1. Problem 3, Lang p.253

Let \( E \) be a field and \( \alpha, \beta \) be two algebraic elements over \( E \). Let \( f(x) \) and \( g(x) \) be respectively the irreducible polynomials of \( \alpha \) and \( \beta \) over \( E \). Put \( n = \deg f(x) \) and \( m = \deg g(x) \). Suppose that \( \gcd(n,m) = 1 \), we show that \( g(x) \) is also irreducible over \( E(x) \).

Because \( g(x) \in F(x)[x] \) and \( g(\beta) = 0 \), \( \beta \) is algebraic over \( F(x) \) and the irreducible polynomial \( h(x) \) of \( \beta \) over \( F(x) \) divides \( g(x) \) as polynomials over \( F(x) \). Since \( F \subset F(x) \), \( h(x) \) is also irreducible over \( F \). To show that \( g(x) \) is irreducible over \( F(x) \), it suffices to show that \( g(x) = h(x) \). Then it suffices to show that \( \deg h = \deg g = m \). We have

\[
[F(x, \beta) : F] = [F(x, \beta) : F(x)] [F(x) : F] = n \left[ F(x) : F(x) \right] = n (\deg h),
\]

\[
[F(x, \beta) : F] = [F(x, \beta) : F(\beta)] [F(\beta) : F] = m \left[ F(x, \beta) : F(\beta) \right].
\]

Thus \( \deg h = m \left[ F(x, \beta) : F(\beta) \right] \). Since \( \gcd(n,m) = 1 \), \( m \mid (\deg h) \).

Thus \( \deg h \geq m = \deg g \). Since \( h(x) | g(x) \), \( \deg h \leq \deg g \). Thus \( \deg h = \deg g \) and \( h(x) = g(x) \) (because both are monic polynomials).
2. Problem 7, Lang, p. 253

Let $E$ and $F$ be two finite extensions of $K$, contained in a larger field $K$. Let $n = [E:k]$ and $m = [F:k]$. As a vector field over $k$, $E$ has dimension $n$. Thus it has a basis $\{x_1, \ldots, x_n\}$. Then $E = k(x_1, \ldots, x_n)$, which is the smallest subfield of $K$ that contains $k$ and $x_1, \ldots, x_n$. The compositum $EF$ is the smallest subfield of $K$ that contains both $E$ and $F$. This is the same as the smallest subfield of $K$ that contains $F$ and $x_1, \ldots, x_n$. Thus

$$EF = F(x_1, \ldots, x_n)$$

Therefore, as a vector space over $F$, $EF$ is generated by $x_1, \ldots, x_n$. Thus it is a finite dimensional vector space and $[EF:F] \leq n$. We have

$$[EF:k] = [EF:F][F:k] \leq n[F:k] = [E:k][F:k]. \quad (\ast)$$

Now suppose that $\gcd(m, n) = 1$. We have $[EF:k] = [EF:F][F:k] = m[EF:F]$. Similarly, $[EF:k] = [EF:E][E:k] = m[EF:E]$. Therefore,

$$m[EF:F] = n[EF:E].$$

Because $\gcd(m, n) = 1$, $m \mid [EF:F]$. Since $[EF:F] \leq n$, we must have $[EF:F] = n$. Then the equality at $(\ast)$ occurs.

3. Problem 8, Lang, p. 253

Let $f(X) \in k[X]$ with $\deg f = n$. $K$ is the splitting of $f(X)$
(note that we can assume $k \subseteq K \subseteq \overline{k}$). Then we'll show by induction in $n \in \mathbb{N}$ that $[K : k]$ divides $n!$

For $n = 1$: $f(x) = a(x - a)$ where $a \in k, a \neq 0$.

Thus $a \in k$. Then $f(x)$ is already split in $k[x]$. Thus $K = k$ and $[K : k] = 1$.

Now suppose that the statement of the problem is true for all $n < m$ and for all choices of function field $k$ and polynomial $f(x) \in k[x]$, where $m > 2$. We'll show that it is also true for $n = m$. Let $f(x) \in k[x]$ be a polynomial of degree $m > 2$. We consider two cases:

- **$f(x)$ is irreducible over $k$**

  Then $f(x) = c(x - \alpha_1) \cdots (x - \alpha_m)$ where $c \in k \setminus \{0\}$ and $\alpha_i \in \overline{k}$.

  Then the splitting field of $f(x)$ is $K = k(\alpha_1, \ldots, \alpha_m)$. We have $f(\alpha_1) = 0$ and $f(x)$ is irreducible in $k[x]$. Thus $f(x)/c$ is the irreducible polynomial of $\alpha_1$ over $k$. Thus $[k(\alpha_1) : k] = \deg f = m$.

  Put $F = k(\alpha_1)$ and $g(x) = (x - \alpha_2) \cdots (x - \alpha_m) \in \overline{k}[x]$. Then

  $$f(x) = (x - \alpha_1)g(x)$$

  as polynomials in $\overline{k}[x]$.

  Since $f(x), (x - \alpha_1) \in F[x]$, there exist $q(x) \in F[x]$ and $\beta \in F$ such that $f(x) = (x - \alpha_1)q(x) + \beta$ and $\deg q > 1$. 

This identity is also an identity of polynomials in $\overline{k}[X]$. By the uniqueness of quotient and remainder in $\overline{k}[X]$, we conclude $q(X)=g(X)$ and $r=0$. Thus $g(X) \in F[X]$. Thus $F(\alpha_1, \ldots, \alpha_m)$ is the splitting field of $g(X)$. Because $\deg g = m-1 < m$, by the induction hypothesis we have $[F(\alpha_1, \ldots, \alpha_m) : F] \mid (m-1)!$. We have

$$[k : k] = [k(\alpha_1, \ldots, \alpha_m) : k] = [k(\alpha_1) : k(\alpha_1)] [k(\alpha_1) : k] = [F(\alpha_1, \ldots, \alpha_m) : F] m,$$

which divides $(m-1)! m = m!$.

$f(X)$ is reducible over $k$.

Then there are $g(X), h(X) \in k[X]$ with $1 \leq \deg g, \deg h < m$ such that $f(X) = g(X) h(X)$. Let $g(X) = \gamma_1 (X-\beta_1) \cdots (X-\beta_e)$,

$$h(X) = \gamma_2 (X-\gamma_1) \cdots (X-\gamma_s),$$

where $\gamma_1, \gamma_2 \in \overline{k} \setminus \{0\}$, $\beta_i, \gamma_j \in \overline{k}$, $1 \leq e, s < m$ and $e+s = m$.

Then the splitting field of $f(X)$ is $K = k(\beta_1, \ldots, \beta_e; \gamma_1, \ldots, \gamma_s)$.

Put $F = k(\beta_1, \ldots, \beta_e)$. Then $F$ is the splitting field of $g(X)$. By the induction hypothesis, $[F : k] \mid e!$.

Since $k \subset F$, $h(X) \in F[X]$. Thus $F(\gamma_1, \ldots, \gamma_s)$ is the splitting field of $h(X)$. By the induction hypothesis, $[F(\gamma_1, \ldots, \gamma_s) : F] \mid s!$.
Then \( [K:k] = \left[ k \left( \beta_1, \ldots, \beta_t, \delta_1, \ldots, \delta_s \right); k \right] \)
\[ = \left[ k \left( \beta_1, \beta_2 \right); k \right] \left[ k \left( \beta_1, \beta_2 \right); k \right] \]
\[ = \left[ F \left( \delta_1, \ldots, \delta_s ; F \right) ; F \right] \left[ F; k \right], \]

which divides \( (m-1)! s! = (m-1)! (m-t)! \). Thus \( [K:k] \) divides \( m! \),

4. Problem 10, Lang, p. 253

Let \( x \in \mathbb{R} \) such that \( x^4 = 5 \). We first notice that \( r + is\sqrt{5} \) for some \( r, s \in \mathbb{Q} \). Then \( r^2 + 5s^2 = (r + is\sqrt{5})(r - is\sqrt{5}) = r^2 + 5s^2 \in \mathbb{Q} \). Thus \( r = s = 0 \). Consequently, \( r + is\sqrt{5} \in \mathbb{Q} \) if and only if \( s = 0 \).

(a) We will show that \( \mathbb{Q}(i\sqrt{5}) \) is normal over \( \mathbb{Q} \). Because \( i\sqrt{5} \) is a root of the polynomial \( X^2 + 5 \in \mathbb{Q}[X] \), it is algebraic over \( \mathbb{Q} \). Thus \( \mathbb{Q}(i\sqrt{5}) \) is an algebraic extension of \( \mathbb{Q} \). For any \( g(X) \in \mathbb{Q}[X] \), we write \( g(X) = \sum a_j X^j \in \mathbb{Q} \) as an extension.

Thus \( g(i\sqrt{5}) = \sum a_j (i\sqrt{5})^j = \sum a_k \sum_{\text{even } k} a_k (-5)^{k/2} + (i\sqrt{5}) \sum_{\text{odd } k} a_k (-5)^{(k-1)/2} \in \mathbb{Q} \).

Thus every element of \( \mathbb{Q}(i\sqrt{5}) \) is of the form \( r + si\sqrt{5} \) for some \( r, s \in \mathbb{Q} \).

Conversely, each number of the form \( r + si\sqrt{5} \) where \( r, s \in \mathbb{Q} \) is the value of the polynomial \( r + sX \in \mathbb{Q}[X] \) evaluated at \( i\sqrt{5} \). Thus,
\(Q(\sqrt[3]{5}) = \{ r + is\sqrt[3]{5} : r, s \in \mathbb{Q} \}\).

Take an arbitrary element \(r + is\sqrt[3]{5} \in Q(\sqrt[3]{5})\). Suppose that \(f(X) \in \mathbb{Q}[X]\) is an irreducible polynomial over \(\mathbb{Q}\) and \(f(r + s\sqrt[3]{5}) = 0\). We'll show that \(f(X)\) splits into linear factors in \(Q(\sqrt[3]{5})[X]\). WLOG, we can assume \(f(X)\) is monic. Then \(f(X)\) is the irreducible polynomial of \(r + is\sqrt[3]{5}\) over \(\mathbb{Q}\).

- If \(s = 0\), then \(f(r) = 0\). Then \((X - r) | f(X)\). Since \(f(X)\) is irreducible over \(\mathbb{Q}\), \(f(X) = X - r\).

- If \(s \neq 0\), then \(r \pm is\sqrt[3]{5} \notin \mathbb{Q}\). We see that the polynomial

\[g(X) = X^2 - 2rX + (r^2 + 5s^2) = (X - (r + is\sqrt[3]{5}))(X - (r - is\sqrt[3]{5})) \in \mathbb{Q}[X].\]

Moreover, \(g(r + is\sqrt[3]{5}) = 0\) and \(g(X)\) is irreducible over \(\mathbb{Q}\) because \(\sqrt[3]{5} \pm is\sqrt[3]{5} \notin \mathbb{Q}\). Thus \(f(X) = g(X)\), which splits into linear factors in \(Q(\sqrt[3]{5})[X]\).

(b) We'll show that \(Q(\sqrt{i\alpha})\) is normal over \(Q(i\alpha^2)\). Put \(\beta = \alpha + i\alpha\). We have \(\beta^2 = \alpha^2(1 + i)^2 = 2i\alpha^2\). Thus \(Q(\beta^2) = Q(i\alpha^2)\).

We want to show that \(Q(\beta)\) is normal over \(Q(\beta^2)\).

We have \(\beta^4 = (2i\alpha^2)^2 = -4\alpha^4 = -20\). Thus \(\beta\) vanishes the polynomial \(X^4 + 20 \in \mathbb{Q}[X]\). Moreover, \(X^4 + 20 = X^4 + 0 \cdot X^3 + 0 \cdot X^2 + 0 \cdot X + 20\)

- \(5\) doesn't divide \(20\).
- \(5\) divides \(20\).
- \(5\) divides \(20\), but not \(25\).
Thus, by Eisenstein's criterion, \( X^4 + 20 \) is irreducible over \( \mathbb{Q} \). Thus, \( X^4 + 20 \) is the irreducible polynomial of \( \beta \) over \( \mathbb{Q} \).

For any \( g(X) \in \mathbb{Q}[X] \), we write \( g(X) = a_n X^n + \ldots + a_1 X + a_0 \) with \( a_j \in \mathbb{Q} \). Then

\[
g(\beta) = \sum_{k=0}^{n} a_k \beta^k = \sum_{\substack{0 \leq k \leq n \\ k \text{ even}}} a_k (\beta^2)^{k/2} + \beta \sum_{\substack{0 \leq k \leq n \\ k \text{ odd}}} a_k (\beta^2)^{(k-1)/2}
\]

Thus, every element of \( \mathbb{Q}(\beta) \) is of the form \( u + \beta v \) for some \( u, v \in \mathbb{Q}(\beta^2) \).

Conversely, each number of the form \( u + \beta v \) where \( u, v \in \mathbb{Q} \) is the value of the polynomial \( u + vX \in \mathbb{Q}(\beta^2) \) evaluated at \( \beta \). Thus,

\[
\mathbb{Q}(\beta) = \{ u + \beta v : u, v \in \mathbb{Q}(\beta^2) \}
\]

Next, we'll show that if \( u + \beta v \in \mathbb{Q}(\beta^2) \) for some \( u, v \in \mathbb{Q}(\beta^2) \) then \( v = 0 \). Suppose by contradiction that \( v \neq 0 \). We have \( \beta v \in \mathbb{Q}(\beta^2) \). Note that \( \mathbb{Q}(\beta^2) = \mathbb{Q}(i\sqrt{5}) \). By Part (i), we showed that every element of \( \mathbb{Q}(\beta^2) \) has the form \( r + s\beta^2 \) for some \( r, s \in \mathbb{Q} \). Thus, \( \beta v = r + s\beta^2 \) for some \( r, s \in \mathbb{Q} \). Since \( v \in \mathbb{Q}(\beta^2) \), \( v = r' + s'\beta^2 \) for some \( r', s' \in \mathbb{Q} \). Then

\[
\beta(r' + s'\beta^2) = r + s\beta^2
\]

\( \implies s'\beta^3 - s\beta^2 + r'\beta - r = 0 \)

Since \( v \neq 0 \), either \( r' 
eq 0 \) or \( s' 
eq 0 \). Then the above polynomial

\[
s'X^3 - sX^2 + r'X - r \]

is of degree 3, 2, or 1. This is a contradiction.
because the irreducible polynomial of $\beta$ over $\mathbb{Q}$ is of degree 4.

Next, for each element $u + \beta v \in \mathbb{Q}(\beta)$, we call $f(x) \in \mathbb{Q}(\beta^2)$ any polynomial irreducible over $\mathbb{Q}(\beta^2)$ such that $f(u + \beta v) = 0$. We want to show that $f(x)$ splits into linear factors in $\mathbb{Q}(\beta)[x]$. WLOG, we can assume $f(x)$ is monic. Then $f(x)$ is the irreducible polynomial of $\beta$ over $\mathbb{Q}(\beta^2)$. But $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta^2)$ and we consider two cases:

- If $v = 0$, then $f(u) = 0$. Then $(x - u) | f(x)$. Then $f(x) = x - u$ because $f(x)$ is irreducible.

- If $v \neq 0$, then $u + \beta v \notin \mathbb{Q}(\beta^2)$ for what we have shown above. But

$$g(x) = x^2 - 2ux + (u^2 - \beta^2 v^2) = (x - (u + \beta v))(x - (u - \beta v)) \in \mathbb{Q}(\beta^2).$$

We see that $g(u + \beta v) = 0$ and $g(x)$ is irreducible over $\mathbb{Q}(\beta^2)$ because $u + \beta v \notin \mathbb{Q}(\beta^2)$. Thus $f(x) = g(x)$, which splits into linear factors in $\mathbb{Q}(\beta)[x]$.

(c) We will show that $\mathbb{Q}(\beta)$ is not normal over $\mathbb{Q}$.

First we see that $\alpha$ is a root of the polynomial $x^4 - 5 \in \mathbb{Q}[x]$. By the Eisenstein's criterion for $p = 5$, we conclude that $x^4 - 5$ is irreducible over $\mathbb{Q}[x]$. Thus $x^4 - 5$ is the irreducible polynomial of $\alpha$ over $\mathbb{Q}$.

Now suppose by contradiction that $\mathbb{Q}(\beta)$ is normal over $\mathbb{Q}$. Since
\( \beta \) is a root of \( X^4 + 20 \in \mathbb{Q}[X] \), all other roots of its also belong to \( \mathbb{Q}(\beta) \). We have \((i\beta)^4 + 20 = \beta^4 + 20 = 0\). Thus \(i\beta\) is a root of \( X^4 + 20 \). Thus \(i\beta \in \mathbb{Q}(\beta)\). Then \(i \in \mathbb{Q}(\beta)\). Then there exist \( u, v, \alpha, \beta \in \mathbb{Q}(\beta) \) such that \( i = u + \beta v \). Since \( u, v, \alpha, \beta \in \mathbb{Q}(\beta^2) \), there exist \( r, r', s, s' \in \mathbb{Q} \) such that \( u = r + is\sqrt{5} \) and \( v = r' + is'\sqrt{5} \). Then:
\[
\begin{align*}
  i &= (r + is\sqrt{5}) + \beta (r' + is'\sqrt{5}) \\
  &= (r + is\sqrt{5}) + \alpha (1 + i)(r' + is'\sqrt{5}) \\
  &= (r + is\sqrt{5}) + \alpha (r' - s'\sqrt{5} + ir' + is'\sqrt{5}) \\
  &= (r + \alpha (r' - s'\sqrt{5})) + i (s\sqrt{5} + \alpha r' + \alpha s'\sqrt{5})
\end{align*}
\]
Thus:
\[
\begin{align*}
  r + \alpha (r' - s'\sqrt{5}) &= 0 \\
  s\sqrt{5} + \alpha r' + \alpha s'\sqrt{5} &= 1
\end{align*}
\]
(\( \Rightarrow \))
\[
\begin{align*}
  r + \alpha (r' - s'\sqrt{5}) &= 0 \\
  5\alpha^2 + \alpha r' + s'\alpha^3 &= 1
\end{align*}
\]
Then \( s'\alpha^3 + 5\alpha^2 + r'\alpha - 1 = 0 \). This is a contradiction because the irreducible polynomial of \( \alpha \) over \( \mathbb{Q} \) is of degree 4.

(5) Problem 20, Lang, p. 254

(a) Let \( E = F(x) \) where \( x \) is transcendental over \( F \). Let \( K \neq F \) be a subfield of \( E \) which contains \( F \). We'll show that \( x \) is algebraic over \( K \). Because \( x \) is transcendental over \( F \), we can view \( E \) as a field of polynomials with variable \( x \) and coefficients in \( F \). In other words,
\[ E = \mathbb{F}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0 \right\} \]

Since \( K \neq F \), there exists \( \frac{f(x)}{g(x)} \in K \setminus F \). By multiplying by a nonzero factor in \( F \), we can always assume that \( f(x) \) and \( g(x) \) are monic polynomials. Since \( \frac{f(x)}{g(x)} \notin F \), \( f(x) \neq g(x) \) and the degree of at least one of them is positive. Put \( h(x) = f(x) - \frac{f(x)}{g(x)} g(x) \).

Since \( F \subset K \), \( f(x), g(x) \in K[x] \). Since \( \frac{f(x)}{g(x)} \in K \), \( h(x) \in K[x] \).

Since \( \frac{f(x)}{g(x)} \neq 1 \) and \( \deg f \geq 1 \) or \( \deg g \geq 1 \), \( \deg h \geq 1 \). We have \( h(x) = f(x) - \frac{f(x)}{g(x)} g(x) = f(x) - f(x) = 0 \). Thus \( x \) is algebraic over \( K \).

(b) Let \( F \) be a field and \( x \) be transcendental over \( F \). Put \( E = \mathbb{F}(x) \) and let \( z \) be a variable over \( E \). Let \( f(z), g(z) \in \mathbb{F}[z] \) such that \( n = \min(\deg f, \deg g) \geq 1 \) and \( \gcd(f(z), g(z)) = 1 \). Put \( y = \frac{f(z)}{g(z)} \in E \).

We'll show that \([F(x) : F(y)] = n\).

First, let's show that \( y \) is a variable over \( F \). Suppose by contradiction that there is a polynomial \( u(z) \in \mathbb{F}[z] \), \( u(z) \neq 0 \) such that \( u(y) = 0 \). We write \( u(z) = a_m z^m + \cdots + a_1 z + a_0 \) with \( a_i \in \mathbb{F} \), \( m \geq 1 \). Then
First, let's show that $y$ is a variable over $F$. Suppose by contradiction that there is a polynomial $u(z) \in \mathbb{F}(z)$, $u(z) \neq 0$ such that $u(y) = 0$. We write $u(z) = a_m z^m + \ldots + a_0 z + a_0$ with $a_i \in \mathbb{F}$, $m > 0$ and $a_m \neq 0$. Then

$$0 = u(y) = \sum_{k=0}^{m} a_k \frac{f(x)^k}{g(x)^k} = \frac{1}{g(x)^m} \sum_{k=0}^{m} a_k f(x)^k g(x)^{m-k}.$$  

Thus

$$0 = a_0 g(x)^m + a_1 g(x)^{m-1} f(x) + \ldots + a_{m-1} g(x) f(x)^m - a_m f(x)^m. \quad (*)$$  

Since $a_m \neq 0$, $m > 0$, then all terms on the right hand side are divisible by $g(x)$ except for the last term. Since $g(x)$ and $f(x)$ are relatively prime, so are $g(x)$ and $f(x)^m$. Thus $g(x) | a_m f(x)^m$ if and only if $g(x) \in \mathbb{F}$. Because $n = \max(\deg f, \deg g) > 1$, $\deg f > 1$.  

Put $g(x) = c \in \mathbb{F}$, $(*)$ becomes

$$a_m f(x)^m + a_{m-1} c f(x)^{m-1} + \ldots + a_0 c^m = 0.$$  

Since $x$ is a variable over $F$, $f(x)$ is a polynomial over $F$. Then the degree on the left hand side is $m \deg(f) > 1$. This is a contradiction. Therefore, $y$ is a variable over $F$.

Put $K = F(y)$. Then $F \subseteq K \subseteq \mathbb{E}$ and $y \in K \setminus F$. Then $K$ is a subfield of $\mathbb{E}$ and $K \neq F$. By part (a), we conclude that $x$ is algebraic over $K$. We have
\[ E = F(x) = F\left( \frac{f(x)}{g(x)}, x \right) = F\left( \frac{f(x)}{g(x)} \right)(x) = K(x). \]

Thus, \([F(x) : F(y)] = [E : K] = [K(x) : K]\), which is equal to the degree of the irreducible polynomial of \(x\) over \(K\). Put
\[ h(z) = f(x) - yg(z) \in K[z] \]

Because \(y \notin F\), \(\deg h = \max(\deg f, \deg g) = n\). Moreover,
\[ h(x) = f(x) - yg(x) = f(x) - \frac{f(x)}{g(x)} g(x) = 0 \]

Thus, we only need to show that \(h(z)\) is irreducible over \(K\).

We see that \(K = F(y)\) is the field of fractions of \(F[y]\) and \(h(z) \in (F[y])[z]\). Thus, we need to show that \(h(z)\) is not of the form \(h(z) = u(z)v(z)\) where \(u(z), v(z) \in (F[y])[z]\), \(\deg u, \deg v \geq 1\).

Suppose by contradiction that there exist such \(u(z)\) and \(v(z)\). Because \(y\) is a variable over \(F\) and \(z\) is a variable over \(K = F[y]\), \(y\) and \(z\) are algebraically independent over \(F\). Thus, we can view
\[ (F[y])[z] = F[y, z] = (F[z])[y] \]

Thus, we can view \(h(z)\) as \(h(y) \in (F[z])[y]\),
\[ u(z) \text{ as } u(y) \in (F[z])[y], \]
\[ v(z) \text{ as } v(y) \in (F[z])[y]. \]

We have \(h(y) = f(z) - yg(z) = \tilde{u}(y)\tilde{v}(y), \)
\(\text{degree } 1\).
Thus $\deg \tilde{u} = 1$, $\deg \tilde{v} = 0$ or vice versa. WLOG, we can assume $\deg \tilde{u} = 0$ and $\deg \tilde{v} = 1$. Then $u(z)$ has coefficients in $F$, and $v(z)$ has coefficients of the form $a + by$ with $a, b \in F$. Thus

$$\begin{cases} u(z) \in F[z], \\ v(z) = r(z) + ys(z), \text{ with } r(z), s(z) \in F[z] \end{cases}$$

The identity $d(z) = u(z)v(z)$ becomes

$$f(z) - yg(z) = u(z)(r(z) + ys(z)) = u(z)r(z) + yu(z)s(z).$$

Since $y$ is a variable over $F[z]$, we get $f(z) = u(z)r(z)$ and $g(z) = -u(z)s(z)$. Thus $u(z) \mid f(z)$ and $u(z) \mid g(z)$. Thus $u(z) \mid \gcd (f(z), g(z))$, which results in $u(z) \mid 1$. This is impossible because $\deg u \geq 1$.

6 (The additional problem)

Let $k$ be a field, $a$ be a variable over $k$, $E$ be a subfield of $k(x)$ such that $k \not\subset E \subset k(x)$. We'll show that $E$ is ring-isomorphic to $k(z)$.

To do so, we'll look for some $y \in E \setminus k$ such that $k(y) = E$.

For each pair $f(x), g(x) \in k[x] \setminus \{0\}$, we define

$$\phi(f(x), g(x)) = \max \{\deg f(x), \deg g(x)\} \in \mathbb{N} \cup \{0\}.$$ 

Since $E \not\subset k$, we can pick a pair $(f(x), g(x))$ such that $\frac{f(x)}{g(x)} \in E \setminus k$ and $\phi(f(x), g(x))$ is smallest possible. We'll show that there is such a
pair that $\deg f(x) > \deg g(x)$.

If $\deg f(x) < \deg g(x)$ then we pick $(g(x), f(x))$ instead. Note that 
$g(x)/f(x) = (f(x)/g(x))^{-1} \in E \setminus k$, and $\phi(g(x), f(x)) = \phi(f(x), g(x))$ by definition of $\phi$.

If $\deg f(x) = \deg g(x)$, then $f(x) \neq g(x)$. Indeed, otherwise $f(x)/g(x) = 1$ which is contained in $k$. Hence, we have $\phi(f(x), f(x) - g(x)) = \deg f(x) = \phi(f(x), g(x))$.

Moreover, $v(x) = \frac{f(x)}{f(x) - g(x)} = \frac{f(x)/g(x)}{f(x)/g(x) - 1} \in E$ since $E$ is a field. Since $v(x) \neq 1$, we have a backward relation $f(x)/g(x) = v(x)/(v(x) - 1)$.

Since $f(x)/g(x) \notin k$, so is $v(x)$. Then we pick the pair $(f(x), f(x) - g(x))$ instead of $(f(x), g(x))$. In short, we can pick a pair $(f(x), g(x))$ such that $\frac{f(x)}{g(x)} \in E \setminus k$, $\phi(f(x), g(x))$ is smallest possible, with $\deg f(x) > \deg g(x)$.

Since $k \subseteq E$, we can divide $f(x)$ by its leading coefficient, and divide $g(x)$ by its leading coefficient to get another admissible rational pair. Thus, we can assume that $f(x)$ and $g(x)$ are both monic.

The case $\gcd(f(x), g(x)) \neq 1$ doesn't happen. Indeed, if that happen then we can reduce the fraction $f(x)/g(x)$ to a form $\tilde{f}(x)/\tilde{g}(x)$ where $\phi(\tilde{f}(x), \tilde{g}(x)) < \phi(f(x), g(x))$, this contradicts the choice of $f(x)$ and $g(x)$. Thus,
we must have \( \gcd(f(x), g(x)) = 1 \).

Put \( y = \frac{f(x)}{g(x)} \) and \( n = \phi(f(x), g(x)) = \deg f(x) \).

We have \( k(y) \subseteq E \subseteq k(x) \). By the previous problem, we know that

\[ n = \left[ k(x) : k(y) \right] \geq \left[ k(x) : E \right] \]

Let \( z \) be a variable over \( k(x) \). Put \( h(z) = f(z) - yg(z) \in E[z] \).

Then we have

- \( \deg h(z) = \deg f(z) = n \),
- \( h(z) \) is monic because \( f(z) \) is monic,
- \( h(x) = f(x) - yg(x) = 0 \).

Thus the irreducible polynomial of \( x \) over \( E \), namely \( \text{Irr}(x, E, z) \), divides \( h(z) \). Then \( \deg \text{Irr}(x, E, z) \leq \deg h(z) = n \). We have

\[ k(x) = k(E, x) = E(x) \]

Then
\[ \left[ k(x) : E \right] = \left[ E(x) : E \right] = \deg \text{Irr}(x, E, z) \]

To show that \( E = k(y) \), we only need to show that \( \deg \text{Irr}(x, E, z) = n \). That is, to show that \( \text{Irr}(x, E, z) = h(z) \). That is, to show that \( h(z) \) is irreducible over \( E \).

Suppose by contradiction that \( h(z) \) is reducible in \( E[z] \). Then there are \( u(z), v(z) \in E[z] \) with \( \deg u(z), \deg v(z) \geq 1 \) such that

\[ h(z) = u(z) v(z) \]

Since \( h(z) \) is monic, we can assume that \( u(z) \) and \( v(z) \) are both monic.
We have \( h(z), u(z), v(z) \in k(z)[z] \) and \( k(z) \) is the field of fractions of the ring \( k[z] \). Thus we can write

\[
h(z) = \text{cont}(h) \tilde{h}(z) \quad \text{where} \quad \text{cont}(h) \in k(z), \quad \tilde{h}(z) \in (k[z])[z],
\]
\[
u(z) = \text{cont}(u) \tilde{u}(z) \quad \text{where} \quad \text{cont}(u) \in k(z), \quad \tilde{u}(z) \in (k[z])[z],
\]
\[
v(z) = \text{cont}(v) \tilde{v}(z) \quad \text{where} \quad \text{cont}(v) \in k(z), \quad \tilde{v}(z) \in (k[z])[z].
\]

By Gauss's Lemma, \( \text{cont}(h) = \text{cont}(u) \text{cont}(v) \). Thus \( \tilde{h}(z) = \tilde{u}(z) \tilde{v}(z) \).

We have

\[
h(z) = \frac{1}{g(z)} \left( g(z) f(z) - f(z) g(z) \right) \in (k[z])[z].
\]

The coefficient of \( z^n \) in \( g(z) f(z) - f(z) g(z) \) is \( g(z) \); the coefficient of \( z^m \), with \( m = \deg g(z) \), is \( \alpha g(z) - f(z) \), for some \( \alpha \in k \). We have \( \gcd(g(z), \alpha g(z) - f(z)) = \gcd(g(z), f(z)) = 1 \). Therefore,

\[
\text{cont}(h) = \frac{1}{g(z)} \quad \text{and} \quad \tilde{h}(z) = g(z) f(z) - f(z) g(z).
\]

We recall the definition of content:

Let \( K \) be the field of fractions of a ring \( A \) and \( f(X) \in K[X] \).

We write \( f(X) = \frac{a_n}{b_n} X^n + \ldots + \frac{a_1}{b_1} X + \frac{a_0}{b_0} \) with \( a_i, b_i \in A \).

Then

\[
\text{cont}(f) = \frac{\gcd(a_n, a_{n-1}, \ldots, a_1)}{\text{lcm}(b_n, b_{n-1}, \ldots, b_1)}.
\]

Consequently, if \( f(X) \) is monic, i.e. \( a_n = b_n = 1 \), then \( \text{cont}(f) = \frac{1}{a} \) for some \( a \in A \).
Because \( u(t) \) is monic, \( \text{cont}(u) = \frac{1}{a(x)} \) for some \( a(x) \in k[x] \).

We write \( \tilde{u}(t) = a_r(x) t^r + \cdots + a_1(x) t + a_0(x) \), with \( a_i(x) \in k[x] \).

Then \( \tilde{u}(t) = \frac{1}{a(x)} \tilde{u}(t) = \frac{a_r(x)}{a(x)} t^r + \cdots + \frac{a_1(x)}{a(x)} t + \frac{a_0(x)}{a(x)} \).

Since \( u(t) \) is monic, \( a_r(x) = a(x) \). We consider two cases of \( a(x) \).

\( a(x) \in k \)  

Then \( a(x) = c \in k \).

\( a(x) \in k \)  

If \( a_i(x) \in k \) for all \( 0 \leq i < r \) then \( \tilde{u}(t) \in k[t] \).

If there exists \( 0 \leq i < r \) such that \( a_i(x) \not\in k \) then \( \frac{a_i(x)}{a(x)} = c_i \in k \).

Thus \( \phi(a_i(x), c) \geq n \). Thus \( \deg a_i(x) \geq n \). Thus the degree of \( \tilde{u}(t) \) in variable \( x \) is \( \geq n \).

\( a(x) \neq k \)  

Since \( \gcd(a(x), a_{r-1}(x), \ldots, a_1(x), a_0(x)) = \gcd(a_r(x), a_{r-1}(x), \ldots, a_1(x)) = 1 \), there exists \( 0 \leq i < r \) such that \( a(x) \not| a_i(x) \). Then \( a_i(x)/a(x) \in E \setminus k \).

Thus \( \phi(a_i(x), a(x)) \geq n \). Thus \( \max(\deg a_i(x), \deg a(x)) \geq n \). Thus the degree of \( \tilde{u}(t) \) in \( x \) is \( \geq n \).

In both cases, we have only two possibilities: either \( \tilde{u}(t) \in k(t) \) or the degree of \( \tilde{u}(t) \) in \( x \) is \( \geq n \). The same argument is applied for \( \tilde{v}(x) \) and we get the same conclusion for \( \tilde{v}(x) \). We put
\[ \hat{u}(x) = \tilde{u}(z) \in (k[z])^2, \]
\[ \hat{v}(x) = \tilde{v}(z) \in (k[z])^2, \]
\[ \hat{w}(x) = \tilde{w}(z) \in (k[z])^2. \]

Then we have \( \deg \hat{w} = 0 \) or \( \deg \hat{w} = n \),
\( \deg \hat{v} = 0 \) or \( \deg \hat{v} = n \).

Since \( \hat{w}(z) = \tilde{u}(z)\tilde{v}(z) \), we have \( \hat{w}(x) = g(x)f(z) - f(x)g(z) = \tilde{u}(x)\tilde{v}(z) \).

Since \( \deg \hat{w}(z) = n \), there are only two possibilities: either \( (\deg \hat{u}(z) = n, \deg \hat{v}(z) = 0) \) or \( (\deg \hat{u}(z) = 0, \deg \hat{v}(z) = n) \). WLOG, we can assume \( \deg \hat{u}(z) = n \) and \( \deg \hat{v}(z) = 0 \). Then \( \hat{v} = b(z) \in k[z] \). Thus

\[ b(z) \mid \left( f(x)g(z) - g(z)f(x) \right) \quad (\ast) \]
\[ \leq \tilde{u}(x) \in (k[z])^2. \]

Since \( b(z) \in k[z] \) divides \( \tilde{u}(z) \), a polynomial over the ring \( k[z] \), all coefficients of \( \tilde{u}(z) \) must divide \( b(z) \). In particular, the leading coefficient of \( \tilde{u}(z) \), which is \( -g(z) \), must be divisible by \( b(z) \). Since \( b(z) \mid g(z) \), \( (\ast) \) implies \( b(z) \mid (f(x)g(z) - g(z)f(x)) \). Since \( \deg b(z) = \deg \tilde{v}(z) = \deg \tilde{v}(z) > 1 \),

\[ b(z) \mid f(z). \] Thus \( b(z) \mid \text{gcd}(g(z), f(z)) \). This is a contradiction because \( g(z) \) and \( f(z) \) are relatively prime in \( k[z] \).

Until now, we proved that \( E = k(y) \). By the previous problem, we
proved that \( y \) is a variable over \( k \). Then \( E = k(y) \) and \( k(x) \) are fields of rational functions with coefficients in \( k \). They are ring-isomorphic in a natural way, namely via \( \Psi : k(y) \to k(x) \),

\[
\left( \sum a_k y^k \right) / \left( \sum b_j y^j \right) \mapsto \left( \sum a_k x^k \right) / \left( \sum b_j x^j \right).
\]

7. Problem 26, Lang, p. 256

Let \( k \) be a field, \( f(X) \in k[X] \) be monic and irreducible over \( k \). Let \( K \subset \overline{k} \) be a finite normal extension (we can always assume that \( K \subset \overline{k} \)). Let \( g(X), h(X) \in K[X] \) be monic and irreducible over \( K \) such that \( f(X) = h(X) h(X) \). Note that by irreducibility, we implied that \( \deg f \geq 1 \), \( \deg g \geq 1 \), and \( \deg h \geq 1 \). We'll show the existence of a ring isomorphism \( \phi : K \to K \) such that \( g = h^\phi \).

Since \( \deg g, \deg h > 1 \), there are \( \alpha, \beta \in \overline{k} \) such that \( g(x) = 0 \) and \( h(\beta) = 0 \). Since \( g(X) \in K[X] \), monic, irreducible over \( K \) and \( g(\alpha) = 0 \), \( g(X) \) is the irreducible polynomial of \( \alpha \) over \( K \). Similarly, \( h(X) \) is the irreducible polynomial of \( \beta \) over \( K \). We consider two cases:

- \( \beta \) is also a root of \( g(X) \) in \( \overline{k} \):

Then \( h(X) \mid g(X) \). Since \( h(X) \), \( g(X) \) are monic, and \( g(X) \) is irreducible.
over $K$, we must have $h(X) = g(X)$. Then we can choose $\delta = \text{id}_K$.

Then $g = h = h^{\delta}$.

\textbf{Note} $\beta$ is not a root of $g(X)$ in $\overline{k}$

We know that $\alpha$ and $\beta$ are roots of the irreducible $f(X) \in k[X]$. By a Corollary in lecture notes, there exists an isomorphism $\tau: k(\alpha) \to k(\beta)$ which induces identity on $k$ and $\tau(\alpha) = \beta$. Then $\tau$ extends to an embedding $\overline{\tau}: K \to \overline{k}$. Since $K$ is a normal extension of $k$, $\overline{\tau}(K) = K$. Thus $\overline{\tau}: K \to K$ is an automorphism. We'll show that $g = h^{\overline{\tau}}$.

We have $f(X) = g(X)h(X)$. Now apply $\delta$ to every coefficient of $g(X), h(X), f(X)$. We get $f^{\delta}(X) = g^\delta(X)h^\delta(X)$. Because $\delta$ induces identity on $k$, $f^\delta(X) = f(X)$. Because $\delta(K) = K$, $g^\delta(X), h^\delta(X) \in K[X]$. Then we have $g(X)h(X) = g^\delta(X)h^\delta(X)$ as polynomials in $K[X]$. Because $g(X)$ and $h(X)$ are irreducible in the factorial ring $K[X]$, they are prime elements. Since $g(X) \mid (g^\delta(X)h^\delta(X))$, either $g(X) \mid g^\delta(X)$ or $g(X) \mid h^\delta(X)$. Since $\deg g = \deg g^\delta$ and $g(X), g^\delta(X)$ are monic, $g(X) = g^\delta(X)$ if $g(X) \mid g^\delta(X)$. However, this is not the case because $\beta = \delta(\alpha)$ is a root of $g^\delta(X)$, but not a root of $g(X)$. Thus $g(X) \neq g^\delta(X)$ and hence $g(X) \mid h^\delta(X)$. Consequently, $\deg g \leq \deg h$. 

On the other hand, $h(X) | (g^5(X) h^5(X))$. Then, similarly, either

$h(X) = h^5(X)$ or $h(X) | g^5(X)$. Since $g(X) h^5(X) = g^5(X) h^5(X)$ and

$g(X) \neq g^5(X)$, $h(X) \neq h^5(X)$. Thus $h(X) | g^5(X)$. Consequently,

deg $h \leq$ deg $g$. Thus deg $h = $ deg $g$. Since $g(X) \mid h^5(X)$, both of which

have the same degree and monic, we have $g(X) = h^5(X)$.

An example to see that these doesn’t necessarily exist such an

automorphism $\sigma: K \to K$ over $k$ such that $g = h^\sigma$.

Take $h = \sigma$ and $K = \mathbb{Q}(\sqrt[4]{2})$. $K$ is not normal over $k$ because

the polynomial $X^4 - 2$

\[ \text{is irreducible over } \mathbb{Q} \] (applying Eisenstein’s criterion for $p=2$),

\[ \text{has a root } \sqrt[4]{2} \in K, \]

\[ \text{has a root } \sqrt[4]{-2} \notin K. \]

Put $f(X) = X^4 + 1 = \frac{(X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)}{g(X)} \cdot \frac{h(X)}{h(X)}$.

We have $f(X + 1) = X^4 + 4X^3 + 6X^2 + 4X + 2$ is irreducible over $\mathbb{Q}$

(Eisenstein’s criterion for $p=2$). Thus $f(X) \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$.

Since $g(X)$ and $f(X)$ have no $\mathbb{K}$ degree two, and has no real roots, they are

irreducible in $\mathbb{K}[X]$. Suppose by contradiction that there is an automorphism

$s: \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$ such that $g = h^s$. Then
\[ \sqrt{2} = 5(-\sqrt{2}) = 5(-1 \cdot \sqrt{2} \cdot \sqrt{2}) = 5(-1) \cdot 5(\sqrt{2}) \cdot 5(\sqrt{2}) = -a^2, \]

where \( a = 5\sqrt{2} \in \mathbb{R} \). This is a contradiction.