FIELDS AND GALOIS THEORY

GEORGE GILBERT

1. Rings and Polynomials

Given a polynomial of degree n, there exist at most n roots in the field. Given a polynomial that factors completely,

$$\begin{aligned}(x-r_1)(x-r_2)...(x-r_n) &= x^n-(r_1+...+r_n)x^{n-1} \\ &\quad +\left(\underbrace{r_1r_2+...+r_{n-1}r_n}_{\binom{n}{2}\text{ terms}}\right)x^{n-2}+\ldots+(-1)^n r_1\cdots r_n.\end{aligned}$$

We define the first, second, ... symmetric polynomials to be

$$\begin{aligned}s_1(x) &= \sum_j x_j, \\ s_2(x) &= \sum_{j,k} x_jx_k,\end{aligned}$$

etc. A general **symmetric polynomial** $p(x_1,...,x_n)$ is a polynomial that is unchanged whenever the variables are permuted.

Theorem 1. *Every symmetric polynomial in n variables is a polynomial in $s_1(x),...,s_n(x)$.*

Problem 1. Find a polynomial satisfied by the squares of the roots of x^2-5x+3 without finding the roots.

Proof. We have $r_1+r_2=5$, $r_1r_2=3$, so $y^2-(r_1^2+r_2^2)y+r_1^2r_2^2=y^2-(r_1^2+r_2^2)y+9$, with the rest left to the reader. □

The discriminant of a polynomial is

$$(r_1-r_2)^2...(\text{all possible pairs})...(r_{n-1}-r_n)^2.$$

Because it is symmetric, it may be expressed in terms of the coefficients of the polynomial and is 0 if and only if there are repeated roots.

Fitting a polynomial of degree at most n that passes through $n+1$ points (x_i,y_i), $i=0,1,\ldots,n$ requires us to solve the linear system

$$\begin{aligned}a_nx_0^n+...a_1x_0^1+a_0 &= y_0 \\ &... \\ a_nx_n^n+...a_1x_n^1+a_0 &= y_0\end{aligned}$$

for the coefficients $a_0, a_1, ..., a_n$ for any $y_0, y_1, ...y_n$. Then we need to solve

$$\begin{pmatrix} 1 & x_0 & x_0^2... & x_0^n \\ 1 & x_1 & x_1^2... & x_1^n \\ ... & ... & ... & ... \\ 1 & x_n & ... & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{pmatrix},$$

which means the Vandermonde determinant

$$\begin{vmatrix} 1 & x_0 & x_0^2 & ... & x_0^n \\ 1 & x_1 & x_1^2 & ... & x_1^n \\ & & ... & & \\ 1 & x_n & x_n^2 & ... & x_n^n \end{vmatrix} \neq 0.$$

The square of this determinant is the discriminant.

Given a field k, let $k[x]$ be the polynomials over k. This ring is a Euclidean domain. This means that there is a function $d : k[x] - \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $f, g \in k[x]$, $g \neq 0$, there exist q and r such that

$$f = qg + r$$

where either $r = 0$ or $0 \leq d(r) < d(g)$. The other condition is that if $g|f$, then $d(g) \leq d(f)$. For polynomials, $d(f) =$ degree of f. Another example of a Euclidean domain is $\mathbb{Z}$. The Euclidean algorithm is used to to find GCDs of elements of the ring.

Theorem 2. *Every Euclidean domain is a principal ideal domain.*

Note: an **ideal** is a subring that is closed under multiplication by any element in the whole ring. A **principal ideal** is the set of multiples of one particular element of the ring. For example, $(2) = \{2n : n \in \mathbb{Z}\} = (-2)$ is a principal ideal in $\mathbb{Z}$. We say 2 and -2 are **associates** because they generate the same ideal or, equivalently, each is a unit multiple of the other. For example, $x^2 + 3$ and $6 + 2x^2$ are associates in $\mathbb{C}[x]$.

Proof. Let I be a nonzero ideal. Let x have an element such that $d(x)$ is minimal. Choose $y \in I$. Then $y = qx + r$ with $r = 0$ or $d(r) < d(x)$. The second possibility is impossible, so every element of the ideal is a multiple of x. □

Theorem 3. *Every principal ideal domain is a unique factorization domain.*

Note: unique factorization means unique up to rearrangement and up to multiplication by units.

2. Field extensions

The following is useful, especially when working with finite fields.

Theorem 4. *A finite multiplicative subgroup of a field is cyclic.*

For k a field, let $k(x)$ be the field of rational functions, that is

$$\begin{aligned} k(x) &= \left\{ \frac{p(x)}{q(x)} : q(x) \neq 0;\ p(x), q(x) \in k[x] \right\} \\ &= \{(p(x), q(x)) : q(x) \neq 0;\ p(x), q(x) \in k[x]\} \diagup \text{equivalence relation} \end{aligned}$$

If $K \subseteq L$ are fields, we say that L is a **field extension** of K. We write $L \diagup K$ to denote the extension of K by L. If $\alpha \in L$, then there are two types of elements. We say α is

algebraic over K if there exists $p(x) \in K[x]$ such that $p(\alpha) = 0$. Otherwise, α is called **transcendental** over K. Then, if α is transcendental, then $K[\alpha] \cong K[x]$, $K(\alpha) \cong K(x)$. If α is algebraic, then $K[\alpha] = K(\alpha) \cong \frac{K[x]}{(f)}$, where f is the "minimal polynomial" of α, i.e. a polynomial of minimal degree such that $f(\alpha) = 0$, which is necessarily irreducible.
Proof: Map $K[x] \to K[\alpha]$ by $p(x) \mapsto p(\alpha)$, which is clearly an onto map. Then the kernel is $\{g : g(\alpha) = 0\} = (f)$, so by the first isomorphism theorem for rings, we are done. If f is irreducible, (f) is a maximal ideal, which implies our quotient ring is a field.

An ideal P is called a **prime ideal** if $uv \in P$ implies $u \in P$ or $v \in P$. If you quotient a ring by a prime ideal, then the quotient is an integral domain.

If α is algebraic over K, then $K[\alpha]$ is a finite-dimensional vector space over K, where the dimension is the degree of the minimal polynomial f minus one. The basis could be chosen to be

$$1, \alpha, \alpha^2, ..., \alpha^{\deg f - 1}$$

We have L/K is **finite** if L is finite-dimensional as a vector space over K. We denote the dimension $[L : K]$. We say L/K is **algebraic** if every element of L is algebraic over K.

Theorem 5. *Every finite extension is algebraic.*

Theorem 6. *If $K \subseteq L \subseteq M$ are fields, then $[M : K] = [M : L][L : K]$.*

Proof. Take a basis $\{m_1, \ldots\}$ for M over L and a basis $\{\ell_1, ...\}$ for L over K. Then you can prove that $\{m_i \ell_j\}$ is a basis for M over K. □

Theorem 7. *Suppose $K \subseteq L \subseteq M$ are fields. Then M/K is algebraic iff M/L and L/K are algebraic.*

Corollary 8. *If α and β are algebraic over K, then so are $\alpha \pm \beta$, $\alpha\beta$, α/β .*

3. Splitting fields, normal and separable extensions

Definition 9. *For $f \in K[x]$, L is the **splitting field** for f if it is the smallest field over which f splits (i.e. factors completely).*

Theorem 10. *If L is the splitting field of $f \in K[x]$, The index $[L : K]$ divides $(\deg f)!$.*

Proof. (Induction on $n = \deg f$) For $n = 1$, $f(x) = ax + b$ with $a, b \in K$, $a \neq 0$, and so $x = \frac{-b}{a}$ is the only root and is in K. Then $L = K$, and $\deg f = 1 = [L : K]$.
Now assume that for some $k \geq 1$ the result has been proven for $1 \leq n \leq k$.
Consider a polynomial p of degree $k+1$. Then for a fixed root α of f, the minimal polynomial $m_\alpha(x) \in K[x]$ of α divides $p(x)$. There are two cases.

Case 1 If $m_\alpha(x) = p(x)$, then $[K(\alpha), K] = k + 1$, since $\left\{1, \alpha, \alpha^2, ..., \alpha^k\right\}$ is then a basis for the vector space $K(\alpha)$ over K. In that case, $p(\alpha)$ factors as $(x - \alpha)\widetilde{p}(x)$, where $\widetilde{p}$ is a polynomial with coefficients in $K(\alpha)$, of degree $k-1$. By the induction hypothesis, $[L : K(\alpha)]$ divides $k!$, and so $[L : K] = [L : K(\alpha)][K(\alpha) : K]$ must divide $(k+1)!$.

Case 2 If $m_\alpha(x)$ is a nontrivial factor of $p(x)$, then $p(x) = m_\alpha(x) q_\alpha(x)$ for some polynomial $q_\alpha(x) \in K[x]$. Letting $\ell = \deg m_\alpha(x)$, $r = \deg q_\alpha(x)$, then we have $\ell + r = k + 1$ and $\ell, r \geq 1$. Let L_1 be the splitting fields of $m_\alpha(x)$ over $K[x]$. By the induction hypothesis, $[L_1 : K]$ divides $\ell!$ and $[L : L_1]$ divides $r!$ — since $q_\alpha(x) \in K[x] \subset L_1[x]$, so that $[L : K] = [L : L_1][L_1 : K]$ divides $\ell! r!$, which divides $\ell! r! \left(\frac{(k+1)!}{\ell! r!}\right) = (k+1)!$.
Here we are using the fact that $\frac{(k+1)!}{\ell! r!}$ is a binomial coefficient and thus an integer.

Therefore, by induction $[L:K]$ divides $n!$ if f is a polynomial over K of degree n, for any $n \geq 1$. □

Definition 11. *An **algebraic closure** of K is an algebraic extension L of K such that every element in $L[x]$ splits in $L[x]$.*

Theorem 12. *For any field K, the algebraic closure of K exists and is unique up to an isomorphism that fixes every element of K.*

Proof. (uses the Axiom of Choice in the form of Zorn's Lemma) □

Definition 13. *We say that L/K is **normal** if every irreducible polynomial in $K[x]$ that has a root in L splits over L.*

Example 1. The extension $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ is normal.

Example 2. The extension $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is not normal. For example, the polynomial x^3-2 has a root in $\mathbb{Q}\left(\sqrt[3]{2}\right)$, but it does not split in $\mathbb{Q}\left(\sqrt[3]{2}\right)$, since the other two roots are not real.

Theorem 14. *The extension L/K is normal if and only if L is the splitting field of some set of polynomials over K.*

Example 3. The extension $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ is the splitting field of x^2-2 over $\mathbb{Q}$.

Proof. (Sketch). ($\Longrightarrow$) Let the set of polynomials be the set of all minimal polynomials of every element of L.

($\Longleftarrow$) Take $\beta \in L$. The field L is generated by roots of some set of polynomials. Then $\beta = h(\alpha_1, ..., \alpha_n)$ with each α_j a root of one of these polynomials and with $h(x_1, ..., x_n) \in K[x_1, ..., x_n]$. We possibly increase the value of n by also including in all of the other roots of the minimal polynomials of each α_j in $K[x]$, but without changing the polynomial h, so that h depends on more variables but does not depend on the added variables. Form

$$q(x) = \prod_{\sigma \in S_n} \left(x - h\left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, ..., \alpha_{\sigma(n)}\right)\right),$$

which is very symmetric and can be shown to be in $K[x]$, and each $h\left(\alpha_{\sigma(1)}, \alpha_{\sigma(2)}, ..., \alpha_{\sigma(n)}\right)$ is in L. [Idea of proof of symmetric fact: Since it is a symmetric, it is a polynomial in the symmetric functions of the roots. The symmetric functions of the roots can be written in terms of the minimal polynomial coefficients.] Next, given β and an irreducible polynomial $p(x)$ with β as a root, this irreducible polynomial is a scalar multiple of the minimal polynomial of β, and thus $p(x)$ is a factor of $q(x)$ above. But since q splits as above, this implies that $p(x)$ splits in $L[x]$. We have shown that every irreducible polynomial with β as a root factors in $L[x]$, so that L is a normal extension of K. □

If $K \subseteq L$ are fields, let $\mathrm{Aut}_K(L)$ denote the set of all automorphisms of L (i.e. field isomorphisms from L to itself) that fix K.

Theorem 15. *If $K \subseteq L \subseteq M$ are fields and if M is normal over K. Then the following are equivalent:*

1. *L/K is normal.*
2. *$\sigma \in \mathrm{Aut}_K(M)$ implies that $\sigma(L) \subseteq L$.*
3. *$\sigma \in \mathrm{Aut}_K(M)$ implies that $\sigma(L) = L$.*

Proof. Heart of proof: If $p(x)$ has a root in L, then each $\sigma \in \mathrm{Aut}_K(M)$ permutes the roots of $p(x) \in K[x]$ because it must fix the coefficients of the polynomial. □

Definition 16. *If $f \in K[x]$ is irreducible, we say it is **separable** if it has distinct roots (in some algebraic closure).*

Observe that a polynomial $f(x)$ has a multiple root if and only if its derivative shares roots with $f(x)$. [Sketch of proof: $f(x) = (x-\alpha)^2 g(x)$ implies $f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)\{2g(x) + (x-\alpha)g'(x)\}$. You can also show that if f and f' share a root β, then $(x-\beta)^2$ divides $f(x)$.] To determine if f and g (such as f') in $K[x]$ in share a common root, use the Euclidean algorithm to find that there exist $a(x), b(x) \in K[x]$ such that

$$a(x) f(x) + b(x) g(x) = \gcd(x).$$

Suppose now that we have an irreducible polynomial f that is irreducible but not separable. Then f and f' have a nonconstant common factor in $K[x]$, which must be f itself (up to a scalar). This implies that $f' = 0$. How can this happen? If

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0,\ n \geq 1,\ a_n \neq 0,$$

and if

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + ... + a_1 = 0,$$

Then the characteristic $\mathrm{char} K = p$ for some prime, and $f(x) = g(x^p)$ for some polynomial $g(x) \in K[x]$.

By the above, there are no inseparable polynomials in $K[x]$ if K has characteristic zero. There are no examples of inseparable polynomials in $K[x]$ if K is a finite field because all elements of a degree d extension of a field of order p^n satisfy $x^{p^{nd}} - x$, which has no multiple roots.

Example 4. Let K be of characteristic p, and let $K(t)$ be the field of rational functions in t. Then $f(x) = x^p - t \in K[x]$ is irreducible. Observe that $f'(x) = px^{p-1} = 0$, and $f(x) = \left(x - t^{1/p}\right)^p$, since $p \mid \binom{p}{k}$ for $k = 1, 2, ..., k-1$.

Theorem 17. *If $K \subseteq L \subseteq M$ are fields, then M/K is separable if and only if M/L and L/K are separable.*

Theorem 18. *(of the primitive element) A finite, separable extension L of K is simple, meaning that $L = K(\alpha)$ for some α.*

For example, $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}(\alpha)$ for $\alpha = \sqrt{2} + \sqrt{3}$.

4. Galois theory

Let $K \subset L \subset M$, where $K \subset L$ is an algebraic extension, and M is normal over K.

Definition 19. *We say α and β in L are conjugate over K if they have the same minimal polynomial.*

Let $\sigma : L \to M$ be a monomorphism fixing K, such that σ takes an element of L to one of its conjugates. L is normal iff $\sigma(L) = L$ for all such σ. We also have L is separable, finite iff there exist $[L : K]$ different monomorphisms.

Definition 20. *The field extension L/K is **Galois** if it is normal and separable (and finite if you're a wimp). Let $\mathrm{Gal}(L, K) = \mathrm{Aut}_K(L)$ be the **Galois group of** L/K.*

Theorem 21. *(FTGT) Given a Galois extension L/K, there is a $1-1$ correspondence between subgroups of the Galois group and intermediate fields. The correspondence is as follows:*

$$\begin{aligned} H &\leftrightarrow L^H = \{x \in L : Hx = x\} \\ \mathrm{Gal}(L, M) &\leftrightarrow M \\ H \lhd G &\leftrightarrow L^H/K \text{ is normal} \end{aligned}$$

We have the picture

$$G \left\{ \begin{array}{c} L \\ M \\ K \end{array} \right\} H$$

Theorem 22. *Galois groups are transitive on roots of the minimal polynomial of any element.*

(**Transitive** means that if α, β are conjugate over K, then there exits $\sigma \in \mathrm{Gal}(L, K)$ such that $\sigma(\alpha) = \beta$.)

Finite fields: With a finite base field, you never have a problem with checking separability. A field with p^n elements is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ (or any other subfield). This is a separable polynomial, because its derivative is $p^n x^{p^n-1} - 1 = -1$, so it makes sense to say *the* field with p^n elements, which we denote by $\mathbb{F}_{p^n}$. Observe that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and is Galois. So, $|\mathrm{Gal}(\mathbb{F}_{p^n}, \mathbb{F}_p)| = n$. Even better, it's cyclic. The generator, $x \mapsto x^p$ (the *Frobenius* automorphism), fixes exactly the base field. Iterate n times and you get the identity.

Roots of unity:

$$x^6 - 1 = (x-1)(x+1)\left(x^2 + x - 1\right)\left(x^2 - x + 1\right) =: \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).$$

Note the appearance of Euler's ϕ function: degree of $\phi(n) = \Phi_n(x) =$ order of units $(\mathbb{Z}/n\mathbb{Z})^*$. $\Phi_n(x) \in \mathbb{Z}[x]$ is the n^{th} cyclotomic polynomial, irreducible over $\mathbb{Q}$, but not in general. It is the minimal polynomial over $\mathbb{Q}$ of $\exp\left(\frac{2\pi i}{n}\right)$.

Let $K(\xi)$ be an extension, suppose $m(\xi) = 0$, $m(x) \in K[x]$ irreducible, $m(x) | \Phi_n(x)$ (so $\xi^n = 1$). Let $(n, \mathrm{char}\, K) = 1$ or $\mathrm{char}\ K = 0$. So ξ is a multiplicative generator of the n^{th} roots of 1. Also $\xi^k \in K(\xi)$, so $K(\xi)$ is Galois over K, and any automorphism takes $\sigma(\xi) = \xi^i$.

Exercise 1. $K(\xi)/K$ is abelian and is in fact a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.

Example 5. Consider $x^4 - 4$. $x^4 - 4 = (x^2+2)(x^2-2)$.
Over $\mathbb{Q}$: splitting field is $\mathbb{Q}\left(\sqrt{2}, \sqrt{2}i\right)$, and $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$, $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{2}i\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$, so the order of the Galois group is 4. Thus, the group could be $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. Take $\sigma \in$ Gal. Then $\sigma\left(\sqrt{2}\right) = \pm\sqrt{2}$ and $\sigma\left(\sqrt{2}i\right) = \pm\sqrt{2}i$ because the conjugates map to conjugates. The choices determine σ. There are at most 4 automorphisms, so the set of all possible choices is the Galois group. Since the order of every permutation is 2, the Galois group is $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 6. Next, consider $x^4 - 5$.
Over $\mathbb{Q}$: it is irreducible due to the Eisenstein criterion. (Recall that a polynomial $q(x) \in \mathbb{Q}[x]$ is irreducible if there exists a prime p that does not divide the first coefficient, divides all the other coefficients, and p^2 does not divide the constant term. In our case $p = 5$.) Note that $\left[\mathbb{Q}\left(\sqrt[4]{5}\right) : \mathbb{Q}\right] = 4$. Note that $x^4 - 5 = \left(x^2 - \sqrt{5}\right)\left(x^2 + \sqrt{5}\right)$. Then

$\left[\mathbb{Q}\left(i\sqrt[4]{5},\sqrt[4]{5}\right):\mathbb{Q}\left(\sqrt[4]{5}\right)\right]=\left[\mathbb{Q}\left(i,\sqrt[4]{5}\right):\mathbb{Q}\left(\sqrt[4]{5}\right)\right]=2$. So the splitting field is degree 8. For $\sigma\in\text{Gal}$, $\sqrt[4]{5}\mapsto\sqrt[4]{5},-\sqrt[4]{5},i\sqrt[4]{5},-i\sqrt[4]{5}$. By transitivity, all occur, but in fact twice since the order is 8; $-\sqrt[4]{5}\mapsto$ opposite of above choice (no flexibility); $i\mapsto\pm i$ both must occur, 4 times each by transitivity. There are lots of groups over 8. The greatest order of an element is 4. Define: σ by $\sigma\left(\sqrt[4]{5}\right)=\sqrt[4]{5}i$ and $\sigma(i)=i$; τ by $\tau\left(\sqrt[4]{5}\right)=\sqrt[4]{5}$ and $\tau(i)=-i$. Then $o(\tau)=2$, $o(\sigma)=4$. Let $G=\langle\sigma,\tau\rangle$. Then $\sigma^4=1$, $\tau^2=1$. Note that $\langle\sigma\rangle$ is a subgroup of index 2, so it is normal. Thus, $\tau\sigma\tau^{-1}=\tau\sigma\tau=\sigma^3$ by computing. So the group is not abelian. So in fact this group is $D_4=$ dihedral group of order 8 (symmetries of square). In fact, however, all we need to note is that the Galois group must be the 2-Sylow subgroup of the symmetric group S_4, which is unique up to conjugation and is isomorphic to the dihedral group.

Theorem 23. *Let $K=\mathbb{Q}(\alpha)$ be Galois where the minimal polynomial f of α is monic with integer coefficients. Suppose the $p\nmid\text{disc}(f)$ where*

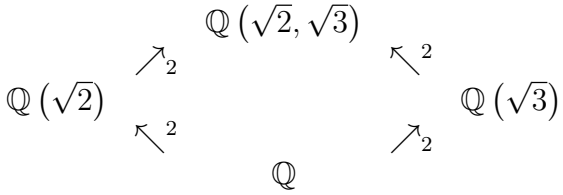
$$\text{disc}(f)=\prod_{roots\ \alpha_j}(\alpha_i-\alpha_j)^2$$

This number lives in the base field and must be preserved by the Galois group. View $f\in\mathbb{F}_p[x]$. There is an injection

$$\text{Gal}(f,\mathbb{F}_p)\hookrightarrow\text{Gal}(K,\mathbb{Q})$$

that preserves the cycle structure on the roots.

Example 7. Consider $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$. Again. Note that we have the diagram



The Galois group is $\mathbb{Z}_4$ or $\mathbb{Z}_2\times\mathbb{Z}_2$ (only groups of order 4). There is only one subgroup of order 2 in $\mathbb{Z}_4$, but by the FTGT and the diagram above, there should be at least two subgroups. Thus, the Galois group is $\mathbb{Z}_2\times\mathbb{Z}_2$. Note that $\mathbb{Q}\left(\sqrt{6}\right)$ is the third intermediate quadratic subfield.

Remark 1. The minimal polynomial of $\sqrt{2}+\sqrt{3}$ is $g(x)=x^4+10x^2+1$. The Galois group over $\mathbb{F}_p$ for any prime p is cyclic and injects into the Galois group of g over $\mathbb{Q}$ as long as p does not divide the discriminant, which is

$$\left(\sqrt[4]{5}-\left(-\sqrt[4]{5}\right)\right)^2\left(\sqrt[4]{5}-i\sqrt[4]{5}\right)^2\left(\sqrt[4]{5}-\left(-i\sqrt[4]{5}\right)\right)^2\left(\left(-\sqrt[4]{5}\right)-i\sqrt[4]{5}\right)^2\cdot$$
$$\cdot\left(\left(-\sqrt[4]{5}\right)-\left(-i\sqrt[4]{5}\right)\right)^2\left(i\sqrt[4]{5}-\left(-i\sqrt[4]{5}\right)\right)^2=-32\,00=-2^8 5^3.$$

In this case, the Galois group over such $\mathbb{F}_p$ is either trivial or $\mathbb{Z}_2$. This guarantees that x^4+10x^2+1 factors into linear and quadratic factors over every $\mathbb{F}_p$.

Example 8. Consider x^4-5. Note that p divides the discriminant if and only if it has repeated factors over $\mathbb{F}_p$.

Let $p = 3$. It has no root (by plugging in). If it factors, it must factor into two quadratics, which we may assume are monic:

$$\begin{aligned} x^4 - 5 &= x^4 + 1 = \left(x^2 + ax \pm 1\right)\left(x^2 - ax \pm 1\right) \\ &= x^4 + \left(\pm 2 - a^2\right) x^2 + 1. \end{aligned}$$

So we need

$$\pm 2 - a^2 \equiv 0 \bmod 3.$$

So $a = 1$ with $-$ works:

$$x^4 - 5 = \left(x^2 + x - 1\right)\left(x^2 - x - 1\right).$$

The Galois group over $\mathbb{F}_3$ is $\mathbb{Z}_2$, since $\mathbb{Z}_n$ is the Galois group of $\mathbb{F}_{p^n}$, the splitting field of $x^{p^n} - x$ and the unique extension $\mathbb{F}_p$ of degree n. Let's say $(1,2)(3,4) \in \mathrm{Gal}(K, \mathbb{Q})$ is the cycle that comes from $\mathbb{F}_3$.

Over $\mathbb{F}_{11}$, the Galois group of $x^4 - 5 = (x-3)(x-2)(x^2+4)$ is $\mathbb{Z}_2$ and over $\mathbb{Q}$, the Galois group of $x^4 - 5$ has a 2-cycle. Given the cycle assumption from $p = 3$, we can't specify the 2-cycle coming from $\mathbb{F}_{11}$, but can assume it is either $(1,2)$ or $(1,3)$ (other possibilities are equivalent to this choice by relabeling).

Over $\mathbb{F}_{17}$, proceeding as for $p = 3$, we see $x^4 - 5$ is irreducible. Thus, its Galois group $\mathbb{Z}_4$. Over $\mathbb{Q}$ that means we have a 4-cycle in the Galois group.

We mention, that the Galois group of $x^4 - 5 = (x-34)(x-37)(x-64)(x-67)$ over $\mathbb{F}_{101}$ is trivial. (This is the first prime for which this happens).

The transitive subgroups of S_4 (transitive means one of the group elements takes a given a to a given b) are

S_4: order 24
A_4: order 12 and consists of all even permutations
D_4: order 8 and is conjugate to $\langle (1,2,3,4), (1,3) \rangle$
$\mathbb{Z}_4$: $\langle (1,2,3,4) \rangle$ and its conjugates.
$\mathbb{Z}_2 \times \mathbb{Z}_2$: $\langle (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \rangle = \langle (1,2)(3,4), (1,3)(2,4) \rangle$

We have 4-cycle (which is an even permutation), so A_4 and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are out.
We have a $(1,2)(3,4)$ type element (this is true for all of the above).
We have a 2-cycle. This rules out A_4, $\mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2$.
The possibilities are D_4 or S_4.

So we factor modulo more primes. If we get an irreducible cubic for some prime p, there must be a 3-cycle in $\mathrm{Gal}(K, \mathbb{Q})$, so the Galois group is S_4. In fact, this will never happen.

Trying to compute the Galois group over $\mathbb{Q}$ through finite fields, you never know you are done unless you get the whole symmetric group. Other partial information (like knowing the degree of the splitting field) can complete the calculation. But we know from the previous calculation that the order of the Galois group is 8, so it must be D_4.

Example 9. Complex conjugation is an element of the Galois group over $\mathbb{Q}$. Take an irreducible polynomial of degree 5 with three real roots. For any irreducible quintic, the Galois group has an element of order 5, hence a 5-cycle, since 5 is prime. Because the irreducible polynomial has three real roots, complex conjugation is a transposition. These two permutations generate S_5, so the Galois group is S_5. (Uses result that a p-cycle and a 2-cycle generate S_p for p prime.)

References

[1] Keith Conrad, Galois Theory At Work: Concrete Examples.
[2] Keith Conrad, Galois Groups Of Cubics And Quartics (Not In Characteristic 2).
[3] Keith Conrad, Recognizing Galois Groups S_n and A_n.