Jason B. Hill – University of Colorado at Boulder

Throughout this set of notes, K will be the desired base field (usually $\mathbb{Q}$ or a finite field) and F will denote the splitting field of the polynomial $f(x) \in K[x]$. We will denote the Galois group $G = \text{Gal}(F/K)$. We assume here the basic definitions (normality, separability, etc.) and the Fundamental Theorem of Galois Theory.

There are several publications that include information about calculating Galois groups. None, at least not any that I have found, include explicitly everything that I have put here – especially in the area of calculating the Galois groups of polynomials over finite fields. I have also left out the general case of Galois groups of quartic polynomials, since the required process and relevant cases are lengthy and probably aren't suited well to a prelim problem.[1]

Theorem 1: *For $f(x) \in K[x]$ separable of degree n, $G = Gal(F/K)$ is isomorphic to a subgroup of S_n. Moreover, if $f(x)$ is irreducible, then G is isomorphic to a transitive subgroup of S_n.*[2]

1 The Galois Group of a Quadratic

If K has characteristic 2, then note that $K(\sqrt{d})$ has a splitting field determined by the roots of

$$x^2 - d = x^2 + 2x\sqrt{-d} - d = \left(x + \sqrt{-d}\right)^2,$$

which is not separable. Hence, the following applies precisely when $\text{char}(K) \neq 2$.

Theorem 2: *If $f(x) \in K[x]$ has degree 2 and is irreducible over K with $char(K) \neq 2$, then $G = Gal(F/K) \simeq Z_2$.*

2 The Galois Group of a Cubic

If $f(x) \in K[x]$ is reducible, then we are left with either a quadratic or trivial extension of K. In either case, $f(x)$ would have a linear factor and hence a

[1] I'm an idiot.

[2] A subgroup $H \leq S_n$ is transitive on S_n iff for all i, j with $0 \leq i, j \leq n$ there is some $\sigma \in H$ such that $\sigma(i) = j$. In this theorem, we have transitivity from the Galois group as applied to S_n, and hence irreducibility is required. For example, if $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then the splitting field, given by $f(x) = (x^2 - 3)(x^2 - 2)$ has normal subfields and hence the Galois group V_4 need not be (in fact isn't) transitive on S_4.

rational root in K. Thus, when given a cubic, we first check for a rational root in K, and reduce to the appropriate case. If $f(x)$ is irreducible over K, then we have from Theorem 1 that $G = \text{Gal}(F/K)$ is transitive on S_3. But, the only transitive subgroup of S_3 is A_3. Hence, a cubic Galois extension (the splitting field of a cubic polynomial) may only have a Galois group isomorphic to S_3 or A_3.

Since a separable cubic may have only either one or three real roots[3], we consider these cases. If $f(x) \in K[x]$ has one real root and a pair of complex conjugate roots, we may consider complex conjugation as an order 2 automorphism creating an order 2 subgroup of $G = \text{Gal}(F/K)$. Hence, we know immediately that any irreducible and separable extension given by a cubic with only one real root has Galois group S_3, since $A_3 \simeq Z_3$ has no subgroup of order 2. Thus, any cubic over $\mathbb{Q}[x]$ with a pair of complex conjugate roots will have Galois group S_3. (We will come back to this idea later for higher degree polynomials.) A cubic with all roots in $\mathbb{R}\backslash\mathbb{Q}$ may have S_3 or A_3 for its Galois group, and so we need more machinery to make the distinction.

2.1 The Polynomial Discriminant

We will use the notion of the polynomial discriminant to determine the even/odd structure of the elements of a Galois group when that group is viewed under Theorem 1 as a subgroup of S_n. Of course, if all permutations inside the Galois group are even, then the Galois group will be entirely contained inside the relevant alternating group.

For K a field such that $\text{char}(K) \neq 2$ and $f(x) \in K[x]$ separable of degree n with roots $\alpha_1, ..., \alpha_n$ in some splitting field F over K, we define:

$$\Delta = \prod_{i<j}(\alpha_i - \alpha_j) \qquad \text{and} \qquad \Delta^2 = d(f) \quad (\text{hence } \Delta = \sqrt{d(f)}).$$

Then $d(f)$ is the *discriminant* of the polynomial $f(x)$. This, of course, coincides with the idea of a quadratic discriminant $b^2 - 4ac$ learned in precalculus level algebra[4]. It is easy to see that $d(f) \in F$. What is potentially more surprising is that $d(f) \in K$. More importantly, for $K = \mathbb{Q}$ with $n < \infty$ we have $d(f) \in \mathbb{Z}$. We will make use of the following:

Theorem 3: *For all $\sigma \in G = Gal(F/K)$, $\sigma(\Delta) = \Delta$ iff σ is an even permutation, and $\sigma(\Delta) = -\Delta$ iff σ is an odd permutation.*

Hence, if $\Delta \in K$ then $\sigma(\Delta) = \Delta$ for all $\sigma \in G$ and therefore G is isomorphic

[3]Notice that separable implies that no root occurs with multiplicity greater than one.

[4]Although what is usually not realized in precalculus is that the quadratic discriminant is simply a function of the distance between the roots of the quadratic.

to some subgroup of A_n. In general, we have the subfield $K(\Delta)$ of the splitting field F corresponding under the Fundamental Theorem of Galois Theory to the subgroup $G \cap A_n$ of the Galois group G. This gives the following.

Corollary 4: *For K a field with $char(K) \neq 2$ and $f(x) \in K[x]$ irreducible and separable of degree 3, the Galois group $G = Gal(F/K)$ is A_3 iff the discriminant of $f(x)$ is the square of an element in K. Otherwise, the Galois group is S_3.*

Notice that this provides another proof that any irreducible cubic in $\mathbb{Q}[x]$ with only one real root has Galois group S_3, since the discriminant will be negative and hence will not be a square in $\mathbb{Q}$. But, notice that positive discriminants may or may not be squares.

Thus, if we can calculate the discriminant of an irreducible and separable cubic over a given field with characteristic other than 2, we may calculate the relevant Galois group. There is a formula for the discriminant of a cubic: If

$$f(x) = ax^3 + bx^2 + cx + d$$

then we have that

$$d(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Even if we reduce this to the monic case ($a = 1$, we may always divide by $a \in K$ and still have a polynomial in $K[x]$) we have

$$d(f) = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd.$$

This is computationally inadequate (namely because it is challenging to remember). Notice that the definition of the discriminant is only based on the difference in roots, which is invariant under horizontal shifts of the cubic itself. If we replace x by $x - b/3$ then we have the fields given by

$$f_1(x) = x^3 + bx^2 + cx + d$$

and

$$\begin{aligned} f_2(x) &= (x - \frac{b}{3})^3 + b(x - \frac{b}{3})^2 + c(x - \frac{b}{3}) + d \\ &= x^3 + \left(-\frac{1}{3}b^2 + c\right)x + \left(\frac{2}{27}b^3 - \frac{1}{3}bc + d\right). \end{aligned}$$

will be isomorphic and have the same discriminant. If we set $p = (-\frac{1}{3}b^2 + c)$ and $q = (\frac{2}{27}b^3 - \frac{1}{3}bc + d)$ then the discriminant is given by $d(f) = -4p^3 - 27q^2$.

We therefore remember the formula $d(f) = -4p^3 - 27q^2$ and also the transformation $x \mapsto x - \frac{b}{3}$. This works on an irreducible cubic whenever $\text{char}(K) \neq 2$. We will deal with finite fields later. For now, we have the following examples.

Examples:

1. Find the $G = \mathrm{Gal}(F/\mathbb{Q})$ where F is a splitting field of $x^3 - 3x + 1$ over $\mathbb{Q}$.

   Solution: The Rational Root Theorem implies that $x^3 - 3x + 1$ is irreducible in $\mathbb{Q}[x]$. Since $b = 0$, we find $-4p^3 - 27q^2 = 81$. Hence, the discriminant is a square in $\mathbb{Q}$, implying that $G \simeq A_3$.

2. If we change the polynomial in the preceeding example to $x^3 - 4x + 1$ then we find that $d(f) = 229$, which is not a square in $\mathbb{Q}$ and so we have $G \simeq S_3$. Notice that both of these polynomials have three real roots. Thus, we know that whenever an irreducible cubic has a pair of complex conjugate embeddings that there will be an automorphism given on the roots by complex conjugation (fixing the real root and having order 2) and thus the Galois group will be S_3. But, this example shows that the converse of that statement does not hold.

3. Find $G = \mathrm{Gal}(F/\mathbb{Q})$ where F is a splitting field of the polynomial $f(x) = x^3 + 3x^2 - x - 2$ over $\mathbb{Q}$.

   Solution: By the Rational Root Theorem, $f(x)$ is irreducible over $\mathbb{Q}[x]$. Using the transformation $x \mapsto x - \frac{b}{3}$ we find that $f(x)$ has the same discriminant as $\hat{f}(x) = x^3 - 4x + 1$ where $p = -4$ and $q = 1$. Thus, we have $d(f) = d(\hat{f}) = 229$, which again gives $G \simeq S_3$.

3 Fields of Prime Degree Index

There is a relatively common Galois theory problem for fields of prime index over $\mathbb{Q}$ that shows up on prelims. It can be solved by the following theorem.

Theorem 5: *If $f(x) \in \mathbb{Q}[x]$ is irreducible and separable of prime degree $p \in \mathbb{Z}^+$ such that $f(x)$ has $p-2$ roots in $\mathbb{R}\backslash\mathbb{Q}$, then the splitting field F of $f(x)$ over $\mathbb{Q}$ has Galois group S_p.*

We shall include the proof of this theorem, since the theorem has been posed in disguise as a question on several prelims.

Proof: *Since $f(x)$ has a single pair of complex conjugate roots, and complex conjugation represents an order 2 automorphism (and hence a $S_2 \simeq Z_2$ subgroup in the Galois group), we have that $G = Gal(F/\mathbb{Q})$ when viewed as a subgroup of S_5 contains an order 2 subgroup generated by a single 2–cycle. Since $[F : \mathbb{Q}] = p$ we have from the fundamental theorem of Galois theory that p divides the order of G. By Cauchy's Theorem, G contains a p–cycle. Since a p–cycle and a 2–cycle generate S_p, the proof is complete.* □

Examples:

1. Find the Galois group of $f(x) = x^5 - 25x - 5$ over $\mathbb{Q}[x]$.

   Solution: Notice that $\frac{df}{dx} = 5x^4 - 25$ has two real roots, and therefore $f(x)$ has one local min and one local max. Since $f(-1) > 0$ and $f(1) < 0$, we know that this quintic has three real roots and one pair of complex conjugate roots. By the preceeding theorem, the Galois group of the splitting field is then S_5. (Usually on a prelim, you'd run through the proof of the theorem for this specific case: Show there is a single 2–cycle and also a 5–cycle.)

4 Extensions of Specific Types

Galois extensions are typically classified according to the structure of the Galois group of the relevant splitting field. An extension is abelian or cyclic iff the Galois group corresponding to the extension is abelian or cyclic, respectively. Usually prelim problems dealing with extensions of $\mathbb{Q}$ deal with cyclotomic extensions, while extensions over finite fields will always deal with cyclic extensions. Many prelim problems also ask about radical extensions.

4.1 Cyclotomic Extensions

We call an extension field F of K a cyclotomic extension of order n if it is the splitting field over $K[x]$ of some polynomial $x^n - 1$ where $n \in \mathbb{Z}^+$. These often occur in the context of $x^n - 1 \in \mathbb{Q}[x]$, but may also occur over other fields, specifically finite fields.

Theorem 6: *If K is a field and $char(K) = p \neq 0$, then for all $n, m, e \in \mathbb{Z}^+$, if $(m, p) = 1$ and $n = mp^e$ then $(x^n - 1) = (x^m - 1)^{p^e}$ and hence the splitting fields over K given by these polynomials are isomorphic.*

Examples:

1. Let $K = F_{11}$ be the finite field of 11 elements. Then the cyclotomic fields generated by $x^{33} - 1 \in F[x]$ and $x^3 - 1 \in F[x]$ are isomorphic since $33 = 3 \cdot 11$.

2. If one wanted to find the splitting field and Galois group of $x^6 + 2x^3 + 1$ over F_4, the field of 4 elements, then noting that in $F_4[x]$ we have

   $$x^6 + 2x^3 + 1 = x^6 - 2x^3 + 1 = (x^3 - 1)^2$$

   where $(2, 3) = 1$ gives that the desired splitting field is the cyclotomic field given by $x^6 - 1$ over F_2.

We will use the notation Z_n^* to denote the multiplicative subgroup of units in the cyclic group Z_n. Recall that for $i \in \mathbb{Z}$ we have $\bar{i}$ a unit in Z_n iff $(i, n) = 1$. Hence, $|Z_n^*| = \varphi(n)$ where φ is the Euler-phi function. The following is the main theorem for determining the structure of Galois groups given by cyclotomic extensions.

Theorem 7: *Given a field K and $n \in \mathbb{Z}^+$ such that $char(K)$ does not divide n and F is a cyclotomic extension of K having order n:*

1. *$F = K(\zeta)$ where ζ is a primitive n^{th} root of unity.*
2. *If $char(K) = 0$ then $G = Gal(F/K) \simeq Z_n^*$. Otherwise, $G \simeq H \leq Z_n^*$.*
3. *If $char(K) = 0$ then $[F : K] = \varphi(n)$. Otherwise $[F : K] | \varphi(n)$.*
4. *If n is prime, the extension is always cyclic (regardless of field characteristic).*

Thus, if we know the structure of Z_n^*, we can completely determine the Galois group of cyclotomic extensions of $\mathbb{Q}$ and restrict the possibilities for cyclotomic extensions over other fields. The following theorem does precisely that for extensions of prime order.

Theorem 8: *The group Z_m^* is given by the following.*

1. *If p is an odd prime and $n \in \mathbb{Z}^+$, then $Z_{p^n}^* \simeq Z_m$ where $m = p^{n-1}(p-1)$.*
2. *If $p = 2$ and $1 \leq n \leq 2$ then $Z_{p^n}^* \simeq Z_m$ where $m = p^{n-1}(p-1)$.*
3. *If $p = 2$ and $n \in \mathbb{Z}_{\geq 3}$ then $Z_{p^n}^* \simeq Z_2 \oplus Z_{2^{n-2}}$*
4. *If $m = p_1^{\alpha_1} p_2^{\alpha^2} \cdots p_k^{\alpha_k}$ for distinct primes p_i, then we have*

$$Z_m \simeq \mathbb{Z}/m\mathbb{Z} \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})$$

is an isomorphism by the Chinese Remainder Theorem. Hence, there must exist an isomorphism on the corresponding unit groups, and we find

$$Z_m^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

Examples:

1. Often the splitting field of a polynomial has a cyclotomic subextension. For example, the splitting field of $x^3 - 2$ over $\mathbb{Q}$ (we already know how to calculate this Galois group in several ways) is $\mathbb{Q}(\zeta, 2^{1/3})$ for ζ a primitive 3rd root of unity. The extension $\mathbb{Q}(\zeta)$ itself is cyclotomic with Galois group Z_2, while $\mathbb{Q}(2^{1/3})$ is an extension of degree 2 that isn't normal. Therefore, the Galois group has an order 3 normal subgroup and an order 2 nonnormal subgroup. Hence $G \simeq S_3$.

2. For cyclotmic extensions of the form given by the splitting field of $x^m - 1$ for composite m, we have several options. For example, consider the splitting field K of $x^{12} - 1$ over $\mathbb{Q}$. We have from the Chinese Remainder Theorem that

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq Z_{12}^{\times} \simeq (\mathbb{Z}/12\mathbb{Z})^{\times} \simeq (\mathbb{Z}/4\mathbb{Z})^{\times} \times (\mathbb{Z}/3\mathbb{Z})^{\times} \simeq Z_2 \times Z_2.$$

   One should notice by now that composite cyclotomic extensions of $\mathbb{Q}$ need not be cyclic, while prime cyclotomic extensions always are. This example may be computer more directly from subfields, as is done in the following example.

3. The splitting field of $x^{12} - 1$ over $\mathbb{Q}$ can be constructed from subfields over $\mathbb{Q}$. Notice that $x^4 - 1$ is cyclotomic, and at the same time may be viewed as the quadratic extension $\mathbb{Q}(i)$ with Galois group Z_2. The splitting field of the cyclotomic extension given by $x^3 - 1$ has Galois group Z_2 as well. Since a 3rd root of unity and i generate all 12th roots of unity, we have $F = \mathbb{Q}(\zeta, i)$ where ζ is a third root of unity. Since we included a third root of unity ζ in a cyclotomic (Galois) extension, we have $-\zeta$ and the conjugate of $-\zeta$ in $\mathbb{Q}(\zeta)$. Hence, $\mathbb{Q}(\zeta) = \mathbb{Q}(\rho)$ where ρ is a primitive 6th root of unity. Therefore, we find that the Galois group is $V_4 \simeq Z_2 \times Z_2$.

4. The idea used in Example 3 is relatively common. For instance, the splitting field of $x^4 + 1$ contains the four roots of -1 in $\mathbb{C}$, and hence is a subfield of the cyclotomic extension given by a primitive 8th root of unity. Hence, the desired Galois group will be a subgroup of $Z_2 \times Z_2$. Notice that a field containing the 4th roots of -1 in $\mathbb{C}$ contains $\pm\sqrt{2} \pm \sqrt{2}i$. Assing the two roots with x–component and dividing by the field element 2 shows that $\sqrt{2}$ is in the field, which we then use to factor $\sqrt{2} + \sqrt{2}i = \sqrt{2}(1 + i)$. Since $\sqrt{2}$ and 1 are in the field already, so must be i. Thus, the field generated by the 4th roots of -1 is identitcal to the cyclotomic extension given by an 8th root of unity and the Galois group is V_4.

5. Find the Galois group for the splitting field K of $x^{1000} - 1$ over $\mathbb{Q}$. Solution: By the Chinese Remainder Theorem we have

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq Z_{1000}^{\times} \simeq (\mathbb{Z}/4\mathbb{Z})^{\times} \times (\mathbb{Z}/125\mathbb{Z})^{\times} \simeq Z_2 \times Z_{100}.$$

5 Galois Groups Over Finite Fields

This section is broken into two subsections. First, the main theorems about finite fields are reviewed. Then, several methods for calculating Galois groups over finite fields are presented.

5.1 In Theory

A key idea here is that the Galois group of a finite extension of a finite field will always be cyclic. Notice that this implies that (finite) Galois groups over finite fields are always abelian.

Given a field F, we define the *prime subfield* of F to be the intersection of all subfields. If the field in question has characteristic zero, then the prime subfield is always isomorphic to $\mathbb{Q}$. Any finite field will have order p^n for some prime p and n where $p, n \in \mathbb{Z}^+$. The prime subfield of a field having characteristic p is thus $F_p \simeq Z_p$.

Theorem 9: *Any finite subgroup of the (multiplicative) group of units of a field is cyclic. Mainly, the group $F_{p^n}^{\times}$ is a multiplicative cyclic group for all finite fields F_{p^n}.*

From this point on, we assume that our fields are finite. The following automorphism provides the main tools for computing the structure of Galois groups over finite fields.

Theorem 10: *Let F be a finite field of characteristic p and let $m \in \mathbb{Z}^+$. Then the mapping*

$$\varphi : F \to F \qquad \text{defined by} \qquad \varphi(\alpha) = \alpha^{p^m}$$

is an automorphism on F. This automorphism (usually in the case of $m = 1$) is known as the Frobenius automorphism.

Notice that the Frobenius automorphism fixes elements in the prime subfield, since $|Z_p| = p - 1$ and hence $\alpha^p = \alpha$ for all $\alpha \in Z_p$. To see that this is indeed an automorphism on F_{p^n} for $1 < n < \infty$, recall that in a field of characteristic p we have

$$(\alpha \pm \beta)^p = \alpha^p \pm \beta^p.$$

If we let $m = n$ where m is the power of p given in the Frobenius automorphism and n is the dimension of the field F_{p^n} viewed as a vector space over F_p, then we have our principal result for extensions of finite fields:

Theorem 11: *Let p be a prime and $n \in \mathbb{Z}^+$. Then F is a field of order F_{p^n} iff F is a splitting field of $f(x) = x^{p^n} - x \in F_p[x]$. In fact, the smallest field splitting $f(x)$ is F. Moreover, $f(x)$ is the product of all irreducible polynomials of degree dividing n in $F_p[x]$.*

Notice that a field of order p^n has a unit group of size $p^n - 1$. Since $x^{p^n} - x = x(x^{p^n-1} - 1)$, every nonzero element in F_{p^n} is seen to be a root of this polynomial. Therefore, it is relatively intuitive that $x^{p^n} - x$ splits and is separable with p^n roots in F_{p^n}.

Recall that for any prime p and any $n \in \mathbb{Z}^+$ we may construct a field having p^n elements, and that all fields of order p^n are isomorphic. We may also construct at will irreducible polynomials over arbitrary degree over F_p. To show that the Galois groups of such extensions[5] are cyclic, we prove the following theorem:

Theorem 12: *For F_{p^n} over the prime subfield F_p, $G = Gal(F_{p^n}/F_p) \simeq Z_n$. Moreover, if $\sigma \in G$ is defined to be the Frobenius automorphism $\sigma : \alpha \mapsto \alpha^p$, then $G = \langle \sigma \rangle$.*

Proof: *Notice that σ^n is the identity automorphism on F_{p^n}. If some $m < n$ in $\mathbb{Z}^+$ satisfied $\sigma^k = id$ then $x^{p^m} - x$ would annihilate all elements of F_{p^n}. Notice that this is a contradiction since $x^{p^m} - x$ has fewer roots than F_{p^n} has elements, and is Galois and hence separable. Thus, n is the smallest integer such that $\sigma^n = id$. By the Fundamental Theorem of Galois Theory, we have $|G| = |Gal(F_{p^n}/F_p)| = n$, completing the proof.* □

5.2 In Practice

There is a small gap between theory and practice. In general, trying to find the Galois group of a polynomial over a finite field starts the same as over $\mathbb{Q}$: We try to factor the polynomial. Since our irreducibility criteria over finite fields aren't generally as strong, this typically amounts to the following:

1. Pull out all linear factors.
2. Attempt to factor the remaining polynomial or exploit the Frobenius automorphism in some creative way. This process can only really be explained by examples.

[5]Notice that since the relevant fields are splitting fields of separable polynomials that they are Galois over $F_p \simeq Z_p$ for some prime p.

Examples:

1. Determine the splitting field of the polynomial $x^5 + 2x^4 + 5x^2 + x + 4$ over $\mathbb{F}_{11}$ and its Galois group.

   Solution: By brute force, we find that $x - 9 = x + 2$ is a root of this polynomial in $\mathbb{F}_{11}[x]$. By long division, we find that

   $$x^5 + 2x^4 + 5x^2 + x + 4 = (x + 2)(x^4 + 5x + 2),$$

   and so our problem is now to compute the Galois group of $f(x) = x^4 + 5x + 2$ over $\mathbb{F}_{11}$. We already know that for all $\alpha \in \mathbb{F}_{11} \backslash \{2\}$, α is not a root of f since it isn't a root of the original polynomial, but we should verify that 9 isn't a repeat root. In fact it isn't a root of f, and so we are left with two possible situations:

   (a) If $f(x)$ is irreducible in $\mathbb{F}_{11}[x]$, then we have a degree 4 extension since $x^{11^4} - x$ will split any irreducible polynomial in $\mathbb{F}_{11}[x]$ having degree dividing 4. In this case, the Galois group is Z_4.

   (b) If $f(x)$ factors as two quadratics, then $x^{11^2} - x$ will split both, and the Galois group is thus Z_2.

   Since the polynomial has nonzero terms between the degree 4 and constant term, it is not efficient to use long division. (See the next example.) We try to factor as follows: Assume $x^4 + 5x + 2 = (x^2 + ax + c)(x^2 + bx + d)$, and then we work through the corresponding equivalences. For example, we know $cd = 2 \mod 11$. This results in the factorization

   $$x^4 + 5x + 2 = (x^2 + 5x + 1)(x^2 + 6x + 2).$$

   Hence, the splitting field is given by $x^{11^2} - x$ and is $\mathbb{F}_{11^2}$, giving that the Galois group is Z_2.