Jason Starr
Spring 2010

MAT 535 Problem Set 5 Solutions

Selected Problems.

(1) Exercise 9, p. 617. Determine the Galois group of the splitting field E over $F = \mathbb{Q}$ of the polynomial $f(x) = x^4 + 4x - 1$.

(2) Exercise 19, p. 618. Describe the Galois group of an irreducible quartic polynomial over $\mathbb{Q}$ with negative discriminant.

(3) Exercise 48, p. 623. Determine the splitting field E and Galois group of the sextic polynomial $f(x) = x^6 - 2x^3 - 2$ over $\mathbb{Q}$.

(4) Exercise 19, p. 638. Prove that a quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is contained in a degree 4 Galois extension of $\mathbb{Q}$ with cyclic Galois group if and only if D is a sum of two rational squares.

(5) Exercise 13, p. 853. Prove that for simple, left R-modules M and N (R is a unital associative ring), every nonzero R-module homomorphism from M to N is an isomorphism. Conclude that $\mathrm{Hom}_R(M, M)$ is a division ring.

Solutions to Selected Problems.

Solution to (1) By Proposition 11 on p. 308, if $f(x)$ has a root then the root is ± 1. But $f(-1)$ equals -4 and $f(1)$ equals 4. So if $f(x)$ factors, it is a product of two irreducible, monic, quadratic polynomials. By Gauss's lemma, the factors are in $\mathbb{Z}[x]$. And by considering the constant coefficient and the coefficient of x^3, the factorization must be

$$(x^2 + (ax + 1))(x^2 - (ax + 1)) = x^4 - a^2x^2 - 2ax - 1.$$

But since the coefficient of x^2 in $f(x)$ is 0, there is no such factorization. Thus $f(x)$ is irreducible.

The resolvent cubic of $f(x)$ is

$$h(z) = z^3 + 4z + 16.$$

Notice that this factors,

$$h(z) = (z + 2)(z^2 - 2z + 8) = (z - (-2))k(z), \quad k(z) = z^2 - 2z + 8 = (z - 1)^2 + 7.$$

Thus the discriminant of $h(z)$ is

$$\mathrm{Disc}(h) = [k(-2)]^2\mathrm{Disc}(k) = [2^4]^2 \cdot (-28) = -2^6 \cdot 7.$$

And the discriminant D of $f(x)$ equals the discriminant of the resolvent cubic $h(z)$. Observe that this is not a square. Up to square factors, the discriminant is congruent to -7. Thus $\mathbb{Q}(\sqrt{D})$ equals $\mathbb{Q}(\sqrt{-7})$.

The claim is that $f(x)$ is irreducible in $\mathbb{Q}(\sqrt{-7})$. Denote by t one of the two square roots of -7. Then the Galois group is $\mathrm{Aut}(\mathbb{Q}(\sqrt{-7})/\mathbb{Q}) = \{1, \sigma\}$, where $\sigma(t)$ equals $-t$. Since $f(x)$ is irreducible of degree 4 over $\mathbb{Q}$, every root generates a field extension of degree 4. Since $[\mathbb{Q}(\sqrt{-7}) : \mathbb{Q}]$ equals 2, $f(x)$ has no roots in $\mathbb{Q}(\sqrt{-7})$. So the only possible factors are irreducible quadratic factors. If $f(x)$ has an irreducible quadratic factor, then it has a monic irreducible quadratic factor, say $q(x)$. Since $f(x)$ is defined over $\mathbb{Q}$, then also $\sigma(q(x))$ is an irreducible quadratic factor. Since $\mathbb{Q}(\sqrt{-7})[x]$ is a UFD, it follows that $f(x) = q(x)\sigma(q(x))$. In particular, $f(0)$ equals $q(0)\sigma(q(0))$. By direct computation we have,

$$q(0) = a + bt, \quad \sigma(q(0)) = a - bt, \quad q(0)\sigma(q(0)) = a^2 - b^2t^2 = a^2 + 7b^2$$

for some elements a, b in $\mathbb{Q}$. Thus $a^2 + 7b^2$ equals $f(0) = -1$. But a^2 and $7b^2$ are nonnegative, thus they cannot sum to the negative number -1. This contradiction proves that $f(x)$ is irreducible in $\mathbb{Q}(\sqrt{-7})$. Thus, by the discussion on p. 615, the Galois group of E over $\mathbb{Q}$ is isomorphic to a conjugate of the dihedral group D_8 as a subgroup of symmetric group S_4.

Solution to (2) For every monic polynomial $f(x)$ of degree $d \geq 2$, in a splitting field K of $f(x)$ the discriminant D equals

$$\left(\prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j) \right)^2$$

where $f(x) = (x - \alpha_1) \cdots (x - \alpha_d)$. Thus D is a square in K. So K contains $\mathbb{Q}(\sqrt{-D})$.

Now let K be any Galois extension of $\mathbb{Q}$. By the fundamental theorem of algebra, there exists an embedding of K into $\mathbb{C}$, say $\phi : K \to \mathbb{C}$. Moreover, for every embedding $\phi' : K \to \mathbb{C}$, there exists a unique element σ of $\mathrm{Aut}(K/\mathbb{Q})$ such that ϕ' equals $\phi \circ \sigma$. In particular, for complex conjugation $\tau : \mathbb{C} \to \mathbb{C}$, $\tau \circ \phi$ equals $\phi \circ \tau_K$ for some element τ_K in $\mathrm{Aut}(K/\mathbb{Q})$. Since $\tau \circ (\tau \circ \phi)$ equals $\mathrm{Id}_{\mathbb{C}} \circ \phi$ equals ϕ, also $(\phi \circ \tau_K) \circ \tau_K$ equals ϕ, i.e., $\tau_K \circ \tau_K$ equals Id_K. Thus τ_K is an element of $\mathrm{Aut}(K/\mathbb{Q})$ of order dividing 2, i.e., of order 1 or order 2. Also observe that since ϕ is only well-defined up to $\phi' = \phi \circ \sigma$, also τ_K is only well-defined up to conjugation $\sigma\tau_K\sigma^{-1}$. Moreover, τ_K is the identity only if $\tau \circ \phi$ equals ϕ, i.e., if and only if $\phi(K)$ is fixed by τ. Since the fixed field of τ is $\mathbb{R}$, τ_K equals Id if and only if $\phi(K)$ is contained in $\mathbb{R}$ for one, and hence every, embedding of K into $\mathbb{R}$. Thus τ_K is an element well-defined up to conjugation, which equals the identity if K is contained in $\mathbb{R}$, and which has order 2 if K is not contained in $\mathbb{R}$.

Now assume that $f(x)$ is an irreducible polynomial of degree 4 over $\mathbb{Q}$. And assume that the discriminant D is negative. Then $\sqrt{D}$ is not contained in $\mathbb{R}$. Since $\mathbb{Q}(\sqrt{D})$ is contained in the splitting field K of $f(x)$, K is not contained in $\mathbb{R}$. Thus τ_K is an element of $\mathrm{Aut}(K/\mathbb{Q})$ of order 2. Moreover, $\mathbb{Q}(\sqrt{D})$ is Galois over $\mathbb{Q}$ of order 2. Thus $\mathrm{Aut}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ is the quotient of $\mathrm{Aut}(K/\mathbb{Q})$ by the normal subgroup $\mathrm{Aut}(K/\mathbb{Q}(\sqrt{D}))$. This quotient group has order 2, thus is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

And clearly τ_K restricts to a nontrivial element of order 2 in $\mathrm{Aut}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$, namely complex conjugation. Thus τ_K is an element of $\mathrm{Aut}(K/\mathbb{Q})$ of order 2 whose image in $\mathrm{Aut}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ also has order 2. But the group $\mathbb{Z}/4\mathbb{Z}$ has a unique surjective homomorphism onto $\mathbb{Z}/2\mathbb{Z}$, and the kernel is precisely the set of elements of order 1 and 2. Since τ_K has order 2 and is not contained in the kernel of the quotient map, $\mathrm{Aut}(K/\mathbb{Q})$ cannot be isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

A bit more generally, let D be a negative element of $\mathbb{Q}$, and let K be a field containing $\mathbb{Q}(\sqrt{D})$ such that $K/\mathbb{Q}$ is Galois of degree 4. Then, as above, τ_K is an element of order 2 in $\mathrm{Aut}(K/\mathbb{Q})$ which maps to an element of order 2 in the quotient $\mathrm{Aut}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$. Thus, for the same reason as above, $\mathrm{Aut}(K/\mathbb{Q})$ is not cyclic of order 4.

Solution to (3) The polynomial $f(x)$ is irreducible of degree 6 by Eisenstein's criterion. Moreover, for each of the 2 roots β of $g(y) = y^2 - 2y - 2$, the three roots of $x^3 - \beta$ are roots of $f(x)$. Thus the splitting field contains $\mathbb{Q}(\mu_3)$ as well as the splitting field $\mathbb{Q}(\sqrt{3})$ of $g(y)$. Notice that $\mathbb{Q}(\mu_3)$ equals $\mathbb{Q}(\sqrt{-3})$. So the splitting field also contains $\sqrt{-3}/\sqrt{3}$, which is a square root of -1. Thus the splitting field contains $\mathbb{Q}(i, \sqrt{3})$. In this field the roots of $g(y) = (y-1)^2 - 3$ are $1 \pm \sqrt{3}$. Thus the roots of $f(x)$ are the cube roots of $1 \pm \sqrt{3}$.

Now let α_+ be a root of $f(x)$ with α_+^3 equals $1 + \sqrt{3}$. Since K contains primitive cube roots of 1, up to multiplication by such we may assume that α_+ is real. Similarly let α_- be a real root of $f(x)$ with α_-^3 equals $1 - \sqrt{3}$. Then $(-\alpha_+\alpha_-)^3$ equals $(-1)^3\alpha_+^3\alpha_-^3$ equals $(-1)(1+\sqrt{3})(1-\sqrt{3}) = 2$. Thus $-\alpha_+\alpha_-$ is a real cube root of 2, i.e., $\alpha_+\alpha_-$ equals $-\sqrt[3]{2}$. Thus the splitting field E of $f(x)$ contains $\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$.

The polynomial $t^3 - 2$ is irreducible of degree 3 over $\mathbb{Q}$ by Eisenstein's criterion. So every root generates an extension of $\mathbb{Q}$ of degree 3. And $\mathbb{Q}(i, \sqrt{3})$ is a biquadratic extension of $\mathbb{Q}$ of degree 4. Thus $\mathbb{Q}(i, \sqrt{3})$ contains no root of $t^3 - 2$. Since $t^3 - 2$ is a cubic polynomial with no root in $\mathbb{Q}(i, \sqrt{3})$, it is irreducible over $\mathbb{Q}(i, \sqrt{3})$. Thus the root field $\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$ is degree 3 over $\mathbb{Q}(i, \sqrt{3})$. So $[\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3}) : \mathbb{Q}]$ equals $3 \cdot 4 = 12$. Denote by L the field $\mathbb{Q}(\sqrt[3]{2}, i, \sqrt{3})$. Then α_+^3 equals $1 + \sqrt{3}$, which is an element of L. Since L contains a primitive cube root of 1, $L(\alpha_+)$ contains every cube root of $1 + \sqrt{3}$, hence it is the splitting field of $t^3 - (1 + \sqrt{3})$. So $[L(\alpha_+) : L]$ equals 3 if there is no cube root of $1 + \sqrt{3}$ in L, and it equals 1 otherwise. Moreover, α_- equals $-\sqrt[3]{2}/\alpha_+$, so $L(\alpha_+)$ contains $L(\alpha_-)$. And then it contains all the roots $\zeta_3^m\alpha_+$ and $\zeta_3^m\alpha_-$ of $f(x)$, where ζ_3 is a primitive cube root of 1 and where $m = 0, 1, 2$. So $L(\alpha_+)$ equals the splitting field E. So $[E : L]$ equals 3 if L contains no cube root of $1 + \sqrt{3}$, and $[E : L]$ equals 1 if L contains a cube root α_+ of $1 + \sqrt{3}$. So $[E : \mathbb{Q}]$ equals 36 or 12.

Now consider the element in K,

$$\alpha = \frac{\alpha_+^2 + \alpha_-^2}{\sqrt[3]{2}}.$$

Observe that

$$\frac{\alpha_+^2\alpha_-^2}{\sqrt[3]{2}^2} = 1, \quad \left(\frac{\alpha_+^2}{\sqrt[3]{2}}\right)^3 = \frac{(1+\sqrt{3})^2}{2} = 2 + \sqrt{3}, \quad \left(\frac{\alpha_-^2}{\sqrt[3]{2}}\right)^3 = \frac{(1-\sqrt{3})^2}{2} = 2 - \sqrt{3}.$$

Thus, we have

$$\alpha^3 = \left[\left(\frac{\alpha_+^2}{\sqrt[3]{2}}\right)^3 + \left(\frac{\alpha_-^2}{\sqrt[3]{2}}\right)^3\right] + 3\frac{\alpha_+^2\alpha_-^2}{\sqrt[3]{2}^2}\left[\frac{\alpha_+^2 + \alpha_-^2}{\sqrt[3]{2}}\right] = 4 + 3\alpha.$$

Therefore α is a root of the cubic polynomial $k(x) = x^3 - 3x - 4$. By Proposition 11 on p. 308, the only possible roots of $k(x)$ in $\mathbb{Q}$ are $\pm 1, \pm 2, \pm 4$. By direct computation, none of these are roots. Therefore $k(x)$ is irreducible over $\mathbb{Q}$. By direct computation, the discriminant equals

$$D = -4(-3)^3 - 27(-4)^2 = 4 \cdot 27(1 - 4) = -2^2 \cdot 3^4.$$

So the splitting field contains the square root $\sqrt{D}$, and thus also $\sqrt{D}/18$ which equals $\sqrt{-1}$.

On the other hand, consider the extension $L/\mathbb{Q}$. This is a Galois extension, the compositum of the splitting field $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})$ of $t^3 - 2$, which has Galois group S_3, and the quadratic extension $\mathbb{Q}(i)$, which has Galois group $\mathbb{Z}/2\mathbb{Z}$. By Corollary 22 on p. 593, the Galois group $\mathrm{Aut}(L/\mathbb{Q})$ equals $\mathrm{Aut}(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}) \times \mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}) \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$. This has 3 subgroups of index 3, i.e., 2-Sylow subgroups. By the Fundamental Theorem of Galois Theory, $L/\mathbb{Q}$ contains 3 subextensions which have degree 3 over $\mathbb{Q}$. But each of the three cube roots of 2 generates a distinct degree 3 extension of $\mathbb{Q}$. Thus these are the only degree 3 subextensions of $\mathbb{Q}$. And for each such degree 3 subextension $E/\mathbb{Q}$ of $L/\mathbb{Q}$, the Galois closure of $E/\mathbb{Q}$ is simply the splitting field of $t^3 - 2$, i.e., $E(\sqrt{-3})$. In particular, this does not contain i, since $L = E(\sqrt{-3}, i)$ has degree 4 over E, not 2. So $\mathbb{Q}(\alpha)$ cannot be one of the degree 3 subextensions $E/\mathbb{Q}$ of $L/\mathbb{Q}$, since the Galois closure of $\mathbb{Q}(\alpha)$ does contain i. Since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a degree 3 extension, it follows that $\mathbb{Q}(\alpha)$ is not contained in L. Therefore α is not contained in L. Since α is contained in K, K properly contains L. Therefore K/L is a degree 3 extension and $[K : \mathbb{Q}]$ equals 36.

By the argument above, K is the compositum of the two Galois extensions $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}$ and $\mathbb{Q}(\alpha, i)/\mathbb{Q}$, each of which is a degree 6 extension with Galois group S_3. By Corollary 20 on p. 592, it follows that these two extensions are linearly disjoint over $\mathbb{Q}$, i.e., their intersection equals $\mathbb{Q}$. And then by Corollary 22 on p. 593, the Galois group of the compositum equals the product of the Galois groups, $\mathrm{Aut}(K/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q}) \times \mathrm{Aut}(\mathbb{Q}(\alpha, i)/\mathbb{Q}) \cong S_3 \times S_3$. To be explicit, $\mathrm{Aut}(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{2})/\mathbb{Q})$ acts as the full symmetric group S_3 on the three roots,

$$\sqrt[3]{2}, \frac{1 + \sqrt{-3}}{2}\sqrt[3]{2}, \frac{1 - \sqrt{-3}}{2}\sqrt[3]{2},$$

of $t^3 - 2$. And $\mathrm{Aut}(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ acts as the full symmetric group S_3 on the three roots,

$$\alpha, -\frac{\alpha}{2} + \frac{\alpha^2 - 2\alpha - 2}{2}i, -\frac{\alpha}{2} - \frac{\alpha^2 - 2\alpha - 2}{2}i.$$

of $x^3 - 3x - 4$.

Nota Bene. If $\mathrm{char}(E) \neq 2, 3$, then for a monic cubic polynomial $h(x) = x^3 + px + q$ in $E[x]$ which has discriminant $D = -4p^3 - 27q^2$ a square δ^2 in E and which has one root α in E, then the other

two roots are in E and given by the formula

$$\frac{-\alpha}{2} \mp \frac{6p\alpha^2 - 9q\alpha + 4p^2}{2\delta}.$$

Solution to (4) Suppose first that D is a sum of two rational squares,

$$D = s^2 + t^2.$$

Since D is squarefree, both s and t are nonzero. Thus $\pm\sqrt{D \pm s\sqrt{D}}$ are four distinct elements. And by direct computation, these are roots of the monic, quartic polynomial

$$f(x) = x^4 - 2Dx^2 + t^2D = (x^2 - D)^2 - s^2D.$$

Each of these roots generates an extension of $\mathbb{Q}$ which contains $\mathbb{Q}(\sqrt{D})$. So the splitting field of $f(x)$ contains $\mathbb{Q}(\sqrt{D})$, and none of the roots of $f(x)$ lies in $\mathbb{Q}$. Thus if $f(x)$ is reducible, it is a product of two irreducible quadratic factors. Since $f(x)$ has no cubic or linear term, the factorization would have to be

$$f(x) = (x^2 + ax + b)(x^2 - ax + b) = x^4 + (2b - a^2)x^2 + b^2.$$

But then t^2D equals b^2, so that D is the rational square $(b/t)^2$. This contradicts that D is squarefree. Therefore $f(x)$ is an irreducible quartic polynomial.

Let α_+ be a root of $f(x)$ with

$$\alpha_+^2 = D + s\sqrt{D}.$$

Now $(D + s\sqrt{D})(D - s\sqrt{D}) = t^2D$ so that

$$D - s\sqrt{D} = \left(\frac{t\sqrt{D}}{\alpha_+}\right)^2.$$

Therefore, defining

$$\alpha_- = \frac{t\sqrt{D}}{\alpha_+} = \frac{-s + \sqrt{D}}{t}\alpha_+$$

it follows that $\mathbb{Q}(\alpha_+)$ contains a root α_- of $f(x)$ with $\alpha_-^2 = D - s\sqrt{D}$. Thus $\pm\alpha_+$ and $\pm\alpha_-$ are the four roots of $f(x)$. So $\mathbb{Q}(\alpha_+)$ is a splitting field of $f(x)$. So $\mathbb{Q}(\alpha_+)/\mathbb{Q}$ is a Galois extension of degree 4.

Let $\sigma : \mathbb{Q}(\alpha_+) \to \mathbb{Q}(\alpha_+)$ be an automorphism with $\sigma(\alpha_+)$ equals α_-. Then $\sigma(\alpha_+^2)$ equals $\sigma(\alpha_+)^2$, which equals $(\alpha_-)^2 = D - s\sqrt{D}$. But α_+^2 equals $D + s\sqrt{D}$. Thus $\sigma(\sqrt{D})$ equals $-\sqrt{D}$. And thus we have

$$\sigma(\alpha_-) = \frac{t\sigma(\sqrt{D})}{\sigma(\alpha_+)} = \frac{t(-\sqrt{D})}{\alpha_-} = -\alpha_+.$$

In particular, $\sigma(\sigma(\alpha_+))$ equals $-\alpha_+$. Thus σ^2 does not equal the identity. Since the order of σ divides $\#\mathrm{Aut}(\mathbb{Q}(\alpha_+)/\mathbb{Q}) = [\mathbb{Q}(\alpha_+) : \mathbb{Q}] = 4$, it follows that σ is an element of order 4. Thus

$\mathrm{Aut}(\mathbb{Q}(\alpha_+)/\mathbb{Q})$ is a cyclic group of order 4. Therefore, if D is a squarefree integer which is a sum of two rational squares, then $\mathbb{Q}(\sqrt{D})$ is contained in a degree 4, Galois extension of $\mathbb{Q}$ with cyclic Galois group.

Conversely, assume that $K = \mathbb{Q}(\sqrt{D})$ is contained in a degree 4, Galois extension $L/\mathbb{Q}$ with cyclic Galois group. In particular, L/K is a degree 2 extension. By Kummer's Theorem, Proposition 37 on p. 626, L/K is of the form $L = K(\sqrt{u})$ for some element $u = a + b\sqrt{D}$ in K. Since $K/\mathbb{Q}$ is a Galois extension, $\mathrm{Aut}(L/K)$ is a normal subgroup of $\mathrm{Aut}(L/\mathbb{Q})$, and the quotient is $\mathrm{Aut}(K/\mathbb{Q})$. In particular, there exists an element σ of $\mathrm{Aut}(L/\mathbb{Q})$ which maps to the nontrivial element of $\mathrm{Aut}(K/\mathbb{Q})$. And then we have

$$(\sigma(\sqrt{u}))^2 = \sigma(\sqrt{u}^2) = \sigma(u) = a - b\sqrt{D}.$$

Therefore $v := \sqrt{u}\sigma(\sqrt{u})$ is an element of L whose square equals

$$v^2 = \sqrt{u}^2(\sigma(\sqrt{u}))^2 = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D.$$

Thus $\mathbb{Q}(v)/\mathbb{Q}$ is a degree 2 subextension of $L/\mathbb{Q}$. Since $L/\mathbb{Q}$ is Galois, degree 2 subextensions are in bijection with index 2 subgroups of $\mathrm{Aut}(L/\mathbb{Q})$. Since $\mathrm{Aut}(L/\mathbb{Q})$ is a cyclic group of order 4, it has a unique index 2 subgroup. Thus the degree 2 subextension $\mathbb{Q}(v)$ must equal $\mathbb{Q}(\sqrt{D})$. So v is an element of $\mathbb{Q}(\sqrt{D})$ with $w := v^2$ an element in $\mathbb{Q}$.

By another part of Kummer's theorem, for every element v in $\mathbb{Q}(\sqrt{D})$ with $w := v^2$ in $\mathbb{Q}$, then either $w = c^2$ or $w = c^2 D$ for some c in $\mathbb{Q}$. Now if w equals c^2, then $v = \pm c$ is in $\mathbb{Q}$. But then $\sigma(u) = v/u$ implies that $\sigma(\sigma(u))$ equals $v/\sigma(u) = u$. So σ^2 fixes the generator u of $\mathbb{Q}(u)$. So σ^2 is the identity, i.e., the order of σ divides 2. But since $\mathrm{Aut}(L/\mathbb{Q})$ is a cyclic group of order 4, and since σ is not in $\mathrm{Aut}(L/K)$, the unique subgroup of index 2, σ is a generator, i.e., σ has order 4. This contradiction proves that w is not of the form c^2. Therefore w is for the form $c^2 D$. And then since $w := v^2$ also equals $a^2 - b^2 D$, this implies the identity,

$$D = \left(\frac{bD}{a}\right)^2 + \left(\frac{cD}{a}\right)^2.$$

Therefore D is a sum of two rational squares. Thus the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is contained in a degree 4, Galois extension of $\mathbb{Q}$ with cyclic Galois group if and only if D is a sum of two rational squares.

In particular, by the same argument as in the solution of Exercise 10, p. 582 on the previous problem set, 3 is not a sum of two rational squares. Thus $\mathbb{Q}(\sqrt{3})$ is not contained in a degree 4, Galois extension of $\mathbb{Q}$ with cyclic Galois group. Similarly, since a negative real number cannot be a sum of two squares, for rational $D < 0$, the extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ is not contained in a degree 4, Galois extension of $\mathbb{Q}$ with cyclic Galois group.

Solution to (5) Let $f : M \to N$ be a nonzero R-module homomorphism. Then $\mathrm{Ker}(f)$ is a left R-submodule of M which does not equal M. Since M is simple, the only proper left R-submodule

of M is $\{0\}$. Thus f is injective. And Image(f) is a submodule of N which is isomorphic to M. By definition, the zero module is not simple, thus M is nonzero, and so also Image(f) is nonzero. Since N is simple, the only nonzero left R-submodule of N is all of N. Thus Image(f) equals N. Thus f is surjective. Since f is injective and surjective, f is an isomorphism of left R-modules.

Now consider the case when $N = M$ is a left R-module. Then $\mathrm{Hom}_R(M, M)$ is a ring under the usual addition, and with composition for multiplication. The identity map is the multiplicative unit. And it is associative since composition is associative. Therefore $\mathrm{Hom}_R(M, M)$ is a unital, associative ring. Also for the center $Z(R)$ of R, scaling by elements in $Z(R)$ gives a ring homomorphism $Z(R) \to \mathrm{Hom}_R(M, M)$ which makes $\mathrm{Hom}_R(M, M)$ into a $Z(R)$-algebra, i.e., the image of $Z(R)$ is in the center of the ring $\mathrm{Hom}_R(M, M)$ (but the center of $\mathrm{Hom}_R(M, M)$ might be strictly larger than the center of R). Finally, if M is simple, then the argument above proves that every nonzero element of $\mathrm{Hom}_R(M, M)$ is invertible in this ring. Thus $\mathrm{Hom}_R(M, M)$ is a division ring.

As one motivating example, when Q_8 is the quaternion group, when R equals $\mathbb{R} \cdot Q_8$ is the group algebra of Q_8 over $\mathbb{R}$, and when M is the simple R-module described in Example 8 on p. 845, then the division ring $\mathrm{Hom}_R(M, M)$ is the usual quaternion algebra $\mathbb{H}$.