Solutions to Homework 4

Nathan Grigg

Section 4, Exercises 1, 2, 3, and 4.

Exercise 1. Let G be a group of automorphisms of a field K. Prove that the fixed elements K^G form a subfield of K.

Proof. By definition, $K^G \subseteq K$. Clearly $0, 1 \in K^G$. Suppose that α and β are in K^G. Then for any $\varphi \in G$, we have $\varphi(\alpha) = \alpha$ and $\varphi(\beta) = \beta$. Then for any $\varphi \in G$, we have

$$\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta) = \alpha + \beta \qquad \varphi(\alpha-\beta) = \varphi(\alpha) - \varphi(\beta) = \alpha - \beta$$
$$\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta) = \alpha\beta \qquad \varphi(\alpha/\beta) = \varphi(\alpha)/\varphi(\beta) = \alpha/\beta$$

All the other field axioms (associativity, commutativity, distributivity) are met since K^G is a subset of K. Hence K^G is a field. □

Exercise 2. Let $\alpha = \sqrt[3]{2}, \zeta = \frac{1}{2}(-1+\sqrt{-3}), \beta = \alpha\zeta$.

(a) Prove that for all $c \in \mathbb{Q}$, $\gamma = \alpha + c\beta$ is a root of a sixth-degree polynomial of the form $x^6 + ax^3 + b$.

(b) Prove that the irreducible polynomial for $\alpha + \beta$ is cubic.

(c) Prove that $\alpha - \beta$ has degree 6 over $\mathbb{Q}$.

Proof.

(a) For this part, we will use the fact that $\zeta = 1/2 + i\sqrt{3}/2$ and $\zeta^2 = \overline{\zeta}$. Also, $\zeta^3 = 1$. We compute

$$\begin{aligned}\gamma^3 &= (\alpha + c\beta)^3 = (\alpha(1+c\zeta))^3 \\ &= \alpha^3(1 + 3c\zeta + 3c^2\zeta^2 + c^3) \\ &= 2(1 + c^3 + 3c(\zeta + c\overline{\zeta})) \\ &= 2(1 + c^3 + (3c/2)(i\sqrt{3}(1-c) - (1+c)))\,.\end{aligned}$$

This is clearly in the field $\mathbb{Q}(i\sqrt{3})$, which is a degree 2 extension of $\mathbb{Q}$. Thus γ^3 must satisfy a quadratic polynomial, which means γ satisfies a polynomial of the form $x^6 + ax^3 + b$.

(b) Note that $\zeta^2 + \zeta + 1 = 0$, so $\alpha + \beta = \alpha(1 + \zeta) = -\alpha\zeta^2$. This is a root of $x^3 + 2$, since $(-\alpha\zeta^2)^3 + 2 = -2 + 2 = 0$. This is an irreducible polynomial.

(c) A straightforward calculation shows that $(1 - \zeta)^6 = -27$. So

$$(\alpha - \beta)^6 = \alpha^6(1 - \zeta)^6 = 4(-27) = -108\,.$$

Therefore $(\alpha - \beta)$ is a root of the polynomial $x^6 + 108$, which is irreducible by Eisenstein's criterion on any prime other than 2 or 3.

□

Note: This last calculation shows that the splitting field $\mathbb{Q}(\alpha, \beta)$ of $x^3 - 2$ can also be expressed as $\mathbb{Q}(\alpha - \beta)$.

Exercise 3. For each of the following sets of automorphisms of the field of rational functions $\mathbb{C}(y)$, determine the group of automorhpism which they generate, and determine the fixed field explicitly.
(a) $\sigma(y) = y^{-1}$ **(b)** $\sigma(y) = iy$ **(c)** $\sigma(y) = -y, \tau(y) = y^{-1}$
(d) $\sigma(y) = \zeta, \tau(y) = y^{-1}$, where $\zeta = e^{2\pi i/3}$ **(e)** $\sigma(y) = iy, \tau(y) = y^{-1}$

Solution.

(a) Clearly σ^2 is the identity, so the group of automorphisms is the cyclic group of order 2, generated by σ. Note that $w = y + \frac{1}{y}$ is fixed by σ, so we have $\mathbb{C}(w) \subseteq \mathbb{C}(y)^G$. Since $[\mathbb{C}(y) : \mathbb{C}(y)^G] = 2$, this means that $[\mathbb{C}(y) : \mathbb{C}(w)] \geq 2$, with equality if and only if $\mathbb{C}(w) = \mathbb{C}(y)^G$. Then note that y is a root of the polynomial $x^2 - wx + 1$ in $\mathbb{C}(w)[x]$, so $[\mathbb{C}(y) : \mathbb{C}(w)] \leq 2$, which means that $\mathbb{C}(w) = \mathbb{C}(y)^G$, as desired. So the fixed field is $\mathbb{C}(y + \frac{1}{y})$.

(b) Here σ has order 4, so the group of automorphisms is the cyclic group of order 4. Now, $w = y^4$ is fixed by σ (hence by all of G). And y is a root of the polynomial $x^4 - w$, so the fixed field is equal to $\mathbb{C}(y^4)$.

(c) Both σ and τ are order 2 and commute, so the group of autmormophisms is isomorphic to V_4. The element $w = y^2 + 1/y^2$ is fixed by both σ and τ, and y is a root of the polynomial $x^4 - wx^2 + 1$, so the fixed field is $\mathbb{C}(y^2 + 1/y^2)$.

(d) Here we have an element of order 2 and an element of order 3. Also, σ and τ satisfy $\sigma\tau = \tau\sigma^2$, so the group is isomorphic to S_3. Note that σ and τ both fix $w = y^3 + 1/y^3$, and y is a root of $x^6 - wx^3 + 1$, so the fixed field is $\mathbb{C}(y^3 + 1/y^3)$.

(e) Here we have an element of order 2 and an element of order 4 with the relation $\sigma\tau = \tau\sigma^3$, so we have D_4. Since σ and τ both fix $w = y^4 + 1/y^4$, and y is a root of $x^8 - wx^4 + 1$, the fixed field is $\mathbb{C}(y^4 + 1/y^4)$.

□

Exercise 4. Show that the group G generated by the automorphisms $\sigma(y) = (y+i)/(y-i), \tau(y) = i(y-1)/(y+1)$ of $\mathbb{C}(y)$ is isomorphic to the alternating group A_4. Determine the fixed field of this group.

Solution. For simplicity, write $A = \sigma(y)$ and $B = \tau(y)$. Some calculation shows

$$\sigma(A) = -1/B \qquad \sigma(B) = -1/y \qquad \tau(A) = -y \qquad \tau(B) = -A$$

Also note that $\sigma^3 = \tau^3 = 1$. From these calulcations, we see σ and τ act as follows:

$$\frac{y}{AB} \overset{\sigma}{\longmapsto} ABy \overset{\sigma}{\longmapsto} \frac{A}{By} \longmapsto \frac{y}{AB}, \qquad \sigma \text{ fixes } \frac{B}{Ay}$$

$$\frac{y}{AB} \overset{\tau}{\longmapsto} \frac{B}{Ay} \overset{\tau}{\longmapsto} \frac{A}{By} \longmapsto \frac{y}{AB}, \qquad \tau \text{ fixes } ABy.$$

Since G permutes elements of the set $\left\{ \frac{y}{AB}, ABy, \frac{A}{By}, \frac{B}{Ay} \right\}$ and is generated by even permutations, G is a subgroup of A_4. Note that G has two distinct subgroups of order 3. From this we get that $|G|$ has to be either 6 or 12. But $|G|$ cannot be 6, because in that case a subgroup of order 3 is normal, since it has index 2. All 3-Sylow subgroups are conjugate, and all conjugates of a normal subgroup are equal, so there would only only be one such subgroup. Therefore $G = A_4$. (A simpler, but less cool sounding way to prove this last bit would be to show that G has at least 7 different elements, which means it must have 12 and we are done.)

Another way to prove this would be to write down all the elements, but then you would also have to prove that there are no others, which would be tedious. If you were wondering, the elements of G are:

$$\{1, \sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \tau^2, \sigma^2\tau, \sigma\tau^2, \tau\sigma^2, \tau^2\sigma, \tau\sigma^2\tau\}$$

The fixed field of G is given $\mathbb{C}(w)$, where

$$\begin{aligned} w &= \left(y^2 + \frac{1}{y^2}\right)\left(A^2 + \frac{1}{A^2}\right)\left(B^2 - \frac{1}{B^2}\right) \\ &= \frac{-4\,y^{12} + 132\,y^8 + 132\,y^4 - 4}{y^{10} - 2\,y^6 + y^2} \end{aligned}$$

It is clear that σ and τ fix w, and y is a root of the degree 12 polynomial

$$f(x) = 4\,x^{12} - 132\,x^8 - 132\,x^4 + \left(x^{10} - 2\,x^6 + x^2\right) w + 4 \in \mathbb{C}(w)[x],$$

so this is the fixed field we are looking for. □