553 Review Questions

1. Let F be a field with prime characteristic $ch(F) = p$. Let L/F be a finite extension s.t. $p \nmid [L:F]$. Show: L/F is a separable extension.

Proof. Suppose L/F is not separable. Then $\exists\, \alpha \in L$ s.t. $f(x) = m_{\alpha,F}(x)$ is not separable.

(*) Since an irreducible polynomial $g(x)$ is separable if $\deg(D_x g(x)) = \deg(g(x)) - 1$, it follows that $\deg(D_x f(x)) < \deg(f(x)) - 1$. Thus, $\deg(f(x))$ is a multiple of p (since $\text{char}(F) = p$). Thus, $p \mid [F(\alpha):F]$. Hence, $p \mid [L:F] = [L:F(\alpha)][F(\alpha):F]$, a contradiction. Therefore, L/F is separable.

(*) Suppose $f(x)$ is an irreducible polynomial of degree n and $D_x f(x)$ is of degree $n-1$. Suppose $f(x)$ is inseparable. Then $D_x f(x)$ and $f(x)$ share a root. Say θ. Let $g(x) = m_{\theta,F}(x)$. Then $g(x) \mid D_x f(x)$, so $\deg(g(x)) \leq n-1$. But $g(x) \mid f(x)$, contradicting the irreducibility of $f(x)$.

2. Let ϵ_5 be a primitive 5th root of unity, and denote $\theta = \epsilon_5 + \epsilon_5^{-1}$, as an element of the cyclotomic field $\mathbb{Q}(\epsilon_5)$. Show that the minimal polynomial of θ over $\mathbb{Q}$ is x^2+x-1. Show that $\mathbb{Q}$ and $\mathbb{Q}(\theta)$ are the only proper subfields of $\mathbb{Q}(\epsilon_5)$.

Proof. First, $(\epsilon_5+\epsilon_5^{-1})^2 + (\epsilon_5+\epsilon_5^{-1}) - 1$

$= \epsilon_5^2 + 2 + \epsilon_5^{-2} + \epsilon_5 + \epsilon_5^{-1} - 1$

$= \epsilon_5^2 + 2 + \epsilon_5^3 + \epsilon_5 + \epsilon_5^4 - 1$

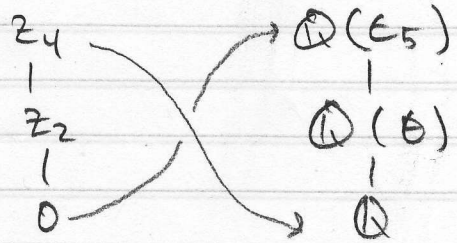
$= \epsilon_5^4 + \epsilon_5^3 + \epsilon_5^2 + \epsilon_5 + 1 = 0$

so θ is a root.

Now $(x+2)^2 + (x+2) - 1 = x^2+4x+4+x+2-1$

$= x^2 + 5x + 5$ is irreducible by Eisenstein. Hence, x^2+x-1 is irreducible, so $x^2+x-1 = m_{\theta,\mathbb{Q}}(x)$.

Now, since $\mathbb{Q}$ is characteristic 0, $\mathrm{Gal}(\mathbb{Q}(\epsilon_5)/\mathbb{Q}) \cong \mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_5^\times \cong \mathbb{Z}_4$. Since $\mathbb{Z}_4$ only has one unique subgroup of order 2, by the Fundamental Theorem of Galois Theory, $\mathbb{Q}(\theta)$ is the only extension of degree 2 under $\mathbb{Q}(\epsilon_5)$. Similarly, $\mathbb{Q}$ is the only other proper subfield since the only other subgroup of $\mathbb{Z}_4$ is trivial.



3. Prove or disprove the following. If $f(x), g(x) \in \mathbb{Q}[x]$ are irreducible polynomials that have the same splitting field, then $\deg(f) = \deg(g)$.

Disproof. Let $f(x) = x^3 - 2$. We know the splitting field of $f(x)$ is $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ where ζ_3 is a primitive cube root of unity. Moreover, $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$. By the Primitive Element Theorem, since $K/\mathbb{Q}$ is a finite separable extension, $K = \mathbb{Q}(\theta)$ for some $\theta \in K$. Let $g(x) = m_{\theta, \mathbb{Q}}(x)$.
$\deg g(x) = [\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$.
Thus, $f(x)$ and $g(x)$ are irreducible polynomials with the same splitting field, but $\deg(f(x)) = 3 \neq 6 = \deg(g(x))$.

---

4. Prove or disprove that every finite algebraic extension field of $\mathbb{F}_{p^n}$ is Galois. (Note: algebraic is redundant)

Proof. Let F be a finite extension of $\mathbb{F}_{p^n}$. Then F must be a finite field of characteristic p, since $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq F$. By the uniqueness of finite fields, $F \cong \mathbb{F}_{p^m}$ for some positive integer m.
$\mathbb{F}_{p^m} / \mathbb{F}_p$ is Galois being the splitting field of the separable polynomial $x^{p^m} - x$.
By the Fundamental Theorem of Galois Theory, since F is Galois over $\mathbb{F}_p$, F is Galois over any subfield containing $\mathbb{F}_p$. Since $\mathbb{F}_p \subseteq \mathbb{F}_{p^n} \subseteq F$, $F / \mathbb{F}_{p^n}$ is Galois.

5. If $[K:\mathbb{F}_p]$ divides $[L:\mathbb{F}_p]$, does it follow that K is isomorphic to a subfield of L?

Yes. Say $[K:\mathbb{F}_p]=n$, $[L:\mathbb{F}_p]=m$, $n|m$.
By the classification of finite fields, $K\cong \mathbb{F}_{p^n}$, $L\cong \mathbb{F}_{p^m}$.
Now, $Gal(L/\mathbb{F}_p)\cong \mathbb{Z}_m$ (generated by the Frobenius automorphism). Since $n|m$, $\mathbb{Z}_m$ has a subgroup isomorphic to $\mathbb{Z}_{m/n}$. Thus, by the Fundamental Theorem of Galois Theory, L has a subfield E s.t.
$[E:\mathbb{F}_p] = |\mathbb{Z}_m|/|\mathbb{Z}_{m/n}| = m/(m/n) = n$.
Thus, by the classification of finite fields,
$E\cong \mathbb{F}_{p^n}\cong K$.

6. Let $\mathbb{F}_p$ be a finite field whose cardinality p is prime. Fix a positive integer n which is not divisible by p, and let ϵ_n be a primitive n^{th} root of unity. Show that $[\mathbb{F}_p(\epsilon_n) : \mathbb{F}_p] = a$ is the least positive integer s.t. $p^a \equiv 1 \pmod{n}$. (Hint: $\mathrm{Gal}(\mathbb{F}_p(\epsilon_n)/\mathbb{F}_p)$ is generated by the Frobenius automorphism.)

Proof. Let $G = \mathrm{Gal}(\mathbb{F}_p(\epsilon_n)/\mathbb{F}_p) = \langle \sigma \rangle$, where σ is the Frobenius automorphism. Since $[\mathbb{F}_p(\epsilon_n) : \mathbb{F}_p] = a$, $o(\sigma) = a$. Since ϵ_n generates $\mathbb{F}_p(\epsilon_n)$, by the Fundamental Theorem of Galois Theory, the identity automorphism is the only automorphism in G which fixes ϵ_n. (*)
Since $\sigma^a = id$, we have $\sigma^a(\epsilon_n) = \epsilon_n$. But $\sigma^a(\epsilon_n) = \epsilon_n^{p^a}$.
Hence $\epsilon_n^{p^a} = \epsilon_n$. Since the n^{th} roots of unity form a cyclic multiplicative group of order n generated by ϵ_n, it follows from the fact that $\epsilon_n^{p^a} = \epsilon_n$ that
$p^a \equiv 1 \pmod{n}$.
Moreover, if b is a positive integer $b < a$, by (*), then $\epsilon_n^{p^b} = \sigma^b(\epsilon_n) \neq \epsilon_n$. Hence $p^b \not\equiv 1 \pmod{n}$.

7. Fix a prime p, and consider the polynomial $f(x) = x^p - x - 1$. Let $F_p(f)$ be the splitting field of $f(x)$ over $\mathbb{F}_p$. Let $a \in F_p(f)$ be a root of f. Show that $a \mapsto a+1$ defines an automorphism of $F_p(f)$. Show that $\mathrm{Gal}(F_p(f)/\mathbb{F}_p) \cong \mathbb{Z}_p$. Prove that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Since $\mathbb{F}_p$ is of characteristic p, we have the Freshman's Dream. In other words, $(a+1)^p - (a+1) - 1 = a^p + 1 - a - 1 - 1 = a^p - a - 1 = 0$, so $a+1$ is also a root of f. Notice that if $a \in \mathbb{F}_p$, then 0 would be a root of f since $a+1, a+2, \ldots, a+(p-a) = 0$ are all roots. But $f(0) = 0^p - 0 - 1 = -1 \neq 0$. Thus, $a \notin \mathbb{F}_p$.
Now, we observe that $\mathbb{F}_p(a) = \mathbb{F}_p(a+1)$.
($a, 1 \in \mathbb{F}_p(a)$, so $a+1 \in \mathbb{F}_p(a)$. Conversely, $a+1, -1 \in \mathbb{F}_p(a+1)$, so $a = a+1-1 \in \mathbb{F}_p(a+1)$.)
Similarly, we get $\mathbb{F}_p(a) = \mathbb{F}_p(a+1) = \mathbb{F}_p(a+2) = \ldots = \mathbb{F}_p(a+p-1)$.
Since all $a, a+1, a+2, \ldots, a+p-1$ are roots of f, and all of these fields are equal, $\mathbb{F}_p(a) = F_p(f)$. Hence, any map sending $a \mapsto a+i$ for $0 \leq i \leq p-1$ determines an automorphism of $F_p(f)$ (since it is generated by a and $a+i$ is a root).
Notice that $a \mapsto a+i$ is just $i-1$ applications of $a \mapsto a+1$.
Hence, $\mathrm{Gal}(F_p(f)/\mathbb{F}_p)$ is cyclic generated by $a \mapsto a+1$.
Moreover, the group is of order p since $a+p = a$ but $a+i \neq a$ if $1 \leq i < p$. Thus, $\mathrm{Gal}(F_p(f)/\mathbb{F}_p) \cong \mathbb{Z}_p$.
Since $f(x)$ is a monic polynomial of degree $p = [\mathbb{F}_p(a) : \mathbb{F}_p]$ with a as a root, it follows that $f(x) = m_{a, \mathbb{F}_p}(x)$.
Hence, $f(x)$ is irreducible in $\mathbb{Z}_p[x]$.
Since $\mathbb{Z}$ is an integral domain, $f(x)$ is a nonconstant monic polynomial in $\mathbb{Z}[x]$, and (p) is a proper ideal of $\mathbb{Z}$, and $\overline{f(x)} = f(x)$ is irreducible in $\mathbb{Z}_p[x] \cong (\mathbb{Z}/p)[x]$, $f(x)$ is irreducible in $\mathbb{Z}[x]$.

8. Let x and y be indeterminates over the field F_2. Prove that there exist infinitely many subfields of $L = F_2(x,y)$ that contain the field $K = F_2(x^2, y^2)$.

Proof. Consider the polynomial $f(T) = T^2 - x^2 \in F_2(x^2,y^2)[T]$. The roots of this polynomial are $x, -x$, neither of which are in $F_2(x^2,y^2)$. Thus, $T^2 - x^2$ is irreducible in $F_2(x^2,y^2)[T]$, and so $[F_2(x,y^2) : F_2(x^2,y^2)] = 2$. Similarly, $T^2 - y^2$ is irreducible over $F_2(x,y^2)[T]$, so by the Tower Theorem, $[F_2(x,y) : F_2(x^2,y^2)] = 2 \cdot 2 = 4$.
For $c \in F_2(x^2,y^2)$ consider $F_2(x+cy)$.
Since $(x+cy)^2 = x^2 + c^2y^2$ (Freshman's Dream), we have $F_2(x^2,y^2) \subseteq F_2(x+cy)$, and $F_2(x+cy) \subseteq F_2(x,y)$ is clear.
Now, $T^2 - x^2 - c^2y^2$ has $x+cy$ as a root, so $[F_2(x+cy) : F_2(x^2,y^2)] \leq 2$. But if there were only finitely many subfields, then for some $c \neq c' \in F_2(x^2,y^2)$, $F_2(x+cy) = F_2(x+c'y)$, so $x+cy, x+c'y \in F_2(x+cy)$.
Thus, $(x+cy) - (x+c'y) = (c-c')y \in F_2(x+cy)$, so $y \in F_2(x+cy)$. Then $(x+cy) + (-c)y = x \in F_2(x+cy)$.
Thus, $F_2(x+cy) \subseteq F_2(x,y) \subseteq F_2(x+cy)$, so $F_2(x,y) = F_2(x+cy)$. This is clearly absurd since $[F_2(x,y) : F_2(x^2,y^2)] = 4 \neq 2 = [F_2(x+cy) : F_2(x^2,y^2)]$.
Thus, there are infinitely many intermediate subfields.

(Proof follows Ex 2 pg. 595 and proof of Prop 24).

9. Let K/F be an algebraic field extension. If $K = F(a)$ for some $a \in K$, prove that there are only finitely many subfields of K that contain F.

Proof. Let E be a field s.t. $F \subseteq E \subseteq K$.
Let $f(x) = m_{a,F}(x)$ and $g(x) = m_{a,E}(x)$. Since $F \subseteq E$, $g(x) \mid f(x)$ in $E[x]$. Let $E' = F(a_0, \dots, a_{n-1})$ where $a_0, \dots, a_{n-1}$ are the coefficients of $g(x)$. Clearly, $E' \subseteq E$. However, $g(x)$ is still the minimal polynomial for a over E'. Thus, it follows that $[K : E] = \deg g(x) = [K : E']$. Since $E' \subseteq E$, this implies that $E = E' = F(a_0, \dots, a_{n-1})$. Thus, every intermediate field is generated over F by the coefficients of some irreducible part of $f(x) = m_{a,F}(x)$ in E. Since there are only finitely many potential irreducible factors of $f(x)$, and since since each one has finitely many coefficients, there are finitely many intermediate subfields.

(Proof of Prop 24 on pg. 594).

10. Let p be a prime integer. Recall that a field extension K/F is called a p-extension if K/F is Galois and $[K:F]$ is a power of p. If K/F and L/K are p-extensions, prove that the Galois closure of L/F is a p-extension.

Proof. Let M be the Galois closure of L/F. Let $G = Gal(M/F)$ be a group of order n with elements $\sigma_1, \ldots, \sigma_n$. Define $L_i = \sigma_i(L)$. Let E be the composite field $L_1 L_2 \cdots L_n$. Since each $L_i \subseteq M$, it is true that $E \subseteq M$. Moreover, if $f(x)$ is a polynomial having a root α in E, then the other roots of $f(x)$ are precisely the elements $\sigma_i(\alpha)$ (since $F \subseteq E \subseteq M$ and by the Fundamental Theorem of Galois Theory, since M/F is Galois, M/E is Galois.). But $\forall i$, $\sigma_i(E) = \sigma_i(L_1)\sigma_i(L_2)\cdots\sigma_i(L_n) = E$ since it is merely a permutation on the indices. Thus, $\sigma_i(\alpha) \in E$. Hence every separable polynomial over F having a root in E splits completely in E, so E/F is Galois. Since $L \subseteq E$, E/F is Galois, $E \subseteq M$, and M is the Galois closure of L/F, it follows that $E = M$. Each L_i is Galois over K and $|Gal(L_i/K)| = p^{\alpha_i}$ for some α_i. Thus, $L_1 L_2 \cdots L_n = M$ is Galois over K and $Gal(M/K) \leq Gal(L_1/K) \times \cdots \times Gal(L_n/K)$, hence, is a p-group, so $|Gal(M/K)| = p^{\beta}$ for some positive integer β. By the Tower Theorem, $[M:F] = [M:K][K:F] = p^{\beta}p^{\gamma}$. Since M/F is Galois, M is a p-extension of F.

Give an example where K/F and L/K are p-extensions, but L/F is not Galois.

11. Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$.
Any quadratic extension of a field of characteristic $\neq 2$ is Galois, so K/F is Galois and L/K is Galois. But L/F is not Galois since $\sqrt[4]{2}$ is a root of $x^4 - 2$ (irreducible by Eisenstein), but so is $i\sqrt[4]{2}$. However, $i\sqrt[4]{2}$ is imaginary whereas $\mathbb{Q}(\sqrt[4]{2})$ is a real field. Thus, L is not a splitting field over F, so L/F is not Galois.

Fun fact: In the above example, M = the Galois closure of L/F is $\mathbb{Q}(\sqrt[4]{2}, i)$. But M is still a p-extension since $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. If the question wanted to show L/K Galois as a necessary condition, this example would not work!

13. Give an example of a field F having characteristic $p>0$ and an irreducible monic polynomial $f(x) \in F[x]$ that has a multiple root.

Solution. Let $F = F_2(y^2)$ where y is an indeterminate.
We can determine that the polynomial $x^2 - y^2 \in F_2(y^2)[x]$ is irreducible since it has no roots in $F_2(y^2)$.
Since F is of characteristic 2, $x^2 - y^2 = (x-y)^2$ in $F_2(y)$. Thus, $x^2 - y^2$ has a multiple root.

---

14. Let f be an irreducible polynomial of degree k over F_p. Find the splitting field of f and its Galois group.

Solution. Let α be a root of f. Consider the field $F_p(\alpha)$. Any finite extension of F_p is Galois, so $F_p(\alpha)$ is Galois, and hence, is the splitting field of f.
Notice, any root α of f works. Moreover, $F_p(\alpha) \cong F_{p^k}$ since $[F_p(\alpha) : F_p] = k$.
$\mathrm{Gal}(F_p(\alpha)/F_p) \cong \mathbb{Z}_k$, which is generated by the Frobenius automorphism $\sigma : x \mapsto x^p$ of order k.

15. Let n be a positive integer and d a positive integer that divides n. Suppose $a \in \mathbb{R}$ is a root of the polynomial $x^n - 2 \in \mathbb{Q}[x]$. Prove that there is precisely one subfield F of $\mathbb{Q}(a)$ with $[F : \mathbb{Q}] = d$.

Proof. Notice that $\mathbb{Q}(a)$ is a real field. Hence, any subfields must be real. By Eisenstein $x^n - 2$ is irreducible. Consider $a^{n/d}$. $a^{n/d} \in \mathbb{Q}(a)$ since $a^{n/d}$ is a power of a. Thus, $\mathbb{Q}(a^{n/d})$ is a subfield of $\mathbb{Q}(a)$.
Moreover, $x^d - 2$ is irreducible by Eisenstein and and $(a^{n/d})^d - 2 = a^n - 2 = 0$, so $[\mathbb{Q}(a^{n/d}) : \mathbb{Q}] = d$.
The Galois closure of $\mathbb{Q}(a)/\mathbb{Q}$ is $\mathbb{Q}(a, \zeta_n)$ where ζ_n is a primitive n^{th} root of unity.
The other fields of degree d are the conjugates of a, which are $\zeta_n^i a$ for $1 \leq i \leq n$, all of which either generate $\mathbb{Q}(a)$ or are complex.

16. Let $a = \sqrt[3]{5-\sqrt{7}}$.

(a) Find the minimal polynomial for a, and the conjugates of a.

A: $a^3 = 5-\sqrt{7} \Rightarrow a^3-5 = -\sqrt{7} \Rightarrow (a^3-5)^2 = 7$

$\Rightarrow a^6 - 10a^3 + 25 - 7 = 0$

Thus, we see a is a root of $x^6 - 10x^3 + 18$

This polynomial is monic and irreducible by Eisenstein ($10, 18 \in (2)\mathbb{Z}$, but $18 \notin (4)\mathbb{Z}$). Thus, this is the minimal polynomial of a.

Using the quadratic formula, we get

$$x^3 = \frac{10 \pm \sqrt{100-72}}{2} = 5 \pm \sqrt{7}$$

Thus, the roots of the polynomial (and hence conjugates of a) are

$$\zeta_3^i \sqrt[3]{5 \pm \sqrt{7}} \quad \text{for } i = 1, 2, \text{ or } 3$$

where ζ_3 is a primitive cube root of unity.

(b) Determine the Galois closure of $\mathbb{Q}(a)$.

A: Clearly, $\mathbb{Q}(a)$ is not Galois as it is a real field.
Any field containing a and $\zeta_3 a$ (as the splitting field does), must also contain $\frac{\zeta_3 a}{a} = \zeta_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$. And any such field must hence also contain $\sqrt{-3}$.
Since $a, \sqrt[3]{5-\sqrt{7}}, \sqrt{-3}$ are all in the splitting field, and all roots of $m_{a,\mathbb{Q}}$ can be formed from these over $\mathbb{Q}$, we get the Galois closure of $\mathbb{Q}(a)$ to be...

$$\mathbb{Q}\left(\sqrt[3]{5-\sqrt{7}}, \sqrt[3]{5+\sqrt{7}}, \sqrt{-3}\right)$$

(c) Show that $F/\mathbb{Q}$ is an extension by radicals.

$\mathbb{Q} = K_0$, $K_1 = K_0(\sqrt{-3})$, $K_2 = K_1(\sqrt{7})$,
$(-3 \in K_0 = \mathbb{Q})$ $(7 \in K_1 = \mathbb{Q}(\sqrt{-3}))$
$K_3 = K_2(\sqrt[3]{5-\sqrt{7}})$, $K_4 = K_3(\sqrt[3]{5+\sqrt{7}})$
$(5-\sqrt{7} \in K_1(\sqrt{7}))$ $(5+\sqrt{7} \in K_3 \supset K_2 = K_1(\sqrt{7}))$

K_4 is the Galois closure of $\mathbb{Q}(a)$. Hence, $F/\mathbb{Q}$ is an extension by radicals.

(d) Conclude that $\mathrm{Gal}(F/\mathbb{Q})$ is solvable.

A Galois group is solvable $\Leftrightarrow$ it is the Galois group of the splitting field of a polynomial $f(x)$ which can be solved by radicals

$\Leftrightarrow$ The splitting field of $f(x)$ is a radical extension.

17. Let F be a field of characteristic $p>0$. Fix an element c in F. Prove that $f(x)=x^p-c$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in F.

Proof. ($\Rightarrow$) is trivial for if $f(x)$ has roots, it is reducible.
($\Leftarrow$) Suppose $f(x)$ has no roots in F. Let α be a root of $f(x)$ in a splitting field of $f(x)$ over F. Then $\alpha^p = c$.
We notice that $(x-\alpha)^p = x^p - \alpha^p = x^p - c = f(x)$ (Freshman's Dream)
Hence, if $f(x)$ is reducible, $f(x) = (x-\alpha)^a (x-\alpha)^b$ for some $a, b \in \mathbb{N}$ with $a+b=p$. Since $(x-\alpha)^a \in F[x]$ and $(x-\alpha)^b \in F[x]$, we see that the constant terms $\alpha^a, \alpha^b \in F$.

★ Apparently, $\exists$ integers n, m s.t. $na+mb \equiv 1 \bmod p$. (Why?)
Hence, $na+mb = kp+1$ for some k.
Then $c^k\alpha = \alpha^{kp}\alpha = \alpha^{kp+1} = \alpha^{na+mb} = (\alpha^a)^n(\alpha^b)^m \in F$.
Since $c \in F$ and $c \neq 0$ (else $f(x)$ has 0 as a root),
$\alpha \in F$, a contradiction.
Thus, $f(x)$ is irreducible in $F[x]$.

18. Determine the Galois group of the splitting field over $\mathbb{Q}$ and all its subfields for

(a) $x^3 - 2$.

Solution. The roots are $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, $\zeta_3^2\sqrt[3]{2}$, for ζ_3 a primitive cube root of unity.

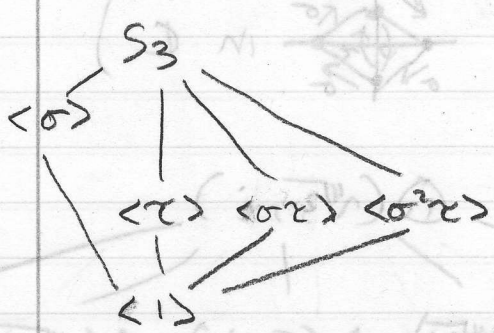
The splitting field is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. $x^3 - 2$ is irreducible by Eisenstein, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Moreover, $\mathbb{Q}(\sqrt[3]{2})$ is real, so $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2})$. Since the primitive cube roots of unity are the roots of $\Phi_3 = x^2 + x + 1$, $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 3 \cdot 2 = 6$. So $|G| = |\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})| = 6$.

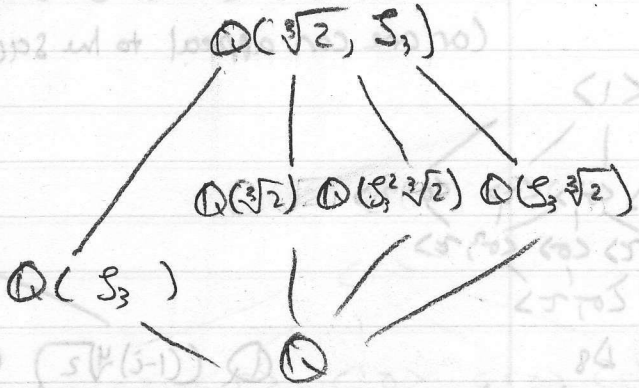
Since $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, $\zeta_3^2\sqrt[3]{2}$ are belong to the same irreducible poly, and ζ_3, ζ_3^2 do as well, we get automorphisms:

σ: $\sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}$, $\zeta_3 \mapsto \zeta_3$ $\qquad$ τ: $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\zeta_3 \mapsto \zeta_3^2$

$o(\sigma) = 3$ and $o(\tau) = 2$, so these generate G.

$\sigma\tau = \tau\sigma^2$, so $G \cong D_6 = S_3$.





Using the Galois correspondence and determing fixed elements of each generator.

18 (b) $f(x) = x^4 + 2$

A Notice, x^4+2 is irreducible by Eisenstein.

One can check that the roots are $\zeta_8\sqrt[4]{2}$, $\zeta_8^3\sqrt[4]{2}$, $\zeta_8^5\sqrt[4]{2}$, $\zeta_8^7\sqrt[4]{2}$

Hence, $\frac{\zeta_8^3\sqrt[4]{2}}{\zeta_8\sqrt[4]{2}} = \zeta_8^2 = \zeta_4 = i$ is in the splitting field.

So is $\zeta_8\sqrt[4]{2} + \zeta_8^7\sqrt[4]{2} = \sqrt{2}\sqrt[4]{2}$ $\left(\zeta_8 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i,\ \zeta_8^7 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)$.

So is $(\sqrt{2}\sqrt[4]{2})\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\sqrt{2} = \left(\frac{1}{2} + \frac{1}{2}i\right)\sqrt{2}$, so $\sqrt{2}$ is also in.

Hence, $\frac{\sqrt{2}\sqrt[4]{2}}{\sqrt{2}} = \sqrt[4]{2}$ is in there. Notice $(\sqrt[4]{2})^2 = \sqrt{2}$.

Since all roots can be made over $\mathbb{Q}$ by $\sqrt[4]{2}, (\sqrt[4]{2})^2, i$,

the splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$, which is degree 8.

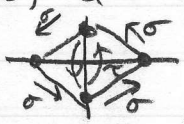
$(x^4-2,\ x^2+1)$

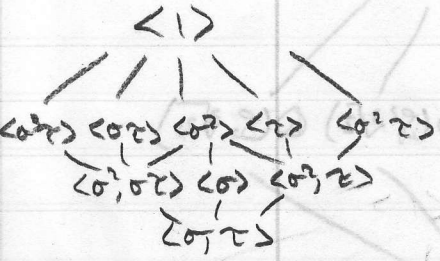
The automorphisms are generated by

$\sigma: \sqrt[4]{2} \mapsto i\sqrt[4]{2}$, $i \mapsto i$; $\tau: \sqrt[4]{2} \mapsto \sqrt[4]{2}$, $i \mapsto -i$

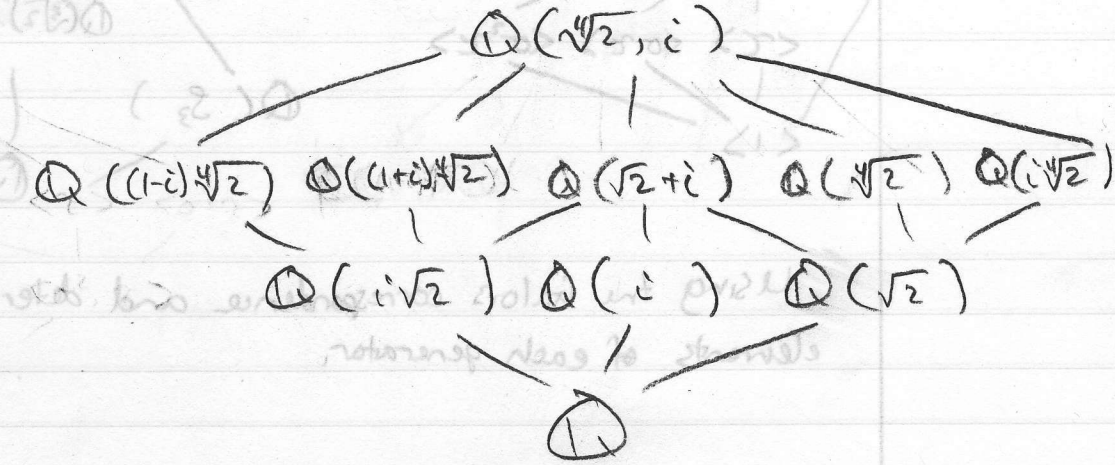
$o(\sigma) = 4$, $o(\tau) = 2$, so these are indeed generators.

One can check that $\sigma\tau = \tau\sigma^3$ so, $G \cong D_8$

(or one can appeal to the square  in $\mathbb{C}$)



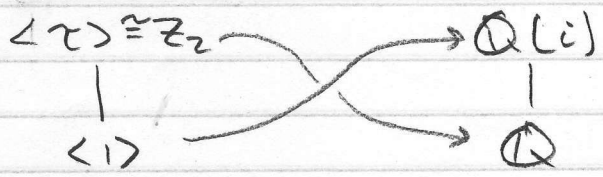
D_8
(upside down)



18 (c) x^4+4

A: One can check that the roots are $1+i, 1-i, -1+i, -1-i$
Thus, the splitting field is $\mathbb{Q}(i)$.
So $[\mathbb{Q}(i):\mathbb{Q}] = 2$ since $x^2+1 = m_{i,\mathbb{Q}}$.
Hence $Gal(\mathbb{Q}(i):\mathbb{Q}) \cong \mathbb{Z}_2$

The sole nontrivial automorphism is
$\tau: i \mapsto -i$



19. Show that $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2}, \epsilon_3)$, where $\epsilon_3^2 + \epsilon_3 + 1 = 0$.

Solution. Suppose $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2}, \epsilon_3)$.
Notice that $\epsilon_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$, so $i\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2}, \epsilon_3)$.
Since $\sqrt{3}$ and $i\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2}, \epsilon_3)$, we must have their quotient as well. Thus, $i \in \mathbb{Q}(\sqrt[3]{2}, \epsilon_3)$.
Hence, $\mathbb{Q}(\sqrt{3}, i) \subseteq \mathbb{Q}(\sqrt[3]{2}, \epsilon_3)$.
Thus, $[\mathbb{Q}(\sqrt[3]{2}, \epsilon_3) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \epsilon_3) : \mathbb{Q}(\sqrt{3}, i)][\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$.
Therefore, we get that 6 is a multiple of 4.
This is absurd, and so $\sqrt{3} \notin \mathbb{Q}(\sqrt[3]{2}, \epsilon_3)$.

---

20. Let L/F be a Galois extension of degree $[L:F] = 2p$, where p is an odd prime.

(a) Show that there exists a unique quadratic subfield E, i.e., $F \subseteq E \subseteq L$ and $[E:F] = 2$.

Solution. Let $G = \mathrm{Gal}(L/F)$. $|G| = [L:F] = 2p$. Since p is odd, $\exists$ subgroup $H \leq G$ with $|H| = p$. Moreover, $[G:H] = \frac{|G|}{|H|} = \frac{2p}{p} = 2$, so $H \trianglelefteq G$. By Sylow's Theorem, since H is a normal Sylow p-subgroup of G, H is the unique subgroup of order p. Let E be the fixed field of H.
By Fund Thm. Gal. Thy., $[E:F] = [G:H] = \frac{2p}{p} = 2$.
Since H is unique, E is the only such field.

(b) Does there exist a unique subfield K of index 2, i.e., $F \subset K \subseteq L$ and $[L:K] = 2$? Prove or give a counterexample.

Counterexample. $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $F = \mathbb{Q}$.
$\mathrm{Gal}(L/F) \cong S_3$ which has 3 subgroups of order 2, providing 3 subfields of L of index 2

$$\mathbb{Q}(\sqrt[3]{2}), \quad \mathbb{Q}(\zeta_3 \sqrt[3]{2}), \quad \mathbb{Q}(\zeta_3^2 \sqrt[3]{2})$$

21. Let L/F be a Galois extension of degree $[L:F]=p^2$ for some prime p. Let K be a subfield satisfying $F \subset K \subset L$. Must K/F be a normal extension?

Yes. Notice that $|G| = p^2$ where $G = Gal(L/F)$, so G is a p-group. Since p-groups have a nontrivial center $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, then G is Abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic, meaning G is Abelian, a contradiction (since $Z(G) \neq G$). Hence, G is Abelian. Let H be the subgroup of G having fixed field K. Since G is Abelian, all subgroups are normal. Thus, $H \trianglelefteq G$. By the Fundamental Theorem of Galois Theory, K/F is Galois. Since all Galois extensions are normal, K/F is normal.

22. Let L/F be the Galois closure of the separable algebraic field extension $F(\theta)/F$. Let p be a prime that divides $[L:F]$. Prove that there exists a subfield K of L such that $[L:K]=p$, and $L=K(\theta)$.

Proof. Let $G=\mathrm{Gal}(L/F)$. Since $p \mid |G|$, by Cauchy's Theorem, G has a subgroup of order p. Let H_0 be the subgroup of G with fixed field $F(\theta)$. By way of contradiction, suppose H_0 contains all subgroups of G having order p. Let H_1 be the subgroup of G generated by all subgroups of order p. $H_1 \subseteq H_0$. Moreover, since an element has order a power of p iff it is in H_1, H_1 char G, so $H_1 \trianglelefteq G$. Let E be the fixed field of H_1. Then E/F is Galois, and since $H_1 \subseteq H_0 \subsetneq L$, E contains $F(\theta)$, but $E \subsetneq L$. This contradicts the minimality of the Galois closure. Thus, H_0 does not contain some subgroup of order p, say H. Let K be the fixed field of H. The composite $KF(\theta) \subseteq L$. Moreover, $\mathrm{Gal}(L/KF(\theta)) = H \cap H_0$. Since all nontrivial elements of H generate H and $H \not\subseteq H_0$, $H \cap H_0 = \langle e \rangle$. Hence, $KF(\theta) = L$. But since $F \subseteq K$, it follows that $L = KF(\theta) = K(\theta)$. Moreover, since $|H| = p$, and K is the fixed field of H, $[L:K] = p$.

23. Suppose $L/\mathbb{Q}$ is a finite extension with $[L:\mathbb{Q}] = 4$. Is it possible that there exist precisely two subfields K_1 and K_2 of L for which $[L:K_i] = 2$? Justify your answer.

No. (Galois Theory Argument). Suppose there are precisely two. K_1, K_2 are quadratic extensions over a field of characteristic $\neq 0$, and hence $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ are Galois. Since $K_1, K_2 \subseteq L$, $K_1K_2 \subseteq L$. Moreover, K_1K_2 is Galois. By the Tower Theorem, $[K_1K_2:\mathbb{Q}] \mid [L:\mathbb{Q}] = 4$, but $K_1 \subsetneq K_1K_2$, so $[K_1K_2:\mathbb{Q}] \geq 2$. Since there are precisely two subfields, $[K_1K_2:\mathbb{Q}] = 4$. Thus, $K_1K_2 = L$, so $L/\mathbb{Q}$ is Galois. $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}_4$ or V_4, and have 1 or 3 subgroups of index 2, a contradiction.

(Quadratic Extension Argument). Since, $[K_i:\mathbb{Q}] = 2$, $\exists\, d_1, d_2 \in \mathbb{Q}$ not squares in $\mathbb{Q}$ s.t. $K_1 = \mathbb{Q}(\sqrt{d_1})$, $K_2 = \mathbb{Q}(\sqrt{d_2})$. Consider $K_3 = \mathbb{Q}(\sqrt{d_1 d_2})$. It must be the case that d_1d_2 is a square in $\mathbb{Q}$, since there are precisely two subfields of degree 2. (If L contains $\sqrt{d_1}$ and $\sqrt{d_2}$, then it contains their product, so $K_3 \subseteq L$). Since $\mathbb{Q}$ is a UFD which is the fraction field of the UFD $\mathbb{Z}$, write $d_1d_2 = \frac{a_1^{\alpha_1} \cdots a_n^{\alpha_n}}{b_1^{\beta_1} \cdots b_m^{\beta_m}}$ in lowest terms as a unique factorization. It follows that $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ are all even. Since neither d_1 nor d_2 are squares, it follows that for some factor γ of d_1d_2, $\gamma \mid d_1$ and $\gamma \mid d_2$. Suppose γ is the largest such factor. Then $d_1 = \delta^{2x}\gamma$, $d_2 = \epsilon^{2y}\gamma$, so $\delta^x\sqrt{\gamma} = \sqrt{d_1}$ and $\epsilon^y\sqrt{\gamma} = \sqrt{d_2}$. Thus, $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2})$, a contradiction.