ALGEBRA HW 6

CLAY SHONKWILER

547.4

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

Proof. Suppose there exists an isomorphism $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Then, of course, it must be the case that $\phi(1) = 1$. Hence

$$2 = 1{+}1 = \phi(1){+}\phi(1) = \phi(1{+}1) = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = \phi(\sqrt{2})\phi(\sqrt{2}) = (\phi(\sqrt{2}))^2.$$

In other words, $\phi(\sqrt{2}) = \pm\sqrt{2}$. However, as we saw on the last homework (problem 8, page 510), since $2 \cdot 3 = 6$ is not a square in $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is an extension of degree 4 over $\mathbb{Q}$ and hence of degree 2 over $\mathbb{Q}(\sqrt{3})$. In other words, $\pm\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. Therefore, we see that there is no such isomorphism ϕ and so $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ cannot be isomporphic. □

547.6

Let k be a field

(a) Show that the mapping $\phi : k[t] \to k[t]$ defined by $\phi(f(t)) = f(at + b)$ for fixed $a, b \in k$, $a \neq 0$ is an automorphism of $k[t]$ which is the identity on k.

Proof. Let $f(t), g(t) \in k[t]$. Then

$$\phi((f + g)(t)) = (f + g)(at + b) = f(at + b) + g(at + b) = \phi(f(t)) + \phi(g(t))$$

and

$$\phi((fg)(t)) = (fg)(at + b) = f(at + b)g(at + b) = \phi(f(t))\phi(g(t)),$$

so ϕ is a homomorphism. Now, suppose $\phi(f(t)) = \phi(g(t))$. Then

$$f(at + b) = g(at + b);$$

if we let $s = at + b$, then we see that $f(s) = g(s)$ in $k[s] = k[t]$, so ϕ is injective.

Now, let $g(t) \in k[t]$. Define

$$f(t) = g(t/a - b/a).$$

Then

$$\phi(f(t)) = f(at + b) = g(a(t/a - b/a) + b) = g(t - b + b) = g(t),$$

so ϕ is surjective. Therefore, we conclude that ϕ is an automorphism of $k[t]$. Now, if $c \in k \subset k[t]$, then

$$\phi(c) = c$$

so ϕ is the identity on k. □

(b) Conversely, let ϕ be an automorphism of $k[t]$ which is the identity on k. Prove that there exist $a, b \in k$ with $a \neq 0$ such that $\phi(f(t)) = f(at + b)$ as in (a).

Proof. Since ϕ is the identity on k, it cannot be of the form

$$\phi(f(t)) = h(t)f(t) + g(t)$$

for any $h, g \in k[t]$. Hence, it must be the case that

$$\phi(f(t)) = f(g(t))$$

for some $g(t) \in k[t]$. Now, suppose the degree n of g is greater than one. Then elements in the image of ϕ must have degree divisible by n. However, if this were the case, it's clear that ϕ could not be surjective. Hence, we see that $\deg(g(t)) \leq 1$. If $\deg(g(t)) = 0$, then $g(t) = b$ for some $b \in k$. Hence, $\phi(f(t)) = f(b)$ is just a constant term for all $f \in k[t]$. Therefore, we conclude that it must be the case that $\deg(g(t)) = 1$, meaning $g(t) = at + b$ where $a, b \in k$ and $a \neq 0$. □

547.7

This exercise 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 that $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.

Proof. Let $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ and let $a = b^2$ be a square in $\mathbb{R}$. Then

$$\sigma a = \sigma(b^2) = \sigma b \sigma b = (\sigma b)^2,$$

which is also a square in $\mathbb{R}$. Now, since every non-negative element of $\mathbb{R}$ is a square and no negative elements are, and it must be true that $\sigma 0 = 0$, we see that it must be the case that σ takes positive reals to positive reals.

Now, let $a, b \in \mathbb{R}$ such that $a < b$. Then there exists some $r \in \mathbb{Q}$ such that

$$a < r < b.$$

Let $\delta = r - a$ and let $\gamma = b - r$. Note that δ and γ are both positive, even though a, r and b need not be. Then since σ is the identity on $\mathbb{Q}$ and takes positive reals to positive reals, we see that

$$r = \sigma(r) = \sigma(r - a + a) = \sigma(r - a) + \sigma(a) = \sigma(\delta) + \sigma(a) > \sigma(a),$$

since $\sigma(\delta) > 0$. Similarly,

$$\begin{aligned} r = \sigma(r) = \sigma(r - b + b) &= \sigma(r - b) + \sigma(b) \\ &= \sigma(-\gamma) + \sigma(b) \\ &= \sigma(-1)\sigma(\gamma) + \sigma(b) \\ &= -\sigma(\gamma) + \sigma(b) \\ &< \sigma(b), \end{aligned}$$

since $\sigma(-1) = -1$ and $\sigma(\gamma) > 0$. Therefore, combining the above two results, we see that

$$\sigma(a) < r < \sigma(b).$$

□

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

Proof. Suppose $a, b \in \mathbb{R}$ such that

$$\frac{-1}{m} < a - b < \frac{1}{m}.$$

Adding b to all terms, this implies that

$$b - \frac{1}{m} < a < b + \frac{1}{m}.$$

By our result in part (a), then, we know that

$$\sigma b - \frac{1}{m} = \sigma b - \sigma(\frac{1}{m}) = \sigma(b - \frac{1}{m} < \sigma a < \sigma(b + \frac{1}{m}) = \sigma b + \sigma(\frac{1}{m}) = \sigma b + \frac{1}{m}.$$

Subtracting σb from all terms, then, we see that

$$-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}.$$

Therefore, if $\epsilon > 0$, there exists a $\delta > 0$ (namely any fraction of the form $\frac{1}{m} < \epsilon$), such that, if $|a - b| < \delta$,

$$|a - b| < \delta < \epsilon,$$

so σ is continuous 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. Let f be a continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$, let $b \in \mathbb{R}$ and let $\epsilon > 0$. Since f is continuous, there exists $\gamma > 0$ such that, if $|b - a| < \gamma$,

$$|f(b) - f(a)| < \epsilon/2.$$

Let $\delta = \min\{\epsilon/2, \gamma\}$. Let $a \in \mathbb{Q}$ such that $|b-a| < \delta$. Then

$$\begin{aligned} |b - f(b)| &= |b - a + a - f(b)| \\ &\leq |b-a| + |a - f(b)| \\ &= |b-a| + |f(a) - f(b)| \\ &= |b-a| + |f(b) - f(a)| \\ &< \delta + \epsilon/2 \\ &\leq \epsilon/2 + \epsilon/2 \\ &= \epsilon. \end{aligned}$$

In other words, $f(b) = b$. Since our choice of b was arbitrary, we conclude that, in fact, f is the identity on all of $\mathbb{R}$. Hence, the identity map is the only element of $\text{Aut}(\mathbb{R}/\mathbb{Q})$, so

$$\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1.$$

□

547.8

Prove that the automorphisms of the rational function field $k(t)$ which fix k are precisely the *fractional linear transformations* determined by $t \mapsto \frac{at+b}{ct+d}$ for $a, b, c, d \in k$, $ad - bc \neq 0$.

Proof. First, suppose ϕ is a map from $k(t)$ to itself such that, for $f(t) \in k(t)$,

$$\phi(f(t)) = f\left(\frac{at+b}{ct+d}\right).$$

Now, suppose $\phi(g(t)) = \phi(f(t))$ for some $f(t), g(t) \in k(t)$. Then

$$g\left(\frac{at+b}{ct+d}\right) = f\left(\frac{at+b}{ct+d}\right).$$

Therefore, $g \equiv f$ in $k\left(\frac{at+b}{ct+d}\right)$. Now, by the work we did in the last homework (Problem 18, Section 13.2), we know that

$$\left[k(t) : k\left(\frac{at+b}{ct+d}\right)\right] = \max(\deg(at+b), \deg(ct+d)) = 1,$$

so $k\left(\frac{at+b}{ct+d}\right) = k(t)$, and so we see that $g \equiv f$ in $k(t)$. Hence, ϕ is injective.

Now, since

$$\text{Im}(\phi) = k\left(\frac{at+b}{ct+d}\right)$$

and, as we just saw, $k\left(\frac{at+b}{ct+d}\right) = k(t)$, ϕ must be surjective.

Now, if $f, g \in k(t)$, then

$$\phi((f+g)(t)) = (f+g)\left(\frac{at+b}{ct+d}\right) = f\left(\frac{at+b}{ct+d}\right) + g\left(\frac{at+b}{ct+d}\right) = \phi(f(t)) + \phi(g(t))$$

and

$$\phi((fg)(t)) = (fg)\left(\frac{at+b}{ct+d}\right) = f\left(\frac{at+b}{ct+d}\right) g\left(\frac{at+b}{ct+d}\right) = \phi(f(t))\phi(g(t)).$$

Therefore, ϕ is a homomorphism. Since it is bijective, we see that ϕ is an automorphism. Therefore, all maps of the given form are automorphisms of $k(t)$. Furthermore, these maps fix any constant functions (i.e., elements of k), so we see that all such maps are automorphisms of $k(t)$ which fix k.

On the other hand, suppose γ is an automorphism of $k(t)$ which fixes k. Then, in principle, it could be the case that, for $f \in k(t)$,

$$\gamma(f(t)) = g(f(h(t))),$$

where $g, h \in k(t)$. However, since γ must fix elements of k, we see that g can only be the identity. In other words,

$$\gamma(f(t)) = f(h(t))$$

where $h(t) = \frac{P(t)}{Q(t)}$ where P and Q are relatively prime polynomials over k. Note that

$$\mathrm{Im}(\gamma) = k(h(t)) = k\left(\frac{P(t)}{Q(t)}\right).$$

Now, again by the work we did last week on Problem 18, Section 13.2, we know that

$$[k(t) : k(h(t))] = \max(\deg(P(t)), \deg(Q(t))).$$

However, since γ is an automorphism, it must be the case that $\mathrm{Im}(\gamma) = k(t)$, which is to say tht

$$[k(t) : k(h(t))] = 1.$$

Hence, we see that both P and Q must be of degree ≤ 1. Hence, $P(t) = at+b$ and $Q(t) = ct + d$ for some $a, b, c, d \in k$. The relative primeness of P and Q means that, if $c \neq 0$, it cannot be the case that $\frac{ad}{c} = b$ (else it would be true that $\frac{a}{c}(ct + d) = at + b$) and, if $c = 0$, it cannot be the case that $a = 0$. Re-arranging, we see that this implies that

$$ad \neq bc \quad \text{or} \quad ad - bc \neq 0.$$

Having shown that all automorphisms of $k(t)$ fixing k are fractional linear transformations and all fractional linear transformations are automorphisms of $k(t)$ fixing k, we conclude that the automorphisms fixing k are precisely the fractional linear transformations. $\square$

561.2

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

Answer: First, note that $\sqrt[3]{4} = \sqrt[3]{2}\sqrt[3]{2}$, so $\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$. Hence, $1 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$ and so

$$\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) \subseteq \mathbb{Q}(\sqrt[3]{2}),$$

which is a Galois extension of degree 6 over $\mathbb{Q}$. Hence, the other roots of the minimal polynomial of $1+\sqrt[3]{2}+\sqrt[3]{4}$ over $\mathbb{Q}$ are the distinct conjugates of $1+\sqrt[3]{2}+\sqrt[3]{4}$ under the Galois group, which we showed in class is simply S_3. Let ζ be the third root of unity $\zeta = -1/2+\sqrt{3}/2i$. Then the possible conjugates of $1+\sqrt[3]{2}+\sqrt[3]{4}$ are

$$1+\sqrt[3]{2}+\sqrt[3]{4}, 1+\zeta\sqrt[3]{2}+\zeta^2\sqrt[3]{4}, 1+\zeta^2\sqrt[3]{2}+\zeta\sqrt[3]{4}.$$

Now, the minimal polynomial $m(x)$ is given by

$$\begin{aligned} m(x) &= (x-(1+\sqrt[3]{2}+\sqrt[3]{4}))(x-(1+\zeta\sqrt[3]{2}+\zeta^2\sqrt[3]{4}))(x-(1+\zeta^2\sqrt[3]{2}+\zeta\sqrt[3]{4})) \\ &= (x^2-(1+\zeta\sqrt[3]{2}+\zeta^2\sqrt[3]{4})x-(1+\sqrt[3]{2}+\sqrt[3]{4})x \\ &\quad +(\sqrt[3]{2}\zeta+\zeta+\zeta^2))(x-(1+\zeta^2\sqrt[3]{2}+\zeta\sqrt[3]{4})) \\ &= x^3-x^2((1+\zeta\sqrt[3]{2}+\zeta^2\sqrt[3]{4})+(1+\sqrt[3]{2}+\sqrt[3]{4})+(1+\zeta^2\sqrt[3]{2}+\zeta\sqrt[3]{4})) \\ &\quad +x((\sqrt[3]{2}\zeta+\zeta+\zeta^2)+(1+\zeta\sqrt[3]{2}+\zeta^2\sqrt[3]{4})(1+\zeta^2\sqrt[3]{2}+\zeta\sqrt[3]{4}) \\ &\quad +(1+\sqrt[3]{2}+\sqrt[3]{4})(1+\zeta^2\sqrt[3]{2}+\zeta\sqrt[3]{4}))-(1+\zeta^2\sqrt[3]{2}+\zeta\sqrt[3]{4})(\sqrt[3]{2}\zeta^2+\zeta+\zeta^2) \\ &= x^3-3x^2-3x-1. \end{aligned}$$

562.3

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.

Answer: The splitting field K of this polynomial is generated by $\sqrt{2}, \sqrt{3}, \sqrt{5}$. By our work below in Problem 15, we know that $\mathbb{Q}(\sqrt{a_i}, \sqrt{a_j})$ is biquadratic and Galois for distinct a_i chosen from $\{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$. This this is true for all these terms, we know that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is an extension of degree 2 over $\mathbb{Q}(\sqrt{a_i}, \sqrt{a_j})$, and hence of degree 8 over $\mathbb{Q}$. Now, since $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is the splitting field of a separable polynomial, it is Galois, and so the Galois group is of order 8. Now, since for $a \in \{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$, the minimal polynomial of a over $\mathbb{Q}$ is x^2-a^2, and since elements of the Galois group are determined by their action on the three choices for a, and since elements of the Galois group can only send a to $\pm a$, we know that there are only 8 possible permutations of the choices of a. Namely

$$\begin{aligned} \sqrt{2} &\mapsto \pm\sqrt{2} \\ \sqrt{3} &\mapsto \pm\sqrt{3} \\ \sqrt{5} &\mapsto \pm\sqrt{5}. \end{aligned}$$

Since the Galois group is of order 8, all these permutations are in the Galois group.

Now, let $a_1 = 2, a_2 = 3, a_3 = 5$ and define σ_i to be the permutation that maps $\sqrt{a_i}$ to $-\sqrt{a_i}$ and fixes a_j for $j \neq i$. Then we see, in fact, that $\text{Gal}(K/\mathbb{Q}) = \{1, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3\}$. Note that $\sigma_i^2 = 1$ for each $i = 1, 2, 3$ and that, therefore, all elements of $\text{Gal}(K/\mathbb{Q})$ are of order 2. From this information and the fact that $|\text{Gal}(K/\mathbb{Q})| = 8$, we can conclude that

$$\text{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Now, the following is a complete list of subgroups of $\mathrm{Gal}(K/\mathbb{Q})$:

$$\{1, \langle\sigma_i\rangle, \langle\sigma_i\sigma_j\rangle, \langle\sigma_1\sigma_2\sigma_3\rangle, \langle\sigma_i, \sigma_j\rangle, \langle\sigma_i, \sigma_j\sigma_k\rangle, \langle\sigma_1\sigma_2, \sigma_1\sigma_3\rangle, \mathrm{Gal}(K/\mathbb{Q})\}.$$

Hence, there are 14 distinct non-trivial proper subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and, therefore, 14 subfields of K, each the fixed field of one of these subgroups.

Now, $\langle\sigma_i\rangle = \{1, \sigma_i\}$, so, since σ_i fixes a_j for $j \neq i$, we see that the fixed field of $\langle\sigma_i\rangle$ is simply

$$\mathbb{Q}(a_j, a_k)$$

where $j \neq i$, $k \neq i$. In other words, these subgroups give rise to the following subfields:

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{3}, \sqrt{5}).$$

Now, since $\langle\sigma_i, \sigma_j\rangle$ permutes $\sqrt{a_i}$ and $\sqrt{a_j}$, we see that the subfields corresponding to subgroups of this type are:

$$\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}).$$

Turning to subgroups of the form $\langle\sigma_i, \sigma_j\sigma_k\rangle$, we see that none of the elements of the form $\sqrt{a_i}$ are fixed under these permutations. However,

$$\sigma_j\sigma_k(\sqrt{a_j}\sqrt{a_k}) = (-\sqrt{a_j})(-\sqrt{a_k}) = \sqrt{a_j}\sqrt{a_k}.$$

Hence, the subfields corresponding to these subgroups are:

$$\mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{15}).$$

In fact, using what we know about the fixed elements under $\sigma_j\sigma_k$, we see that the subfields associated with $\langle\sigma_i\sigma_j\rangle$ are:

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

Now, we turn to

$$\langle\sigma_1\sigma_2, \sigma_1\sigma_3\rangle = \langle\sigma_1\sigma_3, \sigma_2\sigma_3\rangle$$

Obviously, elements of this subgroup permute any element of the form $\sqrt{a_i}$, and some element of this group will permute any element of the form $\sqrt{a_j}\sqrt{a_k}$. However,

$$\sigma_i\sigma_j(\sqrt{2}\sqrt{3}\sqrt{5}) = \sqrt{2}\sqrt{3}\sqrt{5}.$$

Hence, the corresponding subfield is

$$\mathbb{Q}(\sqrt{30}).$$

Finally, $\sigma_1\sigma_2\sigma_3$ permutes all elements of the form $\sqrt{a_i}$, but no elements of the form $\sqrt{a_j}\sqrt{a_k}$. Hence, the corresponding subfield is:

$$\mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10}).$$

In the above, we've constructed 14 subfields of K; since there are exactly 14 non-trivial proper subgroups of $\mathrm{Gal}(K/F)$, these must be all such subfields.

♣

562.6

Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$, $F_3 = \mathbb{Q}(\sqrt{-2})$. Prove that $\mathrm{Gal}(K/F_1) \simeq \mathbb{Z}/8\mathbb{Z}$, $\mathrm{Gal}(K/F_2) \simeq D_8$, $\mathrm{Gal}(K/F_3) \simeq Q_8$.

Proof. Using the subgroup and subfield diagrams given in the chapter, we see that, as a subfield of K, F_1 is associated with the subgroup $\langle\sigma\rangle$, F_2 is associated with the subgroup $\langle\sigma^2, \tau\rangle$ and F_3 is associated with the subgroup $\langle\sigma^2, \tau\sigma^3\rangle$, where

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma, \tau | \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3\rangle.$$

Now, by the Fundamental Theorem of Galois Theory, this implies that

$$\begin{aligned} \mathrm{Gal}(K/F_1) &= \langle\sigma\rangle \\ \mathrm{Gal}(K/F_2) &= \langle\sigma^2, \tau\rangle \\ \mathrm{Gal}(K/F_3) &= \langle\sigma^2, \tau\sigma^3\rangle \end{aligned}$$

where each of these groups is subject to the relations on $\mathrm{Gal}(K/F)$. Now, it's immediately clear that

$$\mathrm{Gal}(K/F_1) = \langle\sigma\rangle \simeq \mathbb{Z}/8\mathbb{Z},$$

since σ has order 8. To calculate $\mathrm{Gal}(K/F_2)$, let $\gamma = \sigma^2$. Then the first relation in the presentation tells us that $\gamma^4 = 1$. To be able to use the second relation, we multiply both sides on the left by σ, yielding

$$\sigma^2\tau = \sigma\tau\sigma^3 = \tau\sigma^6.$$

Translating this in terms of τ and γ, we see that

$$\gamma\tau = \tau\gamma^3 = \tau\gamma^{-1},$$

since $\gamma^4 = 1$. Hence, combining this information, we see that

$$\mathrm{Gal}(K/F_2) = \langle\sigma^2, \tau\rangle \simeq \langle\gamma, \tau | \gamma^4 = \tau^2 = 1, \gamma\tau = \tau\gamma^{-1}\rangle = D_8$$

Finally, to calculate $\mathrm{Gal}(K/F_3)$, let $\gamma = \sigma^2$ and $\delta = \tau\sigma^3$. Then we see immediately that

$$\gamma^4 = (\sigma^2)^4 = \sigma^8 = 1.$$

Also,

$$\begin{aligned} \delta^2 = (\tau\sigma^3)^2 &= (\sigma\tau)^2 \\ &= \sigma\tau\sigma\tau \\ &= \tau\sigma^3\sigma\tau \\ &= \tau\sigma^3\tau\sigma^3 \\ &= \tau\sigma^2\tau\sigma^6 \\ &= \tau\sigma\tau\sigma^9 \\ &= \tau\sigma\tau\sigma \\ &= \tau\tau\sigma^4 \\ &= \tau^2\sigma^4 \\ &= \sigma^4 \\ &= \gamma^2. \end{aligned}$$

Hence, we have the relations $\gamma^2 = \delta^2$ and $\delta^4 = 1$. Now, we calculate

$$\begin{aligned} \gamma\delta &= \sigma^2\tau\sigma^3 \\ &= \sigma\tau\sigma^6 \\ &= \tau\sigma^9 \\ &= \tau\sigma^3\sigma^6 \\ &= \delta\gamma^3 \\ &= \delta\gamma^{-1} \end{aligned}$$

Hence, multiplying on the left by δ^{-1},

$$\delta^{-1}\gamma\delta = \gamma^{-1}.$$

Therefore,

$$\mathrm{Gal}(K/F_3) = \langle \sigma^2, \tau\sigma^3 \rangle \simeq \langle \gamma, \delta | \gamma^4 = \delta^4 = 1, \delta^{-1}\gamma\delta = \gamma^{-1}, \gamma^2 = \delta^2 \rangle.$$

However, this is precisely the quaternion group Q_8, so we see that $\mathrm{Gal}(K/F_3) \simeq Q_8$. □

562.15

Let F be a field of characteristic $\neq 2$.

(a) If $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, D_1D_2 is a square in F, prove that K/F is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group.

Proof. We showed on the last homework (Problem 8 from Section 13.2), that, since D_1, D_2, and D_1D_2 are not squares in F, K is an extension of degree 4 over F. Furthermore, K is the splitting field of the polynomial

$$(x^2 - D_1)(x^2 - D_2),$$

which has four distinct roots, $\pm\sqrt{D_1}, \pm\sqrt{D_2}$, and is therefore separable. Since K is the splitting field of a separable polynomial, K/F is Galois. Now, there are a total of 4 possibilities for elements in $\mathrm{Gal}(K/F)$, the identity, σ, τ and $\sigma\tau$, where

$$\begin{aligned} \sigma(\sqrt{D_1}) &= -\sqrt{D_1}, & \sigma(\sqrt{D_2}) &= \sqrt{D_2} \\ \tau(\sqrt{D_1}) &= \sqrt{D_1}, & \tau(\sqrt{D_2}) &= -\sqrt{D_2}. \end{aligned}$$

Since there are only four such possibilities, all of them must be realized in the Galois group, and so we see that $\mathrm{Gal}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$. Since both σ and τ (and, hence, $\sigma\tau$) are of order 2, this implies that $\mathrm{Gal}(K/F)$ is isomorphic to the Klein 4-group. □

(b) Conversely, suppose K/F is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group. Prove that $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, D_1D_2 is a square in F.

Proof. Since $\mathrm{Gal}(K/F)$ is isomorphic to the Klein 4-group, it must be the case that $\mathrm{Gal}(K/F) = \{1, \sigma, \tau, \sigma\tau\}$. Hence, all proper non-trivial subgroups in $\mathrm{Gal}(K/F)$ are of index 2; the following is a list: $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$. Each of these three subgroups corresponds to its fixed field, which will be an extension of degree 2 over F. In other words, these subgroups correspond, respectively, to field extensions

$$F(\sqrt{\alpha_1}), F(\sqrt{\alpha_2}), F(\sqrt{\alpha_3})$$

where $\alpha_1, \alpha_2, \alpha_3 inF$ and each is distinct. Since these fields are extensions of degree 2, we see that $\alpha_1, \alpha_2, \alpha_3$ cannot be squares in F. Now, clearly

$$F(\sqrt{\alpha_i}, \sqrt{\alpha_j}) \subseteq K$$

for each $i, j = 1, 2, 3$. Now, if $F(\sqrt{\alpha_i}\sqrt{\alpha_j}) = F(\sqrt{\alpha_i})$ for each choice of i, j, then it's clear that

$$F(\sqrt{\alpha_1}) = F(\sqrt{\alpha_2}) = F(\sqrt{\alpha_3}).$$

However, this in turn implies that $\sigma = \tau = \sigma\tau$, which cannot be true. Hence, there exist i, j such that $F(\sqrt{\alpha_i}, \sqrt{\alpha_j})$ is an extension of degree larger than 1 over $F(\sqrt{\alpha_i})$ and $F(\sqrt{\alpha_j})$. Since K is an extension of degree 2 over each $F(\sqrt{\alpha_k})$, this implies that

$$F(\sqrt{\alpha_i}, \sqrt{\alpha_j}) = K$$

for some choice of i, j. Suppose, without loss of generality that $i = 1, j = 2$. Now, as we saw in last week's homework (same reference as before, Problem 8 Section 13.2), in order for K to be an extension of degree 4, it must be the case that $\sqrt{\alpha_1}\sqrt{\alpha_2}$ is not a square in F. Since K is indeed an extension of degree 4, it must be the case that none of $\sqrt{\alpha_1}, \sqrt{\alpha_2}, \sqrt{\alpha_1}\sqrt{\alpha_2}$ is a square in F. $\square$

563.17

Let K/F be any finite extension and let $\alpha \in K$. Let L be a Galois extension of F containing K and let $H \leq \mathrm{Gal}(L/F)$ be the subgroup corresponding to K. Define the *norm* of α from K to F to be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

where the product is taken over all embeddings of K into an algebraic closure of F. This is a product of Galois conjugates of α. In particular, if K/F is Galois this is $\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

(a) Prove that $N_{K/F}(\alpha) \in F$.

Proof. Since this fact is not necessary to the proof of part (d) below, we simply note that it is a consequence of part (d). $\square$

(b) Prove that $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, so that the norm is a multiplicative map from K to F.

Proof. Since embeddings of K into an algebraic closure of F containing L are homomorphisms, it must be the case that $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ for $\alpha, \beta \in K$, since σ is just an embedding of K into such an algebraic closure. Hence,

$$N_{K/F}(\alpha\beta) = \prod_\sigma \sigma(\alpha\beta) = \prod_\sigma \sigma(\alpha)\sigma(\beta) = \prod_\sigma \sigma(\alpha) \prod_\sigma \sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta).$$

□

(c) Lt $K = F(\sqrt{D})$ be a quadratic extension of F. Show that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$.

Proof. Since K is a quadratic extension,

$$|G : H| = [K : F] = 2,$$

meaning there are only two Galois conjugates of $(a + b\sqrt{D})$ in the product $N_{K/F}(a + b\sqrt{D})$. Furthermore, since K/F is necessarily Galois (since it is of degree 2), the conjugate other than $a + b\sqrt{D}$ must be $a - b\sqrt{D}$, since the only non-identity element of $\mathrm{Gal}(K/F)$ is the map that sends $\sqrt{D}$ to $-\sqrt{D}$. Therefore,

$$N_{K/F}(\alpha) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - (b\sqrt{D})^2 - a^2 - Db^2.$$

□

(d) Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over F. Let $n = [K : F]$. Prove that d divides n, that there are d distinct Galois conjugates of α which are all repeated n/d times in the product above and conclude that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

Proof. We know that $m_\alpha(x)$ is a product of linear terms of the form $(x - \alpha_i)$, where the α_i are the distinct Galois conjugates of α, since the roots of the minimal polynomial must be precisely the Galois conjugates of α. Therefore, since $\deg(m_\alpha(x)) = d$ (and, hence, $m_\alpha(x)$ has exactly d distinct roots), it must be the case that α has exactly d distinct Galois conjugates.

Let E be the splitting field of $m_\alpha(x)$ and let H' be the corresponding subgroup of $\mathrm{Gal}(L/F)$. Then, since $\alpha \in K \cap E$, we see that the corresponding Galois subgroup, $\langle H, H' \rangle$ is non-trivial; since it contains H, $|G : \langle H, H' \rangle|$ must divide n. Since $K \cap E$ contains α, which has minimal polynomial of degree d, it must be the case that $[K \cap E : F] = kd$ for some integer k. Since $[K \cap E : F] = |G : \langle H, H' \rangle|$ which divides $|G : H| = n$, we see that d divides n.

Furthermore, since there are n embeddings of K into an algebraic and each sends α to a Galois conjugate of itself, of which there are d, we see that each conjugate must be hit by n/d of these maps. Hence,

$$N_{K/F}(\alpha) = \prod_\sigma \sigma(\alpha) = \left(\prod_{i=1}^{d} \alpha_i \right)^{n/d}.$$

Now, we know that

$$x^d + \ldots + a_1 x + a_0 = m_\alpha(x) = \prod_{i=1}^{d}(x - \alpha_i)$$

Therefore, the constant term a_0 is given by

$$a_0 = \prod_{i=1}^{d} -\alpha_i = (-1)^d \prod_{i=1}^{d} \alpha_i,$$

or

$$(-1)^d a_0 = \prod_{i=1}^{d} \alpha_i.$$

Hence,

$$N_{K/F}(\alpha) = \left(\prod_{i=1}^{d} \alpha_i\right)^{n/d} = \left((-1)^d a_0\right)^{n/d} = (-1)^n a_0^{n/d}.$$

□

563.18

With notation as in the previous problem, define the *trace* of α from K to F to be

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_\sigma \sigma(\alpha),$$

a sum of Galois conjugates of α.

(a) Prove that $\mathrm{Tr}_{K/F}(\alpha) \in F$.

Proof. Since this fact is not necessary to the proof of part (d) below, we simply note that it is a consequence of part (d). □

(b) Prove that $\mathrm{Tr}_{K/F}(\alpha + \beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$, so that the trace is an additive map from K to F.

Proof. Since embeddings of K into an algebraic closure of F containing L are homomorphisms, it must be the case that $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ for $\alpha, \beta \in K$, since σ is just an embedding of K into such an algebraic closure. Hence,

$$\begin{aligned} \mathrm{Tr}_{K/F}(\alpha + \beta) = \textstyle\sum_\sigma \sigma(\alpha + \beta) = \sum_\sigma \sigma(\alpha) + \sigma(\beta) &= \textstyle\sum_\sigma \sigma(\alpha) + \sum_\sigma \sigma(\beta) \\ &= \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta). \end{aligned}$$

□

(c) Let $K = F(\sqrt{D})$ be a quadratic extension of F. Show that $\mathrm{Tr}_{K/F}(a + b\sqrt{D}) = 2a$.

Proof. By the same reasoning as in Problem 17(c) above, we know that $a + b\sqrt{D}$ has only a single Galois conjugate aside from itself, $a - b\sqrt{D}$. Hence,

$$\mathrm{Tr}_{K/F}(\alpha) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a.$$

□

(d) Let $m_\alpha(x)$ be as in the previous problem. Prove that $\mathrm{Tr}_{K/F}(\alpha) = \frac{-n}{d} a_{d-1}$.

Proof. As we saw in 17(d) above, each of the d distinct Galois conjugates of α is repeated n/d times in the sum that yields the trace. Hence,

$$\mathrm{Tr}_{K/F}(\alpha) = n/d \sum_{i=1}^{d} \alpha_i,$$

where $\alpha_1, \ldots, \alpha_d$ represent the d distinct conjugates of α. Now, we know that

$$m_\alpha(x) = \prod_{i=1}^{d} (x - \alpha_i);$$

hence, if a_{d-1} is the coefficient on the $d - 1$ term in m_α, then

$$a_{d-1} = -\sum_{i=1}^{d} \alpha_i.$$

Hence, we see that

$$\mathrm{Tr}_{K/F}(\alpha) = \frac{-n}{d} a_{d-1}.$$

□

DRL 3E3A, University of Pennsylvania
E-mail address: shonkwil@math.upenn.edu