ALGEBRA 4: algebraic numbers

Algebraic numbers

Definition 4.1. Let $k \subset K$ be a field contained in the field K (one says that k is a **subfield** of K and K is an **extension** of k). Element $x \in K$ is **algebraic over** k if x is a root of a non-zero polynomial with coefficients from k.

One often means complex numbers which are algebraic over $\mathbb{Q}$ (that is, roots of polynomials with rational coefficients)when saying simply "algebraic numbers" .

Exercise 4.1. Let k be a subfield in K and x be an element in K. Consider K as a linear space over k. Let $K_x \subset K$ be a linear subspace of K generated by the powers of x. Prove that K_x is finite dimensional iff x is algebraic.

Exercise 4.2. Let k be a subfield in K, x be an algebraic element of K nd $K_x \subset K$ be a linear subspace generated by powers of x. Consider an operation m_v of multiplication by a non-zero vector $v \in K_x$ defined on K. Prove that m_v is a k-linear mapping that preserves a subspace $K_x \subset K$.

Exercise 4.3. Consider the previous problem, prove that the restriction of m_v on $K_x \subset K$ is invertible.

Exercise 4.4 (!). Conclude that K_x is a subfield of K.

Definition 4.2. Finite extension of a field k is a field $K \supset k$ which is finite dimensional vector subspace over k.

Exercise 4.5. Let $K_1 \supset K_2 \supset K_3$ be fields such that K_1 is finite dimensional over K_2 which is finite dimensional over K_3. Prove that K_1 is a finite extension of K_3.

Exercise 4.6 (!). Conclude that the sum, the product and the factor of elements which are algebraic over k are also algebraic over k.

Exercise 4.7. Prove that any finite field is a finite extension of a field of remainders modulo p for some prime p. Conclude that a finite field has p^n elements (for some p, n, p is prime).

Exercise 4.8 (*). Prove that there exists a non-algebraic complex number.

Exercise 4.9 (**). Prove that the number $0,0100100001000000001...$ (there are 2^i zeros after the ith one) is non-algebraic.

Exercise 4.10 (*). Let the complex number x be algebraic. Prove that its conjugate $\overline{x}$ is also algebraic.

Hint. Use the fact that complex conjugation is an automorphism of $\mathbb{C}$ that preserves $\mathbb{Q}$.

Exercise 4.11 (*). Let the complex number $x = a + b\sqrt{-1}$ be algebraic. Prove that real numbers a and b are algebraic.

Algebraic closure

Exercise 4.12. Let $P(t), Q(t) \in k[t]$ be polynomials of a positive degree over a field k which are co-prime. Prove that 1 can be represented as a linear combination of P and Q over $k[t]$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Hint. Use the algorithm of Euclid for polynomials.

Exercise 4.13. Let $P(t)$ be an irreducible polynomial (it cannot be represented as a product of polynomials of a positive degree with coefficients from k) and a product $Q(t)Q_1(t)$ is divisible by $P(t)$ where $Q(t)$, $Q_1(t)$ are non-zero polynomials. Prove that either $Q(t)$ or $Q_1(t)$ is divisible by $P(t)$.

Hint. Suppose $Q(t)$ is not divisible by $P(t)$. Use the previous exercise to represent 1 as a linear combination of $Q(t)$ and $P(t)$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Then $1 \cdot Q_1(t) = Q(t)Q_1(t)A(t) + P(t)B(t)Q_1(t)$ is divisible by $P(t)$.

Exercise 4.14. Let $P(t)$ be a polynomial over k. Consider a ring $k[t]$ of polynomials of t and a quotient space $k[t]/Pk[t]$ of all polynomials factored by polynomials that are divisible by P. Prove that $k[t]/Pk[t]$ is a ring (with respect to naturally defined multiplication and addition).

Exercise 4.15. Prove that multiplication by a polynomial $Q(t)$ acts on $k[t]/Pk[t]$ as an endomorphism (an endomorphism is a homomorphism from a space to itself).

Exercise 4.16. Suppose that multiplication by $Q(t)$ maps all elements $k[t]/Pk[t]$ to zero. Prove that Q is divisible by P in the ring $k[t]$.

Exercise 4.17. Suppose that $P(t)$ is irreducible. Suppose that $Q(t)$ is a polynomial that is not divisible by $P(t)$. Prove that the operator m_Q of multiplication by $Q(t)$ on the space $k[t]/Pk[t]$ is a monomorphism.

Hint. Suppose v belongs to the kernel of m_Q and $Q_1(t)$ is a polynomial representing v. Then QQ_1 is divisible by P by the previous exercise statement. Use the algorithm of Euclid for polynomials to deduce that either Q is divisible by P or Q_1 is divisible by P.

Exercise 4.18 (*). Let $A: V \longrightarrow V$ be a linear operator. Prove that there exists a polynomial $P(t) = t^n + a_n t^{n-1} + \ldots$ such that $P(A) = 0$. Is it possible in general to find an irreducible polynomial $P(t)$ such that $P(A) = 0$?

Exercise 4.19 (!). Let $P(t)$ be irreducible. Prove that $k[t]/Pk[t]$ is a field.

Hint. Use the previous exercise to prove that if Q is not divisible by P then multiplication by $Q(t)$ defines an invertible linear operator on $k[t]/Pk[t]$.

Definition 4.3. Let $P(t)$ be an irreducible polynomial. We say that the field $k[t]/Pk[t]$ is an **extension obtained by adding the root** $P(t)$.

Definition 4.4. **Algebraic extension** of a field k is a field $K \supset k$ such that all elements of K are algebraic over k.

Exercise 4.20. Prove that any finite extension is algebraic.

Exercise 4.21 (*). Prove that not every algebraic extension is finite.

Definition 4.5. Let k be a field. The field k is called **algebraically complete** if any polynomial of a positive degree $P \in k[t]$ has a root in k.

Definition 4.6. Algebraic closure of a field k is an algebraic extension $\overline{k} \supset k$ which is algebraically complete.

Exercise 4.22 (*). Let K be an extension of the field k and $z \in K$ is a root of a non-zero polynomial $P(t)$ with coefficients which are algebraic over k. Prove that z is algebraic over k.

Exercise 4.23 (*). Suppose K is an algebraic extension of the field k such that any polynomial $P(t) \in k[t]$ has a root in K. Prove that any polynomial $P(t) \in k[t]$ can be represented as a product of linear polynomials from $K[t]$.

Exercise 4.24 (*). Take the statement of the previous exercise and prove that K is algebraically complete.

Hint. Let $P \in K[t]$ be an irreducible polynomial with coefficients K. Add its root α to K. Using the exercise 4.22 we obtain that α is algebraic over k. Then α is a root of a polynomial from $k[t]$. Every such polynomial can be represented as a product $\prod(t - \alpha_i)$, $\alpha_i \in K$ as follows from the previous exercise. Deduce that $\alpha \in K$.

Exercise 4.25 (*). Prove that any field k has an algebraic closure.

Hint. Take any algebraic extension of the field k. If it is algebraically complete then the proof is over. Otherwise there exists a polynomial $P(t) \in k[t]$ which has no roots in K. Add its root to K and obtain a field K_1. Now consider K_1 instead of K and prove the statement for it. After having applied this argument as many times as it would be necessary consider the union of all algebraic extensions of k. We have obtained a field that contains a root of any polynomial from $k[t]$. Use the previous exercise to ensure that this field is algebraically closed.

Exercise 4.26 (**). In the proof sketch for the previous exercise we have used implicitly the Zorn's lemma. Find a proof for a countable field k that does not use Zorn's lemma and therefore does not depend on the axiom of choice.

Exercise 4.27 (**). Can you prove existence of an algebraic closure for an arbitrary field without using the axiom of choice?

Exercise 4.28 (**). Prove that algebraic closure of a field is unique up to isomorphism.