Exercises from Dummit and Foote Chapter 14 on Galois Theory

Wesley Basener

July 16, 2025

Problem 1.1. **(a)** Show that if the field K is generated over F by the elements $\alpha_1, ..., \alpha_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(\alpha_1), ..., \sigma(\alpha_n)$. In particular show that an automorphism fixes K if and only if it fixes a set of generators for K.

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

Proof. (a) Let σ be any automorphism on K fixing F. Then, for any $k = a_0 + a_1\alpha_1 + ... + a_n\alpha_n$ in K, $\sigma(k) = \sigma(a_0)+\sigma(a_1)\sigma(\alpha_1)+...+\sigma(a_n)\sigma(\alpha_n)$. Using the fact that σ fixes F, we have $\sigma(k) = a_0+a_1\sigma(\alpha_1)+...+a_n\sigma(\alpha_n)$. Hence the image of any $k \in K$ on σ is uniquely determined by $\sigma(\alpha_1), ..., \sigma(\alpha_n)$. From this, it is obvious that σ fixes K if it fixes the generators for K. □

(b). Denote the generators of E over F by $\alpha_1, ..., \alpha_m$. Suppose G fixes E/F. From part (a), this is true if and only if $\sigma_i(\alpha_j) = \alpha_j$ for all $i \in [1, k], j \in [1, m]$. Hence, any element of a E/F is fixed by any element of G. □

Problem 1.3. Determine the fixed field of complex conjugation on $\mathbb{C}$.

Proof. Complex conjugation is the function $\sigma : a + bi \mapsto a - bi$, which obviously fixes a. Hence, the fixed field of complex conjugation is $\mathbb{R}$ the real numbers. □

Problem 1.5. Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly.

Proof. There is only one basis element to this extension, namely $\sqrt[4]{2}$. Since $-\sqrt[4]{2} \neq \sqrt[4]{2}$, the automorphism $\sigma : a + b\sqrt[4]{2} \mapsto a - b\sqrt[4]{2}$ is not the identity. Hence, the automorphisms of this extension are $\{1, \sigma\}$. □

Problem 1.7. This problem determines $\text{Aut}(\mathbb{R}/\mathbb{Q})$.

(a) Prove that any $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$ Conclude that $a < b$ implies $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.

(b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbb{R}$.

(c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Proof. (a) Let σ be an automorphism on $\mathbb{R}/\mathbb{Q}$. Suppose x is a real square. Then, $x = p^2$ for real number p. Hence, we have $\sigma(x) = \sigma(p^2) = \sigma(p)\sigma(p)$. Thus, σ sends squares to squares.

Let y be any positive real number. Since y is positive, $\sqrt{y}$ is real. From the first part of this proof, we know that $\sigma(y) = \sigma(\sqrt{y}\sqrt{y}) = q^2$ for some real number q. Since we are limited to the real numbers, q^2 is positive. Hence, $\sigma(y)$ is positive.

For any $a, b \in \mathbb{R}$, $a < b$ implies $0 < b - a$. Hence, from the prior paragraph, $0 < \sigma(b) - \sigma(a)$. Adding $\sigma(a)$ to both sides yields $\sigma(a) < \sigma(b)$. Note that setting $b = 0$ proves that σ sends negatives to negatives. □

(b). Suppose a, b are real numbers such that $-\frac{1}{m} < a - b < \frac{1}{m}$ for some positive integer m.

Since m is an integer, it can be rewritten as $\Sigma_{i=0}^{m} 1$. Hence, $\sigma(m) = \Sigma_{i=0}^{m}\sigma(1) = \Sigma_{i=0}^{m} 1 = m$.

We can rewrite the above inequality as $-1 < m(a-b) < 1$. Which is the same as having $m(a-b)-1$ is negative and $m(a-b)+1$ is positive. From part (a), we know σ sends positives to positives and negatives to negatives. Hence, $\sigma(m(a-b)-1) = m(\sigma(a)-\sigma(b))-1$ is negative and $\sigma(m(a-b)-1) = m(\sigma(a)-\sigma(b))+1$ is positive. Which of course implies $-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$

To show that σ is continuous, let x be any real number and let $\epsilon > 0$. We can find a natural number N such that $\frac{1}{N} < \epsilon$. Then, for any x_0 such that $|x - x_0| < \frac{1}{N}$, we have $|\sigma(x) - \sigma(x_0)| < \frac{1}{N} < \epsilon$. Hence, σ is continuous. □

(c). Suppose $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ fixes $\mathbb{Q}$. Let x be any real number. Then by the density of the rationals in $\mathbb{R}$, for any $\epsilon > 0$, there exists some $q \in \mathbb{Q}$ such that $|x - q| < \epsilon$ Hence, $|\sigma(x-q)| = |\sigma(x) - q| < \epsilon$ which is only possible if $\sigma(x) = x$. Thus, any such σ mus be the identity function. Therefore, $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$. □

Problem 1.9. Determine the fixed field of the automorphism $t \mapsto t+1$ of $k(t)$.

Proof. Any element of $k(t)$ will have the form $\frac{\Sigma a_i t^i}{\Sigma b_i t^i}$ with $\gcd(\Sigma a_i x^i, \Sigma b_i x^i) = 1$. Suppose we have an element such that $\frac{\Sigma a_i (t+1)^i}{\Sigma b_i (t+1)^i} = \frac{\Sigma a_i t^i}{\Sigma b_i t^i}$. Then, $\frac{\Sigma a_i (t+1)^i}{\Sigma b_i (t+1)^i} - \frac{\Sigma a_i t^i}{\Sigma b_i t^i} = 0$ and since both fractions remain irreducible, we would have $\Sigma b_i (t+1)^i = \Sigma b_i t^i$. Thus, we would also have $\Sigma a_i (t+1)^i = \Sigma a_i (t)^i$. Hence, the fixed field of $k(t)$ is precisely the set of rational functions whose numerators and denominators are both fixed by the automorphism.

//TODO: finish this proof. □

Problem 2.1. Determine the minimal polynomial over $\mathbb{Q}$ for the element .

Proof. We have that $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ is a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, which is the splitting field of $(x^2-2)(x^2-5)$. Since this polynomial is separable, $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is Galois.

We can therefore find the other roots of the minimal polynomial of $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ by considering the action of $\mathrm{Aut}(\mathbb{Q}/\mathbb{Q}(\sqrt{2}, \sqrt{5})$ on $\sqrt{2}+\sqrt{5}$. This yields $\pm\sqrt{2} \pm \sqrt{5}$, which are indeed distinct.

Hence, the minimal polynomial of $\sqrt{2}+\sqrt{5}$ is $(x - \sqrt{2} + \sqrt{5})(x + \sqrt{2} + \sqrt{5})(x - \sqrt{2} - \sqrt{5})(x + \sqrt{2} - \sqrt{5})$ which multiplies to $x^4 - 14x^2 + 9$.

Remark 1. *The inverse of $\sqrt{2}+\sqrt{5}$ on $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ is $\frac{\sqrt{2}-\sqrt{5}}{-3}$. Hence, the field $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ contains $\sqrt{5}$ and $\sqrt{2}$. Given that $\mathbb{Q}(\sqrt{2}+\sqrt{5})$ is a subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, we have that $\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.*

From this, I initially though that the minimal polynomial of $\sqrt{2}+\sqrt{5}$ would be the same as the minimal polynomial with roots $\sqrt{2}$ and $\sqrt{5}$. But this is obviously not the case since $(\sqrt{2}+\sqrt{5})$ is not a root of $(x^2-5)(x^2-2)$.

This is a case of being disillusioned of unjustified assumptions. Just because $F(a) = F(b, c)$, does not mean that the minimal polynomial of a and the minimal polynomial with roots b, c are the same. In this case, $(x^2-5)(x^2-2)$ is not reducible, so it is not a minimal polynomial for anything. □

Problem 2.3. 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.

Proof. This polynomial is separable with roots $\pm\sqrt{2}$, $\pm\sqrt{3}$, and $\pm\sqrt{5}$. Hence, its splitting field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is Galois.

Any automorphism in $\mathrm{Aut}(K/\mathbb{Q})$ must fix $\mathbb{Q}$. This excludes any function sending $\pm\sqrt{a}$ to $\pm\sqrt{b}$ when $a \neq b$. To see this, let ϕ be a function where $\phi(\sqrt{2}) = \sqrt{3}$. Then, $\phi(2) = \phi(\sqrt{2}\sqrt{2}) = 3$, meaning ϕ does not fix $\mathbb{Q}$.

The remaining possible set of non trivial automorphisms are those swapping the signs of any root. Let such automorphism be defined as φ, σ, and τ swapping the signs of $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{5}$ respectively, and 1 being the identity. These automorphisms fix $\mathbb{Q}$ since $\phi\sigma\tau(a^2) = (-a)^2 = a^2$ for $a = 2, 3, 5$.

The Galois group is therefore all combinations of these functions, namely the set $\{1, \varphi, \sigma, \tau\, \varphi\sigma, \varphi\tau, \sigma\tau, \varphi\sigma\tau\}$. The subgroups of this are those generated by $\{\varphi\}, \{\sigma\}, \{\tau\}, \{\varphi, \sigma\}, \{\varphi, \tau\}, \{\sigma, \tau\}, \{\varphi\sigma\}, \{\varphi\tau\}, \{\sigma\tau\}, \{\tau, \varphi\sigma\}, \{\sigma, \varphi\tau\}, \{\varphi, \sigma\tau\}$, and $\{\varphi\sigma\tau\}$.

By the FTGT, there is a one to one correspondence between these subgroups and the subfields of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$, given by the fixed field of the subgroup. The first six fixed fields are easily seen to be $\mathbb{Q}(\sqrt{3},\sqrt{5}), \mathbb{Q}(\sqrt{2},\sqrt{5}), \mathbb{Q}(\sqrt{2},\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{2})$. The next six are given by considering the products of roots. For example, $\varphi\sigma(\sqrt{6}) = \varphi\sigma(\sqrt{2}\sqrt{3}) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{6}$. All together, we have $\mathbb{Q}(\sqrt{5},\sqrt{6}), \mathbb{Q}(\sqrt{3},\sqrt{10}), \mathbb{Q}(\sqrt{2},\sqrt{15}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{15})$. The final subfield is given by $\mathbb{Q}(\sqrt{6},\sqrt{10},\sqrt{15})$ □

Problem 2.5. Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p, a \neq 0$.

Proof. The splitting field of this polynomial is $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$, where $\sqrt[p]{2}$ is any fixed pth root of 2 and ζ_p is the primitive pth root of unity.

From section 13.6, we know that the dimension of $\mathbb{Q}(\zeta_p)$ is $p-1$. It is also easy to see that $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}(\zeta_p)]$ is p. Taken together, we have $[\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}(\sqrt[p]{2})][\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p(p-1)$.

Since the polynomial $x^p - 2$ is separable, $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ is Galois. Hence, $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1) = \mathrm{Aut}(\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q})$ There are hence $p(p-1)$ automorphism in $\mathrm{Aut}(\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q})$.

The Galois group is determined by the action on the generators $\sqrt[p]{2}$ and ζ_p, lending possible automorphisms $\sigma_{a,b} : \zeta_p \mapsto \zeta_p^a, \sqrt[p]{2} \mapsto \zeta_p^b \sqrt[2]{p}$, where $0 < a < p$ and $0 \leq b < p$. (Letting a equal 0 would remove all primitive roots of unity from the field, so we can negate this option as not being an automorphism). We know the group is of order $p(p-1)$; hence, each $\sigma_{a,b}$ is distinct.

Now, consider the function $\phi : \sigma_{a,b} \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. We have constrained a and b in such a way that this function is obviously a bijection. So we need only show that it is an isomorphism. Note that $\sigma_{c,d}\sigma_{a,b}$ is the mapping $\zeta_p \mapsto \zeta_p^c a, \sqrt[p]{2} \mapsto \sigma_{a,b}(\zeta_p)^d \sigma_{a,b}(\sqrt[2]{p}) = \zeta^{ad+b}\sqrt[p]{2}$. So we can write it as $\sigma_{ac,bc+d}$ Now, for any $\sigma_{a,b}, \sigma_{c,d}$, we have $\phi(\sigma_{a,b})\phi(\sigma_{c,d}) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & bc+d \\ 0 & 1 \end{pmatrix} = \phi(\sigma_{ac,bc+1}) = \phi(\sigma_{c,d}\sigma_{a,b})$. Hence, the function is an isomorphism, completing the proof.

Remark 2. *This proof took a while because I am not used to working with roots of unity; I understand they are very important in some areas of math. What is ironic, is that I barely did anything with the actual field, relying instead on the fundamental theorem of Galois theory.* □

Problem 2.7. Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois.

Proof. From TFTGT, this is equivalent to finding the fixed fields of all normal subgroups of the Galois group of the splitting field for $x^8 - 2$.

We are given earlier in this chapter that the Galois group of this field is the quasihedral group defined by

$$\langle \sigma, \tau | \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

//TODO □

Problem 2.9. Give an example of fields $\mathbb{F}_1, \mathbb{F}_2, \mathbb{F}_3$ with $\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3$, $[\mathbb{F}_3 : \mathbb{Q}] = 8$ and each field is Galois over all its subfields with the exception that $\mathbb{F}_2$ is not Galois over $\mathbb{Q}$.

Proof. Consider $\mathbb{F}_3 = \mathbb{Q}(\sqrt[4]{2}, i), \mathbb{F}_2 = \mathbb{Q}(\sqrt[4]{2}), \mathbb{F}_1 = \mathbb{Q}(\sqrt{2})$. Clearly, this collection satisfies the chain of subset inclusions. The fields $\mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q}(i)$ are degree 4 and 2 respectively. Since i and $\sqrt[4]{2}$ are linearly independent, $[\mathbb{F}_3 : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}][\mathbb{Q}(i) : \mathbb{Q}] = 4 \cdot 2 = 8$. $\mathbb{F}_3$ is the splitting field of $x^4 - 2$, $x^2 + \sqrt{2}$, and $x^4 - 1$ over $\mathbb{Q}$, $\mathbb{F}_1$, and $\mathbb{F}_2$ respectively. $\mathbb{F}_2$ is the splitting field of $x^2 - \sqrt{2}$ over $\mathbb{F}_1$ is not a splitting field over $\mathbb{Q}$ since it does not contain $\pm i\sqrt[2]{2}$. Finally, $\mathbb{F}_1$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$. This completes the proof. □

Problem 2.11. Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field has Galois group S_4 over $\mathbb{Q}$ (there are many such quartics, cf. Section 6). Let θ be a root of $f(x)$ and set $K = \mathbb{Q}(\theta)$. Prove that K is an extension of $\mathbb{Q}$ of degree 4 which has no proper subfields. Are there any Galois extensions of $\mathbb{Q}$ of degree 4 with no proper subfields?

Proof. We write the polynomial in question as $(x-\theta)(x-\theta_1)(x-\theta_2)(x-\theta_3)$. The Galois subgroup associated with K is the subset of S_4 fixing θ, which is clearly S_3. If K has a nontrivial subfield, then their is a nontrivial subgroup of S_4 containing S_3. Such a subgroup would be generated by S_3 and some function σ swapping θ for another root. But this pair would generate S_4. Hence, no such subgroup exists and K therefore has no proper subfields.

To see that K is degree 4, note that by the fundamental theorem, $[K : \mathbb{Q}] = |S_4 : S_3| = 4$

If a Galois extension has degree 4, then its Galois group would either be the cyclic four-group, or the Klein four-group, both of which have nontrivial subgroups. Thus, //TODO □

Problem 2.13. Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

Proof. Let $p(x)$ be the polynomial in question. Suppose for the sake of contradiction that $p(x)$ has at least one imaginary root. From calculus, we know $p(x)$ must have at least one real root. By assumption, there is an automorphism σ sending an imaginary root to the real one. But such a function cannot be an automorphism because $\sigma(i)^2 = -1$, where $\sigma(i)$ is real. Hence, all roots of $p(x)$ are real. □

Problem 2.15. content...