Q1 Problem 14.2.15 (*Biquadratic Extensions*) Let F be a field of characteristic $\neq 2$.

In particular, $\operatorname{char} F \neq 2$ implies that $2 = 1_F + 1_F \in F^\times$; this fact will be used implicitly in the following proofs.

(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, or 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. Since K is a splitting field for the separable polynomial $(x^2 - D_1)(x^2 - D_2) \in F[x]$, then K/F is a Galois extension. An automorphism of $K = F(\sqrt{D_1}, \sqrt{D_2})$ fixing F (i.e., an element of $\mathrm{Gal}(K/F)$) is completely determined by the images of $\sqrt{D_1}$ and $\sqrt{D_2}$. Moreover, each must map to a root of its minimal polynomial over F, i.e.,

$$\sqrt{D_1} \mapsto \pm\sqrt{D_1} \quad \text{and} \quad \sqrt{D_2} \mapsto \pm\sqrt{D_2}.$$

There are four such maps, namely $\mathrm{id}_K, \sigma, \tau, \sigma\tau$, where σ and τ are maps from K to itself defined by

$$\sigma : \begin{cases} \sqrt{D_1} \mapsto -\sqrt{D_1}, \\ \sqrt{D_2} \mapsto \sqrt{D_2}, \end{cases} \qquad \text{and} \quad \tau : \begin{cases} \sqrt{D_1} \mapsto \sqrt{D_1}, \\ \sqrt{D_2} \mapsto -\sqrt{D_2}. \end{cases}$$

We will show that there are four distinct elements of $\mathrm{Gal}(K/F)$, proving that the above four maps are in fact automorphisms of K fixing F.

Since K/F is Galois,

$$|\,\mathrm{Gal}(K/F)| = [K : F] = [K : F(\sqrt{D_1})][F(\sqrt{D_1}) : F] = [K : F(\sqrt{D_1})] \cdot 2.$$

We claim that $[K : F(\sqrt{D_1})] = 2$, and will prove this by showing that the minimal polynomial of $\sqrt{D_2}$ over $F(\sqrt{D_1})$ is the same as the minimal polynomial over F, i.e.,

$$m_{\sqrt{D_2}, F(\sqrt{D_1})}(x) = m_{\sqrt{D_2}, F}(x) = x^2 - D_2.$$

Since the minimal polynomial over $F(\sqrt{D_1})$ divides $x^2 - D_2$, it suffices to show that $\sqrt{D_2} \notin F(\sqrt{D_1})$. Suppose to the contrary that D_2 is the square of some $a + b\sqrt{D_1} \in F(\sqrt{D_1})$ for $a, b \in F$, then

$$D_2 = (a + b\sqrt{D_1})^2 = a^2 + 2ab\sqrt{D_1} + b^2 D_1.$$

It cannot be the case that $a = 0$; otherwise $D_2 = b^2 D_1$, implying that

$$D_1 D_2 = D_1(b^2 D_1) = (bD_1)^2$$

is a square in F, which is false by assumption. Similarly, it cannot be the case that $b = 0$; otherwise $D_2 = a^2$ is a square in F. Therefore, with $a, b, D_2 \in F$ nonzero, we find that

$$\sqrt{D_1} = \frac{D_2 - a^2 - b^2 D_2}{2ab} \in F,$$

which is a contradiction. Hence, $\sqrt{D_2} \notin F(\sqrt{D_1})$, so indeed

$$|\operatorname{Gal}(K/F)| = [K : F(\sqrt{D_1})] \cdot 2 = 4.$$

From this, we deduce that $\operatorname{Gal}(K/F) = \{\mathrm{id}_K, \sigma, \tau, \sigma\tau\}$, where σ and τ are as above. There is now an obvious isomorphism

$$\begin{aligned} \operatorname{Gal}(K/F) &\xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \sigma &\mapsto (1, 0) \\ \tau &\mapsto (0, 1). \end{aligned}$$

That is, $\operatorname{Gal}(K/F)$ is isomorphic to the Klein 4-group.

□

(b) Conversely, suppose that K/F is a Galois extension with $\operatorname{Gal}(K/F)$ 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, or D_1D_2 is a square in F.

Lemma 1. If L/F is a field extension with $[L : F] = 2$, then $L = F(\sqrt{D})$ for some $D \in F$ such that $m_{\sqrt{D},F} = x^2 - D \in F[x]$.

Proof. For any element $\alpha \in L \setminus F$, the degree of the minimal polynomial of α over F must divide $[L : F] = 2$, snd since $\alpha \notin F$, then the degree must be exactly 2. Then

$$m_{\alpha,F}(x) = x^2 + bx + c \in F[x],$$

which we can rewrite to be

$$\left(x + \tfrac{b}{2}\right)^2 - \left(\tfrac{b^2}{4} - c\right) \in F[x].$$

Define $D = \frac{b^2}{4} - c \in F$, then

$$D = \left(\alpha + \tfrac{b}{2}\right)^2.$$

Naturally, we define $\sqrt{D} = \alpha + \frac{b}{2}$, which is an element of L, but not of F, with

$$m_{\sqrt{D},F} = x^2 - D \in F[x].$$

The fact that $x^2 - D$ is irreducible in $F[x]$ can be seen by that fact that its roots are precisely $\pm\sqrt{D} \notin F$. Since $F(\sqrt{D})/F$ is a subextension of L/F of degree 2, and $[L : F] = 2$, then we must have $L = F(\sqrt{D})$.

□

Denote by Z_2 the cyclic group of 2 elements: $\mathbb{Z}/2\mathbb{Z}$. We now prove the main result.

Proof. Given that $\mathrm{Gal}(K/F)$ is isomorphic to the Klein 4-group ($Z_2 \times Z_2$), then there is a normal subgroup $H \trianglelefteq \mathrm{Gal}(K/F)$ isomorphic to Z_2 (explicitly, we could take $H \cong Z_2 \times \{0\}$, under the same isomorphism which gives us $\mathrm{Gal}(K/F) \cong Z_2 \times Z_2$). By the fundamental theorem of Galois theory, this corresponds to a Galois extension K^H/F, where K^H is the subfield of K fixed by H. Then

$$\mathrm{Gal}(K^H/F) \cong \mathrm{Gal}(K/F)/H \cong (Z_2 \times Z_2)/(Z_2 \times \{0\}) \cong Z_2,$$

from which we deduce that

$$[K^H : F] = |\,\mathrm{Gal}(K^H/F)| = |Z_2| = 2.$$

By Lemma 1, $K^H = F(\sqrt{D_1})$ for some $D_1 \in F$. In particular, D_1 is not a square in F, since the only roots of $m_{\sqrt{D_1},F}(x) = x^2 - D_1$ are $\pm\sqrt{D_1} \notin F$.

Since we also have

$$[K : K^H] = |H| = |Z_2 \times \{0\}| = 2,$$

then, by Lemma 1, $K = K^H(\sqrt{\beta})$ for some $\beta \in K^H$ such that $m_{\sqrt{\beta},K^H}(x) = x^2 - \beta \in K^H[x]$. Since $K^H = F(\sqrt{D_1})$, then $\beta = a + b\sqrt{D_1}$ for some $a, b \in F$. We now write

$$m_{\sqrt{\beta},K^H}(x) = \left(x - \tfrac{b}{2}\sqrt{D_1}\right)^2 - \left(\tfrac{b^2}{4}D_1 - a\right).$$

Define $D_2 = \frac{b^2}{4}D_1 - a \in F$, then

$$D_2 = \left(\sqrt{\beta} - \tfrac{b}{2}\sqrt{D_1}\right)^2.$$

Naturally, we define $\sqrt{D_2} = \sqrt{\beta} - \frac{b}{2}\sqrt{D_1}$, which is an element of K, but not $K^H \supseteq F$, with

$$m_{\sqrt{D_2},K^H}(x) = x^2 - D_2 \in F[x].$$

The fact that $x^2 - D_2$ is irreducible in $K^H[x]$ follows from the fact that its only roots are $\pm\sqrt{D_2} \notin K^H$. In particular, D_2 is not a square in F. Since $K^H(\sqrt{D_2})/K^H$ is a degree 2 subextension of K/K^H and $[K : K^H] = 2$, then we must have

$$K = K^H(\sqrt{D_2}) = F(\sqrt{D_1}, \sqrt{D_2}).$$

It remains to show that D_1D_2 is not a square in F. The the only roots of $x^2 - D_1D_2 \in F[x]$ are $\pm\sqrt{D_1}\sqrt{D_2} \in K$. If it were the case that $\sqrt{D_1}\sqrt{D_2} = a$ for some $a \in F$, then we would have

$$\sqrt{D_2} = (\sqrt{D_1})^{-1}a \in F(\sqrt{D_1}) = K^H,$$

which is not the case. Hence, neither D_1, D_2, nor D_1D_2 is a square in F.

$\square$

Q2 Let K/F be a separable finite extension. Show that K has finitely many subfields containing F.

Proof. Fix an algebraic closure $\overline{F} = \overline{K}$ of F containing K. Since K/F is a finite extension, then $K = F(\alpha_1, \ldots, \alpha_n)$ for some algebraic elements $\alpha_1, \ldots, \alpha_n \in K$. Define $S \subseteq \overline{F}$ to be the set of all roots in $\overline{F}$ of the minimal polynomials $m_{\alpha_j,F}(x)$ for $j = 1, \ldots, n$. Since K is separable, $F(S)$ is a Galois closure of K over F. In particular, S is a finite set, so

$$[F(S) : F] = |\operatorname{Gal}(F(S)/F)|$$

is finite. Therefore, $\operatorname{Gal}(F(S)/F)$ has finitely many subgroups.

Every subfield of K containing F is a subextension of $F(S)/F$, so there are at least as many subextensions of $F(S)/F$ as there are subfields of K containing F. Since the subextensions of $F(S)/F$ correspond bijectively (by the fundamental theorem of Galois theory) to the subgroups of $\operatorname{Gal}(F(S)/F)$, then there are finitely many subextensions of $F(S)/F$. Hence, there are finitely many subfields of K containing F.

$\square$

Q3 Let K be the Galois closure of $\mathbb{Q}(\sqrt{1+\sqrt{3}})$.

(a) Show that $[K:\mathbb{Q}] = 8$.

Proof. The polynomial $f(x) = x^4 - 2x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, by Eisenstein's criterion, and has $\sqrt{1+\sqrt{3}}$ as a root; so $f(x)$ is the minimal polynomial of $\sqrt{1+\sqrt{3}}$ over $\mathbb{Q}$. Note that $f(x)$ is indeed separable, with the four distinct roots $\pm\sqrt{1\pm\sqrt{3}} \in \overline{\mathbb{Q}}$, so the definition of K as a Galois closure over $\mathbb{Q}$ makes sense.

We now consider the field $F = \mathbb{Q}(\sqrt{3})$ and define $D_1 = 1+\sqrt{3}$ and $D_2 = 1-\sqrt{3}$, which are elements of F. It can be seen that F is a subfield of K containing $\mathbb{Q}$, so K/F is a Galois extension with

$$K = \mathbb{Q}(\pm\sqrt{D_1}, \pm\sqrt{D_2}) = F(\sqrt{D_1}, \sqrt{D_2}).$$

In order to apply Q1(a), we must check that none of D_1, D_2, or D_1D_2 are squares in F. For any $a + b\sqrt{3} \in F$, we have

$$(a+b\sqrt{3})^2 = a^2 + 2ab\sqrt{3} + b^2 3 = (a^2+3b^2) + 2ab\sqrt{3}.$$

One can check that no values of $a, b \in \mathbb{Q}$ will yield D_1, D_2, or D_1D_2.

Applying Q1(a), we find $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so

$$[K:F] = |\,\mathrm{Gal}(K/F)| = |\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4.$$

Recall that $F = \mathbb{Q}(\sqrt{3})$, and we have seen that $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2$. Then

$$[K:Q] = [K:F][F:\mathbb{Q}] = 4 \cdot 2 = 8.$$

□

(b) Show that $\mathrm{Gal}(K/\mathbb{Q})$ is not commutative.

This proof uses the result of (d), the proof of which does not rely on this result.

Proof. From (d), $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$, and we know that the dihedral group D_{2n} is non-abelian for $n \geq 3$. In particular, $sr = r^{n-1}s \neq rs$ when $n \geq 3$. Where $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ as in (d), we can say more specifically that $\sigma\tau = \tau^3\sigma \neq \tau\sigma$. Hence, $\mathrm{Gal}(K/\mathbb{Q})$ is non-abelian.

□

(c) Show that $\mathrm{Gal}(K/\mathbb{Q})$ has a normal subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. As in part (a), we have $F = \mathbb{Q}(\sqrt{3})$, so $F/\mathbb{Q}$ is a Galois extension (as the splitting field of the separable polynomial x^2-3). In particular, $F/\mathbb{Q}$ is a Galois subextension of the Galois extension $K/\mathbb{Q}$; the fundamental theorem of Galois theory implies $\mathrm{Gal}(K/F) \trianglelefteq \mathrm{Gal}(K/\mathbb{Q})$. And, from part (a), we know that $\mathrm{Gal}(K/F)$ is isomorphic to the Klein 4-group.

□

(d) Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_8$.

Proof. We will use the fact that $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 8$ to characterize the elements of $\mathrm{Gal}(K/\mathbb{Q})$. Any automorphism of K fixing $\mathbb{Q}$ is completely determined by the images of

$$\sqrt{D_1} = \sqrt{1+\sqrt{3}} \quad \text{and} \quad \sqrt{D_2} = \sqrt{1-\sqrt{3}}.$$

Moreover, such an automorphism must permute the roots of irreducible polynomials in $\mathbb{Q}[x]$; in particular $x^4 - 2x^2 - 2$, which has the four roots $\pm\sqrt{D_1}, \pm\sqrt{D_2}$.

Given $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we know that $\sigma(-\alpha) = -\sigma(\alpha)$ for all $\alpha \in K$. From the fact that $\sqrt{D_2} \neq \pm\sqrt{D_1}$, it follows that $\sigma(\sqrt{D_2}) \neq \pm\sigma(\sqrt{D_1})$. In other words,

$$\begin{aligned} \sigma : \sqrt{D_1} \mapsto \pm\sqrt{D_1} \quad &\Longrightarrow \quad \sigma : \sqrt{D_2} \mapsto \pm\sqrt{D_2}, \\ \sigma : \sqrt{D_1} \mapsto \pm\sqrt{D_2} \quad &\Longrightarrow \quad \sigma : \sqrt{D_2} \mapsto \pm\sqrt{D_1}. \end{aligned}$$

This means that σ can map $\sqrt{D_1}$ to any of the four options $\pm\sqrt{D_1}, \pm\sqrt{D_2}$, which determines the image of $-\sqrt{D_1}$. Once the images of $\pm\sqrt{D_1}$ is determined, σ must map $\sqrt{D_2}$ to one of the two remaining options, which then determines the whole of sigma.

From this, we deduce that there are eight possible automorphisms of K fixing $\mathbb{Q}$ which permute the roots of $x^4 - 2x - 2$. Since $|\mathrm{Gal}(K/\mathbb{Q})| = 8$, then $\mathrm{Gal}(K/\mathbb{Q})$ is precisely the set of all those eight possible maps described in the previous paragraph. Define the following automorphism of K fixing $\mathbb{Q}$:

$$\sigma : \begin{cases} \sqrt{D_1} \mapsto \sqrt{D_2}, \\ \sqrt{D_2} \mapsto \sqrt{D_1}. \end{cases} \qquad \text{and} \quad \tau : \begin{cases} \sqrt{D_1} \mapsto \sqrt{D_2}, \\ \sqrt{D_2} \mapsto -\sqrt{D_1}. \end{cases}$$

One can check that $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$, i.e., all possible automorphisms of K fixing $\mathbb{Q}$ can be written as a composition of finitely many copies of σ and τ. Moreover, it can be seen that $\tau^4 = \sigma^2 = (\sigma\tau)^2 = \mathrm{id}_K$, which suggests a natural choice of isomorphism

$$\begin{aligned} \mathrm{Gal}(K/\mathbb{Q}) &\xrightarrow{\sim} D_8 \\ \sigma &\mapsto s \\ \tau &\mapsto r. \end{aligned}$$

□

Q4 Show that if $K/\mathbb{Q}$ is a finite Galois extension with $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$, then K is the splitting field for some irreducible cubic polynomial in $\mathbb{Q}[x]$.

Proof. Representing S_3 as the set of permutations on three elements, we have

$$S_3 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}.$$

Let $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ correspond to $(1\,2\,3), (1\,2) \in S_3$, respectively, under some fixed isomorphism of $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$. Then $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$, and $\langle \sigma \rangle$ is the only normal subgroup. We consider the non-normal subgroup $\langle \tau \rangle = \{\mathrm{id}_K, \tau\}$, and the corresponding fixed field $K^{\langle \tau \rangle}$. Since $K^{\langle \tau \rangle}$ is a subfield of K containing $\mathbb{Q}$, then $K^{\langle \tau \rangle}/\mathbb{Q}$ is a non-Galois subextension of $K/\mathbb{Q}$; in particular, $K^{\langle \tau \rangle}/\mathbb{Q}$ is separable but not normal.

We see that $K^{\langle \tau \rangle}/\mathbb{Q}$ is a finite extension and compute its degree to be

$$[K^{\langle \tau \rangle} : \mathbb{Q}] = \frac{[K : \mathbb{Q}]}{[K : K^{\langle \tau \rangle}]} = \frac{|\mathrm{Gal}(K/\mathbb{Q})|}{|\langle \tau \rangle|} = \frac{|S_3|}{2} = \frac{6}{2} = 3.$$

As a finite separable extension, the primitive element theorem implies that $K^{\langle \tau \rangle} = \mathbb{Q}(\alpha)$ for some $\alpha \in K^{\langle \tau \rangle}$. Then

$$\deg m_{\alpha,\mathbb{Q}}(x) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [K^{\langle \tau \rangle} : \mathbb{Q}] = 3,$$

which means that $m_{\alpha,\mathbb{Q}}(x)$ is an irreducible cubic polynomial in $\mathbb{Q}[x]$. Since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a separable non-normal extension, then $m_{\alpha,\mathbb{Q}}(x)$ is separable but does not split over $\mathbb{Q}(\alpha)$. However, $m_{\alpha,\mathbb{Q}}(x)$ does split in $K[x]$ (because $K/\mathbb{Q}$ is Galois), so there is a splitting field of $m_{\alpha,\mathbb{Q}}(x)$ which is a subfield of K strictly containing $\mathbb{Q}(\alpha)$.

If E is a subfield of K containing $\mathbb{Q}(\alpha)$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ must divide $[E : \mathbb{Q}]$ which, in turn, must divide $[K : \mathbb{Q}] = 6$. Therefore, $[E : \mathbb{Q}]$ must be either 3, in which case $E = \mathbb{Q}(\alpha)$, or 6, in which case $E = K$.

Since the splitting field of $m_{\alpha,\mathbb{Q}}(x)$ is a subfield of K strictly containing $\mathbb{Q}(\alpha)$ (i.e., $\neq \mathbb{Q}(\alpha)$), we conclude that K is the splitting field of the irreducible cubic polynomial $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$.

$\square$