Problem 1

Answer the following:

(a) Find $u \in \mathbb{R}$ such that $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

(b) Describe how you would find all $w \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ such that $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

(Solution)

Let $\alpha = \sqrt{2} + \sqrt[3]{5}$. We claim that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. We already have $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ as $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$, so let's show the converse. Observe that we have the following:

$$\begin{aligned}
\alpha &= \sqrt{2} + \sqrt[3]{5} \\
\alpha - \sqrt{2} &= \sqrt[3]{5} \\
(\alpha - \sqrt{2})^3 &= 5 \\
\alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} &= 5 \\
\alpha^3 + 6\alpha - 5 &= \sqrt{2}(3\alpha^2 + 2)
\end{aligned}$$

But $3\alpha^2 + 2 \neq 0$, so we have

$$\sqrt{2} = (3\alpha^2 + 2)^{-1}(\alpha^3 + 6\alpha - 5) \in \mathbb{Q}(\alpha)$$

Then we also have $\sqrt[3]{5} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) \subset \mathbb{Q}(\alpha)$. So $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\alpha)$.

(b)

Note that $\sqrt{2}$ and $\sqrt[3]{5}$ are both algebraic over $\mathbb{Q}$ via

$$f = t^2 - 2 \quad \text{and} \quad g = t^3 - 5$$

respectively, which are both irreducible by Eisenstein. In particular, both polynomials are monic irreducible, so we have

$$m_{\mathbb{Q}}(\sqrt{2}) = t^2 - 2 \quad \text{and} \quad m_{\mathbb{Q}}(\sqrt[3]{5}) = t^3 - 5$$

In particular, by problem 2, we have $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) : \mathbb{Q}] = 6$. Moreover, we have that $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{5})$ for otherwise $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbb{Q}(\sqrt[3]{5})$ which contradicts that $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$. Similarly $\sqrt[3]{5} \notin \mathbb{Q}(\sqrt{2})$. Then we claim that

$$\mathcal{B} = \{1, \sqrt{2}, \sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{2}\sqrt[3]{5}, \sqrt{2}(\sqrt[3]{5})^2\}$$

is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. Certainly $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ is $\mathbb{Q}$-linearly as it is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt[3]{5})$. Then appending $\sqrt{2}$ keeps it linearly independent as $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{5})$. Also, $\sqrt{2}\sqrt[3]{5}$ is not a $\mathbb{Q}$-linear combination of $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{2}\}$ because it requires a irrational coefficient (i.e. $\sqrt{2}$ or $\sqrt[3]{5}$) so $\{1, \sqrt{2}, \sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{2}\sqrt[3]{5}\}$ is $\mathbb{Q}$-linearly independent. Similarly, $\{1, \sqrt{2}, \sqrt[3]{5}, (\sqrt[3]{5})^2, \sqrt{2}\sqrt[3]{5}, \sqrt{2}(\sqrt[3]{5})^2\}$ is $\mathbb{Q}$-linearly independent. Hence $\mathcal{B}$ is a linear independent set with $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) = 6$ elements, so is a basis.

Now to find all $w \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ such that $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. We can enumerate elements of $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ (as it is vector space over $\mathbb{Q}$) and for each $w \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$ compute the "change of basis" matrix from $\mathcal{B}$ to $\mathcal{C} = \{1, w, w^2, w^3, w^4, w^5\}$ (order them in some way) where we treat $\mathcal{C}$ as a basis. In particular if this matrix is invertible (use some method to compute), then $\mathcal{C}$ is indeed a basis so $\mathbb{Q}(w)$ has $\mathbb{Q}$-dimension 6, i.e. $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$. If this matrix is not invertible, then $\mathcal{C}$ is linearly dependent, so $[\mathbb{Q}(w) : \mathbb{Q}] < 6$ for otherwise $\mathcal{C}$ would be a basis, i.e. $\mathbb{Q}(w) \neq \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

Problem 2

If $a, b \in K$ are algebraic over F are of degree m, n respectively, with $(m, n) = 1$, show that $[F(a, b) : F] = mn$.

(Solution)

Since a, b are algebraic, we have that (Corollary 47.18) $F[a, b] = F(a, b)$ and

$$[F(a, b) : F] \leq [F(a) : F][F(b) : F] = mn$$

In particular, we have $F(a), F(b) \subset F(a, b)$, so

$$[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] = [F(a, b) : F(a)]m$$

and

$$[F(a, b) : F] = [F(a, b) : F(b)][F(b) : F] = [F(a, b) : F(b)]n$$

so $m, n \mid [F(a, b) : F]$. Then since m and n are relatively prime, we can use the Lemma 6.8 of the Chinese Remainder Theorem to get that $mn \mid [F(a, b) : F]$. So $[F(a, b) : F] = kmn$ for some $k \in \mathbb{Z}^+$ as degrees are positive. Our upper bound from above forces $k = 1$, so $[F(a, b) : F] = mn$.

Problem 3

If $|F| = q < \infty$ show:

(a) There exists a prime p such that char $F = p$.

(b) $q = p^n$ some n.

(c) $a^q = a$ for all $a \in F$.

(d) If $b \in K$ is algebraic over F then $b^{q^m} = b$ for some $m > 0$.

(Solution)

(a)

Let $\iota : \mathbb{Z} \to F$ denote the unique ring homomorphism. Since $\mathbb{Z}$ is a PID, write $\ker(\iota) = (p)$ where $p \in \mathbb{Z}$ unique up to units, so assume $p \geq 0$. By definition char $F = p$. If $p = 0$, then we have that ι is injective, but this is a contradiction as F is finite, so $p > 0$. Then by the First Isomorphism Theorem, $\mathbb{Z}/(p) \subset F$ a subring hence a domain, so (p) is a prime ideal, so p is a prime.

(b)

We have that F is a F-module. Then taking the induced homomorphism $\mathbb{Z}/(p) \to F$ via the First Iso. Theorem and ι, we have that F becomes a $\mathbb{Z}/(p)$-module. Then since nonzero prime ideal of a PID is maximal, we have that (p) is maximal, hence $\mathbb{Z}/(p)$ is a field, so F is a $\mathbb{Z}/p\mathbb{Z}$-vectorspace.

Moreover, F is finite, so it must be finite-dimensional, so for some $n \in \mathbb{Z}^+$, we have

$$F \cong (\mathbb{Z}/p\mathbb{Z})^n$$

so $q = |F| = |(\mathbb{Z}/p\mathbb{Z})^n| = p^n$.

(c)

Let $a \in F$. If $a = 0$, then the result is true. So assume $a \neq 0$. Then since F is a field, $a \in F^\times = F \setminus \{0\}$ the unit group of F. In particular $|F^\times| = q - 1$, so by Lagrange, $\mathrm{o}(a) \mid q - 1$. So $o(a) = k(q-1)$ some k. Then we have

$$a^q = a \cdot a^{q-1} = a \cdot a^{k\mathrm{o}(a)} = a(a^{\mathrm{o}(a)})^k = a(1)^k = a$$

as desired.

(d)

Suppose $b \in K$ is algebraic. Then $F(b)$ is a finite-dimensional F-vectorspace. In particular, $F(b) \cong F^m$ some m. Hence $|F(b)| = |F^m| = q^m$. If $b = 0$, then the result is certainly true, so assume $b \neq 0$. Then $b \in F(b)^\times$ the unit group of $F(b)$. So by Lagrange, $\mathrm{o}(b) \mid |F(b)^\times| = q^m - 1$; write $k \cdot \mathrm{o}(b) = (q^m - 1)$ Then we have

$$b^{q^m} = b \cdot b^{q^m - 1} = b \cdot b^{k \cdot \mathrm{o}(b)} = b(b^{\mathrm{o}(b)})^k = b(1)^k = b$$

as desired.

Problem 4

Let u be a root of $f = t^3 - t^2 + t + 2 \in \mathbb{Q}[t]$ and $K = \mathbb{Q}(u)$.

(a) Show that $f = m_{\mathbb{Q}}(u)$.

(b) Express $(u^2 + u + 1)(u^2 - u)$ and $(u-1)^{-1}$ in the form $au^2 + bu + c$, for some $a, b, c \in \mathbb{Q}$.

(Solution)

(a)

Since $f(u) = 0$ with $0 \neq f \in \mathbb{Q}[t]$, then we have that $m_{\mathbb{Q}}(u) \mid f$ in $\mathbb{Q}[t]$, so $f = m_{\mathbb{Q}}(u)g$ for some $g \in \mathbb{Q}[t]$. In particular since f is monic, we have that $\text{lead}(g) = 1$. Then if we can show that f is irreducible in $\mathbb{Q}$, it must be that $g \in \mathbb{Q}$, which would force $g = 1$ and hence $f = m_{\mathbb{Q}}(u)$. So it suffices to show f irreducible over $\mathbb{Q}$.

Suppose on the contrary that f is reducible over $\mathbb{Q}$, so

$$0 \neq f = gh$$

for some $g, h \in \mathbb{Q}[t] \setminus \mathbb{Q}$. In particular $0 < \deg(g), \deg(h)$. Then since $\mathbb{Q}$ is domain, we have that $3 = \deg(f) = \deg(g) + \deg(h)$ so one of g, h has degree 1. In particular this means that f has a rational root α. Then since f is monic, by rational root test, $\alpha \in \mathbb{Z}$.

If $\alpha = 0$, then $0 = f(\alpha) = 2 \neq 0$, a contradiction.

If $\alpha = 1$, then $0 = f(\alpha) = 1 - 1 + 1 + 2 = 3 \neq 0$, a contradiction. Similarly if $\alpha = -1$, then $0 = f(\alpha) = -1 - 1 - 1 + 2 = -1 \neq 0$.

If $\alpha > 1$, then $\alpha^3 - \alpha^2 > 0$, so $0 = f(\alpha) = \alpha^3 - \alpha^2 + \alpha + 2 > 3$, a contradiction.

If $\alpha < -1$, then $\alpha^3 < -1$, $-\alpha^2 < -1$ so $0 = f(\alpha) = \alpha^3 - \alpha^2 + \alpha + 2 < -3 + 2 = -1$ a contradiction.

As we have a contradiction in any case, it must be that f is irreducible, so we are done.

(b)

As u is a root of f, we have

$$u^3 - u^2 + u + 2 = 0 \iff u^3 = u^2 - u - 2$$

Then multpication by u gives

$$u^4 = u^3 - u^2 - 2u = u^2 - u - 2 - u^2 - 2u = -3u - 2$$

Then we have

$$\begin{aligned}(u^2 + u + 1)(u^2 - u) &= u^4 + u^3 + u^2 - u^3 - u^2 - u \\ &= u^4 - u \\ &= -4u - 2\end{aligned}$$

Then since $\{1, u, u^2\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(u)$, we may write $(u-1)^{-1} = au^2 + bu + c$ for $a, b, c \in \mathbb{Q}$. We shall now solve for a, b, c. We have that

$$\begin{aligned}
1 &= (u-1)(u-1)^{-1} \\
&= (u-1)(au^2 + bu + c) \\
&= au^3 + bu^2 + cu - au^2 - bu - c \\
&= a(u^2 - u - 2) + (b-a)u^2 + (c-b)u - c \\
&= bu^2 + (c - b - a)u + (-c - 2a)
\end{aligned}$$

then since $\mathbb{Q}$-vectorspace, the coordinates are unique, so we have the linear system

$$\begin{cases} b & = 0 \\ c - b - a & = 0 \\ -c - 2a & = 1 \end{cases}$$

So $b = 0$, which gives $c = a$ which gives $-3a = 1$ so $c = a = -\frac{1}{3}$. Hence

$$(u-1)^{-1} = -\frac{1}{3}u^2 - \frac{1}{3}$$

Problem 5

Let $\zeta = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6} \in \mathbb{C}$. Show that $\zeta^{12} = 1$ but $\zeta^r \neq 1$ for $1 \leq r < 12$. Show also that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ and find $m_{\mathbb{Q}}(\zeta)$.

(Solution)

We shall assume trig. identities. We show by induction on n that for any $\theta \in \mathbb{R}$,

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta)$$

The base case $n = 1$ is immediate. Then for the inductive step, assume $n \in \mathbb{Z}^+$ and that the result holds. Then we have (applying inductive hypothesis from lines 1 to 2):

$$\begin{aligned}(\cos\theta + i\sin\theta)^{n+1} &= (\cos\theta + i\sin\theta)(\cos\theta + i\sin\theta)^n \\ &= (\cos\theta + i\sin\theta)(\cos(n\theta) + i\sin(n\theta)) \\ &= \cos\theta\cos(n\theta) + i\cos\theta\sin(n\theta) + i\cos(n\theta)\sin\theta - \sin\theta\sin(n\theta)\end{aligned}$$

Then we have

$$\cos(\theta)\cos(n\theta) = \frac{1}{2}\left(\cos(\theta - n\theta) + \cos(\theta + n\theta)\right)$$

and

$$i\cos\theta\sin(n\theta) = i\frac{1}{2}\left(\sin(\theta + n\theta) - \sin(\theta - n\theta)\right)$$

and

$$\begin{aligned}i\cos(n\theta)\sin\theta &= i\frac{1}{2}\left(\sin(n\theta + \theta) - \sin(n\theta - \theta)\right) \\ &= i\frac{1}{2}\left(\sin(\theta + n\theta) + \sin(\theta - n\theta)\right)\end{aligned}$$

and

$$-\sin\theta\sin(n\theta) = -\frac{1}{2}\left(\cos(\theta - n\theta) - \cos(\theta + n\theta)\right)$$

Hence

$$(\cos\theta + i\sin\theta)^{n+1} = \cos(\theta + n\theta) + i\sin(\theta + n\theta) = \cos((n+1)\theta) + i\sin((n+1)\theta)$$

So by induction we are done. In particular

$$\zeta^{12} = \cos 2\pi + i\sin 2\pi = 1$$

Moreover, if $1 \leq r < 12$, then $\frac{\pi}{6} \leq \frac{r\pi}{6} < \frac{12\pi}{6} = 2\pi$, so $\cos\frac{r\pi}{6} \neq 1$. So viewing $\mathbb{C}$ as a $\mathbb{R}$-vectorspace with basis $\{1, i\}$, we have that $\zeta^r \neq 1$.

Note that $\cos\frac{\pi}{6} + i\sin\frac{\pi}{6} = \frac{\sqrt{3}}{2} + \frac{1}{2}i$. Then we have the following:

$$\begin{aligned}
\zeta &= \frac{\sqrt{3}}{2} + \frac{1}{2}i \\
\zeta - \frac{1}{2}i &= \frac{\sqrt{3}}{2} \\
\zeta^2 - i\zeta - \frac{1}{4} &= \frac{3}{4} \\
\zeta^2 - i\zeta &= 1 \\
\zeta^2 - 1 &= i\zeta \\
\zeta^4 - 2\zeta^2 + 1 &= -\zeta^2 \\
\zeta^4 - \zeta^2 + 1 &= 0
\end{aligned}$$

In particular ζ is a root of $f = t^4 - t^2 + 1 \in \mathbb{Q}[t]$ which is nonzero, so ζ is alg/$\mathbb{Q}$. Moreover, $m_{\mathbb{Q}}(\zeta) \mid f$ in $\mathbb{Q}[t]$. This means that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg m_{\mathbb{Q}}(\zeta) \leq 4$. Then since $\zeta \in \mathbb{Q}(\zeta)$, we have $\zeta^4 \in \mathbb{Q}(\zeta)$, so $\mathbb{Q}(\zeta^4) \subset \mathbb{Q}(\zeta)$. Then we have

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^4)][\mathbb{Q}(\zeta^4) : \mathbb{Q}]$$

We choose ζ^4 since $(\zeta^4)^3 = \zeta^{12} = 1$ so ζ^4 is a root to the polynomial

$$g = t^3 - 1 = (t-1)(t^2+t+1) \in \mathbb{Q}[t]$$

In particular since $\mathbb{Q}(\zeta^4)$ is a field hence domain, and $\zeta^4 - 1 \neq 0$, it must be that ζ^4 is a root to $t^2 + t + 1$. Moreover, suppose on the contrary that $t^2 + t + 1$ is reducible over $\mathbb{Q}$. Then it must be divisible by a linear polynomial, i.e. it has a rational root a. Then by the rational root test $a \in \mathbb{Z}$. But $a^2 + a \geq 0$ always so $a^2 + a + 1 > 0$, so a is not a root, which is a contradiction. Hence $t^2 + t + 1$ is irreducible over $\mathbb{Q}$. So $t^2 + t + 1$ is monic irreducible and has ζ^4 as a root, so it must be that $m_{\mathbb{Q}}(\zeta^4) = t^2 + t + 1$ and hence $[\mathbb{Q}(\zeta^4) : \mathbb{Q}] = 2$.

So now we know that $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is even, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2, 4$. If the former is true, then we must have that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^4)] = 1$, i.e. $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^4)$ which has $\mathbb{Q}$-basis $\{1, \zeta^4\}$ as its degree is 2. So $\zeta \in \mathbb{Q}(\zeta^4)$, so we can write

$$\zeta = a + b\zeta^4$$

for some $a, b \in \mathbb{Q}$. Then since $f(\zeta) = 0$, we have $\zeta^4 = \zeta^2 - 1$.So we have

$$\zeta = a + b(\zeta^2 - 1) = a - b + b\zeta^2$$

Then we have $\zeta^2 = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. So we have

$$\begin{aligned}
\frac{\sqrt{3}}{2} + \frac{1}{2}i &= a - b + b\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \\
\frac{\sqrt{3}}{2} + \frac{1}{2}i &= a - \frac{b}{2} + \frac{b\sqrt{3}}{2}i
\end{aligned}$$

Then viewing over $\mathbb{C}$ a $\mathbb{R}$-vectorspace under basis $\{1, i\}$, we must have

$$\frac{1}{2} = \frac{b\sqrt{3}}{2}$$

which means $b \notin \mathbb{Q}$, a contradiction. Hence $\zeta \notin \mathbb{Q}(\zeta^4)$ and hence $\mathbb{Q}(\zeta) \neq \mathbb{Q}(\zeta^4)$, so it must be that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta^4)] = 2$. Hence

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$$

as desired. Moreover, f satisfies $\deg f = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ and $f(\zeta) = 0$, so f is irreducible. But f is also monic so it must be that $m_{\mathbb{Q}}(\zeta) = f = t^4 - t^2 + 1$.

Problem 6

Let $K = F(u)$, u algebraic over F and of degree u odd. Show that $K = F(u^2)$.

(Solution)

Note that $u \in F(u)$ so $u^2 \in F(u)$ so $F(u^2) \subset F(u)$. So we have

$$[F(u) : F] = [F(u) : F(u^2)][F(u^2) : F]$$

In particular $[F(u) : F(u^2)] \mid [F(u) : F]$. We wish to show that $F(u) = F(u^2)$. It suffices to show that $[F(u) : F(u^2)] = 1$.

We proceed by showing that $F(u)$ is $F(u^2)$-spanned by a subset of cardinality at most 2, so its $F(u^2)$-dimension is at most 2. We claim that $\{1, u\}$ works for this. Let $x \in F(u)$. Then since u is algebraic over F, $F(u) = F[u]$, so write

$$x = \sum_{i=0}^{n} a_i u^i$$

some $a_i \in F$. Then we can separate the sum into:

$$\begin{aligned} x &= \sum_{k=0}^{\lfloor n/2 \rfloor} a_{2k} u^{2k} + \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} a_{2k+1} u^{2k+1} \\ &= \underbrace{\sum_{k=0}^{\lfloor n/2 \rfloor} a_{2k} (u^2)^k}_{\in F(u^2)} + \underbrace{\left(\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} a_{2k+1} u^{2k} \right)}_{\in F(u^2)} u \end{aligned}$$

Hence $F(u)$ is $F(u^2)$-spanned by a $\{1, u\}$, so $[F(u) : F(u^2)] \leq 2$. But it can't be 2 since it divides $[F(u) : F]$ which is odd, so it must be that $[F(u) : F(u^2)] = 1$. So $F(u) = F(u^2)$.

Problem 7

Let u be transcendental over F and $F < E \subset F(u)$. Show that u is algebraic over E.

(Solution)

Since u is trans/F, $u \notin F$, so $u \neq 0$. Then we have that

$$F(u) = qf(F[u])$$

Then since $F < E$, take $x \in E \setminus F$. Then since $x \in F(u) = qf(F[u])$, we can write

$$x = \frac{f(u)}{g(u)}$$

where $f, g \in F[t]$ and $g(u) \neq 0$. Note that if $u \mid f(u)$ and $u \mid g(u)$, then let m, n be such that $u^m \mid\mid f(u)$ and $u^n \mid\mid g(u)$, write $f(u) = u^m \tilde{f}(u)$ and $g(u) = u^n \tilde{g}(u)$ and assume WLOG $m \leq n$. Then we have

$$x = \frac{f(u)}{g(u)} = \frac{u^m \tilde{f}(u)}{u^n \tilde{g}(u)} = \frac{\tilde{f}(u)}{u^{n-m}\tilde{g}(u)}$$

So we can assume WLOG that u divides at most one of $f(u), g(u)$.

Then we have

$$xg(u) = f(u) \iff xg(u) - f(u) = 0$$

Define $h = xg - f \in E[t]$. We have that $h(u) = xg(u) - f(u) = 0$, so u is algebraic over E if we can show that $h \neq 0$. So suppose on the contrary that $h = 0$. Then $xg(0) - f(0) = 0$. If $g(0) \neq 0$, then we have

$$x = f(0)(g(0))^{-1} \in F$$

a contradiction, so it must be that $g(0) = 0$. But then we have

$$-0 = -xg(0) + f(0) = -0 + f(0) = f(0)$$

In particular this means that $t \mid f, g$ in $F[t]$. But this means that $f = t\tilde{f}$ and $g = t\tilde{g}$ for $\tilde{f}, \tilde{g} \in F[t]$. But then this means $f(u) = u\tilde{f}(u)$ and $g(u) = u\tilde{g}(u)$, so u divides both $f(u)$ and $g(u)$, which is a contradiction to our above assumption. Hence it must be that $h \neq 0$. So u is alg/E.

Problem 8

If $f = t^n - a \in F[t]$ is irreducible, $u \in K$ is a root of f and $n/m \in \mathbb{Z}$, show that $[F(u^m) : F] = \frac{n}{m}$. What is $m_F(u^m)$?

(Solution)

Let us denote $k = n/m$. Then

$$0 = f(u) = u^n - a = u^{mk} - a = (u^m)^k - a$$

so u^m is a root to $\widetilde{f} = t^k - a \in F[t]$. We claim that $\widetilde{f}$ is irreducible. So suppose on the contrary that $\widetilde{f}$ is reducible, so there exist nonunit (and nonzero) $g, h \in F[t]$ such that

$$\widetilde{f} = gh$$

Write $g = a_0 + \cdots + a_r t^r$ and $h = b_0 + \cdots + b_s t^s$. Then we have

$$\begin{aligned}
f &= t^n - a \\
&= t^{mk} - a \\
&= (t^m)^k - a \\
&= \widetilde{f}(t^m) \\
&= g(t^m)h(t^m) \\
&= (a_0 + \cdots + a_r t^{rm})(b_0 + \cdots + b_s t^{sm})
\end{aligned}$$

so f is reducible, a contradiction. Hence it must be that $\widetilde{f}$ is irreducible. So $\widetilde{f} \in F[t]$ is monic irreducible and $\widetilde{f}(u^m) = 0$, so it must be that $m_F(u^m) = \widetilde{f} = t^k - a$.

Problem 9

If a^n is algebraic over a field F for some $n > 0$, show that a is algebraic over F.

(Solution)

By definition, there exists $0 \neq f \in F[t]$ such that $f(a^n) = 0$. Write

$$f = \sum_{i=0}^{m} a_i t^i$$

Then set

$$g = \sum_{i=0}^{m} a_i t^{ni} \in F[t]$$

In particular g is nonzero as at least one a_i is nonzero. Then we have

$$g(a) = \sum_{i=0}^{m} a_i a^{ni} = \sum_{i=0}^{m} a_i (a^n)^i = f(a^n) = 0$$

so a is algebraic over F.

Problem 10

If $f \in \mathbb{Q}[t]$ and K is a splitting field of f over $\mathbb{Q}$, determine $[K : \mathbb{Q}]$ if f is:

(a) $t^4 + 1$

(b) $t^6 + 1$

(c) $t^4 - 2$

(d) $t^6 - 2$

(e) $t^6 + t^3 + 1$

(Solution)

We need nth roots of unity.

Lemma: Let $n \in \mathbb{Z}^+$ and set $\zeta_n \coloneqq e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) \in \mathbb{C}$. Then $\zeta_n^n = 1$ and $\zeta_n^r \neq 1$ for $1 \leq r < n$.

Proof. Same as problem 5. $\square$

(a)

Let $f = t^4 + 1$. Note that $\zeta_8, \zeta_8^3, \zeta_8^5$, and ζ_8^7 are roots to f. In particular, they are all distinct, so these all the roots of f. So $K = \mathbb{Q}(\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7) = \mathbb{Q}(\zeta_8)$. So we need $m_{\mathbb{Q}}(\zeta_8)$. We claim that $m_{\mathbb{Q}}(\zeta_8) = t^4 + 1$. It suffices to show that $t^4 + 1$ is irreducible in $\mathbb{Q}[t]$ since monic.

So suppose on the contrary that $t^4 + 1$ is reducible in $\mathbb{Q}[t]$, then we can write $t^4 + 1 = gh$, with $g, h \in \mathbb{Q}[t] \setminus \mathbb{Q}$, i.e. non-units. Note that neither g nor h can be degree 1 since $t^4 + 1$ has no rational roots (as none of the above roots are in $\mathbb{R}$). So both g and h are degree 2. Moreover, we can assume both are monic as $t^4 + 1$ is monic (we can factor out the leading coefficients and they must be inverses of each other). So write

$$g = t^2 + at + b$$

and

$$h = t^2 + xt + y$$

with $a, b, x, y \in \mathbb{Q}$. Then we have

$$\begin{aligned} t^4 + 1 = gh &= (t^2 + at + b)(t^2 + xt + y) \\ &= t^4 + xt^3 + yt^2 + at^3 + axt^2 + ayt + bt^2 + xbt + by \\ &= t^4 + (x + a)t^3 + (y + ax + b)t^2 + (ay + xb)t + by \end{aligned}$$

So matching coefficients gives us:

$$\begin{cases} x + a = 0 \\ y + ax + b = 0 \\ ay + xb = 0 \\ by = 1 \end{cases}$$

So $x = -a$ and we have

$$\begin{cases} y - a^2 + b = 0 \\ a(y-b) = 0 \\ by = 1 \end{cases}$$

Since $\mathbb{Q}$ is a domain, $a = 0$ or $y = b$. If the former is true then $y = -b$, so $-b^2 = 1$, not possible. If the latter is true, then $y = b = 1$ or $y = b = -1$ so $a^2 = \pm 2$, also not possible. So we reach a contradiction, so it must be that $t^4 + 1$ is irreducible.

In total, we have

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \deg m_{\mathbb{Q}}(\zeta_8) = 4$$

(b)

Let $f = t^6 + 1$. Note that $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^9, \zeta_{12}^{11}$ are distinct roots to f, hence

$$K = \mathbb{Q}(\zeta_{12}, \zeta_{12}^3, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^9, \zeta_{12}^{11}) = \mathbb{Q}(\zeta_{12})$$

We already computed $[K : \mathbb{Q}] = 4$ in problem 5, so same proof.

(c)

Let $f = t^4 - 2$. Note that $\sqrt[4]{2}$ is a root of f. Then since $\zeta_4^4 = 1$, we have that $\sqrt[4]{2}\zeta_4$, $\sqrt[4]{2}\zeta_4^2$ and $\sqrt[4]{2}\zeta_4^3$ are some other roots to f. In particular they are distinct by the lemma, i.e. $\zeta_4^r \neq 1$ for $1 \leq r < 4$. So we have

$$K = \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}\zeta_4, \sqrt[4]{2}\zeta_4^2, \sqrt[4]{2}\zeta_4^3) = \mathbb{Q}(\sqrt[4]{2}, \zeta_4)$$

The last equality is seen by $\sqrt[4]{2}, \sqrt[4]{2}\zeta_4, \sqrt[4]{2}\zeta_4^2, \sqrt[4]{2}\zeta_4^3 \in \mathbb{Q}(\sqrt[4]{2}, \zeta_4)$ and

$$\zeta_4 = (\sqrt[4]{2})^{-1}(\sqrt[4]{2}\zeta_4) \in \mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{2}\zeta_4, \sqrt[4]{2}\zeta_4^2, \sqrt[4]{2}\zeta_4^3)$$

Then since $\sqrt[4]{2}$ and ζ_4 are alg/$\mathbb{Q}$ via $t^4 - 2$ and $t^4 - 1$, we have the upper bound:

$$[\mathbb{Q}(\sqrt[4]{2}, \zeta_4) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_4) : \mathbb{Q}]$$

By Eisenstein, we have that $t^4 - 2$ is irreducible in $\mathbb{Q}[t]$. It is also monic, so $m_Q(\sqrt[4]{2}) = t^4 - 2$ Then notice that ζ_4 is a root to $t^2 + 1$ so $\deg m_{\mathbb{Q}}(\zeta_4) \leq 2$, but $\zeta_4 = i \notin \mathbb{Q}$, so $\deg m_{\mathbb{Q}}(\zeta_4) = 2$. So we have

$$[K : \mathbb{Q}] \leq 8$$

but $4 = [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \mid [K : \mathbb{Q}]$, so $[K : \mathbb{Q}] = 4$ or 8. But if $[K : Q] = 4$, then $[\mathbb{Q}(\sqrt[4]{2}, \zeta_4) : \mathbb{Q}(\sqrt[4]{2})] = 1$, so $\zeta_4 \in \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}[\sqrt[4]{2}]$. But this would mean that $\zeta_4 \in \mathbb{R}$, a contradiction, so it must be that

$$[K : \mathbb{Q}] = 8$$

(d)

Let $f = t^6 - 2$. Similarly to part (e), we have that the roots of f are

$$\sqrt[6]{2}, \sqrt[6]{2}\zeta_6, \sqrt[6]{2}\zeta_6^2, \sqrt[6]{2}\zeta_6^3, \sqrt[6]{2}\zeta_6^4, \sqrt[6]{2}\zeta_6^5$$

and

$$K = \mathbb{Q}(\sqrt[6]{2}, \sqrt[6]{2}\zeta_6, \sqrt[6]{2}\zeta_6^2, \sqrt[6]{2}\zeta_6^3, \sqrt[6]{2}\zeta_6^4, \sqrt[6]{2}\zeta_6^5) = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$$

By Eisenstein, we have $t^6 - 2$ is irreducible. Also monic, so $m_{\mathbb{Q}}(\sqrt[6]{2}) = t^6 - 2$. Note that ζ_6 is a root to $t^6 - 1 = (t^3 - 1)(t^3 + 1)$. In particular, ζ_6 is a root to $t^3 + 1$. We have that -1 is also a root to $t^3 + 1$ so factoring out $t + 1$ gives $t^3 + 1 = (t^2 - t + 1)(t + 1)$. In particular, we have that ζ_6 is a root to $t^2 - t + 1$. So $\deg m_Q(\zeta_6) \leq 2$. But $\zeta_6 \notin \mathbb{R}$ so $\zeta_6 \notin \mathbb{Q}$ so $\deg m_{\mathbb{Q}}(\zeta_6) = 2$.

So we have

$$[\mathbb{Q}(\sqrt[6]{2}, \zeta_6) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_6) : \mathbb{Q}] = 12$$

But $6 = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[6]{2}, \zeta_6) : \mathbb{Q}]$ so $[\mathbb{Q}(\sqrt[6]{2}, \zeta_6) : \mathbb{Q}] = 6$ or 12. If $[\mathbb{Q}(\sqrt[6]{2}, \zeta_6) : \mathbb{Q}] = 6$, then $[\mathbb{Q}(\sqrt[6]{2}, \zeta_6) : \mathbb{Q}(\sqrt[6]{2})] = 1$ so $\zeta_6 \in \mathbb{Q}(\sqrt[6]{2})$, so $\zeta_6 \in \mathbb{R}$, a contradiciton so

$$[K : \mathbb{Q}] = 12$$

(e)

Let $f = t^6 + t^3 + 1$. I used Wikipedia on cyclotomic polynomials to get that ζ_9 is a root to f. Direct computation also gives that $\zeta_9^2, \zeta_9^4, \zeta_9^5, \zeta_9^7, \zeta_9^8$ are also roots to f. These are all distinct by the lemma, so

$$K = \mathbb{Q}(\zeta_9, \zeta_9^2, \zeta_9^4, \zeta_9^5, \zeta_9^7, \zeta_9^8) = \mathbb{Q}(\zeta_9)$$

So it suffices to find $m_{\mathbb{Q}}(\zeta_9)$. We claim that $m_{\mathbb{Q}}(\zeta_9) = f$. It suffices to show that f is irreducible in $\mathbb{Q}[t]$ since it is monic. To do this, it suffices to show that $f(t+1) = (t+1)^6 + (t+1)^3 + 1$ is irreducible in $\mathbb{Q}[t]$ by the following argument: Suppose $f(t+1)$ is irreducible in $\mathbb{Q}[t]$ but $f(t)$ is reducible in $\mathbb{Q}[t]$. Then $f = gh$ for some non-units $f, g \in \mathbb{Q}[t]$. Then $f(t+1) = g(t+1)h(t+1)$, where neither $g(t+1)$ nor $h(t+1)$ are units (just look at leading term), a contradiction to $f(t+1)$ irreducible.

So let's show that $f(t+1)$ is irreducible. This follows by Eisenstein with $p = 3$ as we can expand $f(t+1)$ into $t^6 + 6t^5 + 15t^4 + 21t^3 + 18t^2 + 9t + 3$ using the Binomial Theorem.

So we have

$$[K : \mathbb{Q}] = \deg m_{\mathbb{Q}}(\zeta_9) = 6$$

Problem 11

Find the splitting fields K for $f \in \mathbb{Q}[t]$ and $[K : \mathbb{Q}]$ if f is:

(a) $t^4 - 5t^2 + 6$

(b) $t^6 - 1$

(c) $t^6 - 8$

(Solution)

We use the lemma from problem 10.

(a)

Let $f = t^4 - 5t^2 + 6$. Note that $t^4 - 5t^2 + 6 = (t^2 - 3)(t^2 - 2)$ and both these quadratic factors are irreducible in $\mathbb{Q}[t]$ by Eisenstein. The roots of $t^2 - 3$ are $\pm\sqrt{3}$ and the roots of $t^2 - 2$ are $\pm\sqrt{2}$. So the splitting field of f is

$$K = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

(note that we assume everything is in $\mathbb{C}$ so unique splitting field). We have an upper bound:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

We know the quadratic factors above are irreducible and monic, so we have $m_{\mathbb{Q}}(\sqrt{2}) = t^2 - 2$ and $m_{\mathbb{Q}}(\sqrt{3}) = t^2 - 3$. So we have

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] \leq 4$$

But $2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$, so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2$ or 4. But if $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2$, then $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$ so $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

But then we can write $\sqrt{3} = \frac{a}{b} + \frac{x}{y}\sqrt{2}$ for some $a, b, x, y \in \mathbb{Z}$ with $b, y \neq 0$. In particular $x \neq 0$ as $\sqrt{3}$ is not rational. Then we can assume WLOG that x, y are relatively prime. Then $a \neq 0$ for otherwise, we would have $3y^2 = 2x^2$ so y is even so $2x^2 = 3 \cdot 4k^2$ some k, so x is also even, so x, y are not relatively prime, a contradiction. So a, b, x, y are all nonzero.

Then clearing denominators will give

$$by\sqrt{3} = ay + bx\sqrt{2}$$

Squaring both sides gives

$$3b^2y^2 = a^2y^2 + 2abxy\sqrt{2} + 2b^2x^2$$

which gives

$$\sqrt{2} = \frac{3b^2y^2 - a^2y^2 - 2b^2x^2}{2abxy} \in \mathbb{Q}$$

a contradiction.

So it must be that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ so $[K : \mathbb{Q}] = 4$.

(b)

Let $f = t^6 - 1$. The distinct roots are $\zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5, 1$. So the splitting field is

$$K = \mathbb{Q}(\zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5, 1) = \mathbb{Q}(\zeta_6)$$

In problem 10, we found that $\deg m_{\mathbb{Q}}(\zeta_6) = 2$, so $[K : \mathbb{Q}] = 2$.

(c)

Let $f = t^6 - 8$. Note that $\sqrt{2}$ is a root of f. Also we have that $\sqrt{2}\zeta_6, \sqrt{2}\zeta_6^2, \sqrt{2}\zeta_6^3, \sqrt{2}\zeta_6^4, \sqrt{2}\zeta_6^5$ are also roots. These are all distinct by the lemma in problem 10. So the splitting field is

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{2}\zeta_6, \sqrt{2}\zeta_6^2, \sqrt{2}\zeta_6^3, \sqrt{2}\zeta_6^4, \sqrt{2}\zeta_6^5) = \mathbb{Q}(\sqrt{2}, \zeta_6)$$

In previous parts, we showed that $m_{\mathbb{Q}}(\sqrt{2}) = t^2 - 2$ and $\deg m_{\mathbb{Q}}(\zeta_6) = 2$. So we have

$$[\mathbb{Q}(\sqrt{2}, \zeta_6) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_6) : \mathbb{Q}] = 4$$

But $2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \zeta_6) : \mathbb{Q}]$ so $[\mathbb{Q}(\sqrt{2}, \zeta_6) : \mathbb{Q}] = 2$ or 4. But if $[\mathbb{Q}(\sqrt{2}, \zeta_6) : \mathbb{Q}] = 2$ then $[\mathbb{Q}(\sqrt{2}, \zeta_6) : \mathbb{Q}(\sqrt{2})] = 1$ so $\zeta_6 \in \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$, a contradiction. So it must be that

$$[K : \mathbb{Q}] = 4$$

Problem 12

Let $F = \mathbb{Z}/p\mathbb{Z}$ then show:

(a) There exists $f \in F[t]$ with $\deg f = 2$ and f irreducible.

(b) Use the f in (a) to construct a field with p^2 elements.

(c) If $f_1, f_2 \in F[t]$ have $\deg f_i = 2$ and f_i irreducible for $i = 1, 2$, show that their splitting fields are isomorphic.

(Solution)

(a)

If $p = 2$, then let $f = t^2 + t + 1 \in F[t] = (\mathbb{Z}/2\mathbb{Z})[t]$. In particular $f(0) = 0 + 0 + 1 = 1$ and $f(1) = 1 + 1 + 1 = 1$, so f has no roots in $F = \mathbb{Z}/2\mathbb{Z}$. If f was reducible, then $f = gh$ for nonunits $g, h \in \mathbb{Z}/2\mathbb{Z}$. But then g and h would be degree 1, so f would have roots in $F = \mathbb{Z}/2\mathbb{Z}$, a contradiction. So f is irreducible and degree 2.

If $p > 2$, then we claim that there exists a nonsquare in $F = \mathbb{Z}/p\mathbb{Z}$. To prove this, I got hint from https://math.stackexchange.com/questions/1094879/number-of-squares-in-mathbbz-p-mathbbz-times.

We define $\varphi : F^\times \to F^\times$ by $x \mapsto x^2$. This is certainly well-defined with $\varphi(1) = 1^2 = 1$ and $\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$ as $F^\times$ is abelian. So φ is a group homomorphism. In particular we have $\varphi(1) = 1$ and $\varphi(p-1) = p^2 - 2p + 1 = 1$ so $|\ker\varphi| \geq 2$. So by Lagrange, $|F^\times/\ker\varphi| < |F^\times|$. Then by the First Isomorphism Theorem , $\operatorname{im}\varphi \cong F^\times/\ker\varphi$, so $\operatorname{im}\varphi < F^\times$. So there exists a nonsquare in $F^\times$ and hence in F.

Let $a \in F$ be a nonsquare. Then let $f = t^2 - a$. In particular, if f was reducible, then it would have a root in F, so a would be a square in F, a contradiction. Hence f is irreducible and has degree 2.

(b)

Let $f \in F[t]$ be irreducible and degree 2. Then by Kronecker's Theorem, $K = F[t]/(f)$ is a field extension of F containing a root of f with $[K : F] = \deg f = 2$. In particular as a F-vectorspace, K has $|F|^2 = p^2$ elements.

(c)

Let E_i be a splitting field of f_i for $i = 1, 2$. We want to show that $E_1 \cong E_2$. Let $a_i, b_i \in E_i$ be the roots of f_i for $i = 1, 2$. Then $f_i = t^2 - (a_i + b_i)t + a_ib_i$. In particular, $-(a_i + b_i) \in F \subset F(b_i)$ so $b_i - a_i - b_i \in F(b_i)$ so $a_i \in F(b_i)$. So we have $E_i = F(a_i, b_i) = F(b_i)$ for $i = 1, 2$.

Then $\operatorname{lead}(f_i)^{-1}f_i$ is monic irreducible of degree 2 and has b_i as a root so $m_F(b_i) = \operatorname{lead}(f_i)^{-1}f_i$ and $[F(b_i) : F] = 2$. In particular $E_i = F(b_i)$ has p^2 elements (view as F-vectorspace).

Now consider the polynomial $t^{p^2} - t \in F[t]$. By problem 3, every element of E_i is a root to $t^{p^2} - t$. Moreover, E_i is a splitting field of $t^{p^2} - t$ over F as it contains all p^2 roots of $t^{p^2} - t$ and any smaller field would be missing some root. So by uniqueness of splitting fields, there exists an F-isomorphism $E_1 \to E_2$. In particular $E_1 \cong E_2$.

Problem 13

Let K/F and $f \in F[t]$. Show the following:

(a) If $\varphi : K \to K$ is an F-automorphism, then φ takes roots of f in K to roots of f in K.

(b) If $F \subseteq \mathbb{R}$ and $\alpha = a + ib$ is a root of f with $a, b \in \mathbb{R}$ then $\overline{\alpha} = a - ib$ is also a root of f.

(c) Let $F = \mathbb{Q}$. If $m \in \mathbb{Z}$ is not a square and $a + b\sqrt{m} \in \mathbb{C}$ is a root of f with $a, b \in \mathbb{Q}$, then $a - b\sqrt{m}$ is also a root of f in $\mathbb{C}$.

(Solution)

(a)

Write $f = a_0 + a_1 t + \cdots + a_n t^n$ where $a_i \in F$. Suppose $\alpha \in K$ is a root of f. We want to show that $\varphi(\alpha)$ is also a root of f. We have

$$\begin{aligned} 0 = \varphi(0) &= \varphi(f(\alpha)) \\ &= \varphi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \varphi(a_0) + \varphi(a_1)\varphi(\alpha) + \cdots + \varphi(a_n)\varphi(\alpha)^n \end{aligned}$$

since φ is a field homomorphism. Then since φ fixes F we have

$$0 = a_0 + a_1\varphi(\alpha) + \cdots + a_n\varphi(\alpha)^n = f(\varphi(\alpha))$$

as desired. Note that we don't actually need φ to be bijective.

(b)

Let $\overline{} : \mathbb{C} \to \mathbb{C}$ by $x + iy \mapsto x - iy$ with $x, y \in \mathbb{R}$ be complex conjugation. By part (a), it suffices to show that complex conjugation is an $\mathbb{R}$-homomorphism, hence a F-homomorphism. Viewing $\mathbb{C}$ as a $\mathbb{R}$-vectorspace with basis $\{1, i\}$ gives that $\overline{}$ is well-defined. Moreover, we have

$$\overline{0} = 0 \quad \text{and} \quad \overline{1} = 1$$

and

$$\overline{(a+ib)+(x+iy)} = \overline{(a+x)+i(b+y)} = a + x - i(b+y) = a - ib + x - iy = \overline{a+ib} + \overline{x+iy}$$

and

$$\overline{(a+ib)(x+iy)} = \overline{(ax-by)+i(ay+bx)} = ax - by - i(ay+bx) = (a-ib)(x-iy) = \overline{a+ib} \cdot \overline{x+iy}$$

So complex conjugation is a field homomorphism. Viewing $\mathbb{C}$ as an $\mathbb{R}$-vectorspace with basis $\{1, i\}$ also gives that complex conjugation fixes $\mathbb{R}$ and is hence a $\mathbb{R}$-homormorphism.

(c)

Note that $\sqrt{m}$ is alg/$\mathbb{Q}$ via $t^2 - m \in \mathbb{Q}[t]$. Suppose on the contrary that $t^2 - m$ is reducible in $\mathbb{Q}[t]$, then it factors into linear polynomials, so it has a rational root. By the rational root test, such a root is an integer which contradicts that m is not a square. So it must be that $t^2 - m$ is irreducible in $\mathbb{Q}[t]$. Hence $\mathbb{Q}(\sqrt{m})$ is a 2-dimensional $\mathbb{Q}$-vectorspace with basis $\{1, \sqrt{m}\}$. So define

$$\begin{aligned} \varphi : \mathbb{Q}(\sqrt{m}) &\to \mathbb{Q}(\sqrt{m}) \\ a + b\sqrt{m} &\mapsto a - b\sqrt{m} \end{aligned}$$

where $a, b \in \mathbb{Q}$. Following part (a), we just need to show that φ is a $\mathbb{Q}$-homomorphism. Viewing $\mathbb{Q}(\sqrt{m})$ as a $\mathbb{Q}$-vectorspace shows that φ is well-defined. Moreover, φ fixes $\mathbb{Q}$ and

$$\varphi(0) = 0 \quad \text{and} \quad \varphi(1) = 1$$

and

$$\varphi(a+b\sqrt{m}+x+y\sqrt{m}) = \varphi(a+x+(b+y)\sqrt{m}) = a+x-b\sqrt{m}-y\sqrt{m} = \varphi(a+b\sqrt{m})+\varphi(x+y\sqrt{m})$$

and

$$\begin{aligned} \varphi((a + b\sqrt{m})(x + y\sqrt{m})) &= \varphi(ax + bym + (ay + bx)\sqrt{m}) \\ &= ax + bym - (ay + bx)\sqrt{m} \\ &= (a - b\sqrt{m})(x - y\sqrt{m}) \\ &= \varphi(a + b\sqrt{m})\varphi(x + y\sqrt{m}) \end{aligned}$$

Hence φ is a $\mathbb{Q}$-homomorphism.

Problem 14

Prove any (field) automorphism $\varphi : \mathbb{R} \to \mathbb{R}$ is the identity automorphism.

(Solution)

I referenced https://math.stackexchange.com/questions/449404/is-an-automorphism-of-the-field-of-real-numbers-the-identity-map.

In particular, we assume density of $\mathbb{Q}$ in $\mathbb{R}$.

Note that since φ is a ring homomorphism, $\varphi(1) = 1$ and $\varphi(-1) = -1$. Then we immediately have that φ fixes $\mathbb{Z}$, i.e, for any $n \in \mathbb{Z}^{\geq 0}$, we have

$$\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = 1 + \cdots + 1 = n$$

and

$$\varphi(-n) = \varphi(-1 - \cdots - 1) = \varphi(-1) + \cdots + \varphi(-1) = -1 - \cdots - 1 = -n$$

We also get that φ fixes $\mathbb{Q}$:

$$\varphi(\frac{n}{m}) = \varphi(nm^{-1}) = \varphi(n)\varphi(m)^{-1} = nm^{-1} = \frac{n}{m}$$

Note that $\varphi(m) \neq 0$ as φ is injective so the multiplicative inverse makes sense.

Now this is where we got hint from stack exchange. We want to show that φ preserves $\leq$. So we want to show that if $r \leq s$, then $\varphi(r) \leq \varphi(s)$ iff $0 \leq \varphi(s) - \varphi(r)$ iff $0 \leq \varphi(s - r)$. It suffices to show that if $0 \leq x$ then $0 \leq \varphi(x)$. This is immediate as

$$0 \leq \varphi(\sqrt{x})^2 = \varphi(\sqrt{x}^2) = \varphi(x)$$

where $\sqrt{x} \in \mathbb{R}$ as $0 \leq x$. So φ preserves $\leq$. By injectivity, we also have that φ preserves $<$.

Now we prove the result. Let $r \in \mathbb{R}$. Suppose on the contrary that $\varphi(r) \neq r$. Then either $\varphi(r) < r$ or $r < \varphi(r)$. If the former is true, then by density of $\mathbb{Q}$ in $\mathbb{R}$ there exists $x \in \mathbb{Q}$ such that $\varphi(r) < x < r$. Then we have $x = \varphi(x) < \varphi(r)$, a contradiction. Similary if the latter is true, then by density of $\mathbb{Q}$ in $\mathbb{R}$ we have some $x \in \mathbb{Q}$ such that $r < x < \varphi(r)$. Then we have $\varphi(r) < \varphi(x) = x$, a contradiction.

Hence it must be that $\varphi(r) = r$, i.e. $\varphi = 1_{\mathbb{R}}$.

Problem 15

Let $p_1, \ldots, p_n$ be n distinct prime numbers. Let $f = (t^2 - p_1) \cdots (t^2 - p_n) \in \mathbb{Q}[t]$. Show that $K = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$ is a splitting field of f over $\mathbb{Q}$ and $[K : \mathbb{Q}] = 2^n$. Formulate a generalization of the statement for which your proof still works.

(Solution)

We have that $\pm\sqrt{p_1}, \ldots, \pm\sqrt{p_n}$ are $2n$ distinct roots of f, so a splitting field is

$$K = \mathbb{Q}(\pm\sqrt{p_1}, \ldots, \pm\sqrt{p_n}) = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$$

Then since $\sqrt{p_i}$ is alg/$\mathbb{Q}$ for all i via $t^2 - p_i$, we have that $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]$ as desired. Now we proceed by induction to show that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

For the base case we want to show that $[\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] = 2^1 = 2$. But this is immediate as $t^2 - p_1$ is irreducible by Eisenstein so it is the minimal polynomial of $\sqrt{p_1}$ over $\mathbb{Q}$.

For the inductive step, assume the result works for $n - 1$ distinct primes, i.e., assume that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}) : \mathbb{Q}] = 2^{n-1}$. Then we want to show that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$. We have

$$\begin{aligned}
[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})][\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}) : \mathbb{Q}] \\
&= [\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})]2^{n-1}
\end{aligned}$$

So it suffices to show $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})] = 2$. Let $L = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ and $F = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. We claim that $\mathcal{B} = \{1, \sqrt{p_n}\}$ is a F-basis of L.

To show that $\mathcal{B}$ F-generates, we use that

$$\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}] = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}][\sqrt{p_n}]$$

i.e. $L = F[\sqrt{p_n}]$. So if $\alpha \in L$, then we have

$$\alpha = a_0 + a_1(\sqrt{p_n}) + \cdots + a_n(\sqrt{p_n})^n$$

for some n and $a_i \in F$. In particular, we can write the odd and even terms separately:

$$\begin{aligned}
\alpha &= \sum_{k=0}^{\lfloor n/2 \rfloor} a_{2k}(\sqrt{p_n})^{2k} + \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} a_{2k+1}(\sqrt{p_n})^{2k+1} \\
&= \sum_{k=0}^{\lfloor n/2 \rfloor} a_{2k}(p_n)^k + \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} a_{2k+1}(p_n)^k(\sqrt{p_n})
\end{aligned}$$

But $p_n \in \mathbb{Z} \subset \mathbb{Q} \subset F$. So $\mathcal{B}$ F-generates L. In particular $[L : F] \leq 2$. But if $[L : K] = 1$, then we have $\sqrt{p_n} \in F = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. If we show that this is a contradiction, then we have finished the inductive step, so we would be done. We prove this contradiction below.

I tried to prove that $\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$ for all $n \geq 2$, where the p_i are distinct primes by induction, but I got stuck in some subcase in the inductive hypothesis. I found a generalization here: https://math.stackexchange.com/questions/1230173/elementary-proof-for-sqrtp-n1-notin-mathbbq-sqrtp-1-sqrtp-2

Theorem: Let $p_1, \ldots, p_n, q_1, \ldots, q_m \in \mathbb{Z}^+$ be $n+m$ distinct primes. Then $\sqrt{q_1 \cdots q_m} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$.

Proof. We induct on n. For the base case, assume $n = 1$. We want to show $\sqrt{q_1 \cdots q_m} \notin \mathbb{Q}(\sqrt{p_1})$. Suppose on the contrary that

$$\sqrt{q_1 \cdots q_m} \in \mathbb{Q}(\sqrt{p_1})$$

Then since $\sqrt{p_1}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $t^2 - p_1$ which is irreducible by Eisenstein, we can write

$$\sqrt{q_1 \cdots q_m} = a + b\sqrt{p_1}$$

for $a, b \in \mathbb{Q}$. In particular $b \neq 0$ for otherwise, we have $\sqrt{q_1 \cdots q_m} \in \mathbb{Q}$ which would imply that $t^2 - q_1 \cdots q_m$ is reducible over $\mathbb{Q}$, which contradicts Eisenstein as q_i are distinct. Moreover, $a \neq 0$ for otherwise, we would have

$$\sqrt{q_1 \cdots q_m} = b\sqrt{p_1}$$

so

$$\sqrt{q_1 \cdots q_m p_1} = bp_1 \in \mathbb{Q}$$

which would imply that $t^2 - q_1 \cdots q_m p_1$ is reducible over $\mathbb{Q}$ which contradicts Eisenstein. So neither a nor b is zero. So we have the following computation:

$$q_1 \cdots q_m = a^2 + 2ab\sqrt{p_1} + b^2 p_1$$
$$\sqrt{p_1} = \frac{q_1 \cdots q_m - a^2 - b^2 p_1}{2ab}$$

which would imply that $\sqrt{p_1} \in \mathbb{Q}$ which contradicts irreducibility of $t^2 - p_1$ over $\mathbb{Q}$. Hence it must be that the base case is satisfied, i.e., $\sqrt{q_1 \cdots q_m} \notin \mathbb{Q}(\sqrt{p_1})$.

For the inductive step, suppose true for $n-1$, that is for distinct primes $q_1, \ldots, q_m, p_1, \ldots, p_{n-1}$, $\sqrt{q_1 \cdots q_m} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$ (any m). Now suppose we have distinct primes $q_1, \ldots, q_m, p_1, \ldots, p_n$. Suppose on the contrary that $\sqrt{q_1 \cdots q_m} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Then we have

$$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}] = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}][\sqrt{p_n}] = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})[\sqrt{p_n}]$$

as $\sqrt{p_i}$ are all algebraic over $\mathbb{Q}$. Then we can write

$$\sqrt{q_1 \cdots q_m} = a_0 + \cdots + a_k(\sqrt{p_n})^k$$

for some k and $a_i \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. As above, we can separate the sum into even and odd terms and factor out a $\sqrt{p_n}$ to get

$$\sqrt{q_1 \cdots q_m} = a + b\sqrt{p_n}$$

for some $a, b \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. In particular we have that $b \neq 0$ for otherwise we have $\sqrt{q_1 \cdots q_m} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, a contradiction to the inductive hypothesis. Moreover, $a \neq 0$ for otherwise, we have

$$\sqrt{q_1 \cdots q_m} = b\sqrt{p_n}$$
$$\sqrt{q_1 \cdots q_m p_n} = bp_n$$

so $\sqrt{q_1 \cdots q_m p_n} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, a contradiction to the inductive hypothesis (with $q_{m+1} = p_n$). So neither a nor b are zero. As above, we can compute

$$\sqrt{p_n} = \frac{q_1 \cdots q_m - a^2 - b^2 p_n}{2ab} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$$

a contradiction to the inductive hypothesis. So it must be that

$$\sqrt{q_1 \cdots q_m} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$$

So we are done by induction. $\square$

(Generalization)

Now we make a generalization such that our proof still works. The main part of our proof was Eisenstein, which we know works in the following context by last quarter's homework.

Let R be a UFD and $qf(R)$ be the quotient field of R. Let $p_1, \ldots, p_n$ be distinct irreducible/prime elements in R. Let $f = (t^2 - p_1) \cdots (t^2 - p_n) \in qf(R)[t]$. Then $K = qf(R)[\sqrt{p_1}, \ldots, \sqrt{p_n}]$ is a splitting field of f over $qf(R)$ and $[K : qf(R)] = 2^n$.

Problem 16

Find a splitting field of $f \in F[t]$ if $F = \mathbb{Z}/p\mathbb{Z}$ and $f = t^{p^e} - t, e > 0$.

(Solution)

By problem 3, it suffices to find a field extension K of $F = \mathbb{Z}/p\mathbb{Z}$ of order p^e since then every element of K (there are exactly p^e distinct elements) would be a root of f, so f would split over K.

One way to construct such a field K is by finding an irreducible polynomial g of degree e over $\mathbb{Z}/p\mathbb{Z}$. Then $K = (\mathbb{Z}/p\mathbb{Z})[t]/(g)$ satisfies $[K : \mathbb{Z}/p\mathbb{Z}] = \deg g = e$, so viewing as a $\mathbb{Z}/p\mathbb{Z}$-vectorspace, K would have p^e elements.

I saw on stack exchange that we can use the Mobius inversion formula and some counting argument to find an irreducible polynomial of every degree over $\mathbb{Z}/p\mathbb{Z}$, but I couldn't follow.

So I will just show that a splitting field of f is order p^e, which is not really the question, but this could be used to get an irreducible polynomial fo degree e.

Let L be a splitting field of f over $F = \mathbb{Z}/p\mathbb{Z}$. Then set

$$K = \{\alpha \in L \mid f(\alpha) = 0\} = \{\alpha \in L \mid \alpha^{p^e} = \alpha\}$$

We claim that K is a field. Note that $1, 0 \in K$, so K is nonempt. Let $x, y \in K$. Since we can embed $\mathbb{Z}/p\mathbb{Z}$ into L, we have that L has characteristic p so the Children's Binomial Theorem holds, so we have

$$(x+y)^{p^e} = ((x+y)^p)^{p^{e-1}} = (x^p + y^p)^{p^{e-1}} = \cdots = x^{p^e} + y^{p^e} = x + y$$

and

$$(xy)^{p^e} = x^{p^e} y^{p^e} = xy$$

Moreover, if $p = 2$ then $-1 = 1$ so $(-1)^{p^e} = 1^{p^e} = 1 = -1$ and if $p > 2$ then p^e is odd, so $(-1)^{p^e} = -1$, so

$$(x-y)^{p^e} = x^{p^e} + (-y)^{p^e} = x + (-1)^{p^e} y = x - y$$

Hence K is a subring of L hence commutative. Lastly, suppose $x \in K \setminus \{0\}$. Then we have

$$(x^{-1})^{p^e} x^{p^e} = (x^{-1}x)^{p^e} = 1$$

so $(x^{-1})^{p^e} = (x^{p^e})^{-1} = x^{-1}$, so $x^{-1} \in K$, so K is a division ring hence a field. We then have that K contains all the roots of f, so f splits over K so it must be that $L = K$.

Now we show that $L = K$ has p^e elements. It suffices to show that no multiple roots. Note that $f' = p^e t^{p^e - 1} - 1 \in F[t]$ but since F is characterstic p, we have $f' = -1 \neq 0$, so it has no roots. If $\alpha \in K$ has multiplicity $r > 1$ then we can write (in $K[t]$)

$$f = (t - \alpha)^r g$$

where $g(\alpha) \neq 0$. Then

$$f' = r(t-\alpha)^{r-1} g + (t-\alpha)^r g'$$

so α is a root of f' as $r-1>0$, but this contradicts that f' has no roots. Hence f has no multiple roots, so it has exactly p^e distinct roots and hence $|K|=p^e$.

So by uniqueness of splitting fields, a splitting field of f has order p^e.

In particular, since K is a finite field, $K^\times$ is cyclic (Theorem 33.15). So it has a generator α, so $K=F(\alpha)$. Then we have

$$[F(\alpha):F]=[K:F]=e$$

so $m_F(\alpha)$ is irreducible in $F[t]$ of degree e, so we have that $F[t]/(m_F(\alpha))$ is field of degree e over F and hence has p^e elements and hence is a splitting field over f.

Problem 17

Let F be a field of characteristic $p > 0$. Show that $f = t^4 + 1 \in F[t]$ is not irreducible. Let K be a splitting field of f over F. Determine which finite field F must contain so that $K = F$.

(Solution)

We know that p must be (positive) prime as $\mathbb{Z}/(p) \subset F$ must be a domain. So we can consider two cases.

If $p = 2$, then we have $1 + 1 = 0$, so $-1 = 1$, so we have

$$f = t^4 + 1 = t^4 - 1 = (t^2 + 1)(t^2 - 1)$$

where neither quadratic factor is a unit, so f is irreducible.

(For other case, I got hint from https://math.stackexchange.com/questions/427439/why-is-x41-reducible-over-mathbb-f-p-with-p-geq-3-prime)

If $p > 2$, then we can write $p = 2k + 1$, some k. Since F is characteristic p, its prime subfield is $\triangle_F \cong \mathbb{Z}/p\mathbb{Z}$. In particular, we see that $f \in \triangle_F [t]$. Then observe that if we can show f is reducible over $\triangle_F$, then we can write

$$f = gh$$

for $g, h \in \triangle_F [t]$ non-units hence non-constant so at least degree 1. Then we have $g, h \in F[t]$ at least degree 1, so $f = gh$ in $F[t]$, so f is reducible over F. So it suffices to show that f is reducible over $\triangle_F$.

By problem 16, there exists a field extension L of $\triangle_F$ of order p^2. Note that

$$p^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k = 4k(k + 1)$$

where $k(k + 1)$ is even so $8 \mid p^2 - 1$. Then since $L^\times$ is cyclic and $|L^\times| = p^2 - 1$, there exists a cyclic subgroup $H = \langle \alpha \rangle$ of $L^\times$ of order 8. In particular, we have that $\alpha, \alpha^2, \ldots, \alpha^7$ are distinct. Moreover, they account for all of the roots of $t^8 - 1 \in \triangle_F [t]$, so $t^8 - 1$ splits over L. Note that we can write

$$t^8 - 1 = (t^4 + 1)(t^4 - 1)$$

so we have that $f = t^4 + 1$ splits over L. Then by well-ordering, there exists an intermediate field $L/E/\triangle_F$ such that E is a splitting field of $f = t^4 + 1$. Then suppose on the contrary that $f = t^4 + 1$ is irreducible over $\triangle_F$. Then consider a root $\beta \in E \subset L$ of f. Then we have that $f = m_{\triangle_F}(\beta)$, so $[\triangle_F (\beta) : \triangle_F] = 4$. But we have that $L/\triangle_F (\beta)/\triangle_F$ so $4 = [\triangle_F (\beta) : \triangle_F] \mid [L : \triangle_F] = 2$ a contradiction. So it must be that f is reducible over $\triangle_F$.

Hence f is reducible over F.

Now let K be a splitting field of f over F. In order for $K = F$, we need that F contains all the roots of f. By the above work, we have that all the roots of f are roots of $t^8 - 1$. So if F contains a finite field with 9 elements (they exist by problem 16), then F contains all the roots to $t^8 - 1$ and hence all the roots to f.

Problem 18

Let $f = t^6 - 3 \in F[t]$. Construct a splitting field K of f over F and determine $[K : F]$ for each of the cases: $F = \mathbb{Q}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}$. Do the same thing if f is replaced by $g = t^6 + 3 \in F[t]$.

(Solution)

We use the lemma in problem 10.

Case 1: Suppose $F = \mathbb{Q}$.

Splitting field of f:

Then the (distinct) roots of f are $\sqrt[6]{3}$, $\sqrt[6]{3}\zeta_6$, $\sqrt[6]{3}\zeta_6^2$, $\sqrt[6]{3}\zeta_6^3$, $\sqrt[6]{3}\zeta_6^4$, $\sqrt[6]{3}\zeta_6^5$. So we have a splitting field

$$K = \mathbb{Q}(\sqrt[6]{3}, \sqrt[6]{3}\zeta_6, \sqrt[6]{3}\zeta_6^2, \sqrt[6]{3}\zeta_6^3, \sqrt[6]{3}\zeta_6^4, \sqrt[6]{3}\zeta_6^5) = \mathbb{Q}(\sqrt[6]{3}, \zeta_6)$$

By Eisenstein, $t^6 - 3$ is irreducible over $\mathbb{Q}$, so $m_{\mathbb{Q}}(\sqrt[6]{3}) = t^6 - 3$. In problem 10, we showed that $\deg(m_{\mathbb{Q}}(\zeta_6)) = 2$, so we have

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{3}, \zeta_6) : \mathbb{Q}] \leq 12$$

But $6 = [\mathbb{Q}(\sqrt[6]{3}) : \mathbb{Q}] \mid [K : \mathbb{Q}]$, so $[K : \mathbb{Q}] = 6$ or 12. But if $[K : \mathbb{Q}] = 6$, then $[\mathbb{Q}(\sqrt[6]{3}, \zeta_6) : \mathbb{Q}(\sqrt[6]{3})] = 1$, so $\zeta_6 \in \mathbb{Q}(\sqrt[6]{3}) \subset \mathbb{R}$ a contradiction. So $[K : \mathbb{Q}] = 12$.

Splitting field of g:

Similarly, the (distinct) roots of g are $\sqrt[6]{-3}$, $\sqrt[6]{-3}\zeta_6$, $\sqrt[6]{-3}\zeta_6^2$, $\sqrt[6]{-3}\zeta_6^3$, $\sqrt[6]{-3}\zeta_6^4$, $\sqrt[6]{-3}\zeta_6^5$. So a splitting field is

$$L = \mathbb{Q}(\sqrt[6]{-3}, \sqrt[6]{-3}\zeta_6, \sqrt[6]{-3}\zeta_6^2, \sqrt[6]{-3}\zeta_6^3, \sqrt[6]{-3}\zeta_6^4, \sqrt[6]{-3}\zeta_6^5) = \mathbb{Q}(\sqrt[6]{-3}, \zeta_6)$$

But note that

$$\zeta_6 := \cos(\frac{2\pi}{6}) + i\sin(\frac{2\pi}{6}) = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \frac{1}{2} + \frac{\sqrt{-3}}{2}$$

but $\sqrt{-3} = (\sqrt[6]{-3})^3$, so $\zeta_6 \in \mathbb{Q}(\sqrt[6]{-3})$. So we have

$$L = \mathbb{Q}(\sqrt[6]{-3})$$

Then by Eisenstein, $t^6 + 3$ is irreducible over $\mathbb{Q}$, so $m_{\mathbb{Q}}(\sqrt[6]{-3}) = t^6 + 3$ so

$$[L : \mathbb{Q}] = 6$$

Case 2: Suppose $F = \mathbb{Z}/5\mathbb{Z}$.

Splitting field of f:

Let E be a splitting field of f over F. Note that if $\alpha \in E$ is a root of f, then we have $\alpha^6 = 3$ and we have

$$3^1 = 3 \text{ and } 3^2 = 9 = 4 \text{ and } 3^3 = 12 = 2 \text{ and } 3^4 = 6 = 1$$

so $\alpha^{24} = 3^4 = 1$. So in $E^\times$, the order of α divides 24, i.e. $|\langle\alpha\rangle| = 1, 2, 3, 4, 6, 8, 12$, or 24. Since $\alpha^6 = 3 \neq 1$, we cannot have $|\langle\alpha\rangle| = 1, 2, 3, 6$. Also if $|\langle\alpha\rangle| = 12$, then we would have

$1 = \alpha^{12} = 3^2 = 9 = 4$, a contradiction so α is either a primitive 4th, 8th or 24th root of unity. But note that $t^4 - 1 \in F[t]$ has at most 4 roots in an extension field so there are at most 4 distinct 4th roots of unity. Moreover $f' = 6t^5$ and 0 is not a root of $f = t^6 - 3$, so f has no multiple roots in E (we use same proof as in problem 16 and last quarter). Hence there exists a root of f in E which is not a 4th root of unity.

Now any extension of K of F has 5^n elements where $n \in \mathbb{Z}^+$. Moreover, $|K^\times| = 5^n - 1$ and is $K^\times$ is cyclic, so it has elements of every order dividing $5^n - 1$. In particular, we have

$$\begin{aligned} 5^1 - 1 &\equiv 4 \mod 24 \\ 5^2 - 1 &\equiv 24 \mod 24 \equiv 0 \mod 24 \end{aligned}$$

and

$$\begin{aligned} 5^1 - 1 &\equiv 4 \mod 8 \\ 5^2 - 1 &\equiv 24 \mod 8 \equiv 0 \mod 8 \end{aligned}$$

So the smallest field extension of F containing a (and hence all) primitive 8th roots of unity has degree 2. Same with primitive 24th roots of unity. Also a degree 2 extension contains all 4th roots of unity as $5^2 - 1 \equiv 0 \mod 4$. So a degree 2 extension of F contains all the roots of f. Also, above we have that f has no multiple roots, so it has 6 distinct roots so F is not a splitting field of F over f. So any degree 2 extension of F is a splitting field of f over F. Let's construct one. We just need a degree 2 irreducible polynomial. Note that 2 is not a square in F so $t^2 - 2 \in F[t]$ is irreducible over F, so a splitting field of f over F is $K = F[t]/(t^2 - 2)$ since $[K : F] = 2$.

Splitting field of g:

Let E be a splitting field of g over F. Note that $g = t^6 + 3 = t^6 - 2$ and 2 has order 4 in $E^\times$. So if $\alpha \in E$ is a root of $g = t^6 - 2$, then $\alpha^6 = 2$ so $\alpha^{24} = 2^4 = 1$. Then literally by the same argument as for f, we must have that $K = F[t]/(t^2 - 2)$ is a splitting field of g over F since $[K : F] = 2$.

Case 3: Suppose $F = \mathbb{Z}/7\mathbb{Z}$.

Splitting field of f:

Note that

$$\begin{aligned} 3^1 &= 3 \\ 3^2 &= 9 = 2 \\ 3^3 &= 6 \\ 3^4 &= 18 = 4 \\ 3^5 &= 12 = 5 \\ 3^6 &= 15 = 1 \end{aligned}$$

If α is a root of f in some extension field E over F, then we have $\alpha^6 = 3$ so $\alpha^{36} = 1$. So in $E^\times$, we have that $|\langle\alpha\rangle| = 1, 2, 3, 4, 6, 9, 12, 18, 36$. But since $3 \neq 1$ we cannot have that $|\langle\alpha\rangle| = 1, 2, 3, 6$. We also cannot have $|\langle\alpha\rangle| = 4$ for otherwise we have

$$1 = 1^6 = (\alpha^4)^6 = 3^4 = 4$$

Similarly, we cannot have $|\langle\alpha\rangle| = 9$ for otherwise

$$1 = (\alpha^9)^6 = 3^9 = 3^3 3^6 = 3^3 = 6$$

Similarly we cannot have $|\langle\alpha\rangle| = 12$ for otherwise,

$$1 = \alpha^{12} = (\alpha^6)^2 = 3^2 = 2$$

Finally we cannot have $|\langle\alpha\rangle| = 18$ for otherwise

$$1 = \alpha^{18} = 3^3 = 6$$

So it must be that $|\langle\alpha\rangle| = 36$, i.e α is a primitive 36th root of unity. Then any extension K of F has 7^n elements for some n. Moreover $|K^\times| = 7^n - 1$ and $K^\times$ is cyclc so it has elements of every order dividing $7^n - 1$. Since we have shown that every root of f is a primitive 36th root of unity, it suffices to find an extension of F containing a (hence all) primitive 36th roots of unity. We have

$$\begin{aligned}
7^1 - 1 &\equiv 6 \mod 36\\
7^2 - 1 &\equiv 12 \mod 36\\
7^3 - 1 &\equiv 18 \mod 36\\
7^4 - 1 &\equiv 24 \mod 36\\
7^5 - 1 &\equiv 30 \mod 36\\
7^6 - 1 &\equiv 0 \mod 36
\end{aligned}$$

By the same reasoning as in case 2, any field extension of F of degree 6 is a splitting field of f over F. By problem 16, there exists a field extension E of F of degree 6. Since $E^\times$ is cyclic it has a generator x. In particular $E = F(x)$. So $m_F(x)$ is degree 6. So $K = F[t]/(m_F(x))$ is a splitting field of f over F as $[K : F] = 6$.

<u>Splitting field of g</u>:

Note that $g = t^6 + 3 = t^6 - 4$. Moreover $4^1 = 4$, $4^2 = 16 = 2$ and $4^3 = 8 = 1$. So a root α of g in some extension E of F satisfies $\alpha^{18} = 1$. So $|\langle\alpha\rangle| = 1, 2, 3, 6, 9$, or 18. But since $4 \neq 1$ we have $|\langle\alpha\rangle| \neq 1, 2, 3, 6$. So every root of g is a primitive 9th or 18th root of unity. But note that

$$\begin{aligned}
7^1 - 1 &\equiv 6 \mod 9\\
7^2 - 1 &\equiv 3 \mod 9\\
7^3 - 1 &\equiv 0 \mod 9
\end{aligned}$$

and

$$\begin{aligned}
7^1 - 1 &\equiv 6 \mod 18\\
7^2 - 1 &\equiv 12 \mod 18\\
7^3 - 1 &\equiv 0 \mod 18
\end{aligned}$$

so any degree 3 extension of $F = \mathbb{Z}/7\mathbb{Z}$ is a splitting field as it contains all primitive 9th and 18th roots of unity hence all the roots of g (and any smaller degree doesn't). By inspection, we have that 2 is not a cube in F so $t^3 - 2$ is irreducible over F. So $K = F[t]/(t^3 - 2)$ is a splitting field since $[K : F] = 3$.

Problem 19

Show the following:

(a) If $f \in F[t]$, $\text{char}F = 0$, and the derivative $f' = 0$, show $f \in F$.

(b) If char $F = p \neq 0$, $f \in F[t]$, and $f' = 0$, then there exists $g \in F[t]$ such that $f(t) = g(t^p)$.

(Solution)

(a)

Write $f = a_0 + \cdots + a_n t^n$. Then $0 = f' = a_1 + \cdots + n a_n t^{n-1}$, so we have $ia_i = 0$ for all $i = 1, \ldots, n$. In particular $ia_i = a_i + \cdots + a_i = a_i(1 + \cdots + 1)$. But by characteristic zero $1 + \cdots + 1 \neq 0$, so since domain, $a_i = 0$, so $f = a_0 \in F$.

(b)

If f is constant, then $g = f$ works, so assume f is non-constant. Write $f = a_0 + \cdots + a_n t^n$. We claim that for all $1 \leq i \leq n$, if $a_i \neq 0$, then $p \mid i$. To see this, suppose $a_i \neq 0$ for $1 \leq i \leq n$. Then since $f' = 0$, we have $ia_i = 0$. But we have

$$ia_i = \underbrace{a_i + \cdots + a_i}_{i \text{ instances}} = a_i(\underbrace{1 + \cdots + 1}_{i \text{ instances}})$$

Since $a_i \neq 0$ and F is a domain, we must have that $\underbrace{1 + \cdots + 1}_{i \text{ instances}} = 0$. By the division algorithm write $i = pk + r$ with $r = 0$ or $r < p$. Using characteristic p, we have

$$\begin{aligned}
0 = \underbrace{1 + \cdots + 1}_{i \text{ instances}} &= \underbrace{1 + \cdots + 1}_{pk+r \text{ instances}} \\
&= \underbrace{1 + \cdots + 1}_{pk \text{ instances}} + \underbrace{1 + \cdots + 1}_{r \text{ instances}} \\
&= \underbrace{\underbrace{1 + \cdots + 1}_{p \text{ instances}} + \cdots + \underbrace{1 + \cdots + 1}_{p \text{ instances}}}_{k \text{ instances}} + \underbrace{1 + \cdots + 1}_{r \text{ instances}} \\
&= \underbrace{0 + \cdots + 0}_{k \text{ instances}} + \underbrace{1 + \cdots + 1}_{r \text{ instances}} \\
&= \underbrace{1 + \cdots + 1}_{r \text{ instances}}
\end{aligned}$$

In particular, if $r \neq 0$, then we contradict characteristic p, so it must be that $r = 0$, i.e, $p \mid i$. Then by division algorithm write $n = pk + r$ So we can rewrite

$$f = \sum_{i=0}^{k} a_{pi} t^{pi}$$

and $g = \sum_{i=0}^{k} a_{pi} t^i$ works.

Problem 20

Show if x is transcendental over F then $t^2 - x \in F(x)[t]$ is irreducible.

(Solution)

Suppose on the contrary that $t^2 - x$ is reducible over $F(x)$. Then f has a root $\alpha \in F(x)$. In particular, $\alpha^2 = x$, i.e. x is a square in $F(x)$. We want to show this is not possible. We have

$$F(x) = qf(F[x])$$

so if x is a square in $F(x)$, then there exists $f, g \in F[t]$ with $g(x) \neq 0$ such that

$$x = \left(\frac{f(x)}{g(x)}\right)^2$$

So we have

$$xg(x)^2 = f(x)^2$$

In particular define $h = tg^2 - f^2 \in F[t]$. In particular $h(x) = xg(x)^2 - f(x)^2 = 0$, but x is trans/F, so it must be that $h = 0$. So $tg^2 = f^2$ in $F[t]$. But since F is a domain, we have

$$\deg(tg^2) = \deg(t) + 2\deg(g) = 1 + 2\deg(g)$$

and

$$\deg(f^2) = 2\deg(f)$$

In particular we found an integer which is both odd and even, a contradiction, so it must be that $t^2 - x$ is irreducible over $F(x)$.

Problem 21

Suppose that char $F = p \neq 0$. Show the following:

(a) The map $F \to F$ given by $x \mapsto x^p$ is a monomorphism. Denote its image F^p.

(b) If K/F is algebraic and $\alpha \in K$ is separable over $F(\alpha^p)$, then $\alpha \in F(\alpha^p)$.

(c) Every finite field is perfect, i.e. every algebraic extension is separable.

(Solution)

(a)

This is the Frobenius homomorphism $\varphi : F \to F$ by $x \mapsto x^p$ from last quarter. Note that it suffices to show that φ is a (ring/field) homomorphism as fields are simple and $1^p = 1 \neq 0$ so $\ker \varphi = 0$. So let's show that φ is a ring homomorphism, hence field homomorphism.

Certainly, φ is well-defined as if $x = y$, then $x^p = y^p$. Then let's verify the ring homomorphism properties:

$$\varphi(0) = 0^p = 0 \cdots 0 = 0$$

and

$$\varphi(1) = 1^p = 1 \cdots 1 = 1$$

and

$$\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$$

by commutativity of multiplication. Since $\mathrm{char}(R) = p$ prime, we have that $1 + \cdots + 1 = p1 = 0$. Then by the binomial Theorem, we have

$$\begin{aligned}
\varphi(x+y) = (x+y)^p &= \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} \\
&= x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} \\
&= \varphi(x) + \varphi(y) + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i}
\end{aligned}$$

But then we have that $p \mid \binom{p}{i}$ for $i = 1, \cdots p-1$ as a result from Euclid's Lemma (Corollary 2.15 from textbook). So we have

$$\sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} = +\sum_{i=1}^{p-1} \binom{p}{i} 1_R x^i y^{p-i}$$

where $\binom{p}{i} = k_i p$ for some $k_i \in \mathbb{Z}$, so those terms vanish as $p1 = 0$.

(b)

Since $\alpha \in K$ is sep$/F(\alpha^p)$, there exists $f \in F(\alpha^p)[t]$ such that $f(\alpha) = 0$ and f is sep$/F(\alpha^p)$. In particular, α is alg$/F(\alpha^p)$. So $m_{F(\alpha^p)}(\alpha) \mid f$, so $m_{F(\alpha^p)}(\alpha)$ is an irreducible factor of f hence sep$/F(\alpha^p)$.

Now if we can show that $m_{F(\alpha^p)}(\alpha)$ has degree 1, then we will have

$$[F(\alpha^p)(\alpha) : F(\alpha^p)] = 1$$

so $\alpha \in F(\alpha^p)$ as desired. So let's do this.

Note that $g = t^p - \alpha^p \in F(\alpha^p)[t]$ has α as a root, so $m_{F(\alpha^p)}(\alpha) \mid g$ in $F(\alpha^p)[t]$. We can bring this up to $K[t]$ to get $m_{F(\alpha^p)}(\alpha) \mid g$ in $K[t]$. But using Children's Binomial Theorem (as in part a), we know the irreducible factors of g in $K[t]$, i.e.

$$g = (t - \alpha)^p$$

So $m_{F(\alpha^p)}(\alpha) = (t - \alpha)^k$ for some $1 \leq k \leq p$, but if $k > 1$ then $m_{F(\alpha^p)}(\alpha)$ has a multiple root α in $K[t]$, a contradiction to seperability.

(c)

Looking at the wikipedia page for perfect fields, I saw that fields are perfect if the Frobenius endomorphism is an automorphism. So we proceed in this fashion.

First we show that $\varphi : F \to F$ by $x \mapsto x^p$ is an automorphism. By part (a), it suffices to show that φ is surjective. But this is immediate as F is finite and φ is injective.

Now we show that since φ is an automorphism, F is perfect. Let K/F be algebraic. Let $\alpha \in K$. We want to show that α is sep$/F$. Since α is alg$/F$, we have $m_F(\alpha)$ exists. So it suffices to show that $m_F(\alpha)$ is separable, i.e has no multiple roots in any extension of F. We will prove in general that any irreducible polynomial $f \in F[t]$ is separable over F.

Suppose not. Then f has a multiple root $\beta \in F$. Then β is also a root of f'. Since f is irreducible, it is an associate of $m_F(\beta)$, which divides f' so $f \mid f'$. So $\deg f' \geq \deg f$ or $f' = 0$. The former is not possible, so $f' = 0$. So by problem 19, $f = \sum a_i t^{pi}$ for some $a_i \in F$. But since φ is an automorphism, we have that $\widetilde{\varphi}(f) = \sum a_i^p t^{pi}$ is irreducible. But then we can apply the Children's Binomial Theorem again to get

$$\widetilde{\varphi}(f) = \sum a_i^p t^{pi} = \sum (a_i t^i)^p = (\sum a_i t^i)^p$$

In particular, $\widetilde{\varphi}(f)$ is reducible over F, a contradiction. Hence it must be that f is separable over F. Hence all irreducible factors of all nonconstant polynomials are separable, so α is sep$/F$, so K/F is separable.

Hence F is perfect.

Problem 22

Suppoes that char $F = p \neq 0$. Show the following:

(a) If K/F is separable then $K = F(K^p)$.

(b) Suppose that K/F is finite and $K = F(K^p)$. If $\{x_1, \dots, x_n\} \subset K$ is linearly independent over F, then so is $\{x_1^p, \dots, x_n^p\}$.

(c) If K/F is finite and $K = F(K^p)$, then K/F is separable.

(Solution)

(a)

It suffices to show $K \subset F(K^p)$. So suppose $x \in K$. Then x is separable over F, so $m_F(x)$ has no multiple roots in any extension field of F. In particular, $m_F(x) \in F[t] \subset F(x^p)[t]$, so we have that $m_{F(x^p)}(x) \mid m_F(x)$ in $F(x^p)[t]$. Then $m_{F(x^p)}(x)$ cannot have any multiple roots in any extension field for otherwise, $m_F(x)$ would, so x is separable over $F(x^p)$.

Then note that K/F separable implies K/F algebraic so we can apply problem 21(b) to get that $x \in F(x^p) \subset F(K^p)$. So we are done.

(b)

From linear algebra, we know that injective linear maps preserve linear independence, so we wish to find an injective linear map. Also, WLOG assume that $\{x_1, \dots, x_n\}$ is an F-basis for K as we can just extend it to a basis and the same proof will apply.

Linear transformations are completely determined by where they send basis vectors so define

$$T : K \to K$$

by $x_i \mapsto x_i^p$ for each $i = 1, \dots, n$. This is an F-linear map. We need to to be injective. Since K is a finite dimensional F-vectorspace, it suffices to show that T is surjective by rank-nullity theorem. So we need to show that im $(T) = K$. It suffices to show that $K \subset$ im (T).

We first show that im (T) is a subfield of K. It is immediately an additive subgroup since it is an F-submodule of K. Then note that if $a_i, b_i \in F$ for $i = 1, \dots, n$ then

$$\begin{aligned}\left(\sum_{i=0}^{n} a_i x_i^p\right)\left(\sum_{j=0}^{n} b_j x_j^p\right) &= \sum_{i=0}^{n}\left(a_i x_i^p \sum_{j=0}^{n} b_j x_j^p\right) \\ &= \sum_i \sum_j a_i b_j x_i^p x_j^p\end{aligned}$$

Then note that if $x \in K^p$, we can write $x = (\sum c_i x_i)^p = \sum c_i^p x_i^p$, so $x = T(\sum c_i^p x_i) \in$ im (T), hence $K^p \subset$ im (T). So we have $x_i^p x_j^p = (x_i x_j)^p \in K^p \subset$ im (T). Then since im (T) is a F-submodule of K, we have that the above product of sums is in im (T). Moreover $1 = 1^p \in K^p \subset$ im (T), so im (T) is a multiplicative submonoid of K. Hence im (T) is a (commutative) subring of K hence domain.

To show that im (T) is a field, I got a hint from this: https://math.stackexchange.com/questions/3161381/why-does-the-integral-domain-being-trapped-between-a-finite-field-extension-im/

To show that im (T) is a field, we need to show that it is a division ring so let $0 \neq a \in$ im (T). Define λ_a : im $(T) \to$ im (T) by $x \mapsto ax$. Certainly this is well-defined. Moreover if $r \in F$ and $x, y \in$ im (T), we have

$$\lambda_a(rx + y) = a(rx + y) = arx + ay = rax + ay = r\lambda_a(x) + \lambda_a(y)$$

hence λ_a is F-linear. It is also injective as im (T) is a domain, i.e. if $ax = 0$ then $x = 0$. Then since K/F is finite, im $(T)/F$ is finite-dimensional so by rank-nullity λ_a is surjective. And since $1 \in$ im (T), we have that there exists $b \in$ im (T) such that $\lambda_a(b) = ab = 1$, so im (T) is a division ring.

So im (T) is a field. In particular since $1 \in$ im (T) and im (T) is a F-vectorspace we have $r = r \cdot 1 \in$ im (T) for all $r \in F$, so $F \subset$ im (T). Moreover $K^p \subset$ im (T) so since a field, $K = F(K^p) \subset$ im (T).

Hence T is surjective and since K is finite-dimensional over F we have that T is injective by rank-nullity. Then if $\sum c_i x_i^p = 0$ then $0 = T(\sum c_i x_i)$ so by injectivity, $\sum c_i x_i = 0$ so by linear independence $c_i = 0$ for all i, so we are done.

(c)

We use the following lemma, which I got from https://math.stackexchange.com/questions/4534051/show-alpha-is-separable-over-a-field-f-iff-f-alpha-f-alphap:

Lemma: Assume K/F finite and char $F = p \neq 0$. If $\alpha \in K$ is not separable over F, then $[F(\alpha) : F] = p[F(\alpha^p) : F]$.

Proof. If $\alpha \in K$ is not separable over F, then $m_F(\alpha)$ has a multiple root in some extension field so it has a common root with its derivative, hence $m_F(\alpha) \mid m_F(\alpha)'$. But since $\deg m_F(\alpha)' < \deg m_F(\alpha)$, we must have $m_F(\alpha)' = 0$, so by problem 19(b), $m_F(\alpha) = g(t^p)$ for some $g \in F[t]$.

In particular, $g(\alpha^p) = m_F(\alpha)(\alpha) = 0$ and g is forced to be monic. Moreover if g is reducible over F then so is $m_F(\alpha)$, so g must be irreducible. Hence $g = m_F(\alpha^p)$. This gives the result as $\deg m_F(\alpha) = p \deg g$. $\square$

Now let $[K : F] = n < \infty$. Let $\alpha \in K$. To show that α is sep/F, it suffices to show that $F(\alpha) = F(\alpha^p)$ by the lemma (if not separable, then contradiction by degrees).

Note that $F(\alpha^p) \subset F(\alpha)$ is already an F-subspace so it suffices to show that they have the same degree as F-vectorspaces (since finite dimensional vector spaces).

Since K/F is finite, $F(\alpha)/F$ has some degree $m \leq n < \infty$, so α is algebraic so $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a F-basis for $F(\alpha)$. In particular by part (b), $\{1, \alpha^p, \ldots, \alpha^{p(m-1)}\} \subset F(\alpha^p)$ is linearly independent over F. Hence $F(\alpha^p)/F$ is degree m, so we are done.

Problem 23

Let K/F. Show the following:

(a) If $\alpha \in K$ is separable over F, then $F(\alpha)/F$ is separable.

(b) If $\alpha_1, \ldots, \alpha_n \in K$ are separable over F, then $F(\alpha_1, \ldots, \alpha_n)/F$ is separable.

(c) Let $F_{\text{sep}} = \{\alpha \in K \mid \alpha \text{ separable over } F\}$. Then F_{sep} is a field.

(Solution)

(a)

If char $F = 0$, then let $f \in F[t]$ be irreducible. Then if f is not separable over f, then f' and f share a common root x. But since irreducible, $f \approx m_F(x) \mid f'$, so $f' = 0$ since $\deg f' < \deg f$. But then by problem 19(a), $f \in F$, a contradiction to irreducible. So all irreducible polynomials in $F[t]$ are separable. So if $\alpha \in K$ is sep$/F$, then α is algebraic over F, so $F(\alpha)/F$ is finite so algebraic. So $F(\alpha)/F$ is separable as every minimal polynomial over F is separable so all elements in $F(\alpha)$ are separable.

So we can assume that char $F = p \neq 0$. Then by assumption, we have $m_F(\alpha)$ is separable over F. Moreover $m_F(\alpha) \in F[t] \subset F(\alpha^p)[t]$, so $m_{F(\alpha^p)}(\alpha) \mid m_F(\alpha)$. But then $m_{F(\alpha^p)}(\alpha)$ must be separable, i.e., have no multiple roots in any extension field, for otherwise $m_F(\alpha)$ would be not separable. Hence α is separable over $F(\alpha^p)$.

Then by problem 21(b), $\alpha \in F(\alpha^p) \subset F(F(\alpha)^p)$. So $F(\alpha) = F(F(\alpha)^p)$. So by problem 22(c), we have that $F(\alpha)/F$ is separable.

(b)

Again it suffices to do case when char $F = p \neq 0$.

By part (a), we have that $\alpha_i \in F(\alpha_i^p) \subset F(K^p)$ for all i where $K = F(\alpha_1, \ldots, \alpha_n)$. Hence $K = F(K^p)$. So by problem 22(c), K/F is separable.

(c)

Let $\alpha, \beta \in F_{\text{sep}}$. Note that $0, 1 \in F \subset F_{\text{sep}}$. So it suffices to show that $\alpha\beta, \alpha \pm \beta \in F_{\text{sep}}$ and $\beta^{-1} \in F_{\text{sep}}$ when $\beta \neq 0$. Let $\gamma = \alpha\beta, \alpha \pm \beta$ or β^{-1} (if $\beta \neq 0$). Then we have

$$\gamma \in F(\alpha, \beta)$$

By part (b), $F(\alpha, \beta)/F$ is separable, so γ is separable over F, i.e. $\gamma \in F_{\text{sep}}$.

Problem 24

Show any algebraic extension of a perfect field is perfect.

(Solution)

Let F be a perfect field, i.e. every algebraic extension is separable. Then let K/F be an algebraic extension. Let L/K be an algebraic extension. Let $\alpha \in L$. We wish to show that α is sep/K. Note that we have that L/F is algebraic, so α is sep/F. So $m_F(\alpha)$ is separable. Then viewing in $K[t]$, we have that $m_K(\alpha) \mid m_F(\alpha)$, so $m_K(\alpha)$ must be separable otherwise $m_F(\alpha)$ isn't, so α is sep/K. Hence L/K is separable and hence K is perfect.

Problem 25

Let F_o be a field of characteristic $p > 0$, $F = F_o(t_1^p, t_2^p)$, and $L = F_o(t_1, t_2)$. Show

(a) If $\theta \in L \setminus F$, then $[F(\theta) : F] = p$.

(b) There exist infinitely many fields K satisfying $F < K < L$.

(Solution)

(a)

Note that we can write $L = F(t_1, t_2)$. Then note that t_i is algebraic over F via $t^p - t_i^p \in F[t]$. So $[F(t_i) : F] \leq p$, so $[L : F] \leq [F(t_1) : F][F(t_2) : F] \leq p^2$ and $F(t_1, t_2) = F[t_1, t_2]$.

Then suppose $\theta \in L \setminus F$. Then we can write

$$\theta = \sum_{i,j} a_{ij} t_1^i t_2^j$$

for some $a_{ij} \in F$. Then since characterisitic p, we have

$$\theta^p = \sum_{i,j} a_{ij}^p t_1^{pi} t_2^{pj} \in F$$

So $f = t^p - \theta^p \in F[t]$. To get $[F(\theta) : F] = p$, it suffices to show that f is irreducible over F. So suppose on the contrary that f is reducible over F. We can bring f up to $L[t]$ where we can write $f = t^p - \theta^p = (t - \theta)^p$. Since we assume that f is reducible over F and we have $m_F(\theta) \mid f$ over F, we must have that $\deg(m_F(\theta)) < p$. So we can write $m_F(\theta) = (t - \theta)^k = t^k - \theta^k \in F[t]$ for some $1 \leq k < p$. In particular $\theta^k \in F$ and $(k, p) = 1$ since p prime. So there exist integers x, y such that $px + ky = 1$ so we have

$$\theta = \theta^{px+ky} = (\theta^p)^x (\theta^k)^y \in F$$

a contradiction. So it must be that f is irreducible over F hence $m_F(\theta) = f$ and $[F(\theta) : F] = \deg f = p$.

(b)

Based on the question, we will assume that $F < L$, so by part (a), we have $[L : F] \leq p^2$ and $p \mid [L : F]$. So we have $[L : F] = p$ or p^2. However, if $[L : F] = p$, then there are no (strictly) intermediate fields K such that $F < K < L$ as $[K : F] \mid [L : F]$ and p is prime. So we will further assume that $[L : F] = p^2$.

In particular this forces $t_1, t_2 \notin F$ (if both were in F then $L = F$ and if exactly one is in F then by part a we would have $[L : F] = p$). By part (a) and our assumption that $[L : F] = p^2$, it suffices to show that the following set is not finite

$$\mathcal{S} = \{F(\theta) \mid \theta \in L \setminus F\}$$

To do this, I got hint from: https://math.stackexchange.com/questions/4107031/intermediate-fields-between-kx-y-and-kxp-yp

For each $n \in \mathbb{Z}^+$, define $\theta_n := t_1 + t_1^{pn} t_2 \in L$. We claim that $\theta_n \notin F$. Suppose on the contrary that $\theta_n \in F \subset F(t_2)$. Then we would have that $t_1 \in F(t_2) = F_o(t_1^p, t_2)$. But this would imply that $F(t_2) = F(t_1, t_2) = L$, which would imply by part (a) that $[L : F] = [F(t_2) : F] = p$, a contradiction to our assumption that $[L : F] = p^2$.

Hence we have $\theta_n \in L \setminus F$, so $F(\theta_n) \in \mathcal{S}$. Now to show that $\mathcal{S}$ is not finite, it suffices to show that if $m \neq n \in \mathbb{Z}^+$ then $F(\theta_n) \neq F(\theta_m)$, i.e that we can inject $\mathbb{Z}^+$ into $\mathcal{S}$ via $n \mapsto F(\theta_n)$.

Suppose on the contrary that $F(\theta_n) = F(\theta_m)$ where $n \neq m$. Then $\theta_n \in F(\theta_m)$. So we have $\theta_n - \theta_m \in F(\theta_m)$, i.e.,

$$t_1 + t_1^{pn} t_2 - (t_1 + t_1^{pm} t_2) = t_2(t_1^{pn} - t_1^{pm}) \in F(\theta_m)$$

But $t_1^p \in F \subset F(\theta_m)$, so $t_1^{pn} - t_1^{pm} \in F(\theta_m)$ so $t_2 \in F(\theta_m)$. But then we have

$$t_1 = t_1 + t_1^{pm} t_2 - t_1^{pm} t_2 = \theta_m - t_1^{pm} t_2 \in F(\theta_m)$$

So $t_1, t_2 \in F(\theta_m)$, so $L = F(\theta_m)$, a contradiction considering degree over F.

Hence it must be that if $n \neq m$ then $F(\theta_n) \neq F(\theta_m)$, so we can embed $\mathbb{Z}^+$ into $\mathcal{S}$ and we are done.

Problem 26

Show the following:

(a) If $K/\mathbb{Q}$ and $\sigma \in \text{Aut}K$, then σ fixes $\mathbb{Q}$

(b) The fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

(Solution)

(a)

I assume $\text{Aut}K$ is just field automorphisms $K \to K$. Since σ is a ring homomorphism, we have $\sigma(1) = 1$ and $\sigma(0) = 0$ and $\sigma(-1) = -1$. Then we immediately have that σ fixes $\mathbb{Z}$: for all $n \in \mathbb{Z}^+$ we have

$$\sigma(n) = \sigma(1 + \cdots + 1) = \sigma(1) + \cdots + \sigma(1) = 1 + \cdots + 1 = n$$

and

$$\sigma(-n) = \sigma(-1 - \cdots - 1) = \sigma(-1) + \cdots + \sigma(-1) = -1 - \cdots - 1 = -n$$

Now σ fixes $\mathbb{Q}$: for any $\frac{n}{m} \in \mathbb{Q}$ we have

$$\sigma(\frac{n}{m}) = \sigma(nm^{-1}) = \sigma(n)\sigma(m)^{-1} = nm^{-1} = \frac{n}{m}$$

where m is nonzero, so $\sigma(m)$ is nonzero so multiplicative inverse makes sense.

(b)

We have that $\mathbb{Q}(\sqrt{2})$ is a splitting field of $t^2 - 2$ over $\mathbb{Q}$ as the roots of $t^2 - 2$ are $\pm\sqrt{2}$. So suppose on the contrary that $\mathbb{Q}(\sqrt{3})$ was isomorphic to $\mathbb{Q}(\sqrt{2})$ via some field isomorphism $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Then let $f = t^2 - 2 \in \mathbb{Q}[t] \subset \mathbb{Q}(\sqrt{3})[t]$ so that

$$f(\varphi(\sqrt{2})) = \varphi(\sqrt{2})^2 - 2 = \varphi(2) - 2 = \varphi(1 + 1) - 2 = \varphi(1) + \varphi(1) - 2 = 0$$

In particular, a root of f is in $\mathbb{Q}(\sqrt{3})$, so $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Note that $t^2 - 3$ is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}$ so we have that $\{1, \sqrt{3}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{3})$. So we can write

$$\sqrt{2} = a + b\sqrt{3}$$

for some $a, b \in \mathbb{Q}$. Note that $\sqrt{2}$ is irrational so $b \neq 0$. Moreover $a \neq 0$ for otherwise we can write $b = \frac{p}{q}$ with p, q relatively prime so that we have

$$2q^2 = 3p^2$$

In particular this forces p^2 even so p is even. So we can write $p = 2k$ some k. Then we have

$$q^2 = 6k^2$$

so q is even, a contradiction to p, q relatively prime. So a, b are both nonzero. Then we can compute the following:

$$2 = a^2 + 2ab\sqrt{3} + 3b^2$$
$$\frac{2 - a^2 - 3b^2}{2ab} = \sqrt{3}$$

which contradicts that $\sqrt{3}$ is irrational. Hence $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

Problem 27

A **primitive nth root of unity** is an element $z \in \mathbb{C}$ such that $z^n = 1$ and $z^r \neq 1$ for $1 \leq r < n$. Show the following:

(a) There exist $\phi(n) := |\{d \mid 1 \leq d \leq n, (d,n) = 1\}|$ primitive nth roots of unity.

(b) If ω is a primitive nth root of unity, then $\mathbb{Q}(\omega)$ is a splitting field of $t^n - 1 \in \mathbb{Q}[t]$ and $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal.

(c) If $\omega_1, \ldots, \omega_{\phi(n)}$ are the $\phi(n)$ primitive nth roots of unity of $t^n - 1 \in \mathbb{Q}[t]$ and $\sigma \in \mathrm{Aut}\mathbb{Q}(\omega_1)$, then $\sigma(\omega_1) = \omega_i$ for some $i, 1 \leq i \leq \phi(n)$.

(Solution)

(a)

Define $\zeta_n := \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) \in \mathbb{C}$. By the same proof as in problem 5, we have that $\zeta_n^n = 1$ and $\zeta_n^r \neq 1$ for $1 \leq r < n$, i.e. that ζ_n is a primitive nth root of unity. Since ζ_n is primitive, we have that the following are all distinct roots of $t^n - 1$, hence all the nth roots of unity:

$$\zeta_n, \zeta_n^2, \ldots, \zeta_n^n$$

To show the result, it suffices to show that if $1 \leq d \leq n$ then ζ_n^d is a primitive nth root of unity if and only if $(d,n) = 1$. So let $1 \leq d \leq n$.

If ζ_n^d is a primitive nth root of unity then suppose on the contrary that $(d,n) = e \neq 1$ (assume e positive). Then we can write $d = ae$ and $n = be$. In particular b is positive and $b < n$. Then we have

$$(\zeta_n^d)^b = (\zeta_n^{ae})^b = (\zeta_n^n)^a = 1$$

which contradicts that ζ_n^d is primitive. Hence $(d,n) = 1$.

Conversely, if $(d,n) = 1$ then if $(\zeta_n^d)^r = 1$ for any $1 \leq r < n$, then $n \mid dr$ as ζ_n has order n in $\mathbb{C}^\times$. Then by General Euclid Lemma, we have that $n \mid r$ a contradiction as $r < n$. So it must be that ζ_n^d is a primitve nth root of unity.

(b)

Suppose ω is a primitive nth root of unity. Then we have $\omega^r \neq 1$ for any $1 \leq r < n$. This implies that

$$\omega, \omega^2, \ldots \omega^n$$

are distinct as if two of them were equal just cancel the one with lower exponent to contradict primitivity of ω. They are also nth roots of unity as ω is, so a splitting field of $t^n - 1$ over $\mathbb{Q}$ is

$$\mathbb{Q}(\omega, \omega^2, \ldots, \omega^n) = \mathbb{Q}(\omega)$$

In particular $\mathbb{Q}(\omega)/\mathbb{Q}$ is finite as ω is algebraic. Since $\mathbb{Q}(\omega)$ is the splitting field of some non-constant polynomial in $\mathbb{Q}[t]$, namely $t^n - 1$, we have that $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal.

(c)

Let $\omega_1, \ldots, \omega_{\phi(n)}$ be the $\phi(n)$ primitive nth roots of unity of $t^n - 1 \in \mathbb{Q}[t]$ and $\sigma \in \text{Aut } \mathbb{Q}(\omega_1)$. By (b), $\mathbb{Q}(\omega_1)$ is a splitting field of $t^n - 1 \in \mathbb{Q}[t]$ so $w_i \in \mathbb{Q}(\omega_1)$. To get the result, it suffices to show that $\sigma(\omega_1)$ is a primitive nth root of unity.

To see nth root of unity we have:

$$\sigma(\omega_1)^n = \sigma(\omega_1^n) = \sigma(1) = 1$$

To see primitive, let $1 \leq r < n$. Then if

$$\sigma(\omega_1)^r = \sigma(\omega_1^r) = 1$$

then since σ is bijective, we must have $\omega_1^r = 1$, a contradiction to ω_1 being primitive.

Problem 28

Continued from Problem 27. Show

(a) Let $\Phi_n(t) = (t-\omega_1)\cdots(t-\omega_{\phi(n)})$. Then show $\Phi_n(t) \in \mathbb{Q}[t]$. $\Phi_n(t)$ is caleld the nth **cyclotomic polynomial.**

(b) $\Phi_n(t) \in \mathbb{Z}[t]$.

(Solution)

(a)

We use the following lemmas:

Lemma 1: Let K/F be finite, normal extension. Then any irreducible polynomial in $F[t]$ having a root in K splits over K.

Proof. Since K/F is normal, K is the splitting field of some non-constant $f \in F[t]$. Let $g \in F[t]$ be irreducible over F having some root $\alpha \in K$. We want to show that g splits over K, so it suffices to show that K has all of the roots of g.

Let L/K with $\beta \in L$ a root of g. We need to show that $\beta \in K$. Since g is irreducible over F, there exists an F-isomorphism $\sigma : F(\alpha) \to F(\beta)$ with $\sigma(\alpha) = \beta$.

Then we have $K = K(\alpha)$ is a splitting field of f over $F(\alpha)$. We also have that f splits over K so it splits over $K(\beta)$. Moreover, any field extension over $F(\beta)$ in which f splits has to contain $F(\beta)$ as well as all the roots of f, so it contains K and hence $K(\beta)$, so $K(\beta)$ is a splitting field of f over $F(\beta)$. Additionally, $f \in F[t]$ and σ fixes F, so $\widetilde{\sigma}(f) = f$. So there exists a field isomorphism $\tau : K(\alpha) \to K(\beta)$ extending σ.

In particular we have have τ is also an F-isomorphism hence F-linear map so $K(\alpha)$ and $K(\beta)$ are isormorphic as F-vectorspaces and we have

$$[K : F] = [K(\alpha) : F] = [K(\beta) : F] = [K(\beta) : K][K : F]$$

hence $[K(\beta) : K] = 1$ so $\beta \in K$. $\square$

Lemma 2: Let K/F be finite, normal, and separable and $\alpha \in K$. If $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Aut}(K/F)$, then $\alpha \in F$, where $\mathrm{Aut}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma|_F = 1_F\}$.

Proof. To show that $\alpha \in F$, it suffices to show that $\deg(m_F(\alpha)) = 1$. By separability and lemma 1, we have that $m_F(\alpha)$ splits into distinct linear factors in $K[t]$. If $\deg(m_F(\alpha)) > 1$, then there is another root $\alpha' \in K$ distinct from α. But since $m_F(\alpha)$ is irreducible over F, there exists an F-isomorphism $\tau : F(\alpha) \to F(\alpha')$ such that $\tau(\alpha) = \alpha'$.

But then K/F is normal, so K is a splitting field of some non-constant $f \in F[t]$. In particular $\widetilde{\tau}(f) = f$ as τ is F-isomorphism. So there exists a field isomorphism $\sigma : K \to K$ extending τ. In particular σ is an F-automorphism such that $\sigma(\alpha) = \tau(\alpha) = \alpha'$, which contradicts that α is fixed by all of $\mathrm{Aut}(K/F)$, so it must be that $\deg(m_F(\alpha)) = 1$ and we are done. $\square$

By problem 27(b), $\mathbb{Q}(\omega_1)/\mathbb{Q}$ is normal. It is also finite as ω_1 is algebraic. Lastly, it is separable as char $\mathbb{Q} = 0$.

Our proof in 27(a) shows that for all $1 \leq i \leq \phi(n)$:

$$\{\omega_1, \dots, \omega_{\phi(n)}\} = \{\omega_i^k \mid 1 \leq k \leq n, (k,n) = 1\}$$

In particular, $\Phi_n \in \mathbb{Q}(\omega_1)[t]$ so all its coefficients are in $\mathbb{Q}(\omega_1)$. Moreover $\mathrm{Aut}(\mathbb{Q}(\omega_1)/\mathbb{Q}) \subset \mathrm{Aut}\mathbb{Q}(\omega_1)$, so by problem 27(c), we have if $\sigma \in \mathrm{Aut}(\mathbb{Q}(\omega_1)/\mathbb{Q})$ then $\sigma(\omega_1^k) = \sigma(\omega_1)^k = \omega_i^k$ some i. In particular, if $k < n$ is coprime to n, then ω_1^k and ω_i^k are both primitive nth roots of unity. Then since σ is bijective, we have

$$\sigma(\{\omega_1, \dots, \omega_{\phi(n)}\}) = \{\omega_1, \dots, \omega_{\phi(n)}\}$$

So

$$\widetilde{\sigma}(\Phi_n) = \prod_{i=1}^{\phi(n)} \widetilde{\sigma}(t - \omega_i) = \prod_{i=1}^{\phi(n)} (t - \sigma(\omega_i)) = \prod_{i=1}^{\phi(n)} (t - \omega_i) = \Phi_n$$

In particular we apply lemma 2 to every coefficient of Φ_n to get that $\Phi_n \in \mathbb{Q}[t]$.

(b)

We need the following lemma:

Lemma 3: If $f \in \mathbb{Z}[t]$ is monic and $f = gh$ with $g, h \in \mathbb{Q}[t]$ also monic, then $g, h \in \mathbb{Z}[t]$.

Proof. Since $\mathbb{Z}$ is a UFD, $\mathbb{Z}[t]$ is a UFD. So write the irreducible factorization $f = f_1 \cdots f_r$ some r with $f_i \in \mathbb{Z}[t]$ irreducible. Note that none of the f_i can be constant since nonzero, nonunit and f is monic. So f_i are all irreducible in $\mathbb{Q}[t]$. Moreover an even number of f_i are not monic (i.e. $\mathrm{lead}(f_i) = -1$) as f is monic, so we can assume all f_i are monic.

Then in $\mathbb{Q}[t]$ write the irreducible factorizations of g and h:

$$g = g_1 \cdots g_s \quad \text{and} \quad h = g_{s+1} \cdots g_{s+t}$$

where $g_i \in \mathbb{Q}[t]$ irreducible. So we have

$$g_1 \cdots g_{s+t} = f_1 \cdots f_r$$

in the UFD $\mathbb{Q}[t]$, so $s + t = r$ and $g_i \approx f_{\sigma(i)}$ for some $\sigma \in S_r$. In particular there exist $u_i \in \mathbb{Q}^\times$ such that $g_i = u_i f_{\sigma(i)}$. Then we have

$$g = \prod_{i=1}^{s} u_i \prod_{i=1}^{s} f_{\sigma(i)}$$

since g monic and all f_i monic, we have that $\prod_{i=1}^{s} u_i = 1$, so

$$g = \prod_{i=1}^{s} f_{\sigma(i)} \in \mathbb{Z}[t]$$

Similarly $h \in \mathbb{Z}[t]$. $\square$

Now we just apply this to $t^n - 1$. We have that $\Phi_n \mid t^n - 1$ in $\mathbb{Q}[t]$ since the roots of $t^n - 1$ are all the nth roots of unity. So there exists $q \in \mathbb{Q}[t]$ such that

$$t^n - 1 = \Phi_n q$$

In particular Φ_n is monic, so q must also be monic. Then apply lemma 3 to get $\Phi_n \in \mathbb{Z}[t]$.

Problem 29

Continued from Problem 28. Show

(a) $\Phi_n(t) \in \mathbb{Z}[t]$ is irreducible.

(b) Calculate $\Phi_n(t)$ for $n = 3, 4, 6, 8$ explicitly and show directly that $\Phi_n(t) \in \mathbb{Z}[t]$ is irreducible.

(Solution)

(a)

If $n = 1, 2$, then Φ_n is monic degree 1. So it cannot be reducible as if $\Phi_n = fg$ with neither a unit then one of them is degree 1 (say f) and the other is constant. But since Φ_n is monic, both have to be monic, so $g = 1$ is a unit, a contradiction.

If $n > 2$, then $\deg \Phi_n \geq 2$ as $1, n-1$ are relatively prime to n. Then it suffices to show that Φ_n is irreducible over $\mathbb{Q}$ as if Φ_n were reducible over $\mathbb{Z}$, then we could write $\Phi_n = fg$ with neither units. As above, neither f nor g can be constant, so raising to $\mathbb{Q}[t]$ would contradict Φ_n irreducible over $\mathbb{Q}$.

So let's show Φ_n irreducible over $\mathbb{Q}$. We will proceed by showing that $\Phi_n = m_{\mathbb{Q}}(\omega_1)$. We already know that $m_{\mathbb{Q}}(\omega_1) \mid \Phi_n$ in $\mathbb{Q}[t]$, so it suffices to show the converse as both are monic. By problem 28, we know that

$$\Phi_n = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (t - \omega_1^k)$$

so it suffices to show that each (distinct) primitive nth root of unity is a root of $m_{\mathbb{Q}}(\omega_1)$.

I got hint from Lang Chapter 6 Theorem 3.1 and https://math.stackexchange.com/questions/532960/showing-that-nth-cyclotomic-polynomial-phi-nx-is-irreducible-over-mathb.

We claim that if $p_1, \ldots, p_m$ are all primes coprime to n and ω is a primitive nth root of unity, then $\omega^{p_1 \cdots p_m}$ is a root of $m_{\mathbb{Q}}(\omega)$. We proceed by induction.

We do the inductive step first. Let ω be a primitive nth root of unity and suppose true for less than m such primes. Let $p_1, \ldots, p_m$ be primes coprime to n. Then we have that by the inductive hypothesis $\omega^{p_1 \cdots p_{m-1}}$ is a root to $m_{\mathbb{Q}}(\omega)$. But then $m_{\mathbb{Q}}(\omega) = m_{\mathbb{Q}}(\omega^{p_1 \cdots p_{m-1}})$. Moreover, $p_1 \cdots p_{m-1}$ is coprime to n so we can write $p_1 \cdots p_{m-1} = nq + r$ where $0 \leq r < n$. But $r \neq 0$ for otherwise the gcd of $p_1 \cdots p_{m-1}$ and n is n, which we assume is at least 2. Moreover, r must be coprime to n for otherwise, some prime divides r and n and hence $p_1 \cdots p_{m-1}$, which contradicts coprimality of $p_1 \cdots p_{m-1}$ and n. Then we have

$$\omega^{p_1 \cdots p_{m-1}} = \omega^{nq+r} = \omega^r$$

which is a primitive nth root of unity since r is coprime to n. So by the inductive hypothesis $\omega^{p_1 \cdots p_m}$ is a root to $m_{\mathbb{Q}}(\omega^{p_1 \cdots p_{m-1}}) = m_{\mathbb{Q}}(\omega)$, which is the result.

So let's show the base case. Let ω be a primitive nth root of unity and p a prime which is coprime to n.

Then since $m_{\mathbb{Q}}(\omega) \mid \Phi_n$ we can write $\Phi_n = m_{\mathbb{Q}}(\omega)g \in \mathbb{Q}[t]$ where g is monic. Then by lemma 3 of problem 28, $m_{\mathbb{Q}}(\omega), g \in \mathbb{Z}[t]$.

Then by division algorithm, write $p = qn + r$. In particular $0 < r < n$ is coprime to n. So we have that $\omega^p = \omega^{qn+r} = \omega^r$ is a primitive nth root of unity, so a root to Φ_n. If ω^p is a root to $m_{\mathbb{Q}}(\omega)$, then we are done, so assume not. Then ω^p must be a root to g. So ω is a root to $g(t^p)$. So $m_{\mathbb{Q}}(\omega) \mid g(t^p)$ in $\mathbb{Q}[t]$. So we can write

$$g(t^p) = m_{\mathbb{Q}}(\omega)h$$

for some monic $h \in \mathbb{Q}[t]$. By problem 28, lemma 3, $h \in \mathbb{Z}[t]$. Then since $\Phi_n \mid t^n - 1$ in $\mathbb{Q}[t]$ we write $t^n - 1 = \Phi_n q$ for some $q \in \mathbb{Q}[t]$ monic. Again by lemma 3, $q \in \mathbb{Z}[t]$. Note that

$$t^n - 1 = m_{\mathbb{Q}}(\omega)gq.$$

Now all of the polynomials we are working with are in $\mathbb{Z}[t]$, so we will now view all polynomials reduced modulo p, but we keep the same notation. Write

$$g = \sum a_i t^i$$

for some $a_i \in \mathbb{Z}/p\mathbb{Z}$. Then by problem 3 and 21 we have

$$g(t^p) = \sum a_i t^{pi} = \sum a_i^p t^{pi} = (\sum a_i t^i)^p = g^p$$

Since $(\mathbb{Z}/p\mathbb{Z})[t]$ is a UFD, there exists an irreducible polynomial $f \in (\mathbb{Z}/p\mathbb{Z})[t]$ dividing $m_{\mathbb{Q}}(\omega)$, so f divides $g(t^p) = g^p$. But since irreducible is prime in UFD, $f \mid g$. In particular, this means that $f^2 \mid t^n - 1$, so $t^n - 1$ has a multiple root so it shares a root with nt^{n-1}. But since n and p are coprime, nt^{n-1} is not the zero polynomial. In particular the only roots of nt^{n-1} are 0, but 0 is not a root of $t^n - 1$, a contradiction to sharing a root.

Hence ω^p must be a root of $m_{\mathbb{Q}}(\omega)$, so the induction is done.

Now it immediately follows that all the primitive nth roots of unity, i.e., $\{\omega_1^k \mid 1 \leq k \leq n, (k, n) = 1\}$, are roots to $m_{\mathbb{Q}}(\omega_1)$ by taking the standard factorization of k coprime to n. So we are done.

(b)

n=3

The primitive 3rd roots of unity are

$$\omega_3 := \cos(\frac{2\pi}{3} + i\sin(\frac{2\pi}{3}) = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$
$$\omega_3^2 = \cos(\frac{4\pi}{3} + i\sin(\frac{4\pi}{3}) = \frac{-1}{2} - i\frac{\sqrt{3}}{2}$$

So we have

$$\begin{aligned}\Phi_3(t) &= (t - \omega_3)(t - \omega_3^2) \\ &= t^2 - (\omega_3 + \omega_3^2)t + \omega_3^3 \\ &= t^2 - (-1)t + 1 \\ &= t^2 + t + 1\end{aligned}$$

In particular $\Phi_3(t)$ has no roots in $\mathbb{R}$ so it cannot have any roots in $\mathbb{Q}$, so it is irreducible over $\mathbb{Q}$ since degree 2, so irreducible over $\mathbb{Z}$ (same reasoning as previous part).

n=4

The primitive 4th roots of unity are:

$$\begin{aligned}\omega_4 &= \cos(\frac{2\pi}{4}) + i\sin(\frac{2\pi}{4}) = i \\ \omega_4^3 &= -i\end{aligned}$$

So we have

$$\begin{aligned}\Phi_4(t) &= (t-i)(t+i) \\ &= t^2 - i^2 \\ &= t^2 + 1\end{aligned}$$

Again no roots in $\mathbb{Q}$ so irreducible over $\mathbb{Q}$ as degree 2 so irreducible over $\mathbb{Z}$.

n=6

The primitive 6th roots of unity are:

$$\begin{aligned}\omega_6 &= \cos(\frac{2\pi}{6}) + i\sin(\frac{2\pi}{6}) = \frac{1}{2} + i\frac{\sqrt{3}}{2} \\ \omega_6^5 &= \cos(\frac{10\pi}{6}) + i\sin(\frac{10\pi}{6}) = \frac{1}{2} - i\frac{\sqrt{3}}{2}\end{aligned}$$

So we have

$$\begin{aligned}\Phi_6(t) &= t^2 - (\omega_6 + \omega_6^5)t + \omega_6^6 \\ &= t^2 - (1)t + 1 \\ &= t^2 - t + 1\end{aligned}$$

Again no roots in $\mathbb{Q}$ and degree 2 so irreducible over $\mathbb{Q}$ so irreducible over $\mathbb{Z}$.

n=8

The primitive 8th roots of unity are

$$\begin{aligned}\omega_8 &= \cos(\frac{2\pi}{8}) + i\sin(\frac{2\pi}{8}) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \\ \omega_8^3 &= \cos(\frac{6\pi}{8}) + i\sin(\frac{6\pi}{8}) = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \\ \omega_8^5 &= \cos(\frac{10\pi}{8}) + i\sin(\frac{10\pi}{8}) = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2} \\ \omega_8^7 &= \cos(\frac{14\pi}{8}) + i\sin(\frac{14\pi}{8}) = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}\end{aligned}$$

Then we have

$$\begin{aligned}\Phi_8(t) &= (t-\omega_8)(t-\omega_8^3)(t-\omega_8^5)(t-\omega_8^7) \\ &= (t^2 - (\omega_8 + \omega_8^3)t + \omega_8^4)(t^2 - (\omega_8^5 + \omega_8^7) + \omega_8^4) \\ &= (t^2 - i\sqrt{2}t - 1)(t^2 + i\sqrt{2}t - 1) \\ &= t^4 + i\sqrt{2}t^3 - t^2 - i\sqrt{2}t^3 + 2t^2 + i\sqrt{2}t - t^2 - i\sqrt{2}t + 1 \\ &= t^4 + 1\end{aligned}$$

To show $\Phi_8(t)$ is irreducible over $\mathbb{Z}$ it suffices to show irreducible over $\mathbb{Q}$. To do this is suffices to show that $\Phi_8(t+1)$ is irreducible over $\mathbb{Q}$. But this is true by Eisenstein:

$$(t+1)^4 + 1 = t^4 + 4t^3 + 6t^2 + 4t + 2$$

Problem 30

Suppose you knew that, for any integers a and n with $(a, n) = 1$, there are infinitely many primes p that are congruent to a modulo n (this is a famous theorem of Dirichlet). Conclude that every finite abelian group occurs as a Galois group over the rational numbers. (The corresponding statement when the "abelian" is eliminated is an open problem.)

(Solution)

I used the following: https://math.stackexchange.com/questions/131376/every-finite-abelian-group-is-the-galois-group-of-some-finite-extension-of-the-r. I also collaborated with Zane Witter.

We need a few lemmas:

Lemma 1: Let $n \in \mathbb{Z}^+$ and $\omega \in \mathbb{C}$ be a primitive nth root of unity. Let $K = \mathbb{Q}(\omega)$. Then $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ as groups.

Proof. By problem 29, Φ_n is irreducible in $\mathbb{Z}[t]$ hence in $\mathbb{Q}[t]$ by Gauss. Moreover, Φ_n is monic, so $m_\mathbb{Q}(\omega) = \Phi_n$. So $[K : \mathbb{Q}] = \deg \Phi_n = \phi(n)$.

For simplicity, let $G = G(K/\mathbb{Q})$. Since $K/\mathbb{Q}$ is finite, normal (by problem 27), and separable (characteristic 0), we have that $K/\mathbb{Q}$ is Galois (we ended up proving this in problem 28 lemma 2), so $|G(K/\mathbb{Q})| = \phi(n)$. Then in 110AH we showed that $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if $(a, n) = 1$, so $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$.

So if we show that G embeds into $(\mathbb{Z}/n\mathbb{Z})^\times$, then we have that G is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, but G and $(\mathbb{Z}/n\mathbb{Z})^\times$ have the same cardinality, so we would get the result. So let's do this.

Since K is a splitting field of $f = t^n - 1$ over $\mathbb{Q}$ by problem 27, we have that any $\sigma \in G = G(K/\mathbb{Q})$ is uniquely determined by how it acts on the roots $S = \{\omega, \omega^2, \ldots, \omega^n\}$ of f, that is given $\sigma, \tau \in G$ we have $\sigma = \tau$ if and only if $\sigma|_S = \tau|_S$ (remark 49.14). Then if $\sigma, \tau \in G$ such that $\sigma(\omega) = \tau(\omega)$, then $\sigma(\omega^k) = \sigma(\omega)^k = \tau(\omega)^k = \tau(\omega^k)$ for all $k = 1, \ldots, n$. Hence $\sigma|_S = \tau|_S$ if and only if $\sigma(\omega) = \tau(\omega)$. So $\sigma \in G$ is uniquely determined by where it sends ω. Moreover, we know that $\sigma \in G$ sends ω to a primitive nth root of unity by problem 27, which are given by

$$\{\omega^k \mid 1 \leq k \leq n, (k, n) = 1\}$$

which we showed in 27(a). So given $\sigma \in G$, there exists a unique $1 \leq k \leq n$ relatively prime to n such that $\sigma(\omega) = \omega^k$, and this uniquely determines σ. So we can define the map

$$\varphi : G \to (\mathbb{Z}/n\mathbb{Z})^\times$$

by $\sigma \mapsto \overline{k}$, where k is such that $\sigma(\omega) = \omega^k$ as above. This is well-defined since such a k is unique. Moreover, we have that

$$\varphi(1_K) = \overline{1}$$

and if $\sigma(\omega) = \omega^k$ and $\tau(\omega) = \omega^m$, then $\sigma \circ \tau(\omega) = \sigma(\omega^m) = \omega^{km}$. Since k, m are both relatively prime to n, we have that km is relatively prime to n by Lemma 6.8 (of Chinese Remainder Theorem).

Then by division algorithm we can write $km = qn + r$ where $0 \leq r < n$. Moreover, r is relatively prime to n for otherwise km isn't. So we have that

$$\varphi(\sigma \circ \tau) = \overline{r} = \overline{km} = \overline{k} \cdot \overline{m} = \varphi(\sigma)\varphi(\tau)$$

Hence φ is a well-defined group homomorphism. Moreover, if $\varphi(\sigma) = \overline{1}$, then $\sigma(\omega) = \omega^1$, so $\sigma = 1_K$ as it is uniquely determined by where it sends ω. Hence φ is monic. So G is ismorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$, so we are done. $\square$

Lemma 2: If G is a finite abelian group, then there exists $n \in \mathbb{Z}^+$ such that G is isomorphic to a quotient group of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. By the Fundamental Theorem (or Fundamental Theorem of Finite Abelian Groups), we can write G as a direct product of cyclic groups. In particular, we can write

$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$$

for some $n_i \in \mathbb{Z}^+$. Using the Dirichlet theorem, let p_i be a prime such that $p_i \equiv 1 \mod n_i$ for each i. We can assume the p_i are distinct because there are infinitely many such choices for each p_i. Then we have that $n_i \mid p_i - 1$, so $p_i - 1 = n_i k_i$ in $\mathbb{Z}$ for some (nonzero) $k_i \in \mathbb{Z}$.

Then we claim that G is isomorphic to a quotient group of $(\mathbb{Z}/(p_1-1)\mathbb{Z}) \times \cdots \times (\mathbb{Z}/(p_k-1)\mathbb{Z})$. We proceed by First Isomorphism. Define

$$\varphi : (\mathbb{Z}/(p_1-1)\mathbb{Z}) \times \cdots \times (\mathbb{Z}/(p_k-1)\mathbb{Z}) \to (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$$

by $([x_i]_{p_i-1})_i \mapsto ([x_i]_{n_i})_i$ where $[x]_a = \overline{x}$ with $^- : \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$ the canonical epimorphism. To see well-defined note that if $([x_i]_{p_i-1})_i = ([y_i]_{p_i-1})_i$ then $[x_i]_{p_i-1} = [y_i]_{p_i-1}$ for all i, so $p_i - 1 \mid x_i - y_i$ for all i, but $n_i \mid p_i - 1$, so $n_i \mid x_i - y_i$ in $\mathbb{Z}$ so $[x_i]_{n_i} = [y_i]_{n_i}$ for all i, i.e, $\varphi(([x_i]_{p_i-1})_i) = \varphi(([y_i]_{p_i-1})_i)$. Now to see group homomorphism, we have

$$\varphi(([0]_{p_1-1})_i) = ([0]_{n_i})_i$$

and

$$\begin{aligned}
\varphi\Big(([x_i]_{p_i-1})_i + ([y_i]_{p_i-1})_i\Big) &= \varphi\Big(([x_i + y_i]_{p_i-1})_i\Big) \\
&= ([x_i + y_i]_{n_i})_i \\
&= ([x_i]_{n_i})_i + ([y_i]_{n_i})_i \\
&= \varphi(([x_i]_{p_i-1})_i) + \varphi(([y_i]_{p_i-1})_i)
\end{aligned}$$

Lastly, to see surjectivity note that if $([x_i]_{n_i})_i \in (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$, then

$$\varphi(([x_i]_{p_i-1})_i) = ([x_i]_{n_i})_i$$

So by First Isomorphism Theorem, we have

$$((\mathbb{Z}/(p_1-1)\mathbb{Z}) \times \cdots \times (\mathbb{Z}/(p_k-1)\mathbb{Z})) \,/\, \ker\varphi \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}) \cong G$$

Now consider some prime $p > 0$. Then as $\mathbb{Z}/p\mathbb{Z}$ is a finite field, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic with some generator α. Then define $f : \mathbb{Z}/(p-1)\mathbb{Z} \to (\mathbb{Z}/p\mathbb{Z})^\times$ by $\overline{x} \mapsto \alpha^x$, where the bar is for $\mathbb{Z}/(p-1)\mathbb{Z}$. If $\overline{x} = \overline{y}$, then $p - 1 \mid x - y$ in $\mathbb{Z}$ so $\alpha^{x-y} = 1$, so $\alpha^x = \alpha^y$, so f is well-defined. Moreover we have

$$f(\overline{0}) = \alpha^0 = 1$$

and

$$f(\overline{x}+\overline{y}) = f(\overline{x+y}) = \alpha^{x+y} = \alpha^x\alpha^y = f(\overline{x})f(\overline{y})$$

and if $f(\overline{x}) = 1$ then $\alpha^x = 1$, so since α has order $p-1$, we have that $p-1 \mid x$ in $\mathbb{Z}$,so $\overline{x} = \overline{0}$. Hence f is a group monomorphism. Since the domain and codomain are finite sets of the same cardinality, we have that f is a group ismorphism. Hence we have

$$(\mathbb{Z}/(p_1-1)\mathbb{Z}) \times \cdots \times (\mathbb{Z}/(p_k-1)\mathbb{Z}) \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times$$

Since p_i are distinct primes they are pairwise relatively prime, so by 110AH Homework 3 problem 6 (which is result of Chinese Remainder Theorem), we have that

$$(\mathbb{Z}/p_1\cdots p_k\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k\mathbb{Z})^\times$$

Hence $(\mathbb{Z}/p_1\cdots p_k\mathbb{Z})^\times \cong (\mathbb{Z}/(p_1-1)\mathbb{Z}) \times \cdots \times (\mathbb{Z}/(p_k-1)\mathbb{Z})$ so G is isomorphic to a quotient of $(\mathbb{Z}/n\mathbb{Z})^\times$ where $n = p_1\cdots p_k$. $\square$

Conclusion: Let G be a finite abelian group. Then by lemma 2, there exists some $n \in \mathbb{Z}^+$ such that $G \cong (\mathbb{Z}/n\mathbb{Z})^\times/H$ for some $H \subset (\mathbb{Z}/n\mathbb{Z})^\times$ a subgroup.Then let $\omega \in \mathbb{C}$ be a primitive nth root of unity and $K = \mathbb{Q}(\omega)$. By Lemma 1, we have that $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so $G \cong G(K/\mathbb{Q})/H$, where we now assume H is a subgroup of $G(K/\mathbb{Q})$. Then by the Fundamental Theorem of Galois Theory, we have $H = G(K/K^H)$. But $H \triangleleft G(K/\mathbb{Q})$ since $G(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, so using the Fundamental Theorem of Galois Theory again, we get that $K^H/\mathbb{Q}$ is normal so we have an isomorphism

$$G(K/\mathbb{Q})/G(K/K^H) \cong G(K^H/\mathbb{Q})$$

In total, we get the result:

$$G \cong G(K/\mathbb{Q})/H = G(K/\mathbb{Q})/G(K/K^H) \cong G(K^H/\mathbb{Q})$$

where $K^H/\mathbb{Q}$ is Galois since normal and finite as $K/\mathbb{Q}$ is finite.

Problem 31

Let $K = \mathbb{Q}(r)$ with r a root of $t^3 + t^2 - 2t - 1 \in \mathbb{Q}[t]$. Let $r_1 = r^2 - 2$. Show that r_1 is also a root of this polynomial. Find $G(K/\mathbb{Q})$ and show that $K/\mathbb{Q}$ is normal.

(Solution)

Let f denote the polynomial. By Binomial Theorem, we have

$$(r^2 - 2)^3 = r^6 - 6r^4 + 12r^2 - 8$$

and

$$(r^2 - 2)^2 = r^4 - 4r^2 + 4$$

So

$$f(r_1) = (r^2 - 2)^3 + (r^2 - 2)^2 - 2(r^2 - 2) - 1 = r^6 - 5r^4 + 6r^2 - 1$$

But also note that

$$\begin{aligned} 0 = (r^3 - r^2 - 2r + 1)f(r) &= (r^3 - r^2 - 2r + 1)(r^3 + r^2 - 2r - 1) \\ &= r^6 + r^5 - 2r^4 - r^3 \\ &\quad - r^5 - r^4 + 2r^3 + r^2 \\ &\quad\quad - 2r^4 - 2r^3 + 4r^2 + 2r \\ &\quad\quad\quad + r^3 + r^2 - 2r - 1 \\ &= r^6 - 5r^4 + 6r^2 - 1 \\ &= f(r_1) \end{aligned}$$

So r_1 is a root of f. Moreover, if $r = r^2 - 2$, then $r^2 - r - 2 = 0$, so $r = 2, -1$, but neither are roots of f, so r and r_1 are distinct roots. So we can find the third rootr_2 of f by the constant term:

$$1 = rr_1r_2$$

So $r_2 = \frac{1}{rr_1} = \frac{1}{r^3 - 2r} \in \mathbb{Q}(r)$ as $r^3 - 2r \in \mathbb{Q}(r)$. So a splitting field of f over $\mathbb{Q}$ is

$$\mathbb{Q}(r, r^2 - 2, \frac{1}{r^3 - 2r}) = \mathbb{Q}(r)$$

Note that by the rational root test, any rational root of f must be ± 1, but neither are roots of f, so since f is degree 3, it is irreducible over $\mathbb{Q}$ (and also monic). So $[K : \mathbb{Q}] = 3$.

Since K is the splitting field over f over $\mathbb{Q}$, we have that $K/\mathbb{Q}$ is normal. It is also finite and separable (characteristic 0), so $K/\mathbb{Q}$ is Galois, so $|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = 3$, so we have $G(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

Problem 33

Let char $F = p \neq 0$ and $a \in F$. Let $f = t^p - t - a \in F[t]$. Show the following:

(a) f has no multiple roots.

(b) If α is a root of f, then so is $\alpha + k$ for all $0 \leq k \leq p-1$.

(c) f is irreducible if and only if f has no root in F.

(d) Suppose that $a \neq b^p - b$ for any $b \in F$. Find $G(K/F)$ where K is a splitting field of $t^p - t - a \in F[t]$.

(a)

It suffices to show that f and f' has no common root. Note that

$$f' = pt^{p-1} - 1 = -1 \neq 0$$

since characteristic p, so f' has no roots hence no common root with f.

(b)

Suppose α is a root of f. Then we use Children's Binomial Theorem, to get for all $0 \leq k \leq p-1$

$$(\alpha + k)^p - (\alpha + k) - a = \alpha^p + k^p - \alpha - k - a = k^p - k = 0$$

Note that the last equality follows since $k \in \Delta_F$, the prime subfield of F with p elements, so by problem 3, we have $k^p = k$.

(c)

Suppose f has a root $\alpha \in F$. Then by the Remainder Theorem, we have

$$f = (t - \alpha)q + f(\alpha) = (t - \alpha)q$$

for some $q \in F[t]$. In partcular, $\deg q = p - 1 > 0$, so f is reducible over F. By contrapositon, if f is irreducible, then it has no root in F.

Now suppose that f has no roots in F. Then let K be a splitting field of f over F. Then each $\sigma \in G(K/F)$ takes roots of f in K to roots of f in K (problem 13a). In particular, if $\alpha \in K$ is a root of f and $\sigma \in G(K/F)$, then by part (b), we have that $\sigma(\alpha) = \alpha + k$ for some $0 \leq k \leq p-1$. So we can define a group homomorphism:

$$\begin{aligned} \varphi : G(K/F) &\to \Delta_F \\ \sigma &\mapsto \sigma(\alpha) - \alpha \end{aligned}$$

Well-definition is immediate and

$$\varphi(1_K) = \alpha - \alpha = 0$$

and

$$\begin{aligned}\varphi(\sigma\circ\tau) &= \sigma\circ\tau(\alpha)-\alpha\\ &= \sigma(\alpha+n)-\alpha\\ &= \sigma(\alpha)+\sigma(n)-\alpha\\ &= \alpha+m+n-\alpha\\ &= m+n\\ &= \varphi(\sigma)+\varphi(\tau)\end{aligned}$$

where $\sigma(\alpha)=\alpha+m$ and $\tau(\alpha)=\alpha+n$ with $0\le m,n\le p-1$. As an additive group, $\triangle_F\cong\mathbb{Z}/p\mathbb{Z}$, so by Lagrange's Theorem, φ is either the zero map or surjective.

If it is the zero map, then $\sigma(\alpha)=\alpha$ for all $\sigma\in G(K/F)$, so $\alpha\in K^{G(K/F)}$. But K/F is finite as it just adjoins the roots of f to F, which are algebraic over F. Moreover K/F is normal as K is splitting field of $f\in F[t]$. K/F is also separable as f is separable by part (a), so all its roots are separable (we apply problem 23b). So K/F is Galois, so $K^{G(K/F)}=F$, so $\alpha\in F$, a contradiction to no roots in F, so it must be that φ is surjective.

Since φ is surjective, we have that for all $0\le k\le p-1$, there exists $\sigma\in G(K/F)$ such that $\sigma(\alpha)-\alpha=k$, or equivalently $\sigma(\alpha)=\alpha+k$. So every root of f is in the same orbit as α under action by $G(K/F)$, so $G(K/F)$ acts transitively on the roots of f in K. We will show that this forces f to be irreducible.

Suppose on the contrary that f is reducible. Then write the irreducible factorization:

$$f=f_1\cdots f_r$$

with $f_i\in F[t]$ irreducible and $r>1$. Since f is monic, we can assume that all f_i are monic by factoring out $\operatorname{lead} f_i$ from each f_i. In particular if f_i and f_j share a root, then they are both the minimal polynomial of that root over F, hence equal. Note that each f_i splits over K, so let $\alpha_i\in K$ be some root of f_i. Then since $G(K/F)$ acts transitively on the roots of f, there exists some $\sigma\in G(K/F)$ such that $\sigma(\alpha_i)=\alpha$, so α is a root of f_i by problem 13(a). So all the f_i share α as a root hence are all equal, so we have

$$f=f_1^r$$

In particular, $p=r\deg f_1$ where $r>1$, so $r=p$ and $\deg f_1=1$ as p is prime. But this means that f has mulitple roots, a contradiction to part (a). Hence, it must be that f is irreducible.

Thus, we have shown that if f has no root in F, then it is irreducible.

(d)

Let $\alpha\in K$ be a root of f. Then by part (b), $K=F(\alpha)$. Then if f has a root $\beta\in F$, then we have

$$\beta^p-\beta-a=0 \iff \beta^p-\beta=a$$

a contradiction to the assumption, so f has no root in F so by part (c), f is irreducible. Moreover, f is monic, so

$$[K:F]=[F(\alpha):F]=\deg f=p$$

So K/F is finite. It is also normal since K is splitting field of f over F. Lastly, f is separable over F by part (a), so α is separable over F, so K/F is separable by problem 23. So K/F is Galois, so

$$|G(K/F)| = [K : F] = p$$

so $G(K/F) \cong \mathbb{Z}/p\mathbb{Z}$.

Problem 35

Let $F \subset E \subset K$. If K/E and E/F are both normal, is K/F normal? Prove or give a counterexample.

(Solution)

We proceed by counterexample.

Let $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$ and $K = \mathbb{Q}(\sqrt[4]{2})$. Note that $E \subset K$ as $(\sqrt[4]{2})^2 = \sqrt{2}$. Also note that all the extensions we are working with are finite since $\sqrt[4]{2}$ is algebraic over $\mathbb{Q}$.

Note that a splitting field of $t^2 - 2 \in \mathbb{Q}[t]$ is $\mathbb{Q}(\pm\sqrt{2}) = \mathbb{Q}(\sqrt{2}) = E$ and a splitting field of $t^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[t]$ is $\mathbb{Q}(\sqrt{2})(\pm\sqrt[4]{2}) = \mathbb{Q}(\sqrt{2})(\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}) = K$. So K/E is normal and E/F is normal.

To show that K/F is not normal, it suffices to find an irreducible polynomal in $F[t]$ which has a root in K but does not split over K. We claim that $g = t^4 - 2$ works. It is irreducible over $\mathbb{Q}$ by Eisenstein. It has a root $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$. It also has a root $i\sqrt[4]{2} \notin \mathbb{R}$. But $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$, so $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$, so g cannot split over $\mathbb{Q}(\sqrt[4]{2})$.

Problem 36

Let $f, g \in F[t]$ be relatively prime and suppose that $u = f/g$ lies in $F(t) \setminus F$.

(a) Show that $F(t)/F(u)$ is finite of degree $d = \max\{\deg(f), \deg(g)\}$.

(b) $G(F(t)/F)$ consists of all F-automorphisms of $F(t)$ mapping t to $(at + b)/(ct + d)$ where $a, b, c, d \in F$ satisisfies $ad - bc \neq 0$.

(Solution)

(a)

Since $u = \frac{f(t)}{g(t)} \in F(t)$, we have $F(u)(t) = F(t)$. We are then interested in computing $[F(t) : F(u)] = [F(u)(t) : F(u)]$. So it suffices to find $m_{F(u)}(t) \in F(u)[x]$. Note that we change the indeterminate of the polynomial ring to x and we will denote degree with respect to x as $\deg_x$ (similarly for other variables).

Let $h(x) = ug(x) - f(x) \in F(u)[x]$. Note that

$$h(t) = ug(t) - f(t) = \frac{f(t)}{g(t)}g(t) - f(t) = f(t) - f(t) = 0$$

We claim that $h \neq 0$. If $\deg_x g \neq \deg_x f$, this is immediate (note that $u \notin F$, so $u \neq 0$). So suppose $\deg_x g = \deg_x f$. Then by the division algorithm in $F[x]$, we can write

$$f(x) = qg(x) + r(x)$$

with $q \in F[x]$ and $r = 0$ or $\deg_x r < \deg_x g$. Note that we must have $q \in F$. Then we cannot have $r = 0$, for otherwise $\frac{f(t)}{g(t)} = q \in F$. Then we have

$$h(x) = ug(x) - f(x) = ug(x) - qg(x) - r(x) = (u - q)g(x) - r(x)$$

where $u - q \neq 0$ as $u \notin F$. Hence $h \neq 0$ as $\deg_x r < \deg_x g$. So in either case we have $h \neq 0$.

In particular, if $\deg_x g \neq \deg_x f$, then we have $\deg_x h = d$. Similarly if $\deg_x g = \deg_x f$, then $\deg_x h = \deg_x g$, which is d in this case. Hence $h(x)$ is a degree d polynomial in $F(u)[x]$ in which t is a root. To finish, we show that $h(x)$ is irrreducible in $F(u)[x]$.

We first claim that u is trans/F. If not then $F(u)/F$ is algebraic, but we also have $F(t)/F(u)$ is algebraic via $h(x)$. So $F(t)/F$ is algebraic, but this contradicts that t is trans/F (if t was the root of some nonzero polynomial p with coefficients in F, then by equality of polynomials in $F[t]$, $p = 0$, a contradiction). So it must be that u is trans/F.

Hence $F[u] \cong F[t]$ as domains. In particular, $F[t]$ is a UFD, so $F[u]$ is also a UFD. Then by Gauss Lemma, if $h(x)$ is irreducible in $F[u][x]$, then $h(x)$ remains irreducible in $qf(F[u])[x] = F(u)[x]$, which is our desired result, so let's show the irreducibility over $F[u]$.

Note that $F[u][x] = F[u, x] = F[x, u] = F[x][u]$, so it suffices to show that h is irreducible in $F[x][u]$, where h is linear in u. Suppose on the contrary that h was reducible in $F[x][u]$. Then we can write

$$h = pq$$

with (nonzero) nonunits $p, q \in F[x][u]$. Since $\deg_u h = 1$, we can assume $\deg_u p = 1$ and $\deg_u q = 0$. So $q \in F[x]$. Note that $(F[x])[u]^\times = F[x]^\times = F^\times$ since domains. So if $q \in F$, we reach a contradiction that q is nonzero nonunit, so assume $q \notin F$. Then write $p = ur(x) + s(x)$ for some $r, s \in F[x]$ since p is linear in $F[x][u]$. So we have

$$ug(x) - f(x) = q(x)\,(ur(x) + s(x))$$

in $F[x][u]$. Then raising to $F(x)[u]$, we can divide by $q(x)$ since nonzero to get

$$u\frac{g(x)}{q(x)} - \frac{f(x)}{q(x)} = ur(x) + s(x)$$

Then by definition of equality in a polynomial ring (matching coefficients), we have $\frac{g(x)}{q(x)} = r(x)$ and $\frac{f(x)}{q(x)} = -s(x)$. This contradicts that g, f are relatively prime in $F[x]$. Hence it must be that h is irreducible in $F[x][u] = F[u][x]$ hence in $F(u)[x]$.

So we have $[F(t) : F(u)] = \deg_x m_{F(u)}(t) = \deg_x h = d$ as desired.

(b)

Note that an F-automorphism of $F(t)$ of the above form is already in $G(F(t)/F)$, so it suffices to show that if $\sigma \in G(F(t)/F)$, then

$$\sigma(t) = \frac{at+b}{ct+d}$$

where $a, b, c, d \in F$ and $ad - bc \neq 0$. Since $\sigma(t) \in F(t)$, we can write

$$\sigma(t) = \frac{p}{q}$$

where $p, q \in F[t]$ and $q \neq 0$. WLOG assume that p, q are relatively prime $F[t]$. Note that if $\sigma(t) \in F$, then $x - \sigma(t) \in F[x]$ has root $\sigma(t)$. Then since σ^{-1} is an F-automorphism of $F(t)$, we have by problem 13a that $\sigma^{-1}(\sigma(t)) = t$ is also a root of $x - \sigma(t) \in F[x]$, i.e. $t - \sigma(t) = 0 \in F$. But since $\sigma(t) \in F$, we have that $t - \sigma(t) \in F[t]$ is a linear polynomial, so $t - \sigma(t) \notin F$. Hence $\sigma(t) \notin F$.

Then we can apply part (a) to $u = p/q = \sigma(t)$ to get $[F(t) : F(\sigma(t))] = \max\{\deg_t p, \deg_t q\}$. We want to show that $[F(t) : F(\sigma(t))] = 1$, i.e. $F(t) = F(\sigma(t))$. Since σ is surjective onto $F(t)$, we have $\operatorname{im} \sigma = F(t)$. So it suffices to show that $\operatorname{im} \sigma = F(\sigma(t))$. Let $r, s \in F[t]$ with $s \neq 0$. Write

$$r = \sum a_i t^i$$

and

$$s = \sum b_i t_i$$

Then we have

$$\sigma(r/s) = \sigma(rs^{-1}) = \sigma(r)\sigma(s)^{-1}$$

Then since σ fixes F, we have

$$\sigma(r)\sigma(s)^{-1} = (\sum a_i \sigma(t)^i)(\sum b_i \sigma(t)^i)^{-1} = \frac{r(\sigma(t))}{s(\sigma(t)))} \in F(\sigma(t))$$

Hence im $\sigma = \sigma(F(t)) \subset F(\sigma(t))$. Hence $F(t) = F(\sigma(t))$, hence $\max\{\deg_t p, \deg_t q\} = 1$. So we can write $p = at + b$ and $q = ct + d$ (with a, c possibly zero) since p, q are both at most linear. Then we consider the following tautology:

Case 1: Suppose $a = 0$ Then $c \neq 0$ for otherwise the max of the degrees of p and q are is not 1. So we have $p = b$ and $q = ct + d$. Now if $ad = bc$, then $bc = 0$ so $b = 0$ since domain. So $p = 0$ and thus $\sigma(t) = 0$ so since injective, $t = 0 \in F$, a contradiction to t being trans/F. Hence it must be that $ad - bc \neq 0$.

Case 2: Suppose $a \neq 0$. Then if $ad = bc$, then $d = \frac{bc}{a}$. Then we can write

$$q = ct + d = \frac{ca}{a}t + \frac{bc}{a} = \frac{c}{a}(at + b) = \frac{c}{a}p$$

so $p \mid q$ in $F[t]$, but this contradicts that p, q are relatively prime. So it must be that $ad - bc \neq 0$.

Conclusion: Hence it must be that $ad - bc \neq 0$ and we are done.

Problem 37

Suppose that K/F is Galois with Galois group $G(K/F) \cong S_n$. Show that K is the splitting field of an irreducible polynomial in $F[t]$ of degree n over F.

(Solution)

We have $[K : F] = |G(K/F)| = |S_n| = n!$. We have that

$$S_n = \{\text{bijections on } \{1, \ldots, n\}\}$$

Let $H = \{f \in S_n \mid f(1) = 1\}$. This is certainly a subgroup of S_n. Moreover, we have $|H| = (n-1)!$. From here, view H as a subgroup of $G(K/F)$. Then let $E = K^H$. By the Fundamental Theorem of Galois Theory, we have that K/E is Galois and $[K : E] = |H| = (n-1)!$. So we have that $[E : F] = n$.

Moreover, $\mathcal{F}(E/F) \subset \mathcal{F}(K/F)$ so $\mathcal{F}(E/F)$ is finite as (by Fundamental Thm. of Galois Theory) $|\mathcal{F}(K/F)| = |\mathcal{G}(K/F)|$, which is finite as $G(K/F)$ is finite. Then by Primitive Element Theorem, there exists $\alpha \in E$ such that $E = F(\alpha)$. Then $m_F(\alpha)$ is irreducible polynomial of degree n in $F[t]$.

Since K/F is finite Galois, K/F is normal, so $m_F(\alpha)$ splits over K as it has a root $\alpha \in E \subset K$. Now it remains to show that K is indeed a splitting field of $m_F(\alpha)$.

Problem 39

Suppose L/F is a finite Galois extension and $L/K/F$, an intermediate field. Let $N = N_{G(L/F)}(G(L/K))$ denote the normalizer of $G(L/K)$ in $G(L/F)$. Show that L^N is the smallest subfield of K with K/L^N Galois.

(Solution)

First we show that L^N is indeed a subfield of K with K/L^N Galois.

From 110AH, we have that every subgroup is normal in its normalizer, so $G(L/K) \triangleleft N$. [To see this real quick suppose $H \subset G$ and $N_G(H)$. Then if $h \in H$, then $hHh^{-1} = H$, so $h \in N_G(H)$, so $H \subset N_G(H)$. Moreover by definition, for all $g \in N_G(H)$, $gHg^{-1} = H$, so $H \triangleleft N_G(H)$].

Then by the Fundamental Theorem of Galois Theory, we have $L^{G(L/K)} \supset L^N$, but L/F is finite Galois, so L/K is finite Galois, so $L^N \subset L^{G(L/K)} = K$. Then L/L^N is finite Galois since L/F is finite Galois, so by the FTGT, K/L^N is normal so Galois since $G(L/K) \triangleleft G(L/L^N) = N$.

So L^N is indeed a subfield of K with K/L^N Galois. Now suppose $A \in \mathcal{F}(L/F)$ is a subfield of K with K/A Galois. Then we want to show that $L^N \subset A$.

Since L/F is finite Galois, L/A is also finite Galois. Then by the FTGT, K/A is Galois so normal, so $G(L/K) \triangleleft G(L/A)$. So if $x \in G(L/A)$, then $x \in G(L/F)$ and $xG(L/K)x^{-1} = G(L/K)$, so $x \in N$, so $G(L/A) \subset N$, so $L^N \subset L^{G(L/A)} = A$ since L/A Galois. So we are done.

Problem 40

Suppose that K/F is Galois. Let $F \subset E \subset K$ and L the smallest subfield of K containing E and such that L/F is normal. Show that

$$G(K/L) = \bigcap_{\sigma \in G(K/F)} \sigma G(K/E)\sigma^{-1}$$

.

(Solution)

Following the wikipedia page for https://en.wikipedia.org/wiki/Core_(group_theory), we need the following lemma.

Lemma: Let G be a group with $H \subset G$ a subgroup. Then $N \coloneqq \cap_{g\in G}(gHg^{-1})$ is the largest normal subgroup of G contained in H.

Proof. First note that $N \subset e_G H e_G^{-1} = H$. Moreover, the intersection of subgroups is a subgroup so N is a subgroup of G contained in H. Now we show that N is normal. Let $x \in G$. Then we need to show that $xNx^{-1} = N$.

Note that if $\alpha \in N$ then $\alpha \in gHg^{-1}$ for all $g \in G$, so for each $g \in G$ there exists h such that $\alpha = ghg^{-1}$ and thus $x\alpha x^{-1} = xghg^{-1}x^{-1} \in xgH(xg)^{-1}$. Hence $x\alpha x^{-1} \in \cap_{g\in G}(xgH(xg)^{-1})$. So $xNx^{-1} \subset \cap_{g\in G}(xgH(xg)^{-1})$. Conversely if $\alpha \in \cap_{g\in G}(xgH(xg)^{-1})$, then for each $g \in G$, there exists $h \in H$ such that $\alpha = xghg^{-1}x^{-1}$, so $x^{-1}\alpha x \in N$, so $\alpha \in xNx^{-1}$. Hence we have

$$xNx^{-1} = \bigcap_{g\in G} xgH(xg)^{-1}$$

But we also have

$$\bigcap_{g\in G} xgH(xg)^{-1} = \bigcap_{g\in G} gHg^{-1} = N$$

as $xG = G$. So N is indeed a normal subgroup of G contained in H. If M is also a normal subgroup of G contained in H. Then for all $g \in G$ we have $M = gMg^{-1} \subset gHg^{-1}$. So

$$M \subset \bigcap_{g\in G} gHg^{-1} = N$$

□

So to get our result, it suffices to show that $G(K/L)$ is the largest normal subgroup of $G(K/F)$ contained in $G(K/E)$.

First $G(K/L)$ is indeed contained in $G(K/E)$ as $E \subset L$. Then since L/F is normal, by the Fundamental Theorem of Galois Theory, we have that $G(K/L) \triangleleft G(K/F)$.

Now suppose $H \triangleleft G(K/F)$ with $H \subset G(K/E)$. Then we have $H = G(K/K^H)$, so $G(K/K^H) \triangleleft G(K/F)$, so K^H/F normal. Moreover since $H \subset G(K/E)$, we have $K^H \supset K^{G(K/E)} = E$ as K/E Galois since K/F Galois. So K^H is a subfield of K containing E with K^H/F normal, so $L \subset K^H$. We also have $L = K^{G(K/L)}$ since K/L Galois since K/F Galois. So $H \subset G(K/L)$. So we are done.

Problem 41

Suppose that K/F is Galois, p a prime, and $p^r \mid [K:F]$ but $p^{r+1} \nmid [K:F]$. Show that there exist fields L_i, $1 \le i \le r$, satisfying $F \subset L_r < L_{r-1} < \cdots < L_1 < L_0 = K$ such that L_i/L_{i+1} is normal, $[L_i : L_{i+1}] = p$ and $p \nmid [L_r : F]$.

(Solution)

We need the following lemma.

Lemma: If G is a p-group, say order p^r, then it has a subnormal series

$$1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_{r-1} \triangleleft N_r = G$$

such that $[N_i : N_{i-1}] = p$.

Proof. We proceed by induction on r.

For the base case assume $r = 1$. Then $|G| = p$. Then we are done as $1 \triangleleft G$ and $[G:1] = p$.

For the inductive step, assume result is true for r. Suppose G is a group of order p^{r+1}. Then by Generalized First Sylow Theorem, G has subgroup N_r of order p^r hence index p. Note that p is the only hence smallest prime dividing the order of G. So by the corollary to General Cayley Theorem, we have that $N_r \triangleleft G$. Then we apply the inductive hypothesis to N_r to produce

$$1 = N_0 \triangleleft \cdots \triangleleft N_r$$

with $[N_i : N_{i-1}] = p$. So adding $N_{r+1} = G$ to the end gives the result. $\square$

Now we show the main result. If $r = 0$, then there is nothing to show, so assume $r > 0$. Since K/F Galois, $[K:F] = |G(K/F)|$. Then $p^r \mid\mid |G(K/F)|$, so we can write $|G(K/F)| = p^r m$ where $(p,m) = 1$. Then by First Sylow Theorem, $G(K/F)$ contains a subgroup H_r of order p^r. Then apply the lemma to H_r to get

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{r-1} \triangleleft H_r$$

with $[H_i : H_{i-1}] = p$. Then set $L_i = K^{H_i}$ for $0 \le i \le r$. Note that $L_0 = K^1 = K$. Then by the Fundamental Theorem of Galois Theory (FTGT), we have $H_i = G(K/L_i)$, so our subnormal series becomes

$$G(K/K) = G(K/L_0) \triangleleft G(K/L_1) \triangleleft \cdots \triangleleft G(K/L_r)$$

We also have

$$F \subset L_r \subset \cdots \subset L_1 \subset L_0$$

In particular, for $0 \le i \le r-1$, we have $K/L_i/L_{i+1}$ with K/L_{i+1} Galois since K/F finite Galois, so by the FTGT, L_i/L_{i+1} normal since $G(K/L_i) \triangleleft G(K/L_{i+1})$. And since $G(K/L_i) \in \mathcal{G}(K/L_{i+1})$, we have

$$p = [H_{i+1} : H_i] = [G(K/L_{i+1}) : G(K/L_i)] = [K^{H_i} : L_{i+1}] = [L_i : L_{i+1}]$$

Hence we have

$$F \subset L_r < \cdots < L_1 < L_0 = K$$

with $[L_i : L_{i+1}] = p$ and L_i/L_{i+1} normal. Finally, we need to show $p \nmid [L_r : F]$. Suppose on the contrary that $p \mid [L_r : F]$. Then since $[L_r : F] = [K^{H_r} : F] = [G(K/F) : H_r]$, we may write $[G(K/F) : H_r] = pn$ some n. But then by Lagrange, we have

$$|G(K/F)| = [G(K : F) : H_r]|H_r| = np^{r+1}$$

a contradiction to $p^r \mid\mid |G(K/F)|$. Hence we are done.

Problem 42

Suppose $|K| = p^m$ and $F \subset K$. Show that $|F| = p^n$ for some n with $n \mid m$. Moreover, $G(K/F)$ is generated by the Frobenius automorphism $\alpha \mapsto \alpha^{p^n}$.

(Solution)

Viewing as groups and using Lagrange's Theorem, we have that $|F| \mid p^m$, so $|F| = p^n$ some $n \leq m$. Moreover K is finite, so we can view it as a finite-dimensional F-vectorspace of dimension, say d. Then we have

$$K \cong F^d$$

as vectorspaces, so $p^m = |K| = |F|^d = p^{dn}$. In particular, n must divide m.

We first need to verify that the map is indeed an element of $G(K/F)$.
Let $\varphi : \alpha \mapsto \alpha^{p^n}$. This is indeed a (well-defined) homomorphism since characteristic p and Children's Bionomial Theorem. Since K is a field, φ is automatically monic since it is not the zero map as $\varphi(1) = 1 \neq 0$. Moreover, since K is finite, and φ is injective, it must be that φ is also surjective. Hence φ is indeed a field automorphism. By problem 3, we have that φ fixes F (for all $\alpha \in F$, $\alpha^{p^n} = \alpha$). So indeed $\varphi \in G(K/F)$.

Since K/F is finite, $G = G(K/F)$ is finite and $[K : F] \geq |G|$. Then it suffices to show that the order of φ in G is d, where $[K : F] = d$ as above (if so, then the order of G is at least d hence $|G| = d$, so φ generates).

Suppose on the contrary that the order of φ is not d. Note that it cannot be more than d as the size of G is bounded above by d. So we have that the order of φ is some $k < n$. So $\varphi^k = 1_K$. So for all $\alpha \in K$,

$$\alpha^{p^{kn}} = \varphi^k(\alpha) = \alpha$$

So every element of K is a root of $f = t^{p^{kn}} - t \in K[t]$. But f has at most p^{kn} distinct roots. But we just showed that f as at least $p^m = p^{nd} > p^{nk}$ distinct roots, a contradiction. Hence it must be that φ has order d, so we are done.

Problem 43

Show if F is a finite field, $n \in \mathbb{Z}^+$, then there exists an irreducible polynomial $f \in F[t]$ of degree n.

(Solution)

Since F is finite, write $|F| = p^m$ some p. Then suppose we have a degree n extension L/F, so that $|L| = p^{nm}$. Then since L is finite, $L^\times$ is cyclic, so it has some generator α. Then we have $L = F(\alpha)$, so

$$[F(\alpha) : F] = [L : F] = n$$

so $m_F(\alpha) \in F[t]$ works.

So the problem reduces to showing there exists a field extension of F of degree n. But we can get this by considering a splitting field of $t^{p^{mn}} - t$ over F, which follows the same proof as problem 16, so we omit.

Problem 44

Show if F is a finite field, then every element of in F is a sum of two squares.

(Solution)

Write $|F| = p^n$ some $p > 0$ prime. If $p = 2$, then we have that

$$\alpha = \alpha^{2^n} = (\alpha^{2^{n-1}})^2 + 0^2$$

for all $\alpha \in F$, so assume $p > 2$.

Now I got a hint from

https://math.stackexchange.com/questions/1266433/squares-in-a-finite-field.

We need to compute the number of squares in $F^\times$. Let $\varphi : F^\times \to F^\times$ by $x \mapsto x^2$. This is certainly well-defined and $(xy)^2 = x^2y^2$, so it is a group homomorphism. By the First Isomorphism Theoerm, we have

$$F^\times / \ker(\varphi) \cong \text{im } (\varphi)$$

so the number of squares in $F^\times$ is $|\text{im } (\varphi)| = \frac{p^n-1}{|\ker(\varphi)|}$. So we need to compute the size of the kernel. Note that if $\varphi(x) = 1$, then $x^2 = 1$, so $x = 1$ or x is order 2. Since F is finite, $F^\times$ is cyclic with order $p^n - 1$ which is even since p is odd, so by the cyclic subgroup theorem, there exists a unique subgroup of order 2. Hence there is only one element in $F^\times$ of order 2. So there are only 2 elements in the kernel, so $|\text{im } (\varphi)| = \frac{p^n-1}{2}$. Since 0 is a square in F, we have that there are exactly $\frac{p^n-1}{2} + 1 = \frac{p^n+1}{2}$ squares in F.

Then let $\alpha \in F$. To show that α is a sum of two squares in F, define the following sets:

$$S \coloneqq \{x \in F \mid x \text{ is a square}\}$$

and

$$T = \{\alpha - x \mid x \in S\}$$

In particular $|S| = \frac{p^n+1}{2} = |T|$ (we can biject S and T by $x \mapsto \alpha - x$). In particular S and T cannot be disjoint for otherwise, we would have

$$p^n + 1 \leq p^n$$

So they overlap. So there exists some square $x \in F$ such that $x = \alpha - y$ for some square y. Hence $\alpha = x + y$, a sum of two squares.

Problem 45

Show if K is not a finite field and u, v are algebraic and separable over K, then there exists an element $a \in K$ such that $K(u, v) = K(u + av)$. Is this true if $|K| < \infty$ with $K(u) < K(u, v)$ and $K(v) < K(u, v)$?

(Solution)

Since u, v are algebraic over K, then $K(u, v)/K$ is finite as we have an upper bound for the degree. Moreover by problem 23, $K(u, v)/F$ is separable, so by the Primitive Element Theorem, there exists $\alpha \in K(u, v)$ such that $K(u, v) = K(\alpha)$. Then somehow show that α can be written in the desired form.

I suspect that the result is not true for the second scenario by way of problem 25.

Problem 46

(We can assume depressed cubic)

Let $F = \mathbb{R}$. Let $f = t^3 - a_2t - a_3 \in \mathbb{R}[t]$. Show:

(a) The discriminant $\triangle = 4a_2^3 - 27a_3^2$.

(b) f has mulitple roots if and only if $\triangle = 0$.

(c) f has three distinct real roots if and only if $\triangle > 0$.

(d) f has one real root and two non-real roots if and only if $\triangle < 0$

(Solution)

(a)

We followed the computational hint from:
https://math.stackexchange.com/questions/4443994/discriminant-of-depressed-cubic.

Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f in some extension field of F. By definition,

$$\triangle = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$$

Moreover,

$$\begin{aligned} f &= (t - \alpha_1)(t - \alpha_2)(t - \alpha_3) \\ &= t^3 - (\alpha_1 + \alpha_2 + \alpha_3)t^2 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)t - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

So matching coefficients gives:

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = -a_2 \\ \alpha_1\alpha_2\alpha_3 = a_3 \end{cases} \tag{1}$$

Then to reduce the number of variables, define $A = \alpha_1\alpha_2$ and $B = \alpha_1 + \alpha_2$. Note that $B = -\alpha_3$ by the first equation in (1). Then we have

$$(\alpha_1 - \alpha_2)^2 = (\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2) = (B^2 - 4A)$$

Moreover,

$$\begin{aligned} (\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 &= ((\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3))^2 \\ &= (\alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 + \alpha_3^2)^2 \\ &= (A + 2B^2)^2 \\ &= A^2 + 4AB^2 + 4B^4 \end{aligned}$$

Hence

$$\begin{aligned} \triangle &= (B^2 - 4A)(A^2 + 4AB^2 + 4B^4) \\ &= A^2B^2 + 4AB^4 + 4B^6 - 4A^3 - 16A^2B^2 - 16AB^4 \\ &= -15A^2B^2 - 12AB^4 + 4B^6 - 4A^3 \end{aligned}$$

Then the second equation in (1) becomes $a_2 = B^2 - A$ and the third equation in (1) becomes $a_3 = -AB$, so

$$\begin{aligned}
4a_2^3 - 27a_3^2 &= 4(B^2 - A)^3 - 27A^2B^2 \\
&= 4(B^6 - 3AB^4 + 3A^2B^2 - A^3) - 27A^2B^2 \\
&= 4B^6 - 12AB^4 + 12A^2B^2 - 4A^3 - 27A^2B^2 \\
&= 4B^6 - 15A^2B^2 - 12AB^4 - 4A^3 \\
&= \triangle
\end{aligned}$$

as desired.

(b)

Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f.
Suppose f has multiple roots. Then we can assume WLOG that $\alpha_1 = \alpha_2$. Then by definition:

$$\triangle = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = 0(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = 0$$

Conversely suppose that $0 = \triangle = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$. If $(\alpha_1 - \alpha_2)^2 = 0$, then we are done. If not then since domain, $(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = 0$ so $(\alpha_1 - \alpha_3)^2 = 0$ or $(\alpha_2 - \alpha_3)^2 = 0$ which gives the result in either case. Hence f has a multiple root.

(c)

Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f.

Suppose f has three distinct real roots. Then by part (b), $\triangle \neq 0$. Moreover, $\alpha_1 - \alpha_2 \in \mathbb{R} \setminus 0$, so $(\alpha_1 - \alpha_2)^2 > 0$. Similarly $(\alpha_2 - \alpha_3)^2 > 0$ and $(\alpha_1 - \alpha_3)^2 > 0$, so $\triangle > 0$.

Conversely suppose that $\triangle > 0$. Then by part (b), f has three distinct roots. Suppose on the contrary that f has a non-real root, say α_1. Then by problem 13b, $\overline{\alpha_1}$ which is non-real is also a root, say α_2. Then we must have that $\overline{\alpha_3} = \alpha_3$,i.e. α_3 is real for otherwise its complex conjugate is either α_1 so $\alpha_3 = \alpha_2$ or is α_2 so $\alpha_3 = \alpha_1$, which both would contradict distinct roots. Then write $\alpha_1 = a + bi$ so that $\alpha_2 = a - bi$ for $a, b \in \mathbb{R}$ and $b \neq 0$. Then using some computations from part (a) and the fact that $a_2 \in \mathbb{R}$, we have

$$\begin{aligned}
\triangle &= (\alpha_1 - \alpha_2)^2(\alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 + \alpha_3^2)^2 \\
&= (2bi)^2(2\alpha_1\alpha_2 + a_2 + \alpha_3^2)^2 \\
&= -4b^2(2a^2 + 2b^2 + a_2 + \alpha_3^2)^2
\end{aligned}$$

where $(2a^2 + 2b^2 + a_2 + \alpha_3^2) \in \mathbb{R}$, so squaring it is nonnegative, so $\triangle \leq 0$ a contradiction. Hence it must be that f has three distinct real roots.

(d)

Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f.

We use problem 13(b). Suppose f has one real root and two non-real roots. Then the two non-real roots must be complex-conjugates by problem 13(b). In particular, neither is zero as non-real and f has three distinct roots. So by previous two parts, we must have $\triangle < 0$.

If $\triangle < 0$, then by part (b), f has three distinct roots. Moreover by part (c) f has a non-real root, say α_1. But then its (distinct) complex conjugate is also a root and non-real, say α_2. Then if the complex conjugate of α_3 is α_2 then $\alpha_3 = \alpha_1$, contradicting distinct roots. Similarly, the complex conjugate of α_3 cannot be α_2. Hence $\overline{\alpha_3} = \alpha_3$ so $\alpha_3 \in \mathbb{R}$. So we are done.