Definition 1. Let K be a field.

a) We denote by $K[t]$ the set of polynomials $p(t) = \sum_{i=0}^{n} a_i t^i, a_i \in K$ with coefficients in K. If $p(t)$ is not identically zero [we write $p(t) \neq 0$] we assume that $a_n \neq 0$ and say that the *degree* of $p(t)$ to be equal to n. We write $n = \deg p(t)$. If $p(t) = 0$ we define $\deg p(t) := -1$.

b) we say that a polynomial $p(t)$ is *reducible* if $p(t)$ can be written as a product $p(t) = q'(t)q''(t)$ where $q'(t), q''(t)$ are non-constant polynomials with coefficients in K,

c) we say that a polynomial $p(t)$ is *irreducible* if it is not reducible,

d) a root of a polynomial $p(t)$ in K is an element $a \in K$ such that $p(a) = 0$,

e) we say that a subset $I \subset K[t]$ is an *ideal* if

i) for any $p(t), q(t) \in I$ we have $p(t) + q(t) \in I$ and

ii) for any $p(t) \in I, a(t) \in K[t]$ we have $a(t)p(t) \in I$,

f) we say that an ideal $I \subset K[t]$ is *principal* if there exists $p(t) \in I$ such that I is equal to the set of all polynomials $q(t) \in K[t]$ divisible by $p(t)$.

In this case we write $I = (p(t))$.

Problem 1. Show that

a) if $p(t), q(t) \in K[t]$ are two polynomials such that the corresponding principal ideals $(p(t))$ and $(q(t))$ coincide then there exists $c \in K - \{0\}$ such that $p(t) = cq(t)$,

b) for any two non-zero polynomials $p(t), q(t) \in K[t]$ we have

$\deg (p(t)q(t)) = \deg p(t) + \deg q(t)$,

c) if $p(t)$ is a non-zero polynomial of degree n then it has no more then n distinct roots,

d) Show that given $p(t), q(t) \in K[t]$ such that $p(t) \neq 0$ there exists unique pair $a(t), r(t) \in K[t]$ such that

$q(t) = a(t)p(t) + r(t)$ and $\deg r(t) < \deg p(t)$.

Remark The polynomial $r(t)$ is called the *remainder* of $q(t)$ after the division by $p(t)$.

Lemma 1.1 Any ideal $I \in K[t]$ is principal.

Proof. If $I = \{0\}$ we can take $p(t) = 0$. So assume that $I \neq \{0\}$. Let $n_I \geq 0$ be the minimal degree of a non-zero polynomial in I. Choose $p(t) \in I - \{0\}$ such that $\deg p(t) = n_I$.

I claim that $I = (p(t))$. By the definition of an ideal any polynomial $q(t) \in K[t]$ of the form $a(t)p(t)$ belongs to I. So $(p(t)) \subset I$.

To show that $I = (p(t))$ it is sufficient to prove that any $q(t) \in I$ there exist $a(t) \in K[t]$ such that $q(t) = a(t)p(t))$. Let $r(t) = q(t) - a(t)p(t)$ be the remainder of $q(t)$ after the division by $p(t)$. Since I is an ideal

and $q(t), p(t) \in I$ we see that $r(t) = q(t) + (-a(t))p(t) \in I$. But [see problem 1.1.c)] deg $r(t) <$ deg $r(t) = n_I$. By the definition of n_I this is possible only if $r(t) = 0\Box$.

Definition 2. Let L be a field and $K \subset L$ a subset of L.

a) we say that K is a subfield of L [or that L is an extension of K] if for any $a, b \in K$ we have $a+b, a-b, ab \in K$ and for any $c \in K - \{0\}$ we have $c^{-1} \in K$,

b) if L is an extension of K then we can consider L as a K-vector space. We define the *degree* $[K : L]$ of L over K as the dimension $dim_K(L)$,

c) we say that the extension L of K is finite if $[K : L] < \infty$

d) given an an extension L of K and an element $\alpha \in L$ we denote by $K(\alpha) \subset L$ the subset of elements $l \in L$ which could be written in the form $l = p(\alpha)/q(\alpha)$ where

$p(t), q(t) \in K[t]$ and $q(\alpha) \neq 0$,

e) given an an extension L of K and a subset $A \subset L$ we denote by $K(A) \subset L$ the subset of elements $l \in L$ which could be written in the form $l = p(\alpha_1, ..\alpha_n)/q(\alpha_1, ..\alpha_n))$ where

$\{\alpha_1, ..\alpha_n\}$ is any finite subset of A, $p(t_1, ..., t_n), q(t_1, ..., t_n) \in K[t_1, ..., t_n]$ be polynomials in $t_1, ..., t_n$ with coefficients in K such that $q(t_1, ..., t_n) \neq 0$,

f) we say that an extension L of K is elementary if there exists $\alpha \in L$ such that $K(\alpha) = L$.

Problem 2. a) Find $[\mathbb{C} : \mathbb{R}]$,

b) show that the extension $\mathbb{Q} \subset \mathbb{R}$ is not elementary,

c) Let L be a field and $K \subset L$ a subfield of L. Show that for any $\alpha \in L$ the set $K(\alpha) \subset L$ is a subfield of L,

d) Let L be a field and $K \subset L$ a subfield of L. Show that for any subset $A \subset L$ the set $K(A) \subset L$ is a subfield of L,

e) if $p(t) \in \mathbb{R}[t]$ is irreducible then either deg $p(t) = 1$ or deg $p(t) = 2$.

Remark. I assume that you know that any polynomial $p(t) \in \mathbb{C}[t]$ of positive degree has a root $a \in \mathbb{C}$.

Definition 3. Given an an extension L of K and an element $\alpha \in L$ we say that α is *algebraic* over K if there exists a non-zero polynomial $p(t) \in K[t]$ such that $p(\alpha) = 0$.

If α is not algebraic we say that α is *transcendental* over K.

Theorem 1.1. [The product formula] If L is a finite extension of F and F is a finite extension of K then

a) L is a finite extension of K

and

b) $[L:K]=[L:F][F:K]$.

Proof. Let $\alpha_i \in L, 1 \leq i \leq [L:F]$ be a basis of L as an F-vector space and $\beta_j \in F, 1 \leq j \leq [F:K]$ be a basis of F as a K-vector space. Let

$l_{ij} := \alpha_i \beta_j\} \subset L, 1 \leq i \leq [L:F], 1 \leq j \leq [F:K]$.

I claim that the set

$\{l_{ij}\} \subset L$

is a basis of L as an K-vector space. This claim consists of two parts:

a) the set $\{l_{ij}\} \subset L$ generates L as an K-vector space

and

b) elements $l_{ij} \in L$ in the K-vector space L are linearly independent.

I'll prove the part a) and leave the part b) as a homework problem.

Proof of a). Take any $l \in L$. We have to show the existence of $c_{i,j} \in K, 1 \leq i \leq [L:F], 1 \leq j \leq [F:K]$ such that

$l = \sum_{i,j} c_{i,j} l_{ij}$.

Since $\alpha_i \in L, 1 \leq i \leq [L:F]$ is a basis of the F-vector space L we can find $\gamma_i \in F, 1 \leq i \leq [L:F]$ such that $l = \sum_i \gamma_i \alpha_i, 1 \leq i \leq [L:F]$.

On the other hand since $\beta_j \in F, 1 \leq j \leq [F:K]$ a basis of the K-vector space F we can find $c_{i,j} \in K, 1 \leq i \leq [L:F], 1 \leq j \leq [F:K]$ such that for any $i, , 1 \leq i \leq [L:F]$ we have

$\gamma_i = \sum_j c_{i,j} \beta_j$. But then $l = \sum_{i,j} c_{i,j} l_{ij} \square$.

Problem 3. Prove the part b) of the Theorem 1.1.

Problem 4. Let $u \in \mathbb{C}$ be a solution of the equation

$$(\star) u^3 - u^2 + u + 2 = 0$$

and $E = \mathbb{Q}(u)$

a) show that $[E:\mathbb{Q}]$ does not depend on a choice u of a solution of $(\star)$,

b) express $(u^2+u+1)(u^2-u)$ and $(u-1)^{-1}$ in the form

$$au^2 + bu + c$$

where $a, b, c \in \mathbb{Q}$

Let $\xi_n \in \mathbb{C}$ be a primitive n-th root of 1. [That is $\xi_n^n = 1$ but $\xi_n^m \neq 1$ for all $1 \leq m < n$].

c) show that the subfield $L_n := \mathbb{Q}(\xi_n) \subset \mathbb{C}$ does not depend on a choice of a primitive root $\xi_n \in \mathbb{C}$,

d) find $[L_n:\mathbb{Q}]$ for $2 \leq n \leq 4$

Theorem 1.2 Let L be an extension of $K, \alpha \in L$. Then α is algebraic iff [if and only if] $[K(\alpha):K] < \infty$.

Proof. We have to show that

a) if $[K(\alpha):K]<\infty$ then α is algebraic.
and
b) if α is algebraic then $[K(\alpha):K]<\infty$

Proof of a)

For any $n>0$ we define $V_n := span_K(1,\alpha,...,\alpha^{n-1}\} \subset L$ as the K-subspace of L spanned by $1,\alpha,...,\alpha^{n-1}\in L$. It is clear that $V_n \subset V_{n+1}$ and therefore $dim_K V_n \leq dim_K V_{n+1}$. On the other hand for all $n\geq 0$ we have

$$dim_K V_n \leq dim_K K(\alpha) = [K(\alpha):K] < \infty$$

So there exists $n>0$ such that $dim_K V_n = dim_K V_{n+1}$. Therefore $V_n = V_{n+1}$.

Let $n>0$ be the first number such that $V_{n+1}=V_n$. By the definition we have $\alpha^n \in V_{n+1}$. Therefore $\alpha^n \in V_n$ and there exists a polynomial $p(t)=\sum_{i=0}^{n-1} a_i t^i, a_i\in K, a_n=1$ such that $\alpha^n = p(\alpha)\Box$.

Proof of b) Suppose that $\alpha\in L$ is algebraic. Then there exists non-zero polynomials $q(t)$ such that $q(\alpha)=0$. Let n be the minimal degree of such polynomials $q(t)$. Let $V :== span_K(1,\alpha,...,\alpha^{n-1}\} \subset L$.

Since $dim_K(V)=n<\infty$ it is sufficient to show that $K(\alpha)=V$. It is clear that $V\subset K(\alpha)$ is a K-subspace of L invariant under the multiplication by α. To show that $V=K(\alpha)$ it is sufficient to show that $V\subset L$ is a subfield. That is we have to show that for any $\beta\in V-0$ there exists $v_0\in V$ such that $\beta v_0 = 1$.

Since $\beta\in V-0$ there exists a non-zero polynomial $r(t)$ of degree $n-1$ such that $\beta = r(\alpha)$. Consider the K-linear map $B: L\to L$ defined by $A(l):=\beta l$. Since the subspace $V\subset L$ is invariant under the multiplication by $\beta = r(\alpha)$. We define a K-linear map $A: V\to V$ by $A(v):=\beta v$. Since L is a field we see that $\beta v\neq 0$ for $v\neq 0$. So $Ker(A)=\{0\}$.

Now we use the following result from Linear Algebra.

Claim. Let K be a field, V a finite-dimensional K-vector space, $A: V\to V$ a linear map such that $Ker(A)=\{0\}$. Then $A: V\to V$ is onto [and therefore is an isomorphism].

Since $dim_K(V)=n<\infty$ we see that $A: V\to V$ is an isomorphism and there exists $v_0\in V$ such that $A(v_0)=1$ where we consider $1\in K$ as an element of V. Therefore $\beta v_0 = 1\Box$.

Corollary 1 Let L be an extension of $K, \alpha,\beta\in L$ elements algebraic over K. the $\alpha+\beta\in L$, and $\alpha\beta\in L$ are also algebraic.

Proof. I'll prove that $\alpha+\beta$ is algebraic. The proof of the algebraicity of $\alpha\beta$ is completely analogous.

Let $F := K(\alpha) \subset L$ and $G := F(\beta) \subset L$. Since $\beta \in G$ is algebraic over K then by Theorem 1.2 there exists a non-zero polynomial $p(t) \in K[t]$ such that $p(\beta) = 0$. Therefore β is also algebraic over F [you can use the same polynomial $p(t)$] and we see that $[G : F] < \infty$.

So we see that $[G : F], [F : K] < \infty$ and therefore it follows from the Product formula [Theorem 1.1] that $[G : K] < \infty$. Since $K(\alpha+\beta) \subset G$ we see that $[K(\alpha + \beta) : K] < \infty$. Now it follows from Theorem 1.2 that $\alpha + \beta$ is algebraic. $\square$

Problem 5. Let L be an extension of $K, \alpha \in L$ an element algebraic over K. show that $[K(\alpha) : K]$ is the minimal degree of a non-zero polynomial $p(t) \in K[t]$ such that $p(\alpha) = 0$ and that the polynomial is irreducible.