

3. EXAMPLES

I did some examples and explained the theory at the same time.

3.1. roots of unity. Let $L = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/5}$ is a primitive 5th root of unity.

Theorem 3.1. For any prime p ,

$$f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

is irreducible over \mathbb{Q} .

Proof. When you plug in $X = Y + 1$ you get

$$f(Y+1) = \frac{(Y+1)^p - 1}{Y} = Y^{p-1} + pY^{p-2} + \binom{p}{2}Y^{p-3} + \cdots + \binom{p}{2}Y + p$$

which is irreducible by Eisenstein. \square

As I pointed out earlier, $\mathbb{Q}(\zeta)$ is the splitting field of the polynomial $f(X)$ for $p = 5$ since it contains all of the roots (conjugates of ζ): $\zeta, \zeta^2, \zeta^3, \zeta^4$. Since the Galois group $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is a finite group of order equal to the degree of the extension, it has order 4. So, it is either $\mathbb{Z}/4$ or $\mathbb{Z}/2 \oplus \mathbb{Z}/2$.

We also know by Lemma 2.3 (and Lemma 2.9 in more general cases where we need to adjoin more than one root to get the splitting field) that the Galois group acts transitively on the roots. So, there is an element $\sigma \in G$ so that $\sigma(\zeta) = \zeta^2$. But, σ is an automorphism of the field. So, $\sigma(\zeta^2) = \sigma(\zeta)^2 = \zeta^4$, $\sigma(\zeta^3) = (\zeta^2)^3 = \zeta$ and $\sigma(\zeta^4) = \zeta^3$. As a permutation, $\sigma = (1243)$ is a 4-cycle. So, the Galois group is cyclic of order 4.

The group $\mathbb{Z}/4$ has exactly one nonzero proper subgroup $2\mathbb{Z}/4$ which has 2 elements. These elements are $1, \sigma^2$. The automorphism σ^2 is complex conjugation. It switches ζ, ζ^4 and ζ^2, ζ^3 . According to the Galois correspondence, this subgroup corresponds to the subfield fixed by complex conjugation, namely the real subfield. So the unique intermediate fields is

$$\mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^4).$$

3.2. Galois correspondence. Using the theorems that we already proved, the Galois correspondence is easy to derive. The first step is to show that intermediate fields give Galois extensions.

Lemma 3.2. If L is a separable extension of K and E is an intermediate field, i.e., $K \subseteq E \subseteq L$, then L is separable over E .

Proof. Let $a \in L$, $a \notin E$, $f(X) = \text{irr}(a, E)$. We need to show that $f(X)$ has no multiple roots. Let $g(X) = \text{irr}(a, K)$. Then $g(X) \in K[X] \subseteq E[X]$ with $g(a) = 0$. Therefore, $g(X) \in (f(X))$ since this is the ideal of all polynomials in $E[X]$ of which a is a root. Therefore, $g(X) = f(X)h(X)$ for some $h(X) \in E[X]$. The assumption that L/K is separable implies that g has distinct roots. But the roots of f are roots of g . So, they are also distinct. \square

Theorem 3.3. *If L is a Galois extension of K and E is an intermediate field then L is Galois over E .*

Proof. We just showed that L/E is separable. So, we just need to show that any embedding $\phi : L \rightarrow \overline{E} = \overline{K}$ has image $\phi(L) = L$. But, ϕ being the identity on E implies that it is the identity on $K \subseteq E$. So, L being Galois over K implies that $\phi(L) = L$. \square

Lemma 3.4. *If $K \subseteq E \subseteq L$ then*

$$|L : K| = |L : E| \cdot |E : K|.$$

Proof. Suppose that $|L : E| = n$. Then L has a basis x_1, \dots, x_n over E . This means that, for any $a \in L$, there are unique elements $e_i \in E$ so that $a = \sum e_i x_i$.

If $|E : K| = m$, then E has a basis y_1, \dots, y_m over K . This implies that every element of E , for example e_i , is a K -linear combination of the elements y_j . So $e_i = \sum a_{ij} y_j$ for some $a_{ij} \in K$.

Claim: $\{x_i y_j\}$ is a basis for L over K .

We already know that this set spans L since

$$a = \sum e_i x_i = \sum a_{ij} x_i y_j.$$

This set is also linearly independent since

$$\sum a_{ij} x_i y_j = 0 \Rightarrow (\forall j) \sum a_{ij} x_i = 0 \Rightarrow (\forall ij) a_{ij} = 0.$$

So, $|L : K| = nm = |L : E| \cdot |E : K|$. \square

Theorem 3.5 (Galois correspondence). *Suppose L is a Galois extension of K with Galois group G . Then there is a 1-1 correspondence between the intermediate fields $K \subseteq E \subseteq L$ and subgroups $H \leq G$. The correspondence maps E to $H = \text{Gal}(L/E)$ and it maps $H \leq G$ to the fixed field*

$$L^H = \{a \in L \mid \sigma(a) = a \forall \sigma \in H\}.$$

Proof. It follows from the definitions (and Theorem 3.3) that $H = \text{Gal}(L/E)$ is a subgroup of $G = \text{Gal}(L/K)$. And it is straightforward to show that L^H is an intermediate field. The key point is to show that $E = L^H$.

Since $H = \text{Gal}(L/E)$ fixes E by its definition, $E \subseteq L^H$. So, it suffices to show that the degree of this extension is 1, i.e., $|L^H : E| = 1$. But, L^H is an intermediate field. So, L/L^H is a Galois extension. The degree of this extension is the size of the Galois group which I claim is

$$\text{Gal}(L/L^H) = H = \text{Gal}(L/E).$$

The reason is that the elements of $H = \text{Gal}(L/E)$ fix L^H by definition of L^H . So, $H \leq \text{Gal}(L/L^H)$. And any element of $\text{Gal}(L/L^H)$ will also fix $E \subseteq L^H$. So, $\text{Gal}(L/L^H) \leq H$. So, they are equal and their degrees are the same. So, the formula

$$|L : E| = |L : L^H| \cdot |L^H : E|$$

implies that $|L^H : E| = 1$. So $L^H = E$.

The other part of the proof I did not say in class: We should take an arbitrary subgroup H of $G = \text{Gal}(L/K)$ and show that $\text{Gal}(L/L^H) = H$. Let $S = \text{Gal}(L/L^H)$. Then S contains H and $|S| = |L : L^H| = n$. So, all we need to do is to show that H contains at least n elements, i.e., $|L : L^H| \leq |H|$.

For this I need to use the primitive element theorem which I mentioned earlier. It says that L is generated by one element: $L = L^H(a)$. Let $C = \{\sigma(a) \mid \sigma \in H\}$. Then C is a subset of L having $\leq |H|$ number of elements which is invariant under the action of H . This implies that

$$f(X) = \prod_{c \in C} (X - c)$$

is invariant under the action of H , i.e., $f(X) \in L^H[X]$. Since $f(a) = 0$, $f(X)$ is a multiple of $\text{irr}(a, L^H)$. So,

$$|L : L^H| = \deg(\text{irr}(a, L^H)) \leq \deg(f) = |C| \leq |H|$$

which is what we needed to prove. \square

Theorem 3.6. *If L is a finite separable extension of K then $L = K(a)$ for some $a \in L$.*

Proof. First we can exclude the case where K is finite because, in that case, the units of L form a cyclic group generated by one element. So, assume $|K| = \infty$.

Let $a \in L$ be an element of maximal degree, say n . Then I claim that $L = K(a)$. Otherwise there is an element $b \in L$, $b \notin K(a)$. Then

$|K(a, b) : K| = m > n$. Let $\phi_1, \phi_2, \dots, \phi_m : K(a, b) \rightarrow \overline{K}$ be the distinct embeddings of $K(a, b)$ into \overline{K} over K . Then I claim that there is an element $x \in K$ so that

$$\phi_i(a)x + \phi_i(b) = \phi_i(xa + b)$$

are all distinct. The reason is that the polynomial

$$p(X) = \prod_{i < j} ([\phi_i(a)X + \phi_i(b)] - [\phi_j(a)X + \phi_j(b)])$$

is nonzero (each factor being nonzero) and therefore there is an $x \in K$ so that $p(x) \neq 0$ (since $p(X)$ has only a finite number of roots and K is infinite). But then, $ax + b \in L$ has degree at least $m > n$ which is a contradiction. \square

3.3. quadratic extensions. Suppose that L is a degree 2 extension of K . Then $L = K(a)$ and the irreducible polynomial of a is $f(X) = X^2 + bX + c$. Suppose that $\text{char}(K) \neq 2$. Then the roots of this polynomial are

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

and a is one of these roots. Since $b, 1/2 \in K$, the extension $K(a)$ is equal to

$$K(2a + b) = K(\sqrt{b^2 - 4c}) = K(\sqrt{\Delta}).$$

Definition 3.7. The *discriminant* Δ of a polynomial $f(X)$ is equal to the sum of squares of differences between the roots: $\Delta = \delta^2$ where

$$\delta = \prod_{i < j} (\alpha_i - \alpha_j).$$

Note that δ is only well defined up to sign.

Theorem 3.8. *If $\text{char}(K) \neq 2$, every quadratic extension of K has the form $L = K(\sqrt{D})$ for some $D \in K$, $D \notin K^2$.*

The irreducible polynomial of \sqrt{D} is $X^2 - D$ which has two distinct roots $\pm\sqrt{D}$ both of which lie in $K(\sqrt{D})$. Therefore, $K(\sqrt{D})$ is a Galois extension of K with Galois group $\mathbb{Z}/2$.

3.4. cubic extensions. Now suppose that L is a cubic (degree 3) extension of K and $\text{char}(K) \neq 2, 3$. Then $L = K(\alpha)$. Suppose that $f(X) = \text{irr}(\alpha, K)$. Then there are two possibilities:

- (1) L is the splitting field of $f(X)$.
- (2) $f(X)$ factors as

$$f(X) = (X - \alpha)g(X)$$

where $g(X)$ is irreducible over L .

In the first case, L is a Galois extension of K and the Galois group is $\mathbb{Z}/3$.

In the second case, the splitting field of $f(X)$ is $L(\beta) = K(\alpha, \beta)$ where β is a root of $g(X)$. Since $g(X)$ is quadratic, $|K(\alpha, \beta) : K(\alpha)| = 2$ and

$$|K(\alpha, \beta) : K| = |K(\alpha, \beta) : K(\alpha)| |K(\alpha) : K| = 2 \cdot 3 = 6.$$

The Galois group $\text{Gal}(K(\alpha, \beta)/K)$ is the symmetric group on 3 letters. This follows from the following observation.

Theorem 3.9. *The Galois group of the splitting field of a polynomial $f(X)$ is a subgroup of the group of permutations of the roots of $f(X)$.*

Proof. I said in class that this is “obvious.” That is because the splitting field L of $f(X)$ is generated by the roots of $f(X)$ by definition:

$$L = K(\alpha_1, \dots, \alpha_n)$$

and any automorphism ϕ of L over K is determined by its effect on the these generators. Furthermore, ϕ must take roots to roots since it is a homomorphism which fixes the coefficients of $f(X)$. So, ϕ permutes the roots of $f(X)$ and is determined by this permutation. \square

In terms of permutation groups the two cases are

- (1) $G = A_3 = \langle (123) \rangle$ the alternating group since this is the only subgroup of S_3 with 3 elements.
- (2) $G = S_3$.

We discussed the role of the discriminant: $\Delta = \delta^2$ and the fact that δ is *alternating* in the sense that it changes sign if you switch two of the roots.

Lemma 3.10. $\delta = \prod_{i < j} (\alpha_j - \alpha_i)$ has the property that it changes sign if two of the roots are switched. In fact, for any permutation $\sigma \in S_n$ we have:

$$\prod_{i < j} (\alpha_{\sigma(j)} - \alpha_{\sigma(i)}) = \text{sgn}(\sigma)\delta.$$

Proof. It suffices to take the case where σ is a transposition of consecutive integers: $\sigma = (i, i + 1)$. In that case, the factor $\alpha_{i+1} - \alpha_i$ changes sign and all other factors remain the same. \square

Corollary 3.11.

$$\delta \in L^{A_n}.$$

Theorem 3.12. *Let $f(X)$ be an irreducible cubic polynomial over K with discriminant $\Delta \in K$. Assume $\text{char}(K) \neq 2, 3$. Then the splitting field of $f(X)$ has degree 3 over K if and only if $\delta = \sqrt{\Delta} \in K$.*

Proof. In class we figured out that one direction is clear: If the degree of splitting field is 3 then the Galois group is A_3 and $\delta \in L^{A_3} = K$.

As Roger pointed out after class, the converse is also easy: If the splitting field has degree 6 and the Galois group is S_3 then δ is not an element of $K = L^{S_3}$ since it is not fixed by the action of S_3 . \square

3.5. Vandermonde. This product δ is also the sign of the *Vandermonde* determinant:

$$\delta = \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

The proof is by induction on n . Let $X = \alpha_n$. Then, the Vandermonde determinant, call it V_n , is a polynomial in X of degree $n - 1$. If $\alpha_n = \alpha_i$ for some $i < n$ then the determinant of the matrix is zero. So, $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ are the roots of the polynomial. So:

$$V_n = C \prod_{i=1}^{n-1} (X - \alpha_i)$$

where C must be the leading coefficient, i.e., $C = V_{n-1}$ is the smaller Vandermonde which we know by induction:

$$V_{n-1} = \prod_{n-1 \geq j > i \geq 1} (\alpha_j - \alpha_i).$$

Multiplying these we get

$$V_n = V_{n-1} \prod_{i=1}^{n-1} (X - \alpha_i)$$

which gives the formula we wanted when $X = \alpha_n$.

3.6. $\alpha = \sqrt{2} + \sqrt{3}$. We computed the irreducible polynomial of this element by squaring it twice:

$$\begin{aligned}\alpha^2 &= 2 + 3 + 2\sqrt{6} \\ x(\alpha^2 - 5)^2 &= \alpha^4 - 10\alpha^2 + 25 = 4 \cdot 6 = 24\end{aligned}$$

So,

$$f(X) = \text{irr}(\alpha, \mathbb{Q}) = X^4 - 10X^2 + 1.$$

This polynomial is irreducible over \mathbb{Q} because it is irreducible over \mathbb{Z} . This in turn follows from that observation that, if $f(X)$ factors over \mathbb{Z} , it must be as a product of two quadratic terms. This would imply that two of the roots

$$\pm\sqrt{2} \pm \sqrt{3}$$

have both product and sum equal to an integer. But that is not so.

I pointed out that sums of these roots give:

$$\begin{aligned}(\sqrt{2} + \sqrt{3}) + (\sqrt{2} - \sqrt{3}) &= 2\sqrt{2} \\ (\sqrt{2} + \sqrt{3}) + (-\sqrt{2} + \sqrt{3}) &= 2\sqrt{3}\end{aligned}$$

This means that the splitting field of $f(X)$ contains $\sqrt{2}$ and $\sqrt{3}$. And conversely,

$$\pm\sqrt{2} \pm \sqrt{3} \in L = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

So, L must be the splitting field of $f(X)$.

Questions

- (1) What is the Galois group $\text{Gal}(L/\mathbb{Q})$?
- (2) Find all subgroups of G .
- (3) What are the corresponding subfields of L ?

(1) $\text{Gal}(L/\mathbb{Q})$

We know that the Galois group has 4 elements. So, it must be abelian (any group of order p^2 is abelian). So, it is either $\mathbb{Z}/4$ or $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. The group $\mathbb{Z}/4$ has only one nontrivial proper subgroup, $2\mathbb{Z}/4$. By the Galois correspondence this would mean there is only one intermediate field. But we have at least three intermediate fields:

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}).$$

So, $\text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

(2) Subgroups of $\text{Gal}(L/\mathbb{Q})$.

This group has three subgroups of order 2. These must correspond to the three obvious intermediate fields list above. The question is: What is the correspondence?

The elements of the Galois group are: $\sigma, \tau, \sigma\tau, 1$ where σ, τ are defined by:

$$\begin{aligned}\sigma(\sqrt{2}) &= -\sqrt{2}, & \sigma(\sqrt{3}) &= \sqrt{3}, \\ \tau(\sqrt{3}) &= -\sqrt{3}, & \tau(\sqrt{2}) &= \sqrt{2}, \\ \sigma\tau(\sqrt{2}) &= -\sqrt{2}, & \sigma\tau(\sqrt{3}) &= -\sqrt{3}.\end{aligned}$$

To prove this, use the fact that the Galois group acts transitively on the set of roots of $f(X)$. Then $\sigma, \tau, \sigma\tau$ are the elements $Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ which send $\alpha = \sqrt{2} + \sqrt{3}$ to

$$\sigma(\alpha) = -\sqrt{2} + \sqrt{3}, \quad \tau(\alpha) = \sqrt{2} - \sqrt{3}, \quad \sigma\tau(\alpha) = -\alpha.$$

(3) Corresponding intermediate fields.

Since $\sigma, \tau, \sigma\tau$ fix $\sqrt{3}, \sqrt{2}, \sqrt{6}$, resp., we have:

$$\begin{aligned}Gal(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2})) &= \langle \tau \rangle \\ Gal(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{3})) &= \langle \sigma \rangle \\ Gal(\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{6})) &= \langle \sigma\tau \rangle.\end{aligned}$$