Name: Tuan Pham
ID: 4652218

Math 8202: General Algebra
Homework 3

10/10.

① Problem 3, Lang p. 253

Let ~~F~~ be a field and α, β be two algebraic elements over F. Let $f(X)$ and $g(X)$ be respectively the irreducible polynomials of α and β over F. 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 $F(\alpha)$.

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

$$[F(\alpha,\beta) : F] = [F(\alpha,\beta) : F(\alpha)][F(\alpha) : F] = n[F(\alpha)(\beta) : F(\alpha)]$$
$$= n(\deg h),$$

$$[F(\alpha,\beta) : F] = [F(\alpha,\beta) : F(\beta)][F(\beta) : F] = m[F(\alpha,\beta) : F(\beta)].$$

Thus $n(\deg h) = m[F(\alpha,\beta) : F(\beta)]$. Since $\gcd(m,n) = 1$, $m \mid (\deg h)$. Thus $\deg h \geq m = \deg g$. Since $h(X) \mid g(X)$, $\deg h \leq \deg g$. 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. Put $n = [E:k]$ and $m = [F:k]$. As a vector field over k, E has dimension n. Thus it has a basis $\{\alpha_1, \dots, \alpha_n\}$. Then $E = k(\alpha_1, \dots, \alpha_n)$, which is the smallest subfield of K that contains k and $\alpha_1, \dots, \alpha_n$. 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 $\alpha_1, \dots, \alpha_n$. Thus

$$EF = F(\alpha_1, \dots, \alpha_n)$$

Therefore, as a vector space over F, EF is generated by $\alpha_1, \dots, \alpha_n$. Thus it is a finite dimensional vector space and $[EF:F] \leq n$. We have

$$[EF:k] = [EF:F][F:k] \leq n[F:k] = [E:k][F:k]. \qquad (*)$$

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 $\gcd(m,n) = 1$, $n \mid [EF:F]$. Since $[EF:F] \leq n$, we must have $[EF:F] = n$. Then the equality at $(*)$ 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 $k \subset K \subset \bar{k}$). Then we'll show by induction in $n \in \mathbb{N}$ that $[K:f]$ divides $n!$

For $n=1$: $f(X) = a(X-\alpha)$ where $a \in k$, $a\alpha \in k$.

Thus $\alpha \in k$. Then $f(X)$ is already splitted 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 $m \geq 2$. we'll show that it is also true for $n=m$. Let $f(X) \in k[X]$ be a polynomial of degree $m \geq 2$. 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 $\alpha_i \in \bar{k}$.

Then the splitting field of $f(X)$ is $K = k(\alpha_1, \dots, \alpha_m)$. We have $f(\alpha_1) = 0$ and $f(X)$ is irreducible in $k[X]$. Thus $f(X)/c$ is the irreducible polynomial of α_1 over k. Thus $[k(\alpha_1):k] = \deg f = m$.

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

$$f(X) = (X-\alpha_1)\, g(X) \quad \text{as polynomials in } \bar{k}[X].$$

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 $\deg q \geq 1$.

4

This identity is also an identity of polynomials in $\bar{k}[X]$. By the uniqueness of quotient and remainder in $\bar{k}[X]$, we conclude $q(X)=g(X)$ and $\beta=0$. Thus $g(X) \in F[X]$. Thus $F(\alpha_2, \dots, \alpha_m)$ is the splitting field of $g(X)$. Because $\deg g = m-1 < m$, by the induction hypothesis we have $[F(\alpha_2, \dots, \alpha_m) : F] \mid (m-1)!$. We have

$$[K : k] = [k(\alpha_1 \cdots \alpha_m) : k] = [k(\alpha_1)(\alpha_2 \cdots \alpha_m) : k(\alpha_1)][k(\alpha_1) : k]$$
$$= [F(\alpha_2, \dots, \alpha_m) : F]\, m,$$

which divides $(m-1)!\, m = m!$

- $f(X)$ is reducible over k

Then there are $g(X), h(X) \in k[X]$ with $1 \le \deg g, \deg h < m$ such that $f(X) = g(X)h(X)$. Let

$$g(X) = c_1(X-\beta_1)\cdots(X-\beta_\ell),$$
$$h(X) = c_2(X-\gamma_1)\cdots(X-\gamma_s),$$

where $c_1, c_2 \in k \setminus \{0\}$, $\beta_i, \gamma_j \in \bar{k}$, $1 \le \ell, s < m$ and $\ell + s = m$.

Then the splitting field of $f(X)$ is $K = k(\beta_1, \dots, \beta_\ell, \gamma_1, \dots, \gamma_s)$.

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

Since $k \subset F$, $h(X) \in F[X]$. Thus $F(\gamma_1, \dots, \gamma_s)$ is the splitting field of $h(X)$. By the induction hypothesis, $[F(\gamma_1, \dots, \gamma_s) : F] \mid s!$

Then $[K:k] = [k(\beta_1,\dots,\beta_\ell,\gamma_1,\dots,\gamma_s):k]$

$= [k(\beta_1,\dots,\beta_\ell)(\gamma_1,\dots,\gamma_s):k(\beta_1,\dots,\beta_\ell)]\,[k(\beta_1,\dots,\beta_\ell):k]$

$= [F(\gamma_1,\dots,\gamma_s):F]\,[F:k]$,

which divides $\ell!\,s! = \ell!\,(m-\ell)!$ Thus $[K:k]$ divides $m!$

④ Problem 10, Lang, p. 253

Let $\alpha \in \mathbb{R}$ such that $\alpha^4 = 5$. We first notice that $r+is\sqrt{5}$ for some $r,s \in \mathbb{Q}$ then $r^2+5s^2 = (r+is\sqrt{5})(r-is\sqrt{5}) = X^2+\sqrt{5}^2$ 0. Thus $r=s=0$.

Consequently, $r+is\sqrt{5} \in \mathbb{Q}$ iff $s=0$.

(a) We'll 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 deg 2 extension is a normal

$$g(X) = a_n X^n + \cdots + a_1 X + a_0, \text{ where each } a_j \in \mathbb{Q}.$$

Then $g(i\sqrt{5}) = \sum_{k=0}^{n} a_k (i\sqrt{5})^k = \underbrace{\sum_{\substack{0\le k\le n \\ k \text{ even}}} a_k (-5)^{k/2}}_{\in \mathbb{Q}} + (i\sqrt{5}) \underbrace{\sum_{\substack{0\le k\le n \\ k \text{ odd}}} a_k (-5)^{(k-1)/2}}_{\in \mathbb{Q}}$ extension

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,

6

$$\mathbb{Q}(i\sqrt{5}) = \{r + is\sqrt{5} : r, s \in \mathbb{Q}\}.$$

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

- If $s = 0$, then $f(r) = 0$. Then $(X - r) \mid f(X)$. Since $f(X)$ is irreducible over $\mathbb{Q}$, $f(X) = X - r$.
- If $s \neq 0$, then $r \pm is\sqrt{5} \notin \mathbb{Q}$. We see that the polynomial

$$g(X) = X^2 - 2rX + (r^2 + 5s^2) = \left(X - (r + si\sqrt{5})\right)\left(X - (r - si\sqrt{5})\right) \in \mathbb{Q}[X].$$

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

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

We have $\beta^4 = (2i\alpha^2)^2 = -4\alpha^4 = -20$. Thus β 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 $\not$ — 5 divides $\not$ — 5 divides $\not$ but not 25

Thus, by Eisenstein's criterion, X^4+2v is irreducible over $\mathbb{Q}$. Thus, X^4+2v is the irreducible polynomial of β over $\mathbb{Q}$.

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

Then $$g(\beta) = \sum_{k=0}^{n} a_k \beta^k = \underbrace{\sum_{\substack{0 \le k \le n \\ k \text{ even}}} a_k (\beta^2)^{k/2}}_{\in \mathbb{Q}(\beta^2)} + \beta \underbrace{\sum_{\substack{0 \le k \le n \\ k \text{ odd}}} a_k (\beta^2)^{(k-1)/2}}_{\in \mathbb{Q}(\beta^2)}$$

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 β. 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 (a), 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

$$\beta(r' + s'\beta^2) = r + s\beta^2$$

$$\iff s'\beta^3 - s\beta^2 + r'\beta - r = 0$$

Since $v \neq 0$, either $r' \neq 0$ or $s' \neq 0$. 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 β 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 irreducible polynomial 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 β over $\mathbb{Q}(\beta^2)$. But $g(X) \neq f$. We consider two cases:

- If $v=0$, then $f(u)=0$. Then $(X-u) \mid f(X)$. Then $f(X)=X-u$ because $f(X)$ is ireducible.
- If $v \neq 0$, then $u \pm \beta v \notin \mathbb{Q}(\beta^2)$ for what we have shown above. But

$$g(X) = X^2-2uX+(u^2-\beta^2v^2) = \big(X-(u+\beta v)\big)\big(X-(u-\beta v)\big) \in \mathbb{Q}(\beta^2).$$

We see that $g(u+\beta v)=0$ and $g(X)$ is irreducible over $\mathbb{Q}(\beta^2)$ because $u \pm \beta v \notin \mathbb{Q}(\beta^2)$. 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 α 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 α over $\mathbb{Q}$.

Now suppose by contradiction that $\mathbb{Q}(\beta)$ is normal over $\mathbb{Q}$. Since

β is a root of $X^4+20 \in \mathbb{Q}[X]$, all other roots of its also belongs 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 $u, v \in \mathbb{Q}(\beta^2)$ such that $i = u+\beta v$. Since $u, v \in \mathbb{Q}(\beta^2)$, there exist $r, r', s, s' \in \mathbb{Q}$ such that $u = r+is\sqrt{5}$ and $v = r'+is'\sqrt{5}$. Then

$$\begin{aligned} i &= (r+is\sqrt{5}) + \beta(r'+is'\sqrt{5}) \\ &= (r+is\sqrt{5}) + \alpha(1+i)(r'+is'\sqrt{5}) \\ &= (r+is\sqrt{5}) + \alpha(r'-s'\sqrt{5}+ir'+is'\sqrt{5}) \\ &= \left(r+\alpha(r'-s'\sqrt{5})\right) + i\left(s\sqrt{5}+\alpha r'+\alpha s'\sqrt{5}\right) \end{aligned}$$

not an effective way.

Thus

$$\begin{cases} r+\alpha(r'-s'\sqrt{5})=0 \\ s\sqrt{5}+\alpha r'+\alpha s'\sqrt{5}=1 \end{cases} \iff \begin{cases} r+\alpha(r'-s'\alpha^2)=0 \\ s\alpha^2+\alpha r'+s'\alpha^3=1 \end{cases}$$

Then $s'\alpha^3+s\alpha^2+r'\alpha-1=0$. Thus is a contradiction because the irreducible polynomial of α 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 ~~ring of~~ field of ~~polynomials~~ fractions with variable x and coefficients in F. In other words,

[10]

$$E = F(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x],\ g(x) \neq 0 \right\}$$

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 $E = F(x)$ and let z be a variable over E. Let $f(z), g(z) \in F[z]$ such that $n = \max(\deg f, \deg g) \geq 1$ and $\gcd(f(z), g(z)) = 1$. Put $y = \frac{f(x)}{g(x)} \in E$. 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 $u(z) \in F(z)$, $u(z) \neq 0$ such that $u(y) = 0$. We write $u(z) = a_m z^m + \cdots + a_1 z + a_0$ with $a_i \in F$, $m \geq 1$. Then~~

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

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

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

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 $g(x) \mid a_m f(x)^m$ if and only if $g(x) \in F$. Because $n = \max(\deg f, \deg g) \geq 1$, $\deg f \geq 1$. Put $g(x) = c \in F$, (*) becomes $a_m f(x)^m + a_{m-1} c f(x)^{m-1} + \cdots + a_0 c^m = 0$. 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 $F \subset K \subset E$ and $y \in K \setminus F$. Then K is a subfield of E and $K \neq F$. By part (a), we conclude that x is algebraic over K. We have

12

$$E = F(x) = F\left(\frac{f(x)}{g(x)}, x\right) = F\left(\frac{f(x)}{g(x)}\right)(x) = K(x).$$

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

$$h(z) = f(z) - y\,g(z) \in K[z]$$

Because $y \notin F$, $\deg h = \max(\deg f, \deg g) = n$. Moreover,

$$h(x) = f(x) - y\,g(x) = f(x) - \frac{f(x)}{g(x)}\,g(x) = 0$$

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 $K \supseteq F[y]$, 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 $\tilde{h}(y) \in (F[z])[y]$,

$u(z)$ as $\tilde{u}(y) \in (F[z])[y]$,

$v(z)$ as $\tilde{v}(y) \in (F[z])[y]$.

We have $\tilde{h}(y) = \underbrace{f(z) - y\,g(z)}_{\text{degree } 1} = \tilde{u}(y)\,\tilde{v}(y)$.

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 $a + yb$ with $a, b \in F$. Thus

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

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

$$f(z) - y\,g(z) = u(z)\left(r(z) + y\,s(z)\right) = u(z)\,r(z) + y\,u(z)\,s(z).$$

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, x be a variable over k, E be a subfield of $k(x)$ such that $k \subsetneq E \subset k(x)$. We'll show that E is ring-isomorphic to $k(x)$.

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 $E \setminus k \neq \emptyset$, 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 $g(x)/f(x) = \left(f(x)/g(x)\right)^{-1} \in E \setminus k$, and $\phi(g(x), f(x)) = \phi(f(x), g(x))$ by definition of ϕ.

- If $\deg f(x) = \deg g(x)$, then $f(x) \neq g(x)$. Indeed, otherwise $f(x)/g(x) = 1$ which is contained in $k(!)$ we have $\phi(f(x), f(x) - g(x)) = \deg f(x) = \phi(f(x), g(x))$. Moreover, $v(x) = \dfrac{f(x)}{f(x)-g(x)} = \dfrac{f(x)/g(x)}{f(x)/g(x) - 1} \in E$ 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 $\dfrac{f(x)}{g(x)} \in E \setminus k$, $\phi(f(x), g(x))$ is smallest possible, with $\deg f(x) > \deg g(x)$. Since $k \subset E$, 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 $y = \dfrac{f(x)}{g(x)}$ and $n = \phi(f(x), g(x)) = \deg f(x)$.

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

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

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

Then we have
- $\deg h(z) = \deg f(z) = n$,
- $h(z)$ is monic because $f(z)$ is monic,
- $h(x) = f(x) - y\,g(x) = 0$.

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

$$k(x) = k(E, x) = E(x)$$

Then $[k(x) : E] = [E(x) : E] = \deg \mathrm{Irr}(x, E, z)$. To show that $E = k(y)$, we only need to show that $\deg \mathrm{Irr}(x, E, z) = n$. That, to show that $\mathrm{Irr}(x, E, z) = h(z)$. 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 $h(z), u(z), v(z) \in k(x)[z]$ and $k(x)$ is the field of fractions of the ring $k[x]$. Thus we can write

$$h(z) = \mathrm{cont}(h)\, \tilde{h}(z) \quad \text{where } \mathrm{cont}(h) \in k(x),\ \tilde{h}(z) \in (k[x])[z],$$

$$u(z) = \mathrm{cont}(u)\, \tilde{u}(z) \quad \text{where } \mathrm{cont}(u) \in k(x),\ \tilde{u}(z) \in (k[x])[z],$$

$$v(z) = \mathrm{cont}(v)\, \tilde{v}(z) \quad \text{where } \mathrm{cont}(v) \in k(x),\ \tilde{v}(z) \in (k[x])[z].$$

By Gauss's lemma, $\mathrm{cont}(h) = \mathrm{cont}(u)\,\mathrm{cont}(v)$. Thus $\tilde{h}(z) = \tilde{u}(z)\,\tilde{v}(z)$.

We have $$h(z) = \frac{1}{g(x)} \underbrace{\left(g(x) f(z) - f(x) g(z) \right)}_{\in (k[x])[z]}$$

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

$$\mathrm{cont}(h) = \frac{1}{g(x)} \quad \text{and} \quad \tilde{h}(z) = g(x) f(z) - f(x) g(z).$$

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 $f(X) = \frac{a_n}{b_n} X^n + \cdots + \frac{a_1}{b_1} X + \frac{a_0}{b_0}$ with $a_i, b_j \in A$.

Then $$\mathrm{cont}(f) = \frac{\gcd(a_0, a_1, \ldots, a_n)}{\mathrm{lcm}(b_0, b_1, \ldots, b_n)}.$$

Consequently, if $f(X)$ is monic, i.e. $a_n = b_n = 1$, then $\mathrm{cont}(f) = \frac{1}{a}$ for some $a \in A$

Because $u(z)$ is monic, $cont(u) = \frac{1}{a(x)}$ for some $a(x) \in k[x]$.

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

Then $\tilde{\tilde{u}}(z) = \frac{1}{a(x)} \tilde{u}(z) = \underbrace{\frac{a_r(x)}{a(x)}}_{\in E} z^r + \cdots + \underbrace{\frac{a_1(x)}{a(x)}}_{\in E} z + \underbrace{\frac{a_0(x)}{a(x)}}_{\in E}$,

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

- $a(x) \in k$ Then $a(x) \equiv c \in k$.

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

  . If there exists $0 \le i < r$ such that $a_i(x) \notin k$ then $\frac{a_i(x)}{a(x)} = c^{-1} a_i(x) \in E \setminus k$.

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

- $a(x) \notin k$ Since $gcd(a(x), a_{r-1}(x), \ldots, a_1(x), a_0(x)) = gcd(a_r(x), a_{r-1}(x), \ldots, a_0(x)) = 1$, there exists $0 \le i < r$ such that $a(x) \nmid a_i(x)$. Then $a_i(x)/a(x) \in E \setminus k$.

Thus $\phi(a_i(x), a(x)) \ge n$. Thus $\max(\deg a_i(x), \deg a(x)) \ge n$. Then the degree of $\tilde{u}(z)$ in x is $\ge n$.

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

[18]

$$\hat{u}(x) = \tilde{u}(z) \in (k[z])[x],$$

$$\hat{v}(x) = \tilde{v}(z) \in (k[z])[x],$$

$$\hat{h}(x) = \tilde{h}(z) \in (k[z])[x].$$

Then we have $\begin{cases} \deg \hat{u}(x) = 0 \text{ or } \deg \hat{u}(x) \geq n, \\ \deg \hat{v}(x) = 0 \text{ or } \deg \hat{v}(x) \geq n. \end{cases}$

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

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

$$b(z) \mid \underbrace{\left(g(x)f(z) - f(x)g(z)\right)}_{= \hat{h}(x) \in (k[z])[x]} \qquad (*)$$

Since $b(z) \in k[z]$ divides $\hat{h}(x)$, a polynomial over the ring $k[z]$, all coefficient of $\hat{h}(x)$ must ~~divide~~ be divisible $b(z)$. In particular, the leading coefficient of $\hat{h}(x)$, which is $-g(z)$, must be divisible by $b(z)$. Since $b(z) \mid g(z)$, $(*)$ implies $b(z) \mid \left(f(z)g(z)\right)$. Since $\deg b(z) = \deg \tilde{v}(z) = \deg v(z) \geq 1$, $b(z) \mid f(z)$. Thus $b(z) \mid \gcd(g(z), f(z))$. 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 $\Psi : k(y) \longrightarrow k(x)$,

$$\left(\sum a_k y^k\right) \Big/ \left(\sum b_j y^j\right) \longmapsto \left(\sum a_k x^k\right) \Big/ \left(\sum b_j x^j\right).$$

(7) Problem 26, Lang, p. 256

Let k be a field, $f(X) \in k[X]$ be monic and irreducible over k. Let $k \subset K$ be a finite normal extension (we can always assume that $K \subset \bar{k}$). Let $g(X), h(X) \in K[X]$ be monic and irreducible over K such that $f(X) = g(X)\,h(X)$. 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 $\sigma : K \longrightarrow K$ such that $g = h^{\sigma}$.

Since $\deg g, \deg h \geq 1$, there are $\alpha, \beta \in \bar{k}$ such that $g(\alpha) = 0$ 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 α over K. Similarly, $h(X)$ is the irreducible polynomial of β over K. We consider two cases:

- β is also a root of $g(X)$ in $\bar{k}$.

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 $\sigma = id_K$. Then $g = h = h^\sigma$.

- β is not a root of $g(X)$ in $\bar{k}$

We know that α and β 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 ~~induced~~ induces identity on k and $\tau(\alpha) = \beta$. Then τ extends to an embedding $\sigma : K \to \bar{k}$. Since K is a normal extension of k, $\sigma(K) = K$. Thus $\sigma : K \to K$ is an automorphism. We'll show that $g = h^\sigma$.

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

On the other hand, $h(X) \mid (g^5(X) h^5(X))$. Then, similarly, either $h(X) = h^5(X)$ or $h(X) \mid g^5(X)$. Since $g(X) h(X) = g^5(X) h^5(X)$ and $g(X) \neq g^5(X)$, $h(X) \neq h^5(X)$. Thus $h(X) \mid g^5(X)$. 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 there doesn't necessarily exist such an automorphism $\sigma: K \to K$ over k such that $g = h^5$:

Take $k = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt[4]{2})$. K is not normal over k because the polynomial $X^4 - 2$

- is irreducible over $\mathbb{Q}$ (applying Eisenstein's criterion for $p=2$),
- has a root $\sqrt[4]{2} \in K$,
- has a root $i\sqrt[4]{2} \notin K$,

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

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 ~~not~~ degree two, and has no real roots, they are irreducible in $K[X]$. Suppose by contradiction that there is an automorphism $\sigma: \mathbb{Q}(\sqrt[4]{2}) \longrightarrow \mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$ such that $g = h^5$. Then

22

$$\sqrt{2} = \sigma(-\sqrt{2}) = \sigma(-1.\sqrt[4]{2}.\sqrt[4]{2}) = \sigma(-1)\,\sigma(\sqrt[4]{2})\,\sigma(\sqrt[4]{2}) = -\alpha^2,$$

where $\alpha = \sigma(\sqrt[4]{2}) \in \mathbb{R}$. This is a contradiction.