Allman feedback

Homework #6

Dummit and Foote Selected Exercises

§14.1 #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 $\sigma a < \sigma b$ for every $a, b \in \mathbb{R}$.

Proof. Suppose $a \in \mathbb{R}$, $a = b^2$ for some $b \in \mathbb{R}$. Then $\sigma a = \sigma b^2 = (\sigma b)^2$, so σ takes squares to squares. ✓ Moreover, if $a \in \mathbb{R}$, $a > 0$, then a is a square. Since σa is also a square, and all squares are positive, we have that $\sigma a > 0$, and σ takes positive reals to positive reals. ✓

Suppose $a < b$. Then there exists a rational u with $a < u < b$. Thus, we have that $u = \sigma u = \sigma(u - a + a) = \sigma(u - a) + \sigma a > \sigma a$, by properties of automorphisms and the fact that $u - a > 0$, so $\sigma(u - a) > 0$. Thus, $\sigma a < u$. Similarly, $u < \sigma b$, so $\sigma a < u < \sigma b$, and $\sigma a < \sigma b$. ✓ □

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

Proof. Note that $\sigma(\frac{1}{m}) = \frac{1}{m}$, because σ fixes $\mathbb{Q}$. Thus, by part (a), if $-\frac{1}{m} < a - b < \frac{1}{m}$, then $-\frac{1}{m} < \sigma a - \sigma b < \frac{1}{m}$. ✓

Choose $x_0 \in \mathbb{R}$ and let $\varepsilon > 0$. Then choose a positive integer m such that $\frac{1}{m} < \varepsilon$ and let $\delta = \frac{1}{m}$. If $|x - x_0| < \delta$, then since $\delta = \frac{1}{m}$, $|\sigma x - \sigma x_0| < \delta < \varepsilon$, so σ is a continuous map. □ Nice.

(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. Choose $a \in \mathbb{R}$ and suppose σ is a continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$. Let $\varepsilon > 0$. By the continuity of σ, there exists a $\delta > 0$ (and we can choose $\delta < \varepsilon$) such that if $|x - a| < \delta$, then $|\sigma x - \sigma a| < \varepsilon$. Because $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists some rational q such that $|q - a| < \delta$. ✓ Because σ fixes $\mathbb{Q}$, we have that $|q - \sigma a| < \varepsilon$, so by the triangle inequality, $|a - \sigma a| < 2\varepsilon$. However, we can choose ε to be arbitrarily small, so $\sigma a = a$, and σ is the identity map. Thus $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$. Good. □ ✓

§14.1 #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 $a, b, c, d \in k$, $ad - bc \neq 0$ (so $f(t) \in k(t)$ maps to $f\left(\frac{at+b}{ct+d}\right)$).

Proof. Suppose σ is some automorphism of $k(t)$. Then σ is entirely determined by its action on t, and t must map to some element of $k(t)$ not in k. That is $t \mapsto \frac{P(t)}{Q(t)}$ for some P, Q in $k[t]$ with P and Q relatively prime, not both constant.

By exercise #18 from §13.2, we have that if $x = \frac{P(t)}{Q(t)}$, then $[k(t) : k(x)] = \max\{\deg(P), \deg(Q)\}$. For σ to be an automorphism, we must have that $[k(t) : k(x)] = 1$, so both P and Q must be at most degree one. ✓ Moreover, to ensure that $x \notin k$, we require that $P = at + b$ is not a k-multiple of $Q = ct + d$. That is, $at + b \neq r(ct + d)$. To ensure this, we require $ad - bc \neq 0$, which gives us precisely the fractional linear transformations. ✓

Conversely, suppose we define a map σ defined by $t \mapsto \frac{at+b}{ct+d}$, $ad - bc \neq 0$. Then note that this map fixes k, and naturally respects the group operations. Moreover, the map $t \mapsto \frac{-dt+b}{ct-a}$ is a well-defined inverse for σ, so σ is a bijection. Thus, it is an automorphism, and every fractional linear transformation defines an automorphism of $k(t)$ fixing k. ✓ □

Good.

§14.1 #9 Determine the fixed field of the automorphism $t \mapsto t + 1$ of $k(t)$.

Solution: Suppose k is characteristic 0. By the previous problem, as σ defined by $t \mapsto t + 1$ is a fractional linear transformation, σ fixes at least k. Suppose to produce a contradiction that $\frac{P(t)}{Q(t)} = \frac{P(t+1)}{Q(t+1)}$ for all $P, Q \in k[t]$ with P, Q relatively prime, P, Q not both constant.

Then if P has degree n, $\frac{P(t)}{Q(t)}$ has precisely n zeros at the n zeros of P. Similarly, if Q has degree m, then $\frac{P(t)}{Q(t)}$ has precisely m poles at the zeros of Q. We know that P and Q must not share any zeros, as they are relatively prime. Because $\frac{P(t)}{Q(t)} = \frac{P(t+1)}{Q(t+1)}$, they must have the same zeros and poles.

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the n zeros of $P(t)$. Then $\alpha_1 + 1, \alpha_2 + 1, \dots, \alpha_n + 1$ are the n zeros of $P(t+1)$. However, because $\frac{P(t)}{Q(t)}$ and $\frac{P(t+1)}{Q(t+1)}$ have the same zeros, there must be a bijection between the n roots of $P(t)$ and the n roots of $P(t+1)$.

Cycle of length ℓ.

That is, the $\alpha_i + 1$ are a permutation of the α_i; $\alpha_1 = \alpha_{n_1} + 1$, then $\alpha_{n_1} = \alpha_{n_2} + 1$, etc. However, because this is a permuation of a finite number of elements, we must have cycles. That is, there exists an ℓ such that $\alpha_{n_\ell} = \alpha_1 + 1$. Thus, substituting in, we have that $\alpha_{n_\ell} = \underline{\overset{\downarrow}{\alpha_{n_\ell}}} + 2$. Continuing in this mode, we find that $\alpha_{n_\ell} = \alpha_{n_\ell} + (\ell + 1)$. However, because k is a field of characteristic 0, this is a contradiction.

typo: $\alpha_{n_i} + 1$ ↑

Nice. →

Therefore, σ does not fix any elements of $k(t)$ other than k, so the fixed field is precisely k. ✓

§14.1 #10 Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\mathrm{Aut}(K/F) \to \mathrm{Aut}(K'/F')$.

How about this?: Let α be a root of $P(t)$. Then $P(\alpha) = P(\alpha+1) = 0$, and $\alpha+1$ is also a root of $P(t)$. By induction, $\alpha+n$ is a root of $P(t)$ for all $n \in \mathbb{Z}^+$. Since k has characteristic zero, this contradicts that $P(t)$ has only a finite number of roots.

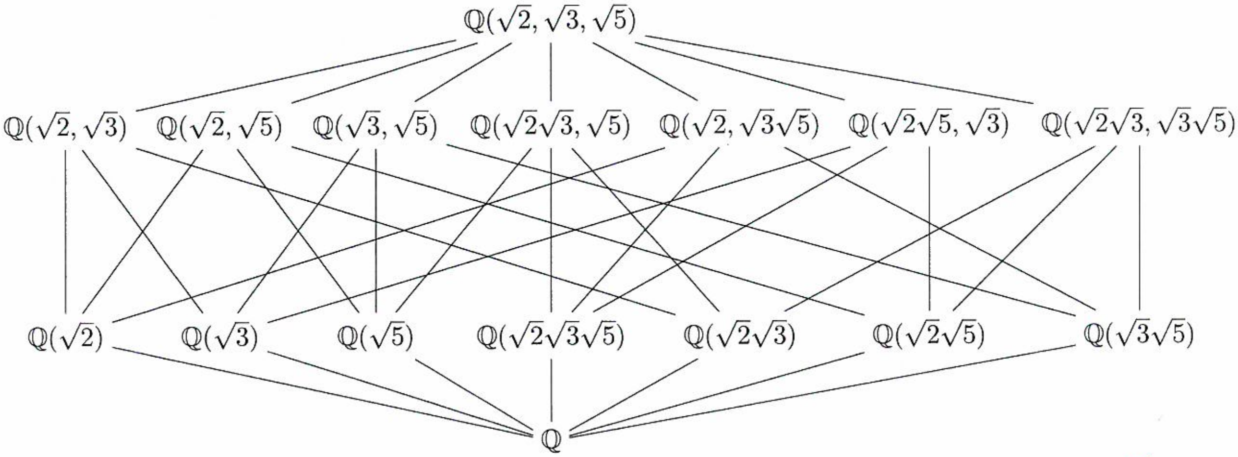
Proof. Let f be the map $\sigma \mapsto \varphi\sigma\varphi^{-1}$. Choose some $\sigma \in \text{Aut}(K/F)$. Then $f(\sigma)$ ~~as~~ is the composition of three bijections, $f(\sigma)$ is itself a bijection. Moreover, as φ and σ are homomorphisms, $f(\sigma)$ is also a homomorphism. Thus, $f(\sigma)$ is an element ~~isomorphism~~ of $\text{Aut}(K'/F')$.

Now, observe that f has a natural inverse: $f^{-1}(\gamma) = \varphi^{-1}\gamma\varphi$ for $\gamma \in \text{Aut}(K'/F')$. This inverse is well-defined, so f is a bijection. Moreover, for $\alpha, \sigma \in \text{Aut}(K/F)$, we have that $f(\alpha\sigma) = \varphi\alpha\sigma\varphi^{-1} = (\varphi\alpha\varphi^{-1})(\varphi\sigma\varphi^{-1}) = f(\alpha)f(\sigma)$. Thus, f is a bijective group homomorphism between $\text{Aut}(K/F)$ and $\text{Aut}(K'/F')$, and is a group isomorphism. □ ✓

§14.2 #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.

Solution: The Galois extension of $(x^2-2)(x^2-3)(x^2-5)$ is $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. Because $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt{5}) = \mathbb{Q}$, and because the Galois groups of $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(\sqrt{5})$ are all C_2, we have that the Galois group of $(x^2-2)(x^2-3)(x^2-5)$ is $C_2 \times C_2 \times C_2$. There are 14 distinct, non-trivial subgroups of C_2^3, and each of them corresponds to a subfield of the splitting field of $(x^2-2)(x^2-3)(x^2-5)$. The subfield lattice is shown below.

by what we proved in class! →



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

Figure 1: Subfield lattice for the splitting field of $(x^2-2)(x^2-3)(x^2-5)$ ✓

§14.2 #7 Determine all the subfields of the splitting field of x^8-2 which are Galois over $\mathbb{Q}$.

Solution: The subfields of the splitting field of x^8-2 which are Galois over $\mathbb{Q}$ are those corresponding under the Fundamental Theorem of Galois Theory to the normal subgroups of the semidihedral group on 16 elements, SD_{16}. The normal subgroups are $\langle\sigma^4\rangle$, $\langle\sigma^2\rangle$, $\langle\sigma\rangle$, $\langle\sigma^2,\tau\rangle$, and $\langle\sigma^2,\tau\sigma^3\rangle$. The corresponding subfields are, respectively, $\mathbb{Q}(i,\sqrt[4]{2})$, $\mathbb{Q}(i,\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$. ✓

↑

I mentioned the splitting field of x^8-2 over $\mathbb{Q}$ too.

★★★ §14.2 #8 Suppose K is a Galois extension of F of degree p^n for some prime p and some $n \geq 1$. Show there are Galois extensions of F contained in K of degrees p and p^{n-1}.

Proof. Because K is Galois, it has Galois group G of order p^n. Because G is a p-group, it has a subgroup, H, of order p^{n-1}. Moreover, because $[G : H] = p$, which is the smallest prime dividing $p^n = |G|$, we know that H is normal in G. Thus, the corresponding field extension of F with degree $\cancel{p^{n-1}}$ is Galois. degree $= p$

By the class equation, G must have non-trivial center. Thus, by Cauchy's theorem, there exists an element $x \in Z(G)$ with order precisely p. Then $\langle x \rangle$ is a normal subgroup of G (as it is a subgroup of $Z(G)$) with order p, and there exists a corresponding field extension of F with degree $\cancel{p}$ that is Galois. □

degree $= p^{n-1}$

14.2.11 Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field has Galois group S_4 over $\mathbb{Q}$ (there are many such quartics, cf. Section 6). Let θ be a root of $f(x)$ and set $K = \mathbb{Q}(\theta)$. Prove that K is an extension of $\mathbb{Q}$ of degree 4 and has no proper subfields. Are there any Galois extensions of $\mathbb{Q}$ of degree 4 with no proper subfields?

Proof. (Thomas) Note that since $f(x)$ is irreducible, for any root θ of $f(x)$ we know $\mathbb{Q}(\theta)$ =deg$(f(x)) = 4$. Let H be the subgroup of G =Gal$(f(x)/\mathbb{Q})$ associated with $\mathbb{Q}(\theta)/\mathbb{Q}$ and note that $[G : H] = 4$ so $|H| = 6$. We then immediately note that $H = S_3$ and since S_3 contains odd permutations, A_4 does not contain H. It then follows that there is no subfield of degree 2 of any subfield of degree 4 in $f(x)/\mathbb{Q}$.

Yes. Say more. Are you using that A_4 is the unique subgroup of S_4 of index 2??

Suppose for contradiction there is a Galois extension $K/\mathbb{Q}$ of degree 4 with no proper subfields. Since $K/\mathbb{Q}$ is Galois of degree 4, it follows that $|\text{Gal}(K/\mathbb{Q})| = 4$. Since the only groups of order 4 are abelian, each have subgroups of order 2 and consequently $K/\mathbb{Q}$ has proper subfields. ✓ □

14.2.12 Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^4 - 14x^2 + 9$.

✓ why? Prove this.

Proof. (Thomas) Note that $x^4 - 14x^2 + 9$ is irreducible over $\mathbb{Z}/7\mathbb{Z}$ and thus is irreducible over $\mathbb{Z}$ and thus $\mathbb{Q}$. Further note that by a double application of the quadratic formula we see that the roots of $x^4 - 14x^2 + 9$ are $\pm\sqrt{7 \pm 2\sqrt{10}}$. Yes! → Then the splitting field of $x^4 - 14x^2 + 9$ is $\mathbb{Q}(\sqrt{7 + 2\sqrt{10}}, \sqrt{7 - 2\sqrt{10}})$. Noting that $\sqrt{7 + 2\sqrt{10}}\sqrt{7 - 2\sqrt{10}} = \sqrt{7^2 - 4(10)} = 3$ ✓ we see that $\sqrt{7 + 2\sqrt{10}} = \frac{3}{\sqrt{7 - 2\sqrt{10}}}$ so $\sqrt{7 + 2\sqrt{10}} \in \mathbb{Q}(\sqrt{7 + 2\sqrt{10}})$. ignore Then we see that the splitting field of $x^4 - 14x^2 + 9$ is $\mathbb{Q}(\sqrt{7 + 2\sqrt{10}})$ which has degree 4 since $x^4 - 14x^2 + 9$ is irreducible. Let G be the Galois group of $\mathbb{Q}(\sqrt{7 + 2\sqrt{10}})/\mathbb{Q}$. Note that the

Okay ★

language choice:

permute

elements of G ~~conjugate~~ the roots of $x^4 - 14x^2 + 9$ so ~~we~~ the elements are defined by:

$$\sigma_1: \quad \sqrt{7+2\sqrt{10}} \mapsto \sqrt{7+2\sqrt{10}}$$

$$\sigma_2: \quad \sqrt{7+2\sqrt{10}} \mapsto -\sqrt{7+2\sqrt{10}}$$

$$\sigma_3: \quad \sqrt{7+2\sqrt{10}} \mapsto \sqrt{7-2\sqrt{10}} = \frac{3}{\sqrt{7+2\sqrt{10}}} \mapsto \frac{3\sqrt{7+2\sqrt{10}}}{3} \checkmark$$

$$\sigma_4: \quad \sqrt{7+2\sqrt{10}} \mapsto -\sqrt{7-2\sqrt{10}} = -\frac{3}{\sqrt{7+2\sqrt{10}}}$$

It is clear that each of these automorphisms have order 2 so G is the Klein-4 group, $C_2 \times C_2$. ✓

wow! I'll mention this in class. □

14.2.13 Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

Proof. (Thomas) Suppose that the Galois group G of the splitting field K of a cubic $f(x)$ over $\mathbb{Q}$ is the cyclic group of order 3. It follows that the splitting field has no subfields so every root generates the entire field extension. ~~It follows~~ that if at least one root is real, they all must be since a real root can't generate a complex extension. Since all cubic polynomials over $\mathbb{Q}$ have one real root, it follows that all the roots of $f(x)$ are real. □

yes!

follows? true, but it is simply because the polynomial is of degree 3.

14.2.14 Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 with cyclic Galois group.

Proof. (Thomas) Note that $\sqrt{2+\sqrt{2}}$ is a root of the polynomial $f(x) = x^4 - 4x^2 + 2$ which is irreducible by Eisenstein's criterion. ✓ It follows that $G = \text{Gal}(f(x)/\mathbb{Q})$ has order 4. Consider the element of G, call it τ, defined by $\sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}$. We will show this element has order 4.

First, note that $\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{2}$ and $(\sqrt{2+\sqrt{2}})^2 = \sqrt{2}+2$ so $(\sqrt{2+\sqrt{2}})^2 - 2 = \sqrt{2}$. Then we see $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \frac{(\sqrt{2+\sqrt{2}})^2-2}{\sqrt{2+\sqrt{2}}}$.

Note that by applying the map $\sqrt{2+\sqrt{2}} \mapsto \sqrt{2-\sqrt{2}}$ we see that $\sqrt{2+\sqrt{2}} \mapsto \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \frac{(\sqrt{2+\sqrt{2}})^2-2}{\sqrt{2+\sqrt{2}}}$ and applying the map twice we see that $\sqrt{2+\sqrt{2}} \mapsto$

Wow!

$$\frac{(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}})^2-2}{\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}} = \frac{2-2(2+\sqrt{2})}{\sqrt{2}\sqrt{2+\sqrt{2}}} = \frac{-2-2\sqrt{2}}{\sqrt{2}\sqrt{2+\sqrt{2}}} = \frac{-4-2\sqrt{2}}{2\sqrt{2+\sqrt{2}}} = \frac{-(\sqrt{2+\sqrt{2}})^2}{\sqrt{2+\sqrt{2}}} = -\sqrt{2+\sqrt{2}}.$$

Since this map applied twice is not the identity and must have order dividing 4, we see that this map has order 4 and generates G. Thus $G = C_4$. ✓ □

14.2.15 (*Biquadratic Extensions*) 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 or $D_1 D_2$ is a square in F, prove that K/F is a Galois with $\mathrm{Gal}(K/F)$ ismorphic to the Klein-4 group.

Proof. (Thomas) Note that $\sqrt{D_1}$ has minimal polynomial $x^2 - D_1$ over F and that $\sqrt{D_2}$ has minimal polynomial $x^2 - D_2$ over F. It follows that the degree of both $F(\sqrt{D_1})/F$ and $F(\sqrt{D_2})/F$ are two and these extensions are Galois. Then we see that $F(\sqrt{D_1})F(\sqrt{D_2}) = F(\sqrt{D_1}, \sqrt{D_2})$ is also Galois. Viewed as a vector space, we note $F(\sqrt{D_1}, \sqrt{D_2})$ has the basis elements $1, \sqrt{D_1}, \sqrt{D_2}, \sqrt{D_1 D_2}$ so K has degree 4 and $G = \mathrm{Gal}(K/F)$ has order 4. The four maps are defined by:

$$\sqrt{D_1} \mapsto \sqrt{D_1}, \sqrt{D_2} \mapsto \sqrt{D_2}$$
$$\sqrt{D_1} \mapsto \sqrt{D_1}, \sqrt{D_2} \mapsto -\sqrt{D_2}$$
$$\sqrt{D_1} \mapsto -\sqrt{D_1}, \sqrt{D_2} \mapsto \sqrt{D_2}$$
$$\sqrt{D_1} \mapsto -\sqrt{D_1}, \sqrt{D_2} \mapsto -\sqrt{D_2}$$

✓

Clearly each of these maps is order 2 so G must be the Klein-4 group. □

(b) Conversely, suppose K/F is a Galois extension with $\mathrm{Gal}(K/F)$ ismorphic 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 $D_1 D_2$ is a square in F.

Proof. (Thomas) Since the Galois group G is the Klein-4 group, we see that K has three subfields of degree 2 over F. It follows that these fields are of the form $F(\sqrt{D_1}, F(\sqrt{D_2}, F(\sqrt{D_3}$ for distinct D_1, D_2, D_3 where D_1, D_2, D_3 are not squares in F (otherwise these extensions would not have degree 2). Note that $D_3 = D_1 D_2$ since otherwise K would have order 8 to contain all three subfields. Then we have $K = F(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_3}) = F(\sqrt{D_1}, \sqrt{D_2}, \sqrt{D_1 D_2}) = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2 or $D_1 D_2$ is a square in F as desired. □ — Expand.

14.2.16 **(a)** Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.

Proof. (Thomas) Note that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Z}$ (and thus $\mathbb{Q}$) by Eisenstein with 2. ✓ □

Easier:

Use the quadratic formula twice.

(b) Show that the roots of this quartic are

$$\alpha_1 = \sqrt{1+\sqrt{3}}, \alpha_3 = -\sqrt{1+\sqrt{3}}$$
$$\alpha_2 = \sqrt{1-\sqrt{3}}, \alpha_4 = -\sqrt{1-\sqrt{3}}.$$

Proof. (Thomas) Note that $(\sqrt{1+\sqrt{3}})^4 = 4+2\sqrt{3}$ and that $(\sqrt{1+\sqrt{3}})^2 = 1+\sqrt{3}$ so we see that $(\sqrt{1+\sqrt{3}})^4 - 2(\sqrt{1+\sqrt{3}})^2 - 2 = (4+2\sqrt{3}) - 2(1+\sqrt{3}) - 2 = 0$. Since $x^4 - 2x^2 - 2$ is even, we see that $-\sqrt{1+\sqrt{3}}$ is also a root.
Note that $(\sqrt{1-\sqrt{3}})^4 = 4-2\sqrt{3}$ and that $(\sqrt{1-\sqrt{3}})^2 = 1-\sqrt{3}$ so we see that $(\sqrt{1-\sqrt{3}})^4 - 2(\sqrt{1-\sqrt{3}})^2 - 2 = (4-2\sqrt{3}) - 2(1-\sqrt{3}) - 2 = 0$. Since $x^4 - 2x^2 - 2$ is even, we see that $-\sqrt{1-\sqrt{3}}$ is also a root. □

Easier:
$\alpha_1 \in \mathbb{R}$
$\alpha_2 \in \mathbb{C} \setminus \mathbb{R}$

(c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$ and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.

Proof. (Thomas) Note that $x^2 - (1-\sqrt{3})$ has a root in K_2 but not in K_1. ** I.e., $\alpha_1 \notin K_2$. This is what you must prove
Clearly $\mathbb{Q}(\sqrt{3}) \subseteq K_1 \cap K_2$. So choose $x \in K_1 \cap K_2$. Since $x \in K_1$, $x = a + b\sqrt{1+\sqrt{3}} + c\sqrt{3} + d\sqrt{3}\sqrt{1+\sqrt{3}}$ for $a, b, c, d \in \mathbb{Q}$ and since $x \in K_2$, $x = e + f\sqrt{1-\sqrt{3}} + g\sqrt{3} + h\sqrt{3}\sqrt{1-\sqrt{3}}$ $e, f, g, h \in \mathbb{Q}$. Since $\sqrt{1-\sqrt{3}} \notin K_1$ and $\sqrt{1+\sqrt{3}} \notin K_2$, we see that $x = m + n\sqrt{3}$ for $m, n \in \mathbb{Q}$ and is in $\mathbb{Q}(\sqrt{3}) = F$. □

**

$\mathbb{Q}(\sqrt{3}) \subseteq K_1 \cap K_2$

$\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}, K_1K_2$

By multiplicative property of index.

(d) Prove that K_1, K_2, and K_1K_2 are Galois over F with $\mathrm{Gal}(K_1K_2/F)$ the Klein-4 group. Write out the elements of $\mathrm{Gal}(K_1K_2)/F$ explictely. Determine all the subgroups of the Galois group and give their corresponding fixed subfield of K_1K_2 containing F.

Proof. (Thomas) Note that $K_1 = F/x^2 - (1+\sqrt{3})$ and $K_2 = F/x^2 - (1-\sqrt{3})$. Then since K_1, K_2 are splitting fields of some collection of polynomials, they are Galois extensions of F. It follows immediately that K_1K_2 is also a Galois extension. Note that $K_1K_2 = F(\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}}) = F(\sqrt{1+\sqrt{3}})(\sqrt{1-\sqrt{3}})$. Since $\sqrt{1-\sqrt{3}} \notin F(\sqrt{1+\sqrt{3}})$, $\sqrt{1-\sqrt{3}}$ has the same minimal polynomial over $F(\sqrt{1+\sqrt{3}})$ as it does over F and thus the degree of $K_1K_2 = 4$ so $G = \mathrm{Gal}(K_1K_2/F)$ has order 4. Note that in G the maps are defined by:

$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3})}_{=2} - \underbrace{K_1 \cap K_2 - K_1}_{\geq 2}$ $\Rightarrow K_1 \cap K_2 = \mathbb{Q}(\sqrt{3})$

corresponding subfields?

σ_1: $\sqrt{1+\sqrt{3}} \mapsto \sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}} \mapsto \sqrt{1-\sqrt{3}}$

σ_2: $\sqrt{1+\sqrt{3}} \mapsto \sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}} \mapsto -\sqrt{1-\sqrt{3}}$

σ_3: $\sqrt{1+\sqrt{3}} \mapsto -\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}} \mapsto \sqrt{1-\sqrt{3}}$

σ_4: $\sqrt{1+\sqrt{3}} \mapsto -\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}} \mapsto -\sqrt{1-\sqrt{3}}$

Please name them.

Clearly each of these maps is order 2 so G must be the Klein-4 group. □

(e) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

✓ ?? meaning ??

Proof. (Thomas) Observe that $\boxed{[x^4 - 2x^2 - 2/\mathbb{Q} : \mathbb{Q}]} = [x^4 - 2x^2 - 2/\mathbb{Q} : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = (4)(2) = 8$ so the splitting field of $x^4 - 2x^2 - 2$ has degree 8 over $\mathbb{Q}$. Noting that $\mathbb{Q}(\sqrt{1+\sqrt{3}})$ is not a splitting field (since it does not contain $\sqrt{1-\sqrt{3}}$, another root of the same minimal polynomial as $\sqrt{1+\sqrt{3}}$) we see that we have a subfield of $x^4 - 2x^2 - 2/\mathbb{Q}$ that is not Galois and thus the Galois group cannot be abelian.

Since the Galois group contains the automorphisms defined by $\sqrt{1+\sqrt{3}} \mapsto -\sqrt{1+\sqrt{3}}$ (and the identity otherwise) and $\sqrt{1-\sqrt{3}} \mapsto -\sqrt{1+\sqrt{3}}$ (and the identity otherwise) we see that the Galois group has at least two elements of order 2 and cannot be Q_8, so the Galois group is dihedral. ✓ □

No: $\sqrt{3} \mapsto -\sqrt{3}$ for instance.

Just watch wording

General Notation Comment: You must include the base field as follows

$\mathrm{Gal}(f(x)/\mathbb{Q})$ or $\mathrm{Gal}(L/K)$ [not $\mathrm{Gal}(L)$, $\mathrm{Gal}(f(x))$]

Also degree $= [K:L]$