Question #6.

Suppose that $f(x)$ and $g(x)$ are irreducible over F and $\deg f(x)$ and $\deg g(x)$ are relatively prime. If a is a zero of $f(x)$ in some extension of F, show that $g(x)$ is irreducible over $F(a)$.

$f, g \in F[x]$, $\quad (\deg f, \deg g) = 1$

$f(a) = 0 \quad$ in $F(a)$

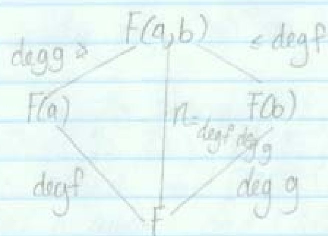
$g(x) = h(x)f(x) + r(x) \in F[x] \qquad \deg f > \deg r \geq 1$

$g(a) = r(a) + h(a)f(a) = r(a)$

$g(x) = h(x)h'(x)$

$h(x) = d(x)f(x) + r(x)$

$h'(x) = d'(x)f(x) + r'(x)$



b root of g

$\deg f \mid n \implies \deg f \cdot \deg g \mid n$

$\deg g \mid n \qquad n \leq \deg f \cdot \deg g$

$\implies n = \deg f \cdot \deg g$

$f \in F[x] \subset F(b)[x] \qquad f(a) = 0$

g_{min} = minimal poly of $b / F(a)$ is g

$g(b) = 0 \quad \therefore g_{min} \mid g \qquad g$ is a constant multiple of g_{min} $\therefore g$ is irreducible of F

See back

$g = g_{min} \cdot h$

$\deg g = \deg g_{min} + \deg h$

$\therefore \deg(h) = 0 \quad \therefore h$ is constant polynomial

Question #8

Find the degree and a basis for $Q(\sqrt{3}+\sqrt{5})$ over $Q(\sqrt{15})$. Find the degree and a basis for $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2})$ over Q.

If we look for the minimal polynomial satisfied by $\sqrt{3}+\sqrt{5}$, compute:

$$x = \sqrt{3}+\sqrt{5}$$
$$x^2 = 8 + 2\sqrt{15}$$

2/2

So if we believe that $\sqrt{3}+\sqrt{5} \notin Q(\sqrt{15})$, then the degree of the extension is 2, since we have found a quadratic polynomial satisfied by $\sqrt{3}+\sqrt{5}$ with coefficients in $Q(\sqrt{15})$

Alternatively, reason this way, $[Q(\sqrt{3}+\sqrt{5}):Q] = 4$ and $[Q(\sqrt{15}):Q] = 2$ and also obviously $Q(\sqrt{15})$ is a subfield of $Q(\sqrt{3}+\sqrt{5})$. Therefore, $[Q(\sqrt{3}+\sqrt{5}):Q(\sqrt{15})] = 2$

Either way, we see that a basis is $\{1, \sqrt{3}+\sqrt{5}\}$.

For the second part, because $\sqrt{4} \in Q(\sqrt[4]{2})$, see that $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}) = Q(\sqrt[3]{2}, \sqrt[4]{2})$. Now, $Q(\sqrt[3]{2}, \sqrt[4]{2})$ contains $Q(\sqrt[3]{2})$ as a subfield, and $[Q(\sqrt[3]{2}):Q] = 3$ Also, $Q(\sqrt[3]{2}, \sqrt[4]{2})$ contains $Q(\sqrt[4]{2})$ as a subfield, and $[Q(\sqrt[4]{2}):Q] = 4$. By the proof for Question #11 $[Q(\sqrt[3]{2}, \sqrt[4]{2}):Q] = 12$.

A basis is given by $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt[4]{2}, \sqrt[4]{2}\sqrt[3]{2}, \sqrt[4]{2}\sqrt[3]{4}, \sqrt[4]{4}, \sqrt[4]{4}\sqrt[3]{2}, \sqrt[4]{4}\sqrt[3]{4}, \sqrt[4]{8}, \sqrt[4]{8}\sqrt[3]{2}, \sqrt[4]{8}\sqrt[3]{4}\}$.

Proof for Question 11 (gallian)

Suppose that E is an extension F, and $a, b \in E$. If a is algebraic over F of degree m, and b is algebraic over F of degree n, where m and n are relatively prime, show that $[F(a,b):F] = mn$.

$[F(a,b):F] = [F(a,b):F(a)][F(a):F]$, which lets us see that

$m \mid [F(a,b):F]$; similarly, $[F(a,b):F] = [F(a,b):F(b)][F(b):F]$, which means that $n \mid [F(a,b):F]$. Since m and n are relatively prime we conclude that $mn \mid [F(a,b):F]$

On the other hand, some thought show that $[F(a,b):F(a)]$ must be bounded by $[F(b):F]=n$. The second equation means that b satisfies an irreducible algebraic equation with coefficients in F, which means that b again satisfies an algebraic equation (not necessarily irreducible) with coefficients in $F(a)$; still, this means that the degree of the minimal polynomial for b over $F(a)$ must be no more than n. Therefore, the equation $[F(a,b):F] = [F(a,b):F(a)][F(a):F]$ shows that $[F(a,b):F] \le mn$.

The inequality along with the divisibility relationship show that $[F(a,b):F] = mn$

Question #12.

Find an example of a field F and elements a and b from some extension field such that $F(a,b) \neq F(a)$, $F(a,b) \neq F(b)$, and $[F(a,b):F] < [F(a):F][F(b):F]$

By the proof of Question #11, the only way to do this is if $[F(a):F]$ and $[F(b):F]$ are not relatively prime. Let $F=Q$, and let $a=\sqrt[4]{2}$ and $b=\sqrt[6]{2}$. We have $[Q(\sqrt[4]{2}):Q]=4$ and $[Q(\sqrt[6]{2}):Q]=6$. But we can see that $Q(\sqrt[4]{2},\sqrt[6]{2}) \subseteq Q(\sqrt[12]{2})$, because $\sqrt[4]{2} = (\sqrt[12]{2})^3$ and $\sqrt[6]{2} = (\sqrt[12]{2})^2$.
Therefore, $[Q(\sqrt[4]{2},\sqrt[6]{2}):Q] \leq [Q(\sqrt[12]{2}):Q]=12$. In fact, this is an equality, since $4 \mid [Q(\sqrt[4]{2},\sqrt[6]{2}):Q]$ and $6 \mid [Q(\sqrt[4]{2},\sqrt[6]{2}):Q]$

perfect!

Question #13

Let K be field extension of F and let $a \in K$. Show that $[F(a):F(a^3)] \leq 3$
Find examples to illustrate that $[F(a):F(a^3)]$ can be 1, 2 or 3.

$F \subseteq F(a^3) \subseteq F(a)$

$|F(a):F(a^3)| \leq 1,2,3$

$= |F(a):F| = |F(a):F(a^3)| \cdot |F(a^3):F|$

2/2

$m(a)=0$ $g(x)=x^3-a^3 - F(a)$

$m_{a^3}=(x-a)^3$ a over $F(a^3)$

coefficient of this polynomial which is $1, -a^3$, which is contain in basis field $F(a^3)$

$f(x)=x^3-a^3$

$f(a)=0$

minimal poly of a over $F(a^3)$ must divide $f(x)$

$m_a | F(a^3)$ $(x-a)$

$\therefore \deg(m) | \deg(g)$ $\deg(g)=3$ so $|F(a):F(a^3)| / 3$

where m is the minimal polynomial of a over $F(a^3)$

$\deg(m) = |F(a):F(a^3)|$

$\therefore \deg(m)/3$

$\therefore \deg(m)$ must be ≤ 3

Case 1: $|F(a):F(a^3)| = 1$ $F=Q$, $a=1$

$F(a) \supseteq F(a^3)$

$|F(a):F(a^3)| = 1$ so $F(a^3)=F(a)$

$Q(2) = Q(2^3)$

$F(a)$ $F(a^3)$

$|K:F|=1 \qquad K \supseteq F$

K is a vector space over F, so there is a basis for K over F with degree 1. So if we pick any element in K it has a minimal polynomial that is less than or equal to 1.

If $a \in K$ then it has minimal polynomial of the form

$$a_1 x + b \qquad a, b \in F$$

$$a_1 x + b = 0$$

$$a = \frac{-b}{a_1} \in F$$

$F = K$

$|F(a):F(a^3)| = 1 \qquad F(a) = F(a^3)$

Case 2: For $[F(a):F(a^3)] = 2$ take $F = Q$, $a = (-1 + i\sqrt{3})/2$

$|Q(e^{2\pi i/3}) : Q(e^{2\pi i})| = |Q(e^{2\pi i/3}) : Q|$

$m \quad x^3 - 1 = 0$

$(x-1)(x^2+x+1) = 0$

$|Q(e^{2\pi i/3}) : Q|$ must be 1, 2, or 3. It can't be 1 b/c $e^{2\pi i/3} \notin Q$. It is less than 3 b/c $m \mid x^2+x+1$ so it must be 2

Case 3: Take $F = Q$ $a = \sqrt[3]{2}$

$3 = |Q(\sqrt[3]{2}) : Q(2)| = |Q(\sqrt[3]{2}) : Q| \quad \sqrt[3]{2}\,c = -2$

$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + bx + c)$

$x^3 = 2$

$\left(\frac{x}{2^{1/3}}\right)^3 = 1$

$\therefore$ the roots are $(2^{1/3}, 2^{1/3}e^{\frac{2\pi i}{3}}, 2^{1/3}e^{\frac{4\pi i}{3}})$

$f(x) = x^3 - 2$ $\quad f(\sqrt[3]{2}) = 0$ $\quad$ so $M_{\sqrt[3]{2}} | f$

Since $f(x)$ factors over $\mathbb{C} \setminus \mathbb{Q}$

it follows that $f(x) = M_{\sqrt[3]{2}}$

Question 16. Find the minimal polynomial for $\sqrt[3]{2} + \sqrt[3]{4}$ over Q.

Compute

$$x = 0 + \sqrt[3]{2} + \sqrt[3]{4}$$
$$x^2 = 4 + 2\sqrt[3]{2} + \sqrt[3]{4}$$
$$x^3 = 6 + 6\sqrt[3]{2} + 6\sqrt[3]{4}$$

Now, $x^3 = 6 + 6x$, so the minimal polynomial for $\sqrt[3]{2} + \sqrt[3]{4}$ is $x^3 - 6x - 6$; This is irreducible by applying the Eisenstein criterion either for $p = 2$ or $p = 3$

Question 18.

Suppose that $[E:Q]=2$. Show that there is an integer d such that $Z=Q(\sqrt{d})$ and d is not divisible by the square of any prime.

The $\deg\left(\frac{E}{Q}\right)=2$ $\alpha, B \in E$

$E = Q\alpha + QB$

Proof: $Q(\alpha,B)=E$

$Q(\alpha,B) \supset E$

Since E can be expressed as $E = Q\alpha + QB$ $\therefore$ the sum of $Q\alpha + QB$ is a linear combination in $Q(\alpha,B)$
$\therefore Q(\alpha,B) \supset E$

$E \supset Q(\alpha,B)$

E is an extension field of $Q(\alpha,B)$ and $\alpha, B \in E$
$\therefore E$ contains $Q(\alpha,B)$.

By the Primitive element Theorem, $r \in E$, $Q(r) = E = Q(\alpha,B)$

By theorem 21.1 Characterization of Extensions

$$Q(r) \cong Q[x] / \langle p(x) \rangle$$

$\deg P = 2$ P mini poly of r/Q

$P(x) = x^2 + ax + b \in Q[x]$

$\therefore$ the root $= \dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$

$= \mathbb{Q}\left(\frac{\pm\sqrt{a^2-4b}}{2}\right)$

$= \mathbb{Q}\left(\sqrt{a^2-4b}\right)$

$= \mathbb{Q}\left(m\sqrt{a^2-4b}\right)$ $\qquad D = m^2a^2 - m^2 4b \qquad m >> 0 \Rightarrow D \in \mathbb{Z}$

$= \mathbb{Q}\left(\sqrt{D}\right)$ $\qquad$ let $D = l^2 \cdot d$

$= \mathbb{Q}\left(l\sqrt{d}\right)$

$= \mathbb{Q}\left(\sqrt{d}\right)$