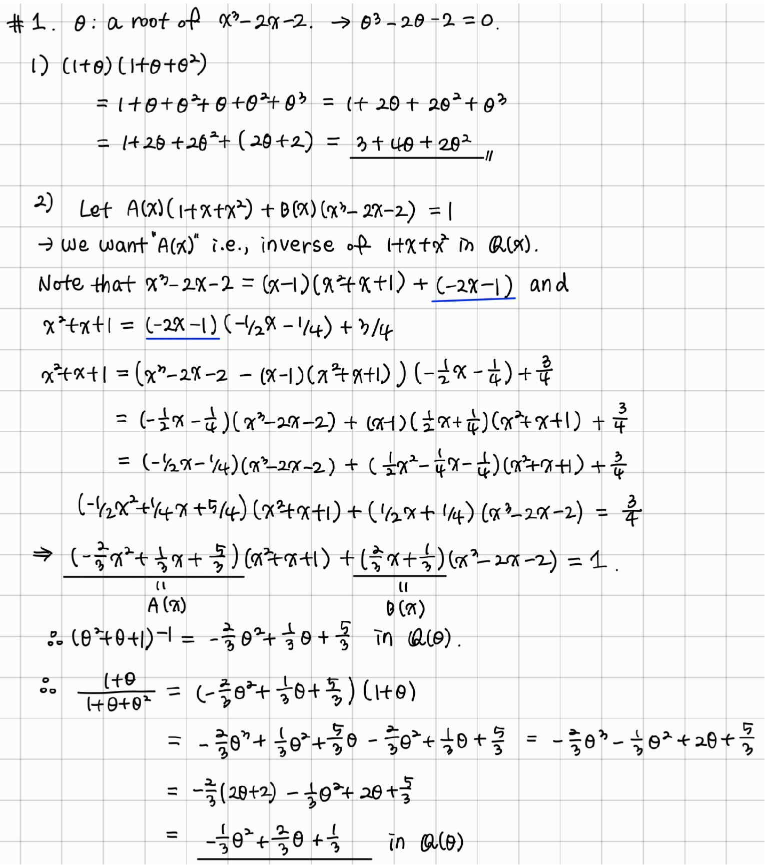
Homework 4 (Due: May 31)

Problem 1 (Section 13.1, Exercise 2)**.** Show that $x^3 - 2x - 2$ is irreducible over $\mathbb{Q}$ and let θ be a root. Compute $(1+\theta)\left(1+\theta+\theta^2\right)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.

Solution.



#1. θ : a root of x^3-2x-2. $\rightarrow \theta^3 - 2\theta - 2 = 0$.

1) $(1+\theta)(1+\theta+\theta^2)$

$$= 1+\theta+\theta^2+\theta+\theta^2+\theta^3 = 1+2\theta+2\theta^2+\theta^3$$

$$= 1+2\theta+2\theta^2+(2\theta+2) = \underline{3+4\theta+2\theta^2}_{//}$$

2) Let $A(x)(1+x+x^2) + B(x)(x^3-2x-2) = 1$

$\rightarrow$ we want "$A(x)$" i.e., inverse of $1+x+x^2$ in $\mathbb{Q}(x)$.

Note that $x^3-2x-2 = (x-1)(x^2+x+1) + \underline{(-2x-1)}$ and

$x^2+x+1 = \underline{(-2x-1)}(-1/2x - 1/4) + 3/4$

$$x^2+x+1 = \left(x^3-2x-2 - (x-1)(x^2+x+1)\right)\left(-\tfrac{1}{2}x - \tfrac{1}{4}\right) + \tfrac{3}{4}$$

$$= \left(-\tfrac{1}{2}x-\tfrac{1}{4}\right)(x^3-2x-2) + (x-1)\left(\tfrac{1}{2}x+\tfrac{1}{4}\right)(x^2+x+1) + \tfrac{3}{4}$$

$$= (-1/2x-1/4)(x^3-2x-2) + \left(\tfrac{1}{2}x^2-\tfrac{1}{4}x-\tfrac{1}{4}\right)(x^2+x+1) + \tfrac{3}{4}$$

$$(-1/2x^2+1/4x+5/4)(x^2+x+1) + (1/2x+1/4)(x^3-2x-2) = \tfrac{3}{4}$$

$$\Rightarrow \underbrace{\left(-\tfrac{2}{3}x^2+\tfrac{1}{3}x+\tfrac{5}{3}\right)}_{\overset{\shortparallel}{A(x)}}(x^2+x+1) + \underbrace{\left(\tfrac{2}{3}x+\tfrac{1}{3}\right)}_{\overset{\shortparallel}{B(x)}}(x^3-2x-2) = 1.$$

$\therefore (\theta^2+\theta+1)^{-1} = -\frac{2}{3}\theta^2+\frac{1}{3}\theta+\frac{5}{3}$ in $\mathbb{Q}(\theta)$.

$$\therefore \frac{1+\theta}{1+\theta+\theta^2} = \left(-\tfrac{2}{3}\theta^2+\tfrac{1}{3}\theta+\tfrac{5}{3}\right)(1+\theta)$$

$$= -\tfrac{2}{3}\theta^3+\tfrac{1}{3}\theta^2+\tfrac{5}{3}\theta-\tfrac{2}{3}\theta^2+\tfrac{1}{3}\theta+\tfrac{5}{3} = -\tfrac{2}{3}\theta^3-\tfrac{1}{3}\theta^2+2\theta+\tfrac{5}{3}$$

$$= -\tfrac{2}{3}(2\theta+2)-\tfrac{1}{3}\theta^2+2\theta+\tfrac{5}{3}$$

$$= \underline{-\tfrac{1}{3}\theta^2+\tfrac{2}{3}\theta+\tfrac{1}{3}} \quad \text{in } \mathbb{Q}(\theta)$$

□

Problem 2 (Section 13.2, Exercise 7)**.** Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ [one inclusion is obvious, for the other consider $(\sqrt{2}+\sqrt{3})^2$, etc.]. Conclude that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$.

Solution.

(1) (a) $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\ \sqrt{3})$: Clear.

(b) $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2},\ \sqrt{3})$:
Observe that $(\sqrt{2}+\sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
Since

$$(\sqrt{2}+\sqrt{3})^{-1} = \frac{1}{\sqrt{2}+\sqrt{3}} = \frac{1}{\sqrt{2}+\sqrt{3}}\frac{\sqrt{2}-\sqrt{3}}{\sqrt{2}-\sqrt{3}} = \frac{\sqrt{2}-\sqrt{3}}{2-3} = -(\sqrt{2}-\sqrt{3}),$$

it folloiws that $\sqrt{2}-\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$.
Therefore,

$$\frac{1}{2}((\sqrt{2}+\sqrt{3})+(\sqrt{2}-\sqrt{3})) = \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

and

$$\frac{1}{2}((\sqrt{2}+\sqrt{3})-(\sqrt{2}-\sqrt{3})) = \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

By (a) and (b), $\mathbb{Q}\Big(\sqrt{2}+\sqrt{3}\Big) = \mathbb{Q}\Big(\sqrt{2},\ \sqrt{3}\Big)$.

(2) We (already) know that $\sqrt{3} \notin \mathbb{Q}\Big(\sqrt{2}\Big) = \Big\{a+b\sqrt{2} : a,\ b \in \mathbb{Q}\Big\}$.
So, $[\mathbb{Q}\Big(\sqrt{2},\ \sqrt{3}\Big) : \mathbb{Q}] > 2$.
Since $\sqrt{2}$ has degree 2 over $\mathbb{Q}$, and $\sqrt{3}$ has same degree over $\mathbb{Q}$, $[\mathbb{Q}\Big(\sqrt{2},\ \sqrt{3}\Big) : \mathbb{Q}] \leqslant 2+2 = 4$.
Therefore $[\mathbb{Q}\Big(\sqrt{2},\ \sqrt{3}\Big) : \mathbb{Q}] = 3$ or 4.
But $[\mathbb{Q}\Big(\sqrt{2},\ \sqrt{3}\Big) : \mathbb{Q}] \neq 3$ since degree of field extensions are multiplicative and 2 does not divide 3.
Therefore $[\mathbb{Q}\Big(\sqrt{2},\ \sqrt{3}\Big) : \mathbb{Q}] = 4$.

(3) The irreducible polynomial satisfied by $\sqrt{2}+\sqrt{3}$ must have degree 4 since $[\mathbb{Q}\Big(\sqrt{2},\ \sqrt{3}\Big) : \mathbb{Q}] = 4$.
Since $\sqrt{2}+\sqrt{3}$ is a root of $f(x) = x^4 - 10x + 1$, and $f(x)$ has degree 4, it must be irreducible. Because if $f(x) = x^4 - 10x + 1$ is not irreducible, then $\sqrt{2}+\sqrt{3}$ would be a root of one of its factors. contradiction. : the minimal polynomial of $\sqrt{2}+\sqrt{3}$ has degree 4.

□

Problem 3 (Section 13.2, Exercise 19)**.** Let K be an extension of F of degree n.

(1) For any $\alpha \in K$ prove that α acting by left multiplication on K is an F-linear transformation of K.

(2) Prove that K is isomorphic to a subfield of the ring of $n \times n$ matrices over F, so the ring of $n \times n$ matrices over F contains an isomorphic copy of every extension of F of degree $\leq n$.

Solution.

(1) Fix $\alpha \in K$.
Since K is a field($\Longrightarrow$ commutative ring),

$$\alpha(a+b) = \alpha a + \alpha b \quad \text{and} \quad \alpha(\beta a) = \beta(\alpha a)$$

for all $a,\ b$ and $\beta \in K$.
If β is in F, we get the result.

(2) Fix a basis for K (as a vector space over F).
By (1), for every $\alpha \in K$, there is an $F-$linear transformation T_α oF K.
And let $[T_\alpha]$ be the matrix of T_α with respect to the basis we already fixed.
Then define a map

$$\varphi : K \longrightarrow \mathrm{Mat}_{n\times n}(F)$$

by $\varphi(\alpha) = [T_\alpha]$.
For every $\alpha, \beta \in K$,

$$T_{\alpha+\beta}(k) = (\alpha+\beta)k = \alpha k + \beta k = T_\alpha(k) + T_\beta(k)$$

for all $k \in K$, and for every $\alpha,\ \beta \in K$,

$$T_{\alpha\beta}(k) = (\alpha\beta)k = \alpha(\beta k) = T_\alpha\left(T_\beta(k)\right) = T_\alpha T_\beta(k)$$

for all $k \in K$. i.e.,

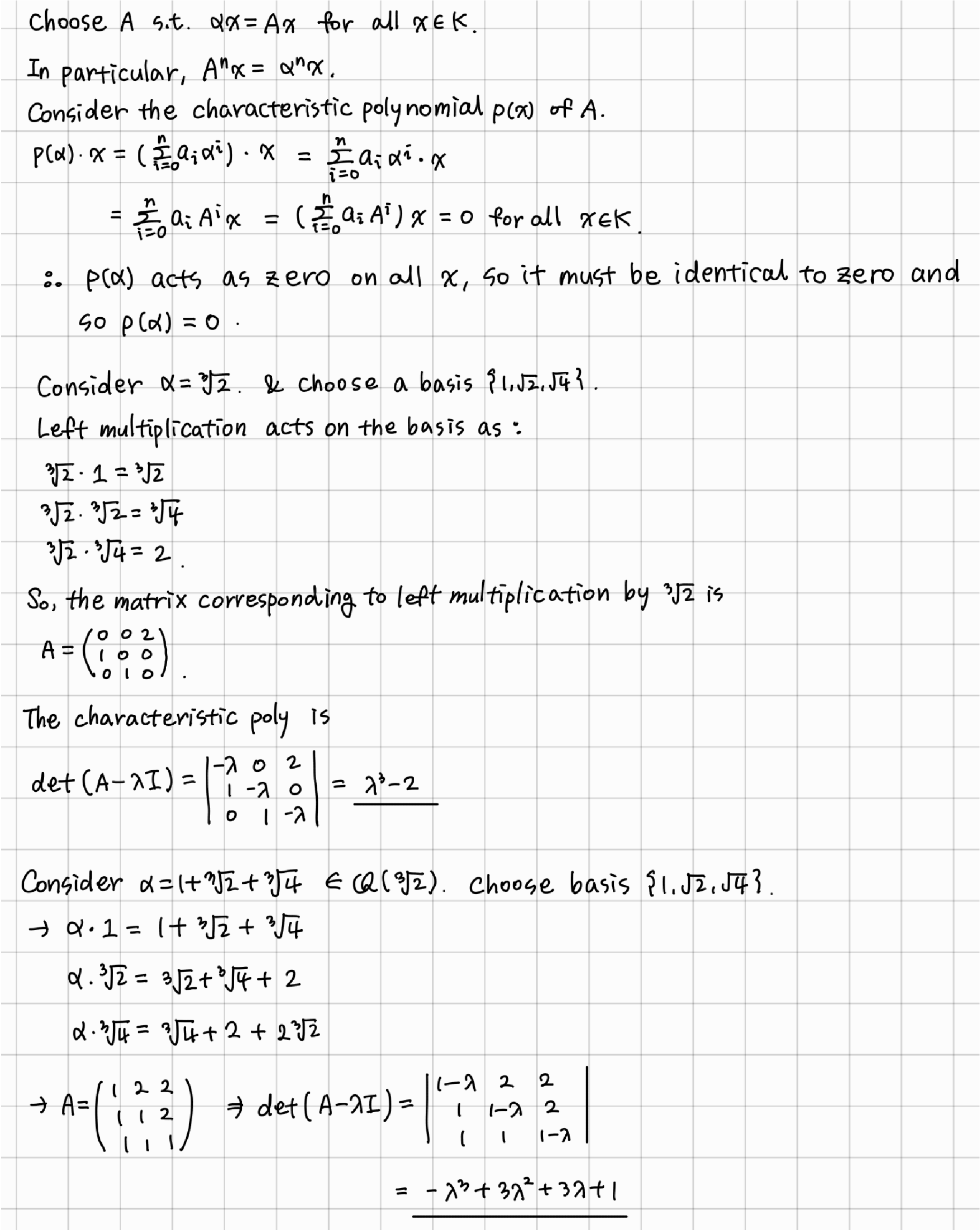
$$T_{\alpha+\beta} = T_\alpha + T_\beta \quad \text{and} \quad T_{\alpha\beta} = T_\alpha T_\beta.$$

Thus, $\varphi(\alpha+\beta) = \varphi(\alpha) + \varphi(\beta)$ and $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$, hence φ is a homomorphism.
Let $\varphi(\alpha) = \varphi(\beta)$, then $\alpha k = \beta k$ for all $k \in K$, so $\alpha = \beta$ if we choose $k = 1$, φ is injective.
Therefore, $\varphi(K)$ is isomorphic to a subfield of $\mathrm{Mat}_{n\times n}(F)$, so the matrix ring $\mathrm{Mat}_{n\times n}(F)$ contains an isomorphic copy of every extension of F of degree $\leqslant n$.

□

Problem 4 (Section 13.2, Exercise 20)**.** Show that if the matrix of the linear transformation "multiplication by α" considered in the previous exercise is A then α is a root of the characteristic polynomial for A. This gives an effective procedure for determining an equation of degree n satisfied by an element α in an extension of F of degree n. Use this procedure to obtain the monic polynomial of degree 3 satisfied by $\sqrt[3]{2}$ and by $1+\sqrt[3]{2}+\sqrt[3]{4}$

Solution.



Choose A s.t. $\alpha x = Ax$ for all $x \in K$.

In particular, $A^n x = \alpha^n x$.

Consider the characteristic polynomial $p(x)$ of A.

$$p(\alpha)\cdot x = \left(\sum_{i=0}^{n} a_i \alpha^i\right)\cdot x = \sum_{i=0}^{n} a_i \alpha^i \cdot x$$

$$= \sum_{i=0}^{n} a_i A^i x = \left(\sum_{i=0}^{n} a_i A^i\right) x = 0 \text{ for all } x \in K.$$

$\therefore$ $p(\alpha)$ acts as zero on all x, so it must be identical to zero and so $p(\alpha) = 0$.

Consider $\alpha = \sqrt[3]{2}$. & choose a basis $\{1, \sqrt{2}, \sqrt{4}\}$.

Left multiplication acts on the basis as:

$\sqrt[3]{2}\cdot 1 = \sqrt[3]{2}$

$\sqrt[3]{2}\cdot\sqrt[3]{2} = \sqrt[3]{4}$

$\sqrt[3]{2}\cdot\sqrt[3]{4} = 2$.

So, the matrix corresponding to left multiplication by $\sqrt[3]{2}$ is

$$A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

The characteristic poly is

$$\det(A-\lambda I) = \begin{vmatrix} -\lambda & 0 & 2 \\ 1 & -\lambda & 0 \\ 0 & 1 & -\lambda \end{vmatrix} = \underline{\lambda^3 - 2}$$

Consider $\alpha = 1+\sqrt[3]{2}+\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$. Choose basis $\{1, \sqrt{2}, \sqrt{4}\}$.

$\rightarrow$ $\alpha \cdot 1 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$

$\alpha \cdot \sqrt[3]{2} = \sqrt[3]{2} + \sqrt[3]{4} + 2$

$\alpha \cdot \sqrt[3]{4} = \sqrt[3]{4} + 2 + 2\sqrt[3]{2}$

$$\rightarrow A = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \Rightarrow \det(A-\lambda I) = \begin{vmatrix} 1-\lambda & 2 & 2 \\ 1 & 1-\lambda & 2 \\ 1 & 1 & 1-\lambda \end{vmatrix}$$

$$= \underline{-\lambda^3 + 3\lambda^2 + 3\lambda + 1}$$

□

Problem 5 (Section 13.4, Exercise 5)**.** Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27.]

Solution.

(1) Assume that K is a splitting field over F.
Then there exists $f(x) \in F[x]$ s.t. K is a splitting field of f.
Let $g(x)$ be an irreducible polynomial in $F[x]$ with a root $\alpha \in K$, and let β be any root of g.
By theorem 8, there is an isomorphism $\varphi : F(\alpha) \xrightarrow{\sim} F(\beta)$ s.t. $\varphi(a) = \beta$.
Also, $K(\alpha)$ is the splitting field of f over $F(\alpha)$, and $K(\beta)$ is the splitting field of f over $F(\beta)$.
By theorem 28, φ extends to isomorphism $\sigma : K(\alpha) \xrightarrow{\sim} K(\beta)$.
Since $K = K(\alpha)$, we get

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

i.e., $K = K(\beta)$, so $\beta \in K$.

(2) Assume that every irreducible polynomial in $F[x]$ has a root in K splits completely in $K[x]$.
Since $[K : F] < +\infty$, we have $K = F(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$ for some $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$.
Now let p_i be the minimal polynomial of α_i over F for all $i = 1,\ 2,\ \cdots,\ n$, and let $f = \prod_{i=1}^{n} p_i$.
Since every α_i is in K, and every p_i has a root in K, it follows that p_i splits completely in K.
Thus, f splits completely in K and K is generated over F by its roots, thus K is the splitting field of $f(x) \in F[x]$.

□

Problem 6 (Section 13.4, Exercise 6)**.** Let K_1 and K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F.

(1) Prove that their composite K_1K_2 is a splitting field over F.
(2) Prove that $K_1 \cap K_2$ is a splitting field over F. [Use the preceding exercise.]

Solution.

Proof. (1): Let K_1 and K_2 be a splitting field of F with S_1 and S_2 respectably.

Want to show: K_1K_2 is the splitting field of F with $S_1 \bigcup S_2$. By the assumption, all polynomials in $S_1 \bigcup S_2$ splits in K_1K_2. Suppose that K' is any extension of F with $S_1 \bigcup S_2$ split. Then K' contains K_1 and K_2 hence contains K_1K_2. Therefore, K_1K_2 is the splitting field over F.

(2): I'll use the result in exercise 5, $K_1 \bigcap K_2$ is splitting over F iff for all irreducible polynomial in $F[x]$ that has a root in $K_1 \bigcap K_2$ splits completely in $(K_1 \bigcap K_2)[x]$. Suppose that $g \in F[x]$ has a root in $K_1 \bigcap k_2$. Then they are splits completely each $K_i (i = 1, 2)$. But they are both in $K[x]$ these decompositions are same. Hence g splits completely in $K_1 \bigcap K_2$ □

□

Problem 7. Let F be a field and let E, E' be algebraic closures of F. Prove that there is an isomorphism $\sigma : E \to E'$ such that $\sigma|_F : F \to F$ is the identity map on F.

Solution.

Proof. I will show that the isomorphism extension theorem of splitting field extension holds on the infinite case. Then, since we know the existence of an algebraic closure, applying the theorem with the identity map, we can show that any two algebraic closures are isomorphic.

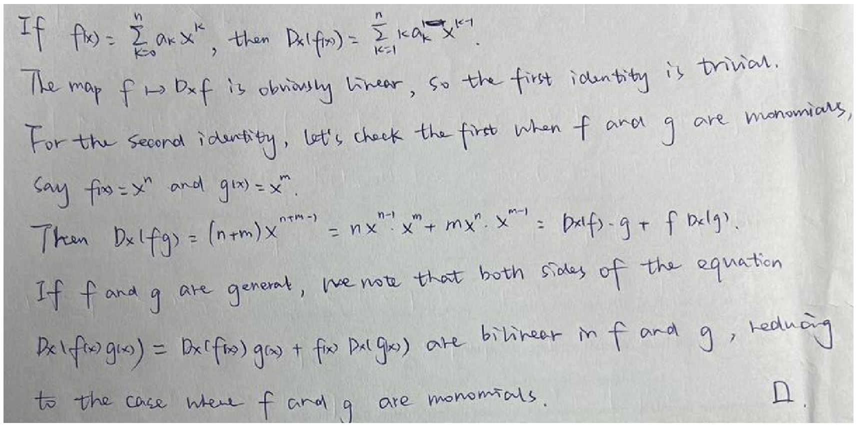
Proof of the isomorphism extending theorem for infinite case: Use Zorn's lemma! Let K be a splitting field of F(with a set of polynomials S) and M be a splitting field of L(with a set of polynomials S', image of the isomorphism σ). Let E, N be intermediate field of the previous splitting fields, and $\tau : E \to N$ be the extended isomorphism of $\sigma : F \to L$. Define the poset on triples $(E_1, \tau_1, N_1) \leq (E_2, \tau_2, N_2)$ if $E_1 \subset E_2$, $N_1 \subset N_2$ and $\tau_2|_{E_1} = \tau_1$. For all chains $\mathcal{C}$ in this poset, we can make an upper bound with (E', τ, N') with $E' = \bigcup E_i$, $N' = \bigcup N_i$ and τ', if $x \in N_i$ $\tau'(x) = \tau_i(x)$. Then by Zorn's lemma there exists a maximal element (K_0, τ_0, M_0). I want to show that $K = K_0$, $M = M_0$ and τ_0 is the extended isomorphism. If $K_0 \neq K$, there exists some $f \in S$ such that f does not split in K_0. Then there is a splitting field of K_0, K_1 with f. and f induce a M_1, splitting extension of M_0 with $\tau_0 f$. Then by the isomorphism extension theorem of splitting field with one polynomial. There exists τ_1 extending τ. It is contradiction to the maximality. We are done!

Hence, applying the above theorem with $1_F : F \to F$ with all polynomials in $K[x]$ we can get the desired result. □

□

Problem 8 (Section 13.5, Exercise 1)**.** Prove that the derivative D_x of a polynomial satisfies $D_x(f(x) + g(x)) = D_x(f(x)) + D_x(g(x))$ and $D_x(f(x)g(x)) = D_x(f(x))g(x) + D_x(g(x))f(x)$ for any two polynomials $f(x)$ and $g(x)$.

Solution.



If $f(x) = \sum_{k=0}^{n} a_k x^k$, then $D_x(f(x)) = \sum_{k=1}^{n} k a_k x^{k-1}$.

The map $f \mapsto D_x f$ is obviously linear, so the first identity is trivial.

For the second identity, let's check the first when f and g are monomials,

say $f(x) = x^n$ and $g(x) = x^m$.

Then $D_x(fg) = (n+m)x^{n+m-1} = nx^{n-1} \cdot x^m + mx^n \cdot x^{m-1} = D_x(f) \cdot g + f\, D_x(g)$.

If f and g are general, we note that both sides of the equation

$D_x(f(x)g(x)) = D_x(f(x))g(x) + f(x)D_x(g(x))$ are bilinear in f and g, reducing

to the case where f and g are monomials. $\square$.

□

Problem 9 (Section 13.5, Exercise 7)**.** Suppose K is a field of characteristic p which is not a perfect field: $K \neq K^p$. Prove there exist irreducible inseparable polynomials over K. Conclude that there exist inseparable finite extensions of K.

Solution.

Since $K \neq K^p$, we can take an element $a \in K$ which is not a p^{th} power of any element of K. Consider $p(x) = x^p - a \in K[x]$. Then $D_x p(x) = px^{p-1} = 0$ since $ch(K) = p$, and hence $p(x)$ and $D_x p(x)$ are not relatively prime in $K[x]$. By Proposition 33, $p(x)$ is inseparable. Now, we prove that $p(x)$ is irreducible over K. Consider a splitting field L for $p(x) = x^p - a$ over K. Then L contains a zero of $p(x)$, say $b \in L$. Note that $b \notin K$ since $a \notin K^p$, and $b^p = a$ in L. We have $x^p - a = (x-b)^p$ in $L[x]$. If $x^p - a$ is reducible over K, then we must have $(x-b)^n \in K[x]$ for some integer $1 \leq n < p$. This implies that $b^n \in K$. Also $b^p \in K$ since $b^p = a$. But then, since p is a prime, we have $(p, n) = 1$ and so $b \in K$, a contradiction.

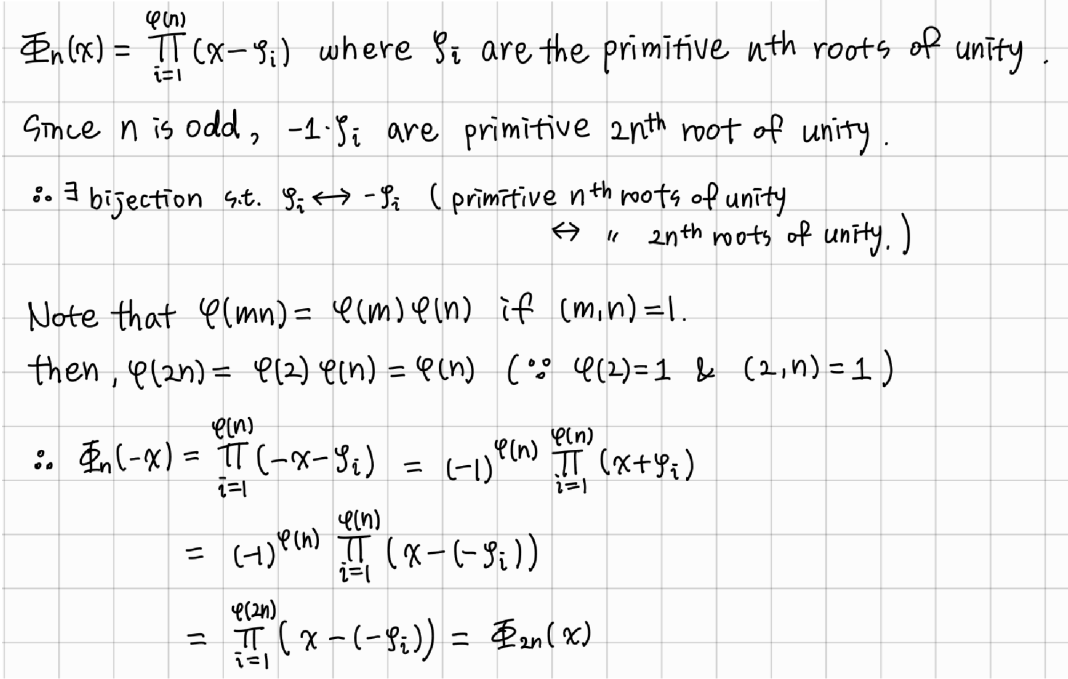
$\therefore$ $p(x)$ is an irreducible inseparable polynomial over K.

Then, the splitting field of $p(x)$ over K is an inseparable finite extension of K, as desired.

□

Problem 10 (Section 13.6, Exercise 6)**.** Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.

Solution.



$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x-\zeta_i)$ where ζ_i are the primitive nth roots of unity.

Since n is odd, $-1\cdot\zeta_i$ are primitive $2n$th root of unity.

$\therefore$ $\exists$ bijection s.t. $\zeta_i \longleftrightarrow -\zeta_i$ (primitive n^{th} roots of unity
$\leftrightarrow$ 〃 $2n^{th}$ roots of unity.)

Note that $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n)=1$.
then, $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$ ($\because$ $\varphi(2)=1$ & $(2,n)=1$)

$$\therefore\ \Phi_n(-x) = \prod_{i=1}^{\varphi(n)} (-x-\zeta_i) = (-1)^{\varphi(n)} \prod_{i=1}^{\varphi(n)} (x+\varphi_i)$$
$$= (-1)^{\varphi(n)} \prod_{i=1}^{\varphi(n)} (x-(-\zeta_i))$$
$$= \prod_{i=1}^{\varphi(2n)} (x-(-\zeta_i)) = \Phi_{2n}(x)$$

□