s(c)$, for some $c \in E$.

    (Examples are provided by $x = \zeta_n \in F$, where $n = |E : F|$ and by $y = 1 \in F$, where $|E : F| = p = \mathrm{char}(F)$. In these cases, a proof is given in Examples 26 and 27 above. The general proof follows along similar lines, using linear independence of the Galois automorphisms to write down appropriate elements $b$ and $c$ in E).

30. Symmetric Functions and The General Equation of Degree $n$. Suppose $x_1, \ldots, x_n$ are indeterminates, $F(x_1, \ldots, x_n)$ the field of rational functions in $n$ variables. The symmetric group $S_n$ acts by permuting the $x_i$. The fixed field is $F(\sigma_1, ..., \sigma_n)$, where $\sigma_j$ is the $j$th elementary symmetric function of the $x_i$. This is seen from Artin's result **??**, along with the identity

$$X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n = (X - x_1) \cdots (X - x_n).$$

    It can be shown directly that $\{\sigma_1, \ldots, \sigma_n\}$ are algebraically independent over $F$, but this is a special case of a general fact about "transcendence degree and transcendence bases" of (non-algebraic) field extensions. A slightly different perspective on the above setup is to start with algebraically independent $a_1, \ldots, a_n$ over $F$, then look at the splitting field of the separable polynomial $X^n - a_1 X^{n-1} + ... + (-1)^n a_n$. If the roots are called $x_1, \ldots, x_n$, then the splitting field is $F(x_1, \ldots, x_n)$ and the Galois group is $S_n$. In any case, one can see by this Galois theory viewpoint that any symmetric rational function of the $x_i$ is a rational function of $\sigma_1, \ldots, \sigma_n$. A symmetric rational function must have symmetric numerator and denominator when written in lowest terms, and thus symmetric polynomials with coefficients in $F$ are polynomials in $\sigma_1, \ldots, \sigma_n$. (It is easy enough to prove this result for symmetric polynomials with coefficients in any commutative ring by an induction on degree.)

    A consequence of Galois theory and non-solvability of $S_n$ is that there can be no iterated radical formulas for the roots of polynomials of degree greater than 4, where the radicals are expressed universally in terms of the coefficients of the polynomial. In the cases $n = 3$ and 4, the composition series for $S_3$ and $S_4$ lead systematically to universal iterated radical formulas for the roots of the general equation, at least if the characteristic is not 2 or 3.

31. The Discriminant. The expression $d = \prod_{i<j}(x_i - x_j)$ is invariant under the alternating group $A_n \subset S_n$. $D = d^2$ is invariant under $S_n$, hence is a polynomial in the symmetric functions $s_n$. When the $x_i$ are roots of a separable polynomial, $D$ is called the discriminant of the polynomial, and is given by a universal formula in terms of the coefficients of the polynomial. If the ground field $F$ has characteristic different from 2, the Galois group is a subgroup of $A_n$ if and only if $D$ is a square in $F$. For the quadratic $X^2 + aX + b$, $D = a^2 - 4b$. For the cubic $X^3 + pX + q$, $D = -4p^3 - 27q^2$. If $\mathrm{char}(F) \neq 3$, any cubic can be put in this form without changing $D$, by replacing $X$ with $(X - a/3)$, where $a$ is the coefficient of $X^2$. There are many interesting formulas for or involving discriminants.

32. Determination of Galois Groups. There are algorithms for determining the Galois group of any polynomial in $\mathbb{Q}[X]$, but these algorithms are not feasible to carry out by hand, even in degrees as low as 5. For irreducible cubics, there are only two possibilities, distinguished by the discriminant. For irreducible quartics, there are five possible Galois groups. For irreducible quintics, there are also only five possible Galois groups, because $S_5$ only has five isomorphism types of transitive subgroups. But determining which group is correct can be difficult without some luck. An irreducible quintic with three real roots always has group $S_5$, because complex conjugation provides a 2-cycle in the Galois group, and, of course, there is a 5-cycle in the Galois group. There is an extremely useful result concerning reduction modulo $p$ that in many cases is adequate for determining a Galois group. Suppose monic $f(X)$ has integer coefficients and suppose the mod $p$ reduction of $f(X)$ has no repeated factors. Then the Galois group of $f(X)$ over $\mathbb{Q}$ contains a permutation of the same cycle form as a generator of

the (cyclic) Galois group over $\mathbb{Z}/p\mathbb{Z}$, described in Example 22 above. Thus, factoring $f(X)$ mod $p$ for various primes may provide enough cycle types in the Galois group to determine the group. The mod $p$ reduction result is proved using the theory of prime ideals in rings of algebraic integers.

33. Inseparability. Suppose $E/F$ is an arbitrary algebraic field extension. The set of all elements $a$ in $E$ separable over $F$ forms a field, $E_s$. This is a consequence of characterization (**??**) of separability. Every element $b$ in $E$ not in $E_s$ is purely inseparable over $E_s$. This means $b^q$ is in $E_s$ for some $q = p^n$, $p = \text{char}(F)$. The minimal polynomial for $b$ over $F$ has form $g(X^q)$, where $g(X)$ is an irreducible separable polynomial over $F$. Since $X^q - b^q = (X - b)^q$, it is clear that any embedding of $E$ into an algebraic closure $\hat{E}$ of $E$ which fixes $E_s$ must be the Identity. Thus, if $E$ is normal over $F$, $\text{Gal}(E/F) = \text{Gal}(E_s/F)$. Also inside $E$ is the field $E_i$ consisting of elements which are purely inseparable over $F$. Always $F$ is the intersection of $E_s$ and $E_i$. In general, the extension $E/E_i$ is not separable, so there is an 'asymmetry' in the two factorizations $F \hookrightarrow E_s \hookrightarrow E$ and $F \hookrightarrow E_i \hookrightarrow E$. In fact, $E_i = F$ is possible even when $E_s$ is a proper subfield of $E$. However, if $E$ is normal over $F$ then $E$ is the composite $E_iE_s$ and $E$ is separable over $E_i$. In this case, $E_i$ is the fixed field of the Galois group $\text{Gal}(E/F)$, and $\text{Gal}(E/E_i) = \text{Gal}(E/F) = \text{Gal}(E_s/F)$.