Homework

Frederick Robinson

10 May 2010

1 Chapter 14 Section 1

1.1 Problem 1

1.1.1 Question

1. Show that if the field K is generated over F by the elements $\alpha_1, \ldots, \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K.

2. Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \ldots, \sigma_k$ are generators for G. Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \ldots, \sigma_k$

1.1.2 Answer

1. *Proof.* Let $\alpha_1, \ldots, \alpha_n$ be a set of generators for K/F. Any element of K can therefore be expressed uniquely in the form $c_0 + c_1\alpha_1 + \ldots + c_n\alpha_n$ with $c_i \in F$. An automorphism of K which fixes F must take $c_i \mapsto c_i$ for any $c_i \in F$ since it fixes F. Therefore, by properties of homomorphism it must take $c_0 + c_1\alpha_1 + \ldots + c_n\alpha_n \mapsto c_0 + c_1\sigma(\alpha_1) + \ldots + c_n\sigma(\alpha_n)$ and the automorphism is uniquely determined by $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ as claimed. □

   If an automorphism fixes K then $\alpha_i \mapsto \alpha_i$ via σ for any basis element α_i. Conversely, by the foregoing if σ fixes a basis for K/F then σ fixes all of K.

2. *Proof.* ($\Leftarrow$) If the generators $\sigma_1, \ldots, \sigma_k$ fix all of E/F then so does the entire subgroup G since by definition any member of G may be written as a combination of the generators and by properties of homomorphism such combinations fix all of E/F if each does.

   Conversely ($\Rightarrow$), if all of G fixes some subfield E/F then it is in particular fixed by generators for G say $\sigma_1, \ldots, \sigma_k$ as claimed. □

1.2 Problem 4

1.2.1 Question

Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

1.2.2 Answer

Any isomorphism φ is completely determined by where it takes a set of generators for $\mathbb{Q}(\sqrt{2})$ in particular it must be of the form $a + b\sqrt{2} \mapsto a(c + d\sqrt{3}) + b(e + f\sqrt{3})$ where $c + d\sqrt{3}$ is the image of 1 under φ and $\varphi(\sqrt{2}) = e + f\sqrt{3}$. Furthermore, we must have $\varphi(1) = 1 \Rightarrow c = 1, d = 0$, so any isomorphism must be of the form $a + b\sqrt{2} \mapsto (a + be) + bf\sqrt{3})$ for some $e, f \in \mathbb{Q}$.

However, in order that φ be a homomorphism we must have $\varphi(x^2) = \varphi(x)^2$. Some computation reveals that for an arbitrary element $x = a + b\sqrt{2}$ we get $\varphi(x^2) = \varphi(a^2 + 2b^2 + 2ab\sqrt{2}) = a^2 + 2b^2 + 2abe + 2abf\sqrt{3}$ whereas $\varphi(x)^2 = ((a + be) + bf\sqrt{3})^2 = (a + be)^2 + 3bf + (2bfa + 2b^2ef)\sqrt{3}$. In order for this equality to hold we must have in particular $2bfa + 2b^2ef = 2abf$ with a, b arbitrary. Thus, $fa + bef = 2af \Rightarrow bef = af \Rightarrow be = a$, a contradiction since a, b were arbitrary.

1.3 Problem 5

1.3.1 Question

Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.

1.3.2 Answer

The automorphisms of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are completely determined by where they take $\sqrt[4]{2}$. However, since the subfield $\mathbb{Q}(\sqrt{2})$ is fixed (in particular the element $\sqrt{2}$) we have $(\sqrt[4]{2})^2 = \varphi((\sqrt[4]{2})^2) = (\varphi(\sqrt[4]{2}))^2$. Thus $\varphi(\sqrt[4]{2}) = \pm\sqrt[4]{2}$ are the only automorphisms of $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$.

1.4 Problem 10

1.4.1 Question

Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F) \to^{\sim} \mathrm{Aut}(K'/F')$

1.4.2 Answer

Proof. Let σ, τ be arbitrary elements of $\mathrm{Aut}(K/F)$. The specified map is a homomorphism since $\varphi(\sigma + \tau)\varphi^{-1} = \varphi\sigma\varphi^{-1} + \varphi\tau\varphi^{-1}$ and $\varphi(\sigma\tau)\varphi^{-1} = \varphi\sigma\varphi^{-1}\varphi\tau\varphi^{-1}$.

It's injective since $\varphi\sigma\varphi^{-1} = \varphi\tau\varphi^{-1} \Rightarrow \varphi\sigma = \varphi\tau \Rightarrow \sigma = \tau$ and surjective since given $\sigma \in \text{Aut}(K'/F')$ setting $\tau = \varphi^{-1}\sigma\varphi$ we have $\varphi\tau\varphi^{-1} = \varphi\varphi^{-1}\sigma\varphi\varphi^{-1} = \sigma$. $\square$

2 Chapter 14 Section 2

2.1 Problem 2

2.1.1 Question

Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

2.1.2 Answer

It is easy to check that $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ is a root of the polynomial

$$f(x) = x^3 - 3x^2 - 3x - 1$$

Moreover, since α is contained in the degree 3 extension $\mathbb{Q}(\sqrt[3]{2})$ its minimal polynomial is of degree 3 or 1. It can't be 1 since $\alpha \notin \mathbb{Q}$ thus the minimal polynomial must have degree 3. Hence, f is the minimal polynomial.

2.2 Problem 3

2.2.1 Question

Determine the Galois group of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$. Determine *all* the subfields of the splitting field of this polynomial.

2.2.2 Answer

The splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, an order 8 extension since $2, 3, 5$ are all prime. The group of automorphisms generated by

$$\sigma : \sqrt{2} \mapsto -\sqrt{2} \quad \tau : \sqrt{3} \mapsto -\sqrt{3} \quad \varphi : \sqrt{5} \mapsto -\sqrt{5}$$

is of order 8, and so this is the entire Galois group. It is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

By Galois correspondence we have subfields of the splitting field in bijective correspondence to subgroups of the Galois group. The degree 4 subfields are in particular

$$\mathbb{Q}(\sqrt{2}, \sqrt{15}), \mathbb{Q}(\sqrt{10}, \sqrt{3}), \mathbb{Q}(\sqrt{6}, \sqrt{5}), \mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{6}, \sqrt{10})$$

The degree 2 subfields are

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{15}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{30}).$$

2.3 Problem 4

2.3.1 Question

Let p be a prime. Determine the elements of the Galois group of $x^p - 2$.

2.3.2 Answer

The splitting field for $x^p - 2$ is generated by θ the real $\sqrt[p]{2}$ and ζ_p a principle pth root of unity. Therefore, since $\mathbb{Q}(\theta) \subset \mathbb{R}$ and $x^p - 2$ is Eisenstein the splitting field has degree $\varphi(p) \cdot p = p(p-1) = p^2 - p$.

A member of the Galois group is completely defined by where it takes these generators. In particular we have the possibilities

$$\begin{cases} \theta \mapsto \theta\zeta^a & a = 1, 2, \ldots, p \\ \zeta_p \mapsto (\zeta_p)^a & a = 1, 2, \ldots, p-1 \end{cases}$$

Since we have already determined that the order of the Galois group is $p^2 - p$ and there are exactly $p^2 - p$ possibilities all of them are elements of the Galois group