

ALGEBRA HW 8

CLAY SHONKWILER

1

(a): Find the degree of $\alpha = \sqrt{2} + \sqrt{3}$ over \mathbb{Q} , and also find its minimal polynomial.

Answer: Note that

$$\alpha^4 - 10\alpha^2 + 1 = (\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = (49 - 20\sqrt{6}) - 10(5 + 2\sqrt{6}) + 1 = 0,$$

so α satisfies the polynomial $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Now, by Math 602 PS7#5(d), the only possible rational roots of f are ± 1 , and $f(1) = f(-1) = -8$, so f is irreducible over \mathbb{Q} . Hence, f is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} and so $\deg \alpha = \deg f = 4$.



(b): Do the same for $\beta = \sqrt{3 + \sqrt[3]{2}}$.

Answer: Note that

$$\begin{aligned} \beta^6 - 9\beta^4 + 27\beta^2 - 29 &= \left(\sqrt{3 + \sqrt[3]{2}}\right)^6 - 9\left(\sqrt{3 + \sqrt[3]{2}}\right)^4 + 27\left(\sqrt{3 + \sqrt[3]{2}}\right)^2 - 29 \\ &= (29 + 27\sqrt[3]{2} + 9\sqrt[3]{2}^2) - 9(9 + 6\sqrt[3]{2} + \sqrt[3]{2}^2) + 27(3 + \sqrt[3]{2}) - 29 \\ &= (29 - 81 + 81 - 29) + (27 - 54 + 27)\sqrt[3]{2} + (9 - 9)\sqrt[3]{2}^2 \\ &= 0, \end{aligned}$$

so β satisfies $g(x) = x^6 - 9x^4 + 27x^2 - 29$. Again using Math 602 PS7#5(d), the only possible rational roots of this polynomial are ± 29 , and $g(29) = g(-29) = 588,480,470$. Hence, g is irreducible over \mathbb{Q} , and so g is the minimal polynomial of β . Thus, $\deg \beta = \deg g = 6$.



(c): Is $\mathbb{Q}(\alpha)$ normal over \mathbb{Q} ? Is $\mathbb{Q}(\beta)$?

Answer: Note, first off, that the four roots of $x^4 - 10x^2 + 1$ are $\pm(\sqrt{2} \pm \sqrt{3})$. Now, $\frac{\alpha^2 - 5}{2} \in \mathbb{Q}(\alpha)$ and

$$\frac{\alpha^2 - 5}{2} = \frac{(5 + 2\sqrt{6}) - 5}{2} = \sqrt{6},$$

so $\sqrt{6} \in \mathbb{Q}(\alpha)$. Hence,

$$\sqrt{6}\alpha = \sqrt{6}(\sqrt{2} + \sqrt{3}) = 2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\alpha),$$

so

$$2\alpha - (2\sqrt{3} + 3\sqrt{2}) = (2\sqrt{2} + 2\sqrt{3}) - (2\sqrt{3} + 3\sqrt{2}) = -\sqrt{2} \in \mathbb{Q}(\alpha)$$

and

$$3\alpha - (2\sqrt{3} + 3\sqrt{2}) = (3\sqrt{2} + 3\sqrt{3}) - (2\sqrt{3} + 3\sqrt{2}) = \sqrt{3} \in \mathbb{Q}(\alpha).$$

Hence, all linear combinations of $\sqrt{2}$ and $\sqrt{3}$ are in $\mathbb{Q}(\alpha)$, so $\pm(\sqrt{2} \pm \sqrt{3}) \in \mathbb{Q}(\alpha)$. Therefore, since these are all the roots of the minimal polynomial of α , we conclude that $\mathbb{Q}(\alpha)$ is normal over \mathbb{Q} .

On the other hand,

$$\begin{aligned} & \left(\sqrt{3 + \zeta_3 \sqrt[3]{2}} \right)^6 - 9 \left(\sqrt{3 + \zeta_3 \sqrt[3]{2}} \right)^4 + 27 \left(\sqrt{3 + \zeta_3 \sqrt[3]{2}} \right)^2 - 29 \\ &= (29 + 27\zeta_3 \sqrt[3]{2} + 9\zeta_3^2 \sqrt[3]{2}^2) - 9(9 + 6\zeta_3 \sqrt[3]{2} + \zeta_3^2 \sqrt[3]{2}^2) + 27(3 + \zeta_3 \sqrt[3]{2}) + 27 \\ &= 0, \end{aligned}$$

so $\sqrt{3 + \zeta_3 \sqrt[3]{2}}$ is a root of $g(x) = x^6 - 9x^4 + 27x^2 - 29$, the minimal polynomial of β . However, $\mathbb{Q}(\beta) \subset \mathbb{R}$ and $\sqrt{3 + \zeta_3 \sqrt[3]{2}} \notin \mathbb{R}$, so $\sqrt{3 + \zeta_3 \sqrt[3]{2}} \notin \mathbb{Q}(\beta)$. Hence, g does not split in $\mathbb{Q}(\beta)$, so $\mathbb{Q}(\beta)$ is not normal over \mathbb{Q} .

♣

2

Let $F = \mathbb{C}(x)$. For $a \in \mathbb{C}$, view $\mathbb{C}((x - a))$ as a field extension of F .

(a): Show that if $a, b \in \mathbb{C}$, then there is a square root of $x - a$ in $\mathbb{C}((x - b))$ if and only if $a \neq b$.

Proof. Suppose $a \neq b$. Then $x - a$ has a square root in $\mathbb{C}((x - b))$ if we can solve the following equation:

(1)

$$(x-b)+(b-a) = x-a = \left(\sum_{j=0}^{\infty} c_j (x-b)^j \right)^2 = c_0^2 + 2c_0c_1(x-b) + (2c_0c_2 + c_1^2)(x-b)^2 + \dots;$$

in other words, if we can solve the following system of equations:

$$\begin{aligned} c_0^2 &= b - a \\ 2c_0c_1 &= 1 \\ 2c_0c_2 + c_1^2 &= 0 \\ 2c_0c_3 + 2c_1c_2 &= 0 \\ &\vdots \end{aligned}$$

Clearly, we can let $c_0 = \sqrt{b-a} \in \mathbb{C}$. Then, if we let $c_1 = \frac{1}{2c_0} = \frac{1}{2\sqrt{b-a}} \in \mathbb{C}$, then $2c_0c_1 = 1$. Then, if $c_2 = \frac{-1}{8(b-a)^{3/2}}$,

$$2c_0c_2 + c_1^2 = 2\sqrt{b-a} \frac{-1}{8(b-a)^{3/2}} + \left(\frac{1}{2\sqrt{b-a}} \right)^2 = \frac{-1}{4(b-a)} + \frac{1}{4(b-a)} = 0.$$

Iterating this process, we see that it is indeed possible to solve (1), so, if $b \neq a$, $x-a$ does have a square root in $\mathbb{C}((x-b))$.

Suppose, on the other hand, that $x-a$ has a square root in $\mathbb{C}((x-a))$. Then

$$\sqrt{x-a} = \sum_{j=0}^{\infty} c_j(x-a)^j$$

for $c_j \in \mathbb{C}$. Then

$$0 = \sqrt{a-a} = \sum_{j=0}^{\infty} c_j(a-a)^j = c_0,$$

so, in fact,

$$\sqrt{x-a} = \sum_{j=1}^{\infty} c_j(x-a)^j.$$

Hence,

$$x-a = (\sqrt{x-a})^2 = \left(\sum_{j=1}^{\infty} c_j(x-a)^j \right)^2.$$

Now, the right hand side of this expression is a power series in $(x-a)$ with all even exponents, so there are no cancellations that reduce it to the left hand side. However, since $x-a$ is entire, it has a unique power series representation centered at a , namely $x-a$. Since the right hand side above represents a *different* power series representation, we see that this is impossible. Therefore, $x-a$ does not have a square root in $\mathbb{C}((x-a))$, and so, if $x-a$ has a square root in $\mathbb{C}((x-b))$, then $b \neq a$.

Thus, having shown both implications, we conclude that $x-a$ has a square root in $\mathbb{C}((x-b))$ if and only if $a \neq b$. \square

- (b):** For each non-negative integer n , let $F_n = F[\sqrt{x}, \sqrt{x-1}, \dots, \sqrt{x-n}]$. Show that each F_n is a field extension of F ; and that F_n can be embedded in $\mathbb{C}((x-m))$ as an F -algebra if and only if $n < m$. Deduce that the inclusions $F_0 \subset F_1 \subset F_2 \subset \dots$ are strict.

Proof. We prove this by induction. In the base case, $F_0 = F[\sqrt{x}]$. Now, \sqrt{x} satisfies the polynomial

$$t^2 - x \in F[t],$$

so \sqrt{x} is algebraic over F and, therefore, $F[\sqrt{x}]$ is a field extension of F .

Now, if F_{k-1} is a field extension of F , then consider $F_k = F_{k-1}[\sqrt{x-k}]$. Then $\sqrt{x-k}$ satisfies the polynomial

$$t^2 - (x-k) \in F[t] \subset F_{k-1}[t],$$

so $\sqrt{x-k}$ is algebraic over F_{k-1} and, therefore, $F_k = F_{k-1}[\sqrt{x-k}]$ is a field extension of F_{k-1} . Since F_{k-1} is a field extension of F , this implies that F_k is a field extension of F . Therefore, by induction, we conclude that F_n is a field extension of F for all n .

Now, if $n < m$ then, by our result in part (a), $\sqrt{x-k} \in \mathbb{C}((x-m))$ for all $k \leq n$. Hence, since every element of F_n is a linear combination of $1 \in \mathbb{C}(x)$ and the $\sqrt{x-k}$ for $k \leq n$ with coefficients in $\mathbb{C}(x) \subset \mathbb{C}((x-m))$, we see that $F_n \subset \mathbb{C}((x-b))$.

On the other hand, if $n \geq m$, then $\sqrt{x-m} \in F_n$. Again by our result in (a) above, $\sqrt{x-m} \notin \mathbb{C}((x-b))$, so we see that $F_n \not\subset \mathbb{C}((x-m))$. By contrapositive, then, if $F_n \subset \mathbb{C}((x-m))$, then $n < m$. Having shown both implications, we conclude that F_n can be embedded in $\mathbb{C}((x-m))$ if and only if $n < m$.

Therefore, for any non-negative $k \in \mathbb{Z}$, $F_k \subset \mathbb{C}((x-(k+1)))$, but $F_{k+1} \not\subset \mathbb{C}((x-(k+1)))$, so there are elements of F_{k+1} (e.g. $\sqrt{x-(k+1)}$) contained in F_{k+1} but not in F_k . On the other hand, it's clear that $F_k \subset F_{k+1}$ for all k , so we see that the containments

$$F_0 \subset F_1 \subset F_2 \subset \dots$$

are strict. □

(c): Show that $F_\infty := F[\sqrt{x}, \sqrt{x-1}, \sqrt{x-2}, \dots]$ is a field of infinite degree over F .

Proof. Since the containments $F_0 \subset F_1 \subset F_2 \subset \dots$ are strict, it must be the case that $[F_{k+1} : F_k] \geq 2$ for all $k \geq 0$. Hence, for any $n \geq 0$,

$$(2) \quad [F_n : F] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \cdots [F_1 : F_0][F_0 : F] \geq 2^n.$$

Since F_n is strictly contained in F_∞ ,

$$[F_\infty : F] \geq [F_n : F] \geq 2^n$$

for all $n \in \mathbb{N}$. Therefore, it must be the case that F_∞ is a field of infinite degree over F . □

(d): Is there an integer d such that every element of F_∞ satisfies a polynomial of degree at most d over F ?

Answer: Suppose there exists $d \in \mathbb{N}$ such that every element of F_∞ satisfies a polynomial of degree at most d over F . For each $n \geq 0$, F_n is simply F adjoin finitely many algebraic elements, so F_n is a finite extension of F . Now, since F has characteristic 0, F_d is

separable over F , so, by the Primitive Element Theorem, $F_d = F[\alpha]$ for some $\alpha \in F_d$. Now, since $F_d \subset F_\infty$, α satisfies a polynomial of degree at most d over F , and so, using inequality (2),

$$d = \deg_F(\alpha) = [F[\alpha] : F] = [F_d : F] \geq 2^d$$

which is impossible. From this contradiction, we conclude that there is no such d , so there are elements of F_∞ whose minimal polynomials have arbitrarily large degree.



3

Let K be a field, and $f(x) \in K[x]$. Assume that K has characteristic 0. Let $n \geq 1$.

(a): Let L be a finite field extension of K , and let $\alpha \in L$. Show that α is a root of f with multiplicity n if and only if $0 = f(\alpha) = f'(\alpha) = \dots = f^{(n-1)}(\alpha) \neq f^{(n)}(\alpha)$.

Proof. Suppose α is a root of f with multiplicity n . Then, in $L[x]$,

$$f(x) = (x - \alpha)^n g(x)$$

where $g(x) \in L[x]$ does not have α as a root. Then

$$\begin{aligned} f'(x) &= (x - \alpha)^n g'(x) + n(x - \alpha)^{n-1} g(x) \\ f''(x) &= (x - \alpha)^n g''(x) + 2n(x - \alpha)^{n-1} g'(x) + n(n-1)(x - \alpha)^{n-2} g(x) \\ &\vdots \end{aligned}$$

$$f^{(k)}(x) = \sum_{j=0}^k \binom{k}{j} \left[\prod_{i=0}^{j-1} (n-i) \right] (x - \alpha)^{n-j} g^{(k-j)}(x)$$

for $k \leq n$. Hence, for $k \leq n-1$, each term in the above sum has a factor of $(x - \alpha)$ to some positive power, so $f^{(k)}(\alpha) = 0$. However,

$$f^{(n)}(x) = \sum_{j=0}^n \binom{n}{j} \left[\prod_{i=0}^{j-1} (n-i) \right] (x - \alpha)^{n-j} g^{(n-j)}(x)$$

has a term of the form $n(n-1) \cdots (2)(1)g(x)$ with all other terms being divisible by $(x - \alpha)$; hence,

$$f^{(n)}(\alpha) = n!g(\alpha) \neq 0,$$

since g does not have α as a root. Therefore, we see that if α is a root of f of multiplicity n , then

$$0 = f(\alpha) = f'(\alpha) = \dots = f^{(n-1)}(\alpha) \neq f^{(n)}(\alpha).$$

We prove the converse by induction on n . If α is a root of f but not of f' , then, as we proved in class, α is not a multiple root of f . If

$$0 = f(\alpha) = f'(\alpha) \neq f''(\alpha),$$

then $f(x) = (x - \alpha)h_0(x)$ and

$$\begin{aligned} f'(x) &= h_0(x) + (x - \alpha)h_0'(x) \\ f''(x) &= 2h_0'(x) + (x - \alpha)h_0''(x). \end{aligned}$$

Since $f'(\alpha) = 0$, $(x - \alpha) \mid f'(x)$, so we see that $(x - \alpha) \mid h_0(x)$, meaning $h_0(x) = (x - \alpha)h_1(x)$. However, since $(x - \alpha)$ does not divide $f''(x)$, $(x - \alpha)$ does not divide $h_0'(x)$. Hence, α is not a multiple root of $h_0(x)$, so $h_1(x)$ is not divisible by $(x - \alpha)$. Therefore,

$$f(x) = (x - \alpha)h_0(x) = (x - \alpha)^2h_1(x)$$

where $h_1(\alpha) \neq 0$, so α is a double root of f .

Now, suppose, as an inductive hypothesis, that if

$$0 = g(\alpha) = g'(\alpha) = \dots = g^{(n-2)}(\alpha) \neq g^{(n-1)}(\alpha),$$

then α is a root of g of multiplicity n for any $g(x) \in K[x]$. Suppose that

$$0 = f(\alpha) = f'(\alpha) = \dots = f^{(n-2)}(\alpha) \neq f^{(n-1)}(\alpha).$$

Then, for $k \leq n - 1$, $f^{(k)}(x) = (x - \alpha)h_k(x)$ in $L[x]$ for some $h_k(x) \in L[x]$. Then, differentiating $f(x) = (x - \alpha)h_0(x)$, we see that

$$\begin{aligned} f'(x) &= h_0(x) + (x - \alpha)h_0'(x) \\ f''(x) &= 2h_0'(x) + (x - \alpha)h_0''(x) \\ f'''(x) &= 3h_0''(x) + (x - \alpha)h_0'''(x) \\ &\vdots \end{aligned}$$

$$f^{(n-1)}(x) = (n - 1)h_0^{(n-2)}(x) + (x - \alpha)h_0^{(n-1)}(x)$$

$$f^{(n)}(x) = nh_0^{(n-1)}(x) + (x - \alpha)h_0^{(n)}(x).$$

Since $(x - \alpha)$ divides $f^{(k)}(x)$ for $k \leq n - 1$, we see that $(x - \alpha)$ divides $h_0^{(k-1)}(x)$ for $k \leq n - 1$. Furthermore, since $(x - \alpha)$ does not divide $f^{(n)}(x)$, $(x - \alpha)$ does not divide $h_0^{(n-1)}(x)$. Hence, h_0 satisfies the inductive hypothesis, so we see that α is a root of h_0 of multiplicity $n - 1$. Hence, $h_0(x) = (x - \alpha)^{n-1}g(x)$ for $g(x) \in L[x]$ such that $g(\alpha) \neq 0$. Then

$$f(x) = (x - \alpha)h_0(x) = (x - \alpha)^n g(x)$$

where $(x - \alpha)$ does not divide $g(x)$, so α is a root of f of multiplicity exactly n .

Thus, by induction, that if

$$0 = f(\alpha) = f'(\alpha) = \dots = f^{(n-1)}(\alpha) \neq f^{(n)}(\alpha)$$

then α is a root of f of multiplicity n . Having shown both implications, we conclude that α is a root of f of multiplicity n if and only if

$$0 = f(\alpha) = f'(\alpha) = \dots = f^{(n-1)}(\alpha) \neq f^{(n)}(\alpha)$$

□

(b): Show that f has a root (in some extension of K) of multiplicity at least n if and only if $(f(x), f'(x), \dots, f^{(n-1)}(x))$ is a proper ideal of $K[x]$.

Proof. Suppose f has a root α in some extension of K of multiplicity at least n . Then, by part (a), α is a root of $f(x), f'(x), \dots, f^{(n-1)}(x)$. Now, if $g(x) \in (f(x), f'(x), \dots, f^{(n-1)}(x))$, then

$$g(x) = h_0(x)f(x) + h_1(x)f'(x) + \dots + h_{n-1}(x)f^{(n-1)}(x),$$

for $h_0, \dots, h_{n-1} \in K[x]$. Hence,

$$g(\alpha) = h_0(\alpha)f(\alpha) + h_1(\alpha)f'(\alpha) + \dots + h_{n-1}(\alpha)f^{(n-1)}(\alpha) = 0,$$

so α is a root of g . Since our choice of g was arbitrary, we see that all elements of $(f(x), f'(x), \dots, f^{(n-1)}(x))$ have α as a root. However, there are plenty of polynomials in $K[x]$ (the constant polynomial 1, for example) that do not have α as a root, so we see that $(f(x), f'(x), \dots, f^{(n-1)}(x))$ is a proper ideal of $K[x]$.

On the other hand, suppose $(f(x), f'(x), \dots, f^{(n-1)}(x))$ is a proper ideal of $K[x]$. Then, since $K[x]$ is a PID, $(f(x), f'(x), \dots, f^{(n-1)}(x)) = (g(x))$ for some $g(x) \in K[x]$. Let α be a root of g . Then, since each $f^{(k)}(x)$ is a multiple of $g(x)$ for $k \leq n-1$, $f^{(k)}(\alpha) = 0$. Hence, by part (a), α is a root of f of multiplicity at least n . □

(c): What if instead K has non-zero characteristic?

Answer: Consider the field $K = \mathbb{F}_p[t]$. Then, as we saw in class on 04.01.05,

$$f(x) = x^{2p} - t \in K[x]$$

has two roots, $\pm\sqrt{t}$, each of multiplicity p . However,

$$f'(x) = 2px^{2p-1} = 0 \in K[x],$$

so $f^{(n)}(x) = 0$ for all $n > 0$. In particular, $f^{(p)}(\sqrt{t}) = 0$, even though \sqrt{t} is a root of multiplicity only p . Hence, addressing the issue in (b), $(f(x), f'(x), \dots, f^{(n)}(x)) = (f(x))$ is a proper ideal of $K[x]$ for any $n > 0$, even though the multiplicity of both roots of f is p .

On the other hand, if K is a field of characteristic p and α is a root of multiplicity n of $f(x) \in K[x]$, then the proof given in (a) above suffices to show that

$$0 = f(\alpha) = f'(\alpha) = \cdots = f^{(n-1)}(\alpha);$$

we simply don't know that α is not also a root of the higher derivatives of f . In turn, this implies that $(f(x), f'(x), \dots, f^{(n-1)}(x))$ is a proper ideal of $K[x]$ by the same reasoning as in (b) above, but, as we just saw, we may be able to throw in more derivatives and still have a proper ideal.

Finally, if $f(x) \in K[x]$ has root α in some algebraic extension of a field K of characteristic p such that

$$0 = f(\alpha) = f'(\alpha) = \cdots = f^{(n-1)}(\alpha) \neq f^{(n)}(\alpha),$$

then our proof in (a) demonstrates that α is a root of multiplicity at most n . Equivalently, if f has a root of multiplicity at least n , then our proof in (b) suffices to show that $(f(x), f'(x), \dots, f^{(n-1)}(x))$ is a proper ideal in $K[x]$. Thus, we see that one direction of the statements in (a) and (b) still hold over characteristic p , but not necessarily both directions.



4

For each of the following fields K , explicitly find the group $\text{Aut } K$ of all automorphisms of K (as a field): \mathbb{Q} , $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[\zeta_7]$, $\mathbb{Q}[\zeta_8]$, $\mathbb{Q}[\zeta_3, \sqrt[3]{2}]$.

Answer: \mathbb{Q} : Suppose ϕ is an automorphism of \mathbb{Q} . Then $\phi(1) = 1$. Also, for $\frac{p}{q} \in \mathbb{Q}$, (i.e. $p, q \in \mathbb{Z}$, $q \neq 0$), then

$$\phi(p) = \phi(p \cdot 1) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = 1 + \cdots + 1 = p \cdot 1 = p$$

and, by a similar argument, $\phi(q) = q$. Also,

$$\phi(q^{-1}) = \phi(q)^{-1} = q^{-1}.$$

Hence,

$$\phi\left(\frac{p}{q}\right) = \phi\left(p \cdot \frac{1}{q}\right) = \phi(p)\phi\left(\frac{1}{q}\right) = p \frac{1}{q} = \frac{p}{q}.$$

Since our choice of $\frac{p}{q} \in \mathbb{Q}$ was arbitrary, we see that ϕ must be the identity map. Hence, the only automorphism of \mathbb{Q} is the identity.

$\mathbb{Q}[\sqrt{2}]$: If ϕ is an automorphism of $\mathbb{Q}[\sqrt{2}]$, then $\phi|_{\mathbb{Q}}$ is an automorphism of \mathbb{Q} , so, by the above argument, $\phi|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Hence, ϕ is entirely determined by $\phi(\sqrt{2})$. Now,

$$2 = \phi(2) = \phi(\sqrt{2}^2) = \phi(\sqrt{2})^2,$$

so $\phi(\sqrt{2}) = \pm\sqrt{2}$. These clearly define distinct automorphisms, so we see that there are two different automorphisms of $\mathbb{Q}[\sqrt{2}]$; the only group of order

2 is the cyclic group C_2 , so

$$\text{Aut } \mathbb{Q}[\sqrt{2}] \simeq C_2.$$

$\mathbb{Q}[\sqrt[3]{2}]$: Suppose ϕ is an automorphism of $\mathbb{Q}[\sqrt[3]{2}]$. Then $\phi|_{\mathbb{Q}} = id_{\mathbb{Q}}$ by the same argument as above. Now,

$$2 = \phi(2) = \phi(\sqrt[3]{2^3}) = \phi(\sqrt[3]{2})^3,$$

so $\phi(\sqrt[3]{2})$ must be a third root of 2. The only such in $\bar{\mathbb{Q}}$ are $\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}$ and $\zeta_3^2 \sqrt[3]{2}$. However, neither of the latter two are in $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$, so we see that $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$; since this entirely determines ϕ , we see that the only automorphism of $\mathbb{Q}[\sqrt[3]{2}]$ is the identity, so $\text{Aut } \mathbb{Q}[\sqrt[3]{2}]$ is the trivial group.

$\mathbb{Q}[\zeta_7]$: If ϕ is an automorphism of $\mathbb{Q}[\zeta_7]$, then $\phi|_{\mathbb{Q}} = id_{\mathbb{Q}}$ and ϕ is entirely determined by where it sends ζ_7 . Now,

$$1 = \phi(1) = \phi(\zeta_7^7) = \phi(\zeta_7)^7,$$

so $\phi(\zeta_7)$ must be a seventh root of unity. Furthermore, $\phi(\zeta_7) \neq 1$, since then ϕ would not be injective. Since all other seventh roots of unity have order 7 in $\mathbb{Q}[\zeta_7]$, $\phi(\zeta_7)$ can be ζ_7^k for $1 \leq k \leq 6$. Hence, there are 6 possible distinct automorphisms of $\mathbb{Q}(\zeta_7)$; label them by $\phi_i : \zeta_7 \mapsto \zeta_7^i$. Now, if $i, j \in \{1, \dots, 6\}$, then

$$(\phi_i \circ \phi_j)(\zeta_7) = \phi_i(\zeta_7^j) = \phi_i(\zeta_7)^j = (\zeta_7^i)^j = \zeta_7^{ij}.$$

On the other hand,

$$(\phi_j \circ \phi_i)(\zeta_7) = \phi_j(\zeta_7^i) = \phi_j(\zeta_7)^i = (\zeta_7^j)^i = \zeta_7^{ij},$$

so $\phi_i \circ \phi_j = \phi_j \circ \phi_i$, so $\text{Aut } \mathbb{Q}[\zeta_7]$ is abelian. Since the only abelian group of order 6 is the cyclic group C_6 , we see that $\text{Aut } \mathbb{Q}[\zeta_7] \simeq C_6$.

$\mathbb{Q}[\zeta_8]$: Again, any automorphism ϕ of $\mathbb{Q}[\zeta_8]$ must fix \mathbb{Q} . Now,

$$1 = \phi(1) = \phi(\zeta_8^8) = \phi(\zeta_8)^8,$$

so $\phi(\zeta_8)$ is an eighth root of unity. Furthermore, $\zeta_8^k \neq 1$ if $k < 8$, so $\phi(\zeta_8) \neq \pm 1, \pm i$. Hence, $\phi(\zeta_8)$ can only be $\zeta_8, \zeta_8^3, \zeta_8^5$ or ζ_8^7 . Hence, $\text{Aut } \mathbb{Q}[\zeta_8]$ has order 4. Furthermore, if $\phi : \zeta_8 \mapsto \zeta_8^k$ for $k = 3, 5$ or 7 is a non-identity automorphism of $\mathbb{Q}[\zeta_8]$, then

$$(\phi \circ \phi)(\zeta_8) = \phi(\zeta_8^k) = \phi(\zeta_8)^k = (\zeta_8^k)^k = \zeta_8^{k^2}.$$

Since $3^2 = 9 \equiv 1 \pmod{8}$, $5^2 = 25 \equiv 1 \pmod{8}$ and $7^2 = 49 \equiv 1 \pmod{8}$, we see that all automorphisms of $\mathbb{Q}[\zeta_8]$ have order ≤ 2 . The only group of order 4 in which all elements have order ≤ 2 is $C_2 \times C_2$, so we see that $\text{Aut } \mathbb{Q}[\zeta_8] \simeq C_2 \times C_2$.

$\mathbb{Q}[\zeta_3, \sqrt[3]{2}]$: As in all these examples, if ϕ is an automorphism of $\mathbb{Q}[\zeta_3, \sqrt[3]{2}]$, then $\phi|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Now, ϕ is completely determined by what it does to ζ_3 and $\sqrt[3]{2}$. Also,

$$1 = \phi(1) = \phi(\zeta_3^3) = \phi(\zeta_3)^3,$$

so $\phi(\zeta_3) = \zeta_3$ or ζ_3^2 (since $\phi(\zeta_3) \neq 1$). Similarly,

$$2 = \phi(2) = \phi(\sqrt[3]{2^3}) = \phi(\sqrt[3]{2})^3,$$

so $\phi(\sqrt[3]{2})$ is a third root of 2. Hence, $\phi(\sqrt[3]{2}) = \sqrt[3]{2}, \zeta_3 \sqrt[3]{2}$ or $\zeta_3^2 \sqrt[3]{2}$. Since there are two possibilities for $\phi(\zeta_3)$ and 3 possibilities for $\phi(\sqrt[3]{2})$, we see there are 6 automorphisms of $\mathbb{Q}[\zeta_3, \sqrt[3]{2}]$. Now, if

$$\begin{aligned} \phi : \zeta_3 &\mapsto \zeta_3, & \phi : \sqrt[3]{2} &\mapsto \zeta_3 \sqrt[3]{2} \\ \psi : \zeta_3 &\mapsto \zeta_3^2 & \psi : \sqrt[3]{2} &\mapsto \zeta_3 \sqrt[3]{2}, \end{aligned}$$

then

$$\begin{aligned} (\phi \circ \psi)(\sqrt[3]{2}) &= \phi(\zeta_3 \sqrt[3]{2}) = \zeta_3^2 \sqrt[3]{2} \\ (\psi \circ \phi)(\sqrt[3]{2}) &= \psi(\zeta_3 \sqrt[3]{2}) = \zeta_3^3 \sqrt[3]{2} = \sqrt[3]{2} \end{aligned}$$

so we see that $\text{Aut } \mathbb{Q}[\zeta_3, \sqrt[3]{2}]$ is not abelian. Since the only non-abelian group of order 6 is $S_3 \simeq D_3$, we see that $\text{Aut } \mathbb{Q}[\zeta_3, \sqrt[3]{2}] \simeq D_3$. ♣

5

Let $K = \mathbb{Q}[\sqrt{2}]$ and $L = \mathbb{Q}[\sqrt{2 + \sqrt{2}}]$.

(a): Find the multiplicative inverse of $\sqrt{2 + \sqrt{2}}$ in L .

Answer: Consider $\alpha = \frac{1}{2} \left(4 - \sqrt{2 + \sqrt{2}}^2 \right) \in L$. Then

$$\alpha = \frac{1}{2} \left(4 - \sqrt{2 + \sqrt{2}}^2 \right) = \frac{1}{2} \left(4 - (2 + \sqrt{2}) \right) = \frac{2 - \sqrt{2}}{2}.$$

Let $\beta = \alpha \sqrt{2 + \sqrt{2}}$. Then

$$\beta = \frac{1}{2} \left(4 - \sqrt{2 + \sqrt{2}}^2 \right) \sqrt{2 + \sqrt{2}} = \frac{1}{2} \left(4\sqrt{2 + \sqrt{2}} - \sqrt{2 + \sqrt{2}}^3 \right) \in L.$$

On the other hand,

$$\beta \sqrt{2 + \sqrt{2}} = \alpha \sqrt{2 + \sqrt{2}}^2 = \frac{2 - \sqrt{2}}{2} (2 + \sqrt{2}) = \frac{4 - 2}{2} = 1,$$

so $\beta = \sqrt{2 + \sqrt{2}}^{-1}$ in L . ♣

(b): Show $K \subset L$. What is $[K : \mathbb{Q}]$? $[L : K]$? $[L : \mathbb{Q}]$?

Proof. Note that

$$\sqrt{2 + \sqrt{2}}^2 - 2 = 2 + \sqrt{2} - 2 = \sqrt{2},$$

so $\sqrt{2} \in L$. Hence, since 1 and $\sqrt{2}$ generate K and $1, \sqrt{2} \in L$, $K \subset L$. □

Answer: Since elements of K can be written as $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$, $\{1, \sqrt{2}\}$ form a basis for K as a \mathbb{Q} -vector space, so $[K : \mathbb{Q}] = 2$.

Since $\sqrt{2 + \sqrt{2}} \notin \mathbb{Q}[\sqrt{2}]$, $[L : K] \geq 2$. On the other hand,

$$\left(\sqrt{2 + \sqrt{2}}\right)^2 - (2 + \sqrt{2}) = 0,$$

so $\sqrt{2 + \sqrt{2}}$ satisfies $f(x) = x^2 - (2 + \sqrt{2}) \in K[x]$, so $[L : K] \leq 2$. Hence, $[L : K] = 2$. Therefore, we also see that

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = (2)(2) = 4.$$



(c): Let ϕ be an automorphism of L . What can you say about the restriction $\phi|_{\mathbb{Q}}$?

Answer: Since ϕ is a homomorphism, it must be the case that $\phi(1) = 1$. Now, for $\frac{p}{q} \in \mathbb{Q}$, $\frac{p}{q} = \frac{p}{q} \cdot 1$, so

$$\phi\left(\frac{p}{q}\right) = \phi\left(\frac{p}{q} \cdot 1\right) = \frac{p}{q}\phi(1) = \frac{p}{q} \cdot 1 = \frac{p}{q}.$$

Since our choice of $\frac{p}{q} \in \mathbb{Q}$ was arbitrary, we see that $\phi|_{\mathbb{Q}}$ = identity map on \mathbb{Q} .



(d): Let ϕ be an automorphism of L . What can you say about the restriction $\phi|_K$?

Answer: As above, $\phi|_{\mathbb{Q}} = id_{\mathbb{Q}}$, so $\phi|_K$ is completely determined by $\phi(\sqrt{2})$. Now, if ϕ is an automorphism of L , then

$$2 = \phi(2) = \phi(\sqrt{2}^2) = \phi(\sqrt{2})^2,$$

so $\phi(\sqrt{2}) = \pm\sqrt{2}$. Obviously, the identity automorphism maps $\sqrt{2}$ to $\sqrt{2}$, so we need only see if there is an automorphism mapping $\sqrt{2}$ to $-\sqrt{2}$. Now,

$$\phi\left(\sqrt{2 + \sqrt{2}}\right)^2 = \phi\left(\sqrt{2 + \sqrt{2}}^2\right) = \phi(2 + \sqrt{2}) = \phi(2) + \phi(\sqrt{2}) = 2 \pm \sqrt{2},$$

so we see that $\phi(\sqrt{2 + \sqrt{2}}) = \pm\sqrt{2 \pm \sqrt{2}}$. Hence, if we can show that $\sqrt{2 - \sqrt{2}} \in L$, then ϕ can map $\sqrt{2 + \sqrt{2}}$ to any of these possibilities. Now, $\frac{\sqrt{2}}{\sqrt{2 + \sqrt{2}}} \in L$, and

$$\sqrt{2} = \sqrt{4 - 2} = \sqrt{(2 + \sqrt{2})(2 - \sqrt{2})} = \sqrt{2 + \sqrt{2}}\sqrt{2 - \sqrt{2}},$$

so

$$\sqrt{2 - \sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2 + \sqrt{2}}} \in L.$$

Hence, $\phi : \sqrt{2 + \sqrt{2}} \mapsto \sqrt{2 - \sqrt{2}}$ is an automorphism of L and

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

Hence, we see that there are automorphisms of L mapping $\sqrt{2}$ to $-\sqrt{2}$.



(e): Find an element of order 4 in $\text{Aut } L$. What is the group $\text{Aut } L$ abstractly?

Answer: Let $\phi : \sqrt{2 + \sqrt{2}} \mapsto \sqrt{2 - \sqrt{2}}$ as in (d) above. Note that $\frac{\sqrt{2 + \sqrt{2}}}{\sqrt{2}} \in L$ and

$$\frac{\sqrt{2 + \sqrt{2}}}{\sqrt{2}} \sqrt{2 - \sqrt{2}} = \frac{\sqrt{(2 + \sqrt{2})(2 - \sqrt{2})}}{\sqrt{2}} = \frac{\sqrt{4 - 2}}{\sqrt{2}} = 1,$$

so $\frac{\sqrt{2 + \sqrt{2}}}{\sqrt{2}} = \sqrt{2 - \sqrt{2}}^{-1}$. Now,

$$\begin{aligned} (\phi \circ \phi)(\sqrt{2 + \sqrt{2}}) &= \phi(\sqrt{2 - \sqrt{2}}) = \phi\left(\frac{\sqrt{2}}{\sqrt{2 + \sqrt{2}}}\right) \\ &= \phi(\sqrt{2})\phi(\sqrt{2 + \sqrt{2}})^{-1} \\ &= \phi(\sqrt{2})\phi(\sqrt{2 + \sqrt{2}})^{-1} \\ &= -\sqrt{2}\sqrt{2 - \sqrt{2}}^{-1} \\ &= -\sqrt{2}\frac{\sqrt{2 + \sqrt{2}}}{\sqrt{2}} \\ &= -\sqrt{2 + \sqrt{2}}, \end{aligned}$$

so we see that ϕ has order greater than 2. Since there are 4 automorphisms of L (see (d)) above, $\text{Aut } L$ has order 4, so the order of any automorphism of L must divide 4. Since the order of ϕ is greater than 2, this implies that ϕ has order 4. Since the only group of order 4 with elements of order 4 is the cyclic group C_4 , we see that $\text{Aut } L \simeq C_4$.



(f): Replace $\sqrt{2}$ by $\sqrt{3}$ and $\sqrt{2 + \sqrt{2}}$ by $\sqrt{3 + \sqrt{3}}$. Try to redo parts (a)-(e). Do the results still hold?

Answer: Note that

$$\begin{aligned} \left(\frac{-\sqrt{3+\sqrt{3}}^3}{6} + \sqrt{3+\sqrt{3}} \right) \sqrt{3+\sqrt{3}} &= \frac{-\sqrt{3+\sqrt{3}}^4}{6} + (3+\sqrt{3}) = \frac{-(12+6\sqrt{3})}{6} + 3+\sqrt{3} \\ &= -2 - \sqrt{3} + 3 + \sqrt{3} \\ &= 1, \end{aligned}$$

$$\text{so } \sqrt{3+\sqrt{3}}^{-1} = \left(\frac{-\sqrt{3+\sqrt{3}}^3}{6} + \sqrt{3+\sqrt{3}} \right) \sqrt{3+\sqrt{3}} \in \mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right].$$

Now,

$$(\sqrt{3+\sqrt{3}})^2 - 3 = 3 + \sqrt{3} - 3 = \sqrt{3},$$

so $\mathbb{Q}[\sqrt{3}] \subset \mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right]$. Also, $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$. Furthermore, since

$$\left(\sqrt{3+\sqrt{3}} \right)^2 - (3+\sqrt{3}) = 0,$$

$\sqrt{3+\sqrt{3}}$ satisfies $g(x) = x^2 - (3+\sqrt{3}) \in \mathbb{Q}[\sqrt{3}][x]$, so

$$\left[\mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right] : \mathbb{Q}[\sqrt{3}] \right] \leq 2.$$

On the other hand, since these two fields are not equal, this degree must be at least two, so we see that $\left[\mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right] : \mathbb{Q}[\sqrt{3}] \right] = 2$, which in turn implies that

$$\left[\mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right] : \mathbb{Q} \right] = \left[\mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right] : \mathbb{Q}[\sqrt{3}] \right] [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = (2)(2) = 4.$$

If ϕ is an automorphism of $\mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right]$, then $\phi|_{\mathbb{Q}}$ must be the identity on \mathbb{Q} , by the same argument as in (c) above. As in (d),

$$3 = \phi(3) = \phi(\sqrt{3}^2) = \phi(\sqrt{3})^2,$$

so $\phi(\sqrt{3}) = \pm\sqrt{3}$. However, we claim that, in fact, $\phi(\sqrt{3}) = \sqrt{3}$, so $\phi|_{\mathbb{Q}[\sqrt{3}]} = \text{the identity on } \mathbb{Q}[\sqrt{3}]$. To see this, note that, in $\bar{\mathbb{Q}}$,

$$\sqrt{6} = \sqrt{9-3} = \sqrt{3+\sqrt{3}}\sqrt{3-\sqrt{3}},$$

so, if $\sqrt{3-\sqrt{3}} \in \mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right]$, then

$$\frac{\sqrt{6}}{\sqrt{3+\sqrt{3}}} = \sqrt{3-\sqrt{3}} \in \mathbb{Q} \left[\sqrt{3+\sqrt{3}} \right],$$

so $\sqrt{6} \in \mathbb{Q}[\sqrt{3+\sqrt{3}}]$. In turn, since $\sqrt{3}, \sqrt{3}^{-1} \in \mathbb{Q}[\sqrt{3+\sqrt{3}}]$, this would imply that

$$\frac{\sqrt{6}}{\sqrt{3}} = \sqrt{2} \in \mathbb{Q}[\sqrt{3+\sqrt{3}}].$$

Since $\sqrt{2} \notin \mathbb{Q}[\sqrt{3+\sqrt{3}}]$, we see that $\sqrt{3-\sqrt{3}} \notin \mathbb{Q}[\sqrt{3+\sqrt{3}}]$.

Now, since

$$\phi\left(\sqrt{3+\sqrt{3}}\right)^2 = \phi\left(\sqrt{3+\sqrt{3}}^2\right) = \phi(3+\sqrt{3}) = \phi(3) + \phi(\sqrt{3}) = 3 \pm \sqrt{3},$$

ϕ must map $\sqrt{3+\sqrt{3}}$ to $\pm\sqrt{3 \pm \sqrt{3}}$. Since $\pm\sqrt{3-\sqrt{3}} \notin \mathbb{Q}[\sqrt{3+\sqrt{3}}]$, we see that there are only two possible automorphisms of $\mathbb{Q}[\sqrt{3+\sqrt{3}}]$, the identity and $\sqrt{3+\sqrt{3}} \mapsto -\sqrt{3+\sqrt{3}}$. Hence, if ϕ is an automorphism of $\mathbb{Q}[\sqrt{3+\sqrt{3}}]$, then

$$\phi(\sqrt{3}) = \phi\left(\sqrt{3+\sqrt{3}}^2 - 3\right) = \phi\left(\sqrt{3+\sqrt{3}}\right)^2 - \phi(3) = \left(\pm\sqrt{3+\sqrt{3}}\right)^2 - 3 = 3 + \sqrt{3} - 3 = \sqrt{3}.$$

Hence, if ϕ is an automorphism of $\mathbb{Q}[\sqrt{3+\sqrt{3}}]$, $\phi|_{\mathbb{Q}[\sqrt{3}]}$ = the identity on $\mathbb{Q}[\sqrt{3}]$.

Furthermore, since there are only two automorphisms of $\mathbb{Q}[\sqrt{3+\sqrt{3}}]$, $\text{Aut } \mathbb{Q}[\sqrt{3+\sqrt{3}}] \simeq C_2$, the cyclic group of order 2, so there are no automorphisms of order 4.



6

Find all algebraic field extensions of \mathbb{R} . Justify your assertions.

Answer: Suppose K is an algebraic field extension of \mathbb{R} . Then, since \mathbb{C} is an algebraic field extension of \mathbb{R} that is algebraically closed, $K \subset \mathbb{C}$. Now, $\mathbb{C} = \mathbb{R}[i]$ is an extension of degree 2 over \mathbb{R} , since $\{1, i\}$ is a basis for \mathbb{C} over \mathbb{R} (since every element of \mathbb{C} can be written in the form $a + bi$ for $a, b \in \mathbb{R}$). On the other hand, since $\mathbb{R} \subset K \subset \mathbb{C}$,

$$2 = [\mathbb{C} : \mathbb{R}] = [\mathbb{C} : K][K : \mathbb{R}],$$

so $[K : \mathbb{R}] = 1$ or 2 . If $[K : \mathbb{R}] = 1$, then $K = \mathbb{R}$. On the other hand, if $[K : \mathbb{R}] = 2$, then $[\mathbb{C} : K] = 1$, so $\mathbb{C} = K$. Hence, the only algebraic field extensions of \mathbb{R} are \mathbb{R} and \mathbb{C} .



7

Let K be a field with algebraic closure \bar{K} . Let $K^s = \{a \in \bar{K} \mid a \text{ is separable over } K\}$.

(a): Show that K^s is a subfield of \bar{K} .

Proof. Suppose $a, b \in K^s$. Then, since a is separable over K , $K[a]$ is separable over K . Since b is separable over K , the minimal polynomial of b over K has distinct roots. Now, the minimal polynomial of b over $K[a]$ divides the minimal polynomial of b over K , so it also has distinct roots and hence is separable. Thus, b is separable over $K[a]$, so

$$K[a, b] = K[a][b]$$

is separable over $K[a]$. Therefore, since $K[a, b]$ is separable over $K[a]$ and $K[a]$ is separable over K , $K[a, b]$ is separable over K . Now, $a + b, ab \in K[a, b]$, so $a + b, ab$ are separable over K and, hence, $a + b, ab \in K^s$. Since our choices of a and b were arbitrary, we see that K^s is closed under addition and multiplication.

Furthermore, if $a \in K^s$, then $K[a]$ is separable over K . Since $K[a]$ is algebraic over K , $a^{-1} \in K[a]$, and so a^{-1} is separable over K , meaning that $a^{-1} \in K^s$. Since our choice of a was arbitrary, we see that every element of K^s has an inverse in K^s . Therefore, since K^s is closed under addition and multiplication, contains inverses of each element, and inherits associativity, commutativity and distributivity from \bar{K} , we see that K^s is a subfield of \bar{K} . \square

(b): Show that for every separable polynomial $f(x) \in K[x]$, the field K^s contains a root of f , and $f(x)$ factors over K^s as the product of linear factors.

Proof. Suppose $f(x) \in K[x]$ is separable. Then f splits in $\bar{K}[x]$ as

$$f(x) = (x - a_1) \cdots (x - a_n)$$

for distinct $a_i \in \bar{K}$. Now, for each $i = 1, \dots, n$, the minimal polynomial $m_i(x)$ of a_i must divide $f(x)$, so $m_i(x)$ also has distinct roots and, therefore, is separable. Hence, each a_i is separable over K , so $a_i \in K^s$ for all $i = 1, \dots, n$. Therefore, $f(x)$ splits in $K^s[x]$ as

$$f(x) = (x - a_1) \cdots (x - a_n) \in K^s[x].$$

 \square

(c): Show that K^s is normal over K .

Proof. Suppose $a \in K^s$. Then the minimal polynomial $m(x)$ of a is separable over K . By part (b) above, this implies that m splits in $K^s[x]$. Since our choice of a was arbitrary, we see that the minimal polynomials of all elements of K^s split over K^s , so K^s is normal over K . \square

DRL 3E3A, UNIVERSITY OF PENNSYLVANIA
E-mail address: `shonkwil@math.upenn.edu`