Definition 2.1. Let K be a field. We have a natural homomorphism $\mathbb{Z} \to K$. We will write $n \to \bar{n}$. We say that K is a field of *characteristic* zero if this homomorphism is an imbedding. If this homomorphism is not an imbedding then we define the characteristic of K as the smallest positive number n such that $\bar{n} = 0$.

We denote the characteristic K by ch K.

Remark. You will see that either ch $K = 0$ or it is a prime number .

Definition 2.2.Let L be an extension of K and $\{\alpha_1, ..., \alpha_n\}$ a set of elements in L. We denote by $K(\alpha_1, ..., \alpha_n) \subset L$ the minimal subfield of L containing K and $\{\alpha_1, ..., \alpha_n\}$.

Let L be a finite extension of K. We can ask whether this extension is elementary. To analyze the case when K is a finite field we prove the following result which has an independent interest.

Let K be a field. We denote by $K^* = K - 0$ the commutative group of non-zero elements of K where the group product is the multiplication.

Lemma 2.1. Let $G \subset K^*$ be a finite subgroup. Then G is a cyclic group.

Proof. As you know any finite commutative group G there exists a sequence of distinct prime numbers $p_i, 1 \leq i \leq n$ and finite commutative G^i such that the group that order of G^i is a power of p_i and G is isomorphic to a product $G = \prod_{i=1}^{n} G^i$. Moreover the the group G is cyclic iff all the groups G^i are cyclic.

You also know that a finite commutative p-group H is not cyclic then $|H(p)| > p$ where $H(p) := \{h \in H | h^p = 1\}$. So it is sufficient to show that for any $i, 1 \leq i \leq n$ we have $|G^i(p_i)| \leq p_i$. Therefore it is sufficient to show that for any prime number p we have $|G(p)| \leq p$.

Since G is a subgroup of K^* we have $G(p) \subset K^*(p)$ where $K^*(p) = \{a \in K | a^p = 1\}$. In other words $\{K^*(p)\}$ is the set of roots of the polynomial $t^p - 1$ in K. But it follows from Problem 1.1.c) that $|K^*(p)| \leq$ deg $(t^p - 1) = p$. Therefore $|G(p)| \leq p.\square$.

Corollary. Any extension $L \supset K$ such that $|L| < \infty$ is elementary.

Proof. Since L is a finite field it follows from Lemma 2.1 that there exists $\alpha \in L$ such that and $l \in L^*$ is a power of α. It is clear then that $L = K(\alpha)$.

Definition 2.3. We say that a finite extension $L \supset K$ satisfies the condition $\star$ if there exists only a finite number of subfields $F \subset L$ containing K.

Theorem 2.1. A finite extension $L \supset K$ is elementary iff it satisfies the condition $\star$.

Proof. We have to show that

a) if $L \supset K$ is a finite extension of K which satisfies the condition $\star$ then the extension $L \supset K$ is elementary

and

b) if $L \supset K$ is an elementary extension then it satisfies the condition $\star$.

We will prove now only the part a) and will return to the proof of the part b) later. We also show later that any finite extension L of a field K of characteristic 0 satisfies the condition $\star$.

Proof of a). Assume that $L \supset K$ is a finite extension of K such that there exists only a finite number of subfields $F \subset L$ containing K. Since the extension $L \supset K$ is finite there exists a finite basis $\{\alpha_1, ..., \alpha_n\}$ of L over K. It is clear that $K(\alpha_1, ..., \alpha_n) = L$. The proof is by the induction on the size n of a finite set $\{\alpha_1, ..., \alpha_n\} \in L$ such that $K(\alpha_1, ..., \alpha_n) = L$. If $n = 1$ there is nothing to prove.

Consider the case $n = 2$. For any $c \in K$ consider the subfield $K(\alpha_1 + c\alpha_2) \subset L$. Since the extension $L \supset K$ satisfies the condition $\star$ there exists only a finite number of subfields $F \subset L$ containing K. On the other hand the field K is infinite. Therefore there exists $c_1 \neq c_2 \in K$ such that

$$K(\alpha_1 + c_1\alpha_2) = K(\alpha_1 + c_2\alpha_2)$$

Let $F := K(\alpha_1 + c_2\alpha_2)$. Since $F := K(\alpha_1 + c_1\alpha_2)$ we see that $\alpha_1 + c_1\alpha_2, \alpha_1 + c_2\alpha_2 \in F$. So $(c_1 - c_2)\alpha_2 \in F$ and therefore $\alpha_2 \in F$. Since $\alpha_1 + c_1\alpha_2, \alpha_2 \in F$ we see that $\alpha_1 \in F$. Since $\alpha_1, \alpha_2 \in F$ and $K(\alpha_1, \alpha_2) = L$ we have $K(\alpha_1 + c_2\alpha_2)L$.

Proceeding inductively, we see that if $L = K(\alpha_1, ..., \alpha_n)$ then there exist elements $c_2, ..., c_n \in K$ such that $L = K(\alpha_1 + c_2\alpha_2 + ... + c_n\alpha_n)\square$.

Constructions of fields. We will discuss two ways to construct new fields: the construction of the fraction field and the adjoining of a root of an irreducible polynomial.

Definition 2.3. Let A be a commutative ring. We say that A is *integral* if for any $a, b \in A - \{0\}$ we have $ab \neq 0$.

Let A be an integral commutative ring.

Consider the set X of pairs $(a, s), a \in A, s \in A - \{0\}$. We define operations

$$((a, s), (a', s')) \to (a, s) + (a', s'), ((a, s), (a', s')) \to (a, s)(a', s')$$

on X by

$$(a, s)(a', s') := (aa', ss'), (a, s) + (a', s') := (as' + a's, ss')$$

Consider an equivalence relation $\equiv$ on X defined by
$(a, s) \equiv (a', s')$ if $as' = a's$
[check that $\equiv$ is an equivalence relation] and denote by $K(A)$ the set of equivalence classes under the equivalence relation $\equiv$. As you will show the operations

$$((a, s), (a', s')) \to (a, s) + (a', s'), ((a, s), (a', s')) \to (a, s)(a', s')$$

define operations on the set $K(A)$ and the set $K(A)$ acquires the structure of a field. We call this field the field of *fractions* of A. .

Examples. a) If $A = \mathbb{Z}$ then $K(A) = \mathbb{Q}$,
b) if A is a field then $K(A) = A$,
c) if K is a field we denote the field of fraction of $K[t]$ by $K(t)$ and call it the field of rational functions over K in one variable,
d) analogously K is a field we denote the field of fraction of $K[t_1, ..., t_n]]$ by $K(_1, ..., t_n)$ and call it the field of rational functions over K in n variables.

To define the construction of adjoining of a root of an irreducible polynomial we have prove some results about the ring $K[t]$ of polynomials.

Definition 2.4. a) If a non-zero polynomial $p(t)$ divides $q(t)$ we write $p(t)|q(t)$.
b) A non-zero polynomial $p(t) = \sum_{i=0}^{n} c_i t^i$ of degree n polynomial is *monic* if $c_n = 1$,
c) Let $q(t), r(t) \in K[t]$ be non-zero polynomials. We denote by $I \subset K[t]$ be the set of polynomials $s(t)$ of the form $s(t) = a(t)q(t) + b(t)r(t), a(t), b(t) \in K[t]$. It is clear that $I \subset K[t]$ is a non-zero ideal. As follows from Lemma 1.1 and the Problem 1.1.a) there exists unique monic polynomial $p(t)$ such that $I = (p(t))$. We say that the polynomial $p(t)$ is the *greatest common divisor* of $q(t), r(t) \in K[t]$.
d) we say that $q(t), r(t) \in K[t]$ are *relatively prime* if the greatest common divisor of $q(t), r(t) \in K[t]$ is equal to 1.

Lemma 2.2. If $q(t)$ is irreducible and $a_1(t), ..., a_n(t)$ are polynomials such that $q(t)$ divides the product $a_1(t) \times ... \times a_n(t)$ then there exists $i, 1 \leq i \leq n$ such that $q(t)|a_i(t)$.

Proof . We can assume that $q(t)$ is monic. The proof is by induction in n. If $n = 1$ there is nothing to prove. Consider the case $n = 2$. To prove the Lemma in the case $n = 2$ we have to show for any polynomials $a_1(t), a_2(t) \in K[t]$ such that $q(t)$ does not divide neither $a_1(t)$ nor $a_2(t)$ the polynomial $q(t)$ does not divide $a_1(t)a_2(t)$.

Let $p(t)$ be the greatest common divisor of $q(t)$ and $a_1(t)$. By the definition $q(t) \in (p(t))$ and therefore $p(t)|q(t)$. Since $q(t)$ is irreducible it is possible only either $p(t) = q(t)$ or if $p(t) = 1$. Since $q(t)$ does not divide $a_1(t)$ we see that $p(t) \neq q(t)$. So $p(t) = 1$.

By the definition of the greatest common divisor there exist $b(t), c(t) \in K[t]$ such that $b(t)q(t)+c(t)a_1(t) = 1$. Therefore $a_2(t)b(t)q(t)+c(t)a_1(t)a_2(t) = a_2(t)$. Since $q(t)$ does not divide $a_2(t)$ but divides $a_2(t)b(t)q(t)$ we see that $q(t)$ does not divide $c(t)a_1(t)a_2(t)$. If so it also does not divide $a_1(t)a_2(t)$. This ends the proof of the case when $n = 2$.

Suppose we now the Lemma is know for products of $n-1$ factors. We want to prove it for a product $a_1(t), ..., a_n(t)$ of n factors. Let $b(t) := a_2(t), ..., a_n(t)$. Then $a_1(t), ..., a_n(t) = a_1(t)b(t)$. Since $q(t)|a_1(t)b(t)$ we know that either $q(t)|a_1(t)$ or $q(t)|)b(t)$. In the first case there is nothing to prove. In the second we can apply the inductive assumption.□

Lemma 2.3. a) Let $q(t) \in K[t]$ be a polynomial of positive degree. Then there exists $a \in K - 0$, irreducible monic polynomials $p_i \in K[t]$ and positive numbers $m_i, 1 \leq i \leq n$ such that

$$q(t) = ap_1(t)^{m_1}...p_n(t)^{m_n}$$

b) such a factorization is unique up to the order of $p_i \in K[t]$.

It is clear that is is sufficient to prove Lemma in the case when $q(t) \in K[t]$ is monic.

Proof of a). The proof is by the induction in deg $q(t)$. If deg $q(t) = 1$ then $q(t) = t + b$ and it is clear that $q(t)$ is an irreducible monic polynomial.

Assume now that the part a) of Lemma is known for all polynomial of degree $< n$. Let $q(t) \in K[t]$ be a monic polynomial of degree n. If $q(t)$ is irreducible then there is nothing to prove. So assume that $q(t)$ is reducible. Then there exists polynomials $q'(t), q''(t)$ of positive degrees such that $q(t) = q'(t)q''(t)$. Since deg $q'(t)$,deg $q''(t)$¡deg $q(t)$ we know by the inductive assumption that $q'(t), q''(t)$ are products of irreducible monic polynomials. Therefore $q(t) = q'(t)q''(t)$ is also a product of irreducible monic polynomials. □.

Proof of b). The proof is also by the induction in deg $q(t)$. As before the case when deg $q(t) = 1$ is clear. Assume that the part b) of Lemma is known for all polynomial of degree $< n$. Let $q(t) \in K[t]$ be a monic polynomial of degree n. Suppose that we have two decompositions of $q(t)$ in products of irreducible monic polynomials

$$q(t) = p_1(t)^{m_1}...p_n(t)^{m_n} = r_1(t)^{l_1}...r_s(t)^{l_s}$$

where $p_i(t), r_j(t)$ are irreducible monic polynomials and $m_i, l_j > 0$. We have to show that $n = s$ and there exists a permutation $\sigma : [1, n] \to [1, n]$ such that $p_i(t) = q_{\sigma(i)}(t), m_i = l_{\sigma(i)}$ for all $i, 1 \leq i \leq n$.

Since $p_n(t)|q(t) = r_1(t)^{l_1}...r_s(t)^{l_s}$ we see by Lemma 2.2 that there exists $j, 1 \leq j \leq s$ such that $p_n(t)|r_j(t)$. But since $r_j(t)$ is an irreducible monic polynomial we have $p_n(t) = r_j(t)$. By changing the order of factors $r_i(t)$ we can assume that $j = s$.

Let $\bar{q}(t) := q(t)/p_n(t)$. Then we have $\bar{q}(t) := q(t)/r_s(t)$ and

$$\bar{q}(t) = p_1(t)^{m_1}...p_n(t)^{m_n - 1} = r_1(t)^{l_1}...r_s(t)^{l_s - 1}$$

where we omit factors $p_n(t)$ and/or $r_s(t)$ if $m_n = 1$ and/or $l_s = 1$. Since deg $\bar{q}(t) = n - 1$ we know the uniqueness of the factorization of $\bar{q}(t)$ into the product of irreducible monic polynomials. But this implies immediately the uniqueness of the factorization for $q(t)\square$.

Now we can describe the construction of adjoining of a root of an irreducible polynomial.

Let $p(t) \in K[t]$ be an irreducible polynomial, and $L := K[t]/(p(t))$ be the quotient ring.

Lemma 2.4. a) The ring L is a field,

b) the polynomial $p(t)$ has root in L.

Proof of a). To show that the ring L is a field we have to show that for any $l \in L - \{0\}$ there exists $v \in L$ such that $lv = 1$. Consider L as a K-vector space. It is clear that $\dim_K(L)$=deg $p(t) < \infty$. Let $A : L \to L$ be the operator of the multiplication by l.

Claim. Ker (A)=$\{0\}$.

Proof of the claim. Let m be an element of Ker (A). We want to show that $m = 0$.

Let $l(t), m(t) \in K[t]$ be representatives of l and m in $K[t]$. Then $l(t)m(t) \in K[t]$ is a representative of $A(m)$. Since $m \in$Ker (A) we have $l(t)m(t) \in (p(t))$. In other words $p(t)|l(t)m(t)$. Since $l \neq 0$ we see that $p(t)$ does not divide $l(t)$. It follows now from Lemma 2.3 that $p(t)|m(t)$. In other words $m = 0\square$.

Now we can finish the proof of Lemma 2.4. Since Ker (A)=$\{0\}$ and $\dim_K(L) < \infty$ we see that $A : L \to L$ is onto. Therefore there exists $v \in L$ such that $A(v) = 1\square$.

Proof of b). Let α be the image of $t \in K[t]$ in L. Then $(\alpha) \in L$ is the image of $p(t) \in K[t]$. But by the definition of $L := K[t]/(p(t))$ the image of $p(t)$ in L is equal to 0.$\square$

We will say that the field $L := K[t]/(p(t))$ is obtained from K by adjoining a root of the polynomial $p(t)$.