Homework 3

Frederick Robinson

22 November 2010

1 Question 1

1.1 Question

1. Compute the Galois group of the polynomial $X^6 + 3$ over $\mathbb{Q}$.
2. Find a primitive element for the splitting field of $X^6 + 3$ over $\mathbb{Q}$.
3. List all fields intermediate between $\mathbb{Q}$ and the splitting field $X^6 + 3$ over $\mathbb{Q}$.

1.2 Answer

1. D_6.

   The solutions to $f(X) = X^6 + 3$ are of the form $\zeta_6^n \zeta_{12} \sqrt[6]{3}$ for ζ_n a primitive nth root of unity. The automorphisms fixing $\mathbb{Q}$ may be specified by where they send $\zeta_{12}\sqrt[6]{3}$ and ζ_{12}. In particular they are generated by

   $$\sigma : \begin{cases} \zeta_{12} \mapsto \zeta_{12} \\ \zeta_{12}\sqrt[6]{3} \mapsto \zeta_{12}^5 \sqrt[6]{3} \end{cases} \qquad \tau : \begin{cases} \zeta_{12} \mapsto \zeta_{12}^{-1} \\ \zeta_{12}\sqrt[6]{3} \mapsto \zeta_{12}\sqrt[6]{3} \end{cases} .$$

   It is easy to see that these are generators for D_6 with τ a reflection, and σ a rotation.

2. $\zeta_{12}(1 + \sqrt[6]{3})$ is not fixed by any of the Galois automorphisms, so it is a primitive element.

3. Recall that intermediate fields are those fields fixed by subgroups of the Galois group. There are 4 such nontrivial subgroups. They are generated by $\sigma, \tau, \sigma\tau$, and $\sigma^2\tau$ respectively.

We can determine the fixed field by the action on linear combinations of the basis of roots of the form $\zeta_{12}\zeta_6^m(\sqrt[6]{3})^n$. We compute the fixed field of the subgroup generated by τ below.

$$\zeta_{12}(a\sqrt[6]{3}\zeta_6 + b\sqrt[6]{3}\zeta_6^2 + c\sqrt[6]{3}\zeta_6^3 + d\sqrt[6]{3}\zeta_6^4 + e\sqrt[6]{3}\zeta_6^5 + f\sqrt[6]{3})$$
$$\mapsto \zeta_{12}(e\sqrt[6]{3}\zeta_6 + d\sqrt[6]{3}\zeta_6^2 + c\sqrt[6]{3}\zeta_6^3 + b\sqrt[6]{3}\zeta_6^4 + a\sqrt[6]{3}\zeta_6^5 + f\sqrt[6]{3}).$$

So, to be fixed, an element must have $a = e, b = d$. So, in particular it must be expressible like

$$\zeta_{12}(a(\sqrt[6]{3}\zeta_6 + \sqrt[6]{3}\zeta_6^5) + b(\sqrt[6]{3}\zeta_6^4 + \sqrt[6]{3}\zeta_6^2) + c\sqrt[6]{3}\zeta_6^3 + f\sqrt[6]{3}).$$

We can further simplify to obtain

$$\zeta_{12}\sqrt[6]{3}(a(\zeta_6 + \zeta_6^5) + f) = \zeta_{12}\sqrt[6]{3}(a + f))$$

so we conclude that the fixed field contains $\mathbb{Q}(\zeta_{12}\sqrt[6]{3})$. Now, we continue, computing

$$\zeta_{12}(a\zeta_6 + b\zeta_6^2 + c\zeta_6^3 + d\zeta_6^4 + e\zeta_6^5 + f)$$
$$\mapsto \zeta_{12}^{-1}(a\zeta_6 + b\zeta_6^2 + c\zeta_6^3 + d\zeta_6^4 + e\zeta_6^5 + f)$$
$$\mathbb{Q}(\zeta_{12}\sqrt[6]{3})$$
$$\zeta_{12}(a(\sqrt[6]{3})^2\zeta_6 + b(\sqrt[6]{3})^2\zeta_6^2 + c(\sqrt[6]{3})^2\zeta_6^3 + d(\sqrt[6]{3})^2\zeta_6^4 + e(\sqrt[6]{3})^2\zeta_6^5 + f(\sqrt[6]{3})^2)$$
$$\mapsto \zeta_{12}(a(\sqrt[6]{3})^2\zeta_6 + b(\sqrt[6]{3})^2\zeta_6^2 + c(\sqrt[6]{3})^2\zeta_6^3 + d(\sqrt[6]{3})^2\zeta_6^4 + e(\sqrt[6]{3})^2\zeta_6^5 + f(\sqrt[6]{3})^2)$$
$$\mathbb{Q}(\zeta_{12}\sqrt[3]{3})$$

By now it's easy to see that the entire fixed field is just $\mathbb{Q}(\zeta_{12}\sqrt[6]{3})$.

We perform similar computations with the other subgroups to get $\mathbb{Q}(\zeta_{12}\sqrt[6]{3}\zeta_6), \mathbb{Q}(\zeta_{12})$ and $\mathbb{Q}(\sqrt[6]{3}\zeta_3)$ corresponding to $\sigma\tau, \sigma$, and $\sigma^2\tau$ respectively.

2 Question 2

2.1 Question

Let $K = \mathbb{Q}[i]$.

1. Determine the degree of the splitting field L of $X^{15} - 1$ over K.
2. Determine $\mathrm{Gal}(L/K)$.
3. List all intermediate fields between K and L.

2.2 Answer

1. I claim that the splitting field L of X^15-1 over K is just the same as the splitting field of $X^{15}-1$ over $\mathbb{Q}$.

   Proof. Suppose not, then at least one of the automorphisms which make up the Galois group of $\mathbb{Q}(X^{15}-1)$ does not fix i. Hence, there is some nontrivial linear combination of the primitive 15th roots of unity with coefficients in $\mathbb{Q}(i)$ which is i. [Throughout we will exploit the fact that $p = p'x + p''y$ for $p, p', p'' \in \mathbb{Q}$, x, y irrational implies $x = qy + q$ for some $q, q' \in \mathbb{Q}$.] That is

   $$i = a\zeta_{15} + b\zeta_{15}^2 + c\zeta_{15}^4 + d\zeta_{15}^7 + e\zeta_{15}^8 + f\zeta_{15}^{11} + g\zeta_{15}^{13} + h\zeta_{15}^{14} + j$$

   for $a, b, c, d, e, f, g, h, j \in \mathbb{Q}(i)$. However, clearly we must have

   $$\Re i = \Re\left(a\zeta_{15} + b\zeta_{15}^2 + c\zeta_{15}^4 + d\zeta_{15}^7 + e\zeta_{15}^8 + f\zeta_{15}^{11} + g\zeta_{15}^{13} + h\zeta_{15}^{14} + j\right)$$

   $$0 = \Re(a\zeta_{15})+\Re(b\zeta_{15}^2)+\Re(c\zeta_{15}^4)+\Re(d\zeta_{15}^7)+\Re(e\zeta_{15}^8)+\Re(f\zeta_{15}^{11})+\Re(g\zeta_{15}^{13})+\Re(h\zeta_{15}^{14})+\Re(j)$$

   since the coefficients are from $\mathbb{Q}(i)$

   $$= a\Re(\zeta_{15})+b\Re(\zeta_{15}^2)+c\Re(\zeta_{15}^4)+d\Re(\zeta_{15}^7)+e\Re(\zeta_{15}^8)+f\Re(\zeta_{15}^{11})+g\Re(\zeta_{15}^{13})+h\Re(\zeta_{15}^{14})$$

   $$+a'\Re(i\zeta_{15})+b'\Re(i\zeta_{15}^2)+c'\Re(i\zeta_{15}^4)+d'\Re(i\zeta_{15}^7)+e'\Re(i\zeta_{15}^8)+f'\Re(i\zeta_{15}^{11})+g'\Re(i\zeta_{15}^{13})+h'\Re(i\zeta_{15}^{14})+j$$

   for all variables in $\mathbb{Q}$. Hence, the only possible combinations have

   $$a = h \quad b = g \quad c = f \quad d = e \quad a' = -h' \quad b' = -g' \quad c' = -f' \quad d' = -e'$$

   so rewriting we have

   $$i = a(\zeta_{15} + \zeta_{15}^{14}) + b(\zeta_{15}^2 + \zeta_{15}^{13}) + c(\zeta_{15}^4 + \zeta_{15}^{11}) + d(\zeta_{15}^7 + \zeta_{15}^8)$$

   $$+a'i(\zeta_{15} - \zeta_{15}^{14}) + b'i(\zeta_{15}^2 - \zeta_{15}^{13}) + c'i(\zeta_{15}^4 - \zeta_{15}^{11}) + d'i(\zeta_{15}^7 - \zeta_{15}^8) + j + ij'$$

   with all coefficients from $\mathbb{Q}$. However, we need to have

   $$\Im(i) = \Im(a(\zeta_{15} + \zeta_{15}^{14}) + b(\zeta_{15}^2 + \zeta_{15}^{13}) + c(\zeta_{15}^4 + \zeta_{15}^{11}) + d(\zeta_{15}^7 + \zeta_{15}^8)$$

   $$+a'i(\zeta_{15} - \zeta_{15}^{14}) + b'i(\zeta_{15}^2 - \zeta_{15}^{13}) + c'i(\zeta_{15}^4 - \zeta_{15}^{11}) + d'i(\zeta_{15}^7 - \zeta_{15}^8) + j + ij')$$

   $$1 = a\Im(\zeta_{15} + \zeta_{15}^{14}) + b\Im(\zeta_{15}^2 + \zeta_{15}^{13}) + c\Im(\zeta_{15}^4 + \zeta_{15}^{11}) + d\Im(\zeta_{15}^7 + \zeta_{15}^8)$$

   $$+a'\Re(\zeta_{15} - \zeta_{15}^{14}) + b'\Re(\zeta_{15}^2 - \zeta_{15}^{13}) + c'\Re(\zeta_{15}^4 - \zeta_{15}^{11}) + d'\Re(\zeta_{15}^7 - \zeta_{15}^8)) + j'$$

   $$1 = j'$$

Therefore,

$$0 = a(\zeta_{15} + \zeta_{15}^{14}) + b(\zeta_{15}^{2} + \zeta_{15}^{13}) + c(\zeta_{15}^{4} + \zeta_{15}^{11}) + d(\zeta_{15}^{7} + \zeta_{15}^{8})$$
$$+a'i(\zeta_{15} - \zeta_{15}^{14}) + b'i(\zeta_{15}^{2} - \zeta_{15}^{13}) + c'i(\zeta_{15}^{4} - \zeta_{15}^{11}) + d'i(\zeta_{15}^{7} - \zeta_{15}^{8}) + j$$

Again, we exploit the fact that

$$0 = \Re(a(\zeta_{15} + \zeta_{15}^{14}) + b(\zeta_{15}^{2} + \zeta_{15}^{13}) + c(\zeta_{15}^{4} + \zeta_{15}^{11}) + d(\zeta_{15}^{7} + \zeta_{15}^{8})$$
$$+a'i(\zeta_{15} - \zeta_{15}^{14}) + b'i(\zeta_{15}^{2} - \zeta_{15}^{13}) + c'i(\zeta_{15}^{4} - \zeta_{15}^{11}) + d'i(\zeta_{15}^{7} - \zeta_{15}^{8}) + j)$$
$$\Rightarrow -j = a\Re(\zeta_{15} + \zeta_{15}^{14}) + b\Re(\zeta_{15}^{2} + \zeta_{15}^{13}) + c\Re(\zeta_{15}^{4} + \zeta_{15}^{11}) + d\Re(\zeta_{15}^{7} + \zeta_{15}^{8})$$
$$+a'\Im(\zeta_{15} - \zeta_{15}^{14}) + b'\Im(\zeta_{15}^{2} - \zeta_{15}^{13}) + c'\Im(\zeta_{15}^{4} - \zeta_{15}^{11}) + d'\Im(\zeta_{15}^{7} - \zeta_{15}^{8}).$$

However, this is equivalent to requiring that each coefficient be zero. Contradiction. □

2. This is just the same as $\mathrm{Gal}(L/\mathbb{Q})$ by the above. That is $(\mathbb{Z}/15\mathbb{Z})^{\times}$

3. These are the fields fixed by subgroups of the Galois group. These are in particular the fields $\mathbb{Q}(i, \zeta_p)$ for all $p|15$.

3 Question 3

3.1 Question

Let $f(X)$ be an irreducible polynomial of degree n in $k[X]$, k of characteristic 0. Explain how the Galois group of $f(X)$ may be regarded as a subgroup of S_n, and show that it is a transitive subgroup.

3.2 Answer

The Galois group maps roots of f to one another. We can therefore view it as a permutation of the roots of f $\mathrm{Gal}(k(f)/k) \hookrightarrow S_n$. An automorphism of $k(f)$ must induce a map on the roots of k, since if a root were sent to a non-root by an automorphism this would induce a dependence relation among the roots.

Moreover, the induced map is bijective since, were it not surjective the image of the automorphism would not be the entire field. Since we are only in the finite case surjectivity implies bijectivity.

The subgroup is transitive since given two roots α, β there is some $\sigma \in$Gal$k(f)/k$ such that $\sigma(\alpha) = \beta$ by the existence of splitting fields.

4 Question 4

4.1 Question

Let $f(X) = X^3 + pX + q$ be an irreducible polynomial over a field k of characteristic zero. Let x_1, x_2, x_3 be roots of $f(X)$ in an algebraic closure of k.

1. Show that $\Delta = ((x_1 - x_2)(x_2 - x_3)(x_3 - x_1))^2$ is an element of k.
2. Show that the Galois group of f is either S_3 or A_3 depending on whether or not Δ is a square in k.

4.2 Answer

1. *Proof.* Let $d = \sqrt{\Delta}$ for Δ the discriminant as above. Since the Galois group permutes the roots in some way $\sigma(d) = \pm d$ for any $\sigma \in \text{Gal}(k(f)/k)$. So, $\Delta = d^2$ is in the fixed field. □

2. *Proof.* $\text{Gal}(k(d)/k)$ is a subgroup of $\text{Gal}(k(f)/k)$ since each x_i is in $k(f)$.

   Since f is irreducible a root of f generates an extension of degree 3. Therefore, the degree of the splitting field over k is divisible by 3. Since it is a subgroup of S_3 this means that it's either A_3, or all of S_3.

   Recall that a permutation is a member of A_3 if and only if it fixes the product d.

   If Δ is the square of some element from k then precisely the members of A_3 fix the base field. Hence $\text{Gal}(k(f)/k)$ is A_3.

   If Δ is not the square of some element of k then there must be some permutations in the Galois group which don't fix d, and so $\text{Gal}(k(f)/k)$ is S_3. □

Dummit and Foote p612

5 Question 5

5.1 Question

Determine the splitting field and Galois group of $(X^2 - 2)(X^3 - 2)$ over $\mathbb{Q}$.

5.2 Answer

The splitting field for $(x^2 - 2)$ is just $\mathbb{Q}(\sqrt{2})$, whereas the splitting field of $\mathbb{Q}(\zeta_3 \sqrt[3]{2})$. The splitting field for both polynomials must therefore be a subfield of $\mathbb{Q}(\sqrt{2}, \zeta_3 \sqrt[3]{2})$. In fact, since the order of the extension but be divisible by both 2, and 3 this is the entire field.

Members of the Galois group are defined by where they send these two elements. The entire group can be generated by

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases} \quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2} \end{cases}$$

and is therefore isomorphic to $\mathbb{Z}/2\mathbb{Z} \times S_3$.

6 Question 6

6.1 Question

Give (with proof) the diagram of intermediate fields for $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$.

6.2 Answer

Recall that the 12th cyclotomic polynomial is $x^4 - x^2 + 1$. Let ζ_{12} denote a primitive 12th root of unity. We can check that the automorphisms defined by

$$\zeta_{12} \mapsto \zeta_{12}^n \quad n \in \{1, 5, 7, 11\}$$

fix $\mathbb{Q}$. It has appropriate order, so these 4 elements constitute the Galois group. Each element of the group has order 2 so this group is just isomorphic to V_4.

Knowing the subgroups of V_4 we compute the fixed fields of of the subgroups of the Galois group. In particular we want the fields fixed by each element individually. These are $\mathbb{Q}(\zeta_{12}), \mathbb{Q}(\zeta_4), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{3})$ respectively.

7 Question 7

7.1 Question

1. Find all closed subgroups of $\mathbb{Z}_p$.
2. Determine which of these closed subgroups is also open.
3. Find all intermediate fields in the extension $\cup_{i \geq 0} \mathbb{F}_{q^{l^i}} / \mathbb{F}_q$ where q is a prime power and l is a prime.

7.2 Answer

1. The subgroups of the form,

$$A_n = \{\underbrace{0, 0, \ldots, 0}_{\text{n times}}, a_1, a_2, \ldots\}$$

as well as the trivial subgroup are the only closed subgroups.

Proof. The subgroup consisting of $\{0, 0, \ldots\}$ is clearly closed, since it consists of just one element. Let H be a nontrivial, closed subgroup. Then it contains at least one element say $x \in H$.

$$x = \{x_1, x_2, \ldots, x_i, \ldots\}$$

I claim that every closed subgroup containing x also contains A_k where $k+1$ is the first place that x is nonzero.

Fix some other $y \in \mathbb{Z}_p$ such that for every i that has $x_i = 0$, $y_i = 0$. I claim that $y \in H$. This is immediate, since by adding x to itself repeatedly we can set its first n places arbitrarily (subject to the constraint that we can't change places j with $x_j = 0$. Now we construct a sequence in this manner so that the mth term of the sequence agrees with y in the first m places. By (topological) closure this sequence converges in H.

This suffices to show that all closed subgroups are of the claimed form. A sequence in A_k converges to a value in A_k, so these subgroups are closed. Moreover, these are the only closed subgroups, for if there is a closed subgroup G, then it is contained in A_k where k is the min of the number of leading zeroes in element of G, by the above argument. □

2. The complement of some A_k is the set of sequences $0 \leq j < k$ leading zeroes. This set never has the form A_l for some l. However, the complement of our exceptional set $\{0, 0, \ldots\}$ is just $A_0 = \mathbb{Z}_p$. This then, is the only subgroup set which is also open.

3. Consider a member of $\mathcal{F} = \cup_{i \geq 0} \mathbb{F}_{q^{i!}} / \mathbb{F}_q$ as a p-adic integer, for p prime, $p^n = q$. Under the Krull topology, the subfields are precisely those for which the restriction mappings are continuous.

A function is continuous if the inverse image of all open (closed) is open (closed). So, a restriction of $\mathcal{F}$ is continuous if and only if it is

to a subgroup of the form A_k as above, or to the zero set. Hence, we may write every intermediate field as $\mathbb{F}_{p^m}$ for some $m \geq n$, as these are the fixed fields of the Galois subgroups A_m.