8 Algebras.

In this only section we deal with associative rings with unity, not necessarily commutative. Let k be a field. An associative ring A with unity is called a *k-algebra* (or algebra over k) if there is defined a multiplication $k \times A \to A$ such that A becomes a vector space over k (under the ring addition and the above multiplication) and $\forall a, b \in A\ \forall \lambda \in k\ \lambda \cdot (a \cdot b) = (\lambda \cdot a) \cdot b = a \cdot (\lambda \cdot b)$.

$\diamond$ **8.1** a) Let A be a k-algebra. Prove that $\{\lambda \cdot 1, \quad \lambda \in k\}$ is a subring of A isomorphic to k. (Use that $\forall a \in A\ \forall \lambda \in k\ \ (\lambda \cdot 1) \cdot a = a \cdot (\lambda \cdot 1)$.)
b) Let A be an associative ring with unity having a field k as a subring. Suppose additionally that $\forall a \in A\ \forall \lambda \in k\ \ \lambda \cdot a = a \cdot \lambda$. Prove that then A is a k-algebra.

$\diamond$ **8.2** a) Prove that the set of all $n \times n$ matrices $\mathrm{gl}(n, k)$ is a k-algebra.
b) Prove that the polynomial ring $k[x]$ is a commutative k-algebra.
c) Prove that the formal power series ring $k[[x]]$ is a commutative k-algebra.

$\diamond$ **8.3** Let A be a k-algebra, $a \in A$. Prove that the set $\{\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n, \quad \alpha_i \in k, n \in \mathbb{N}\}$ is the minimal subalgebra of A containing a. It is denoted by $k[a]$. Prove that $k[a]$ is a commutative k-algebra.

$\diamond$ **8.4** Let A be a k-algebra, $a \in A$, $k[x]$ be the polynomial algebra. Define the mapping $\varphi_a \colon k[x] \to A$, $\varphi_a(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n) = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n$.
a) Prove that φ_a is a homomorphism and $\operatorname{Im} \varphi_a = k[a]$. Prove that either $\operatorname{Ker} \varphi_a = \{0\}$ or $\operatorname{Ker} \varphi_a = (P_a(x))$, where $P_a(x)$ is a non-zero polynomial in $k[x]$.
b) If $\operatorname{Ker} \varphi_a = \{0\}$ then the element a is called *transcendental* over k. Prove that for a transcendental element $a \quad k[a] \cong k[x]$.
c) If $\operatorname{Ker} \varphi_a = (P_a(x))$, $P_a(x) \neq 0$, then a is called *algebraic* over k and $P_a(x)$ is called the *minimal polynomial* of the element a. (Since $P_a(x)$ is defined up to a scalar factor we assume the leading coefficient of $P(x)$ to be 1.) Prove that for an algebraic element $a \in A$ $k[a] \cong k[x]/(P_a(x))$.

$\diamond$ **8.5** Let A be a k-algebra, $a \in A$. Define the mapping $L_a \colon A \to A$ by $L_a(b) = ab$. Prove that L_a is a linear operator. Prove that the mapping $A \to \mathrm{gl}(A)$ defined by $a \mapsto L_a$ is an injective homomorphism.

$\diamond$ **8.6** Let A be a finite-dimensional k-algebra.
a) Prove that $\forall a \in A$ is algebraic over k and the minimal polynomial $P_a(x)$ is the divisor of the characteristic polynomial of the linear operator L_a.
b) Give an example of a k-algebra A and $a \in A$ such that these two polynomials do not coincide.

$\diamond$ **8.7** Prove that the polynomials $x^2 - 2$ and $x^3 - 2$ are irreducible over $\mathbb{Q}$. This implies that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}, \quad a, b \in \mathbb{Q}\}$ and $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}, \quad a, b, c \in \mathbb{Q}\}$ are fields. Give an explicit formula for the inverse element in these fields. Find the minimal polynomials for the elements $1 + \sqrt{2}$ and $1 + \sqrt[3]{2}$.

9 Fields.

In this section we discuss *extensions of fields* $k \subset K$. This means that a field k is a subfield of a field K. The extension $k \subset K$ is called *finite* if K is finite-dimensional vector space over k. This dimension is called the *degree* of the extension and denoted by $[K : k]$.

$\diamond$ **9.1** Prove that if $P(x) \in k[x]$ is an irreducible polynomial and $k[\alpha] = k[x]/(P(x))$ then the extension $k \subset k[\alpha]$ is finite and $[k[\alpha] : k] = \deg P(x)$. Therefore $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ and $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

$\diamond$ **9.2** Let $k \subset K \subset L$ be some fields. Prove that the extension $k \subset L$ is finite if and only if both extensions $k \subset K$ and $K \subset L$ are finite. Prove that in this case $[L : k] = [L : K][K : k]$.

$\diamond$ **9.3** Prove that $\mathbb{C}$ has no subfields containing $\mathbb{R}$; $\mathbb{Q}[\sqrt{2}]$ and $\mathbb{Q}[\sqrt[3]{2}]$ have no subfields except $\mathbb{Q}$.

$\diamond$ **9.4** Prove that $L = \{a + b\sqrt{2} + ci + di\sqrt{2}, \quad a, b, c, d \in \mathbb{Q}\}$ is a field; find $[L : \mathbb{Q}]$. Find at least three different fields K such that $\mathbb{Q} \subset K \subset L$; find $[K : \mathbb{Q}]$ and $[L : K]$ for each such K. Are these subfields isomorphic to each other? Find the minimal polynomial for $\alpha = i + \sqrt{2}$ over $\mathbb{Q}$. Prove that $L = \mathbb{Q}[\alpha]$.

$\diamond$ **9.5** Describe the minimal subfield K of $\mathbb{C}$ containing all the three roots of the equation $x^3 = 1$. Find the degree $[K : \mathbb{Q}]$.

$\diamond$ **9.6** Let $K = \mathbb{Q}[\sqrt[3]{2}]$ (see (8.7)). Note that the polynomial $x^3 - 2$ is not irreducible over K since $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$. Prove that the second factor is irreducible over K. Let $L = K[\alpha]$ where α is a root of $x^2 + \sqrt[3]{2}x + \sqrt[3]{4}$. Find the degrees $[K : \mathbb{Q}]$ and $[L : K]$. Find at least three different subfields $M \subset L$, $M \neq \mathbb{Q}$, $M \neq K$. Find $[M : \mathbb{Q}]$ and $[L : M]$ for each such M. (Hint: one of these subfields is described in the previous item.) Which of these subfields are isomorphic to K?

$\diamond$ **9.7** Prove that the extensions $k \subset k(x)$ and $k \subset k((x))$ are not finite. Is the extension $k(x) \subset k((x))$ finite?

$\diamond$ **9.8** Prove that the extension $\mathbb{Q} \subset \mathbb{R}$ is not finite.

$\diamond$ **9.9** The extension $k \subset K$ is called *algebraic* if $\forall a \in K$ is an algebraic element over k. Prove that any finite extension is algebraic. Give an example of an algebraic extension which is not finite.

$\diamond$ **9.10** Recall the Besout theorem: if a polynomial $P(x) \in k[x]$ has a root $\alpha \in k$ (i.e. $P(\alpha) = 0$) then $P(x)$ is divisible by $x - \alpha$ (i.e. $P(x) = (x - \alpha)Q(x)$ for some $Q(x) \in k$). Deduce from the Besout theorem that a degree n polynomial $P(x) \in k[x]$ has at most n roots in k. If $P(x) = \lambda(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$ we say that $P(x)$ *splits.*

$\diamond$ **9.11** Let $k \subset K$ be an extension of fields, $P(x) \in k[x]$ and $P(x) = \lambda(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$ for some $\alpha_1 \dots \alpha_n \in K$. Then the minimal subfield $L \subset K$ containing $\alpha_1 \dots \alpha_n$ is called the *splitting field* for $P(x) \in k[x]$.

$\diamond$ **9.12** Prove that the field $\mathbb{Q}[-\frac{1}{2}+i\frac{\sqrt{3}}{2}]$ is the splitting field for x^3-1.

$\diamond$ **9.13** Prove that the field L from 9.6 is the splitting field for x^3-2.

$\diamond$ **9.14** Prove that the field L from 9.4 is the splitting field for x^4-2x^2+9.

$\diamond$ **9.15** Prove that the field L from 9.4 is the splitting field for x^4-x^2-2.

$\diamond$ **9.16** Prove that each polynomial $P(x)\in k[x]$ has a splitting field. (Hint: for each irreducible factor of $P(x)$ generalize the construction used in 9.6.) Prove that this splitting field is unique. (This means that if there are two splitting fields $k\subset K$ and $k\subset L$ for $P(x)$ then there exists an isomorphism $\varphi : K\to L$ identical on k.)

$\diamond$ **9.17** Prove that a finite subgroup of a multiplicative group of a field is cyclic. (Hint: the polynomial x^n-1 has at most n roots; prove that any finite abelian non-cyclic group G contains more than n order n elements for some $n \mid |G|$.)

$\diamond$ **9.18** Let K be a finite field, $\operatorname{char} K = p$. (Note that this implies that $\mathbb{F}_p\subset K$.) a) Prove that $\forall a,b\in K\ (a+b)^p=a^p+b^p$.
b) Prove that $\forall a\in\mathbb{F}_p\ a^p=a$.
c) Prove that the mapping $\Phi : K\to K$ defined by $\Phi(a)=a^p$ is a homomorphism (and therefore an isomorphism from K to $\operatorname{Im}\Phi\subset K$). Φ is called the *Frobenius mapping.*
d) Prove that $\Phi(a)=a\Leftrightarrow a\in\mathbb{F}_p$.
e)Prove that $\{a\in K,\quad a^{p^n}=a\}$ is a subfield of K containing at most p^n elements. (Hint: $a^{p^n}=\Phi^n(a)$.)

$\diamond$ **9.19** Consider the splitting field for $x^{p^n}-x$ over $\mathbb{F}_p$. According to 9.16 it exists and is unique up to an isomorphism. Denote this field by $\mathbb{F}_{p^n}$. According to 9.18e) $\mathbb{F}_{p^n}$ has at most p^n elements. Prove that $\mathbb{F}_{p^n}$ has exactly p^n elements. (Hint: prove that the polynomial $x^{p^n}-x$ has no multiple roots since its derivative is -1.)

$\diamond$ **9.20** Let K be a finite field, $\operatorname{char} K=p$.
a) Prove that $|K|=p^n$ for some n. (Hint: note that K is n-dimensional $\mathbb{F}_p$-algebra.)
b) Prove that K is the splitting field for $x^{p^n-1}-1$. (Hint: use the Lagrange theorem for K^*.) Therefore $K\cong\mathbb{F}_{p^n}$.
c) Prove that

$$x^{p^n}-x=\prod_{\alpha\in\mathbb{F}_{p^n}}(x-\alpha)\quad\text{and}\quad x^{p^n-1}-1=\prod_{0\neq\alpha\in\mathbb{F}_{p^n}}(x-\alpha).$$

$\diamond$ **9.21** Prove the Wilson theorem: if p is prime then $(p-1)!\equiv -1 \pmod p$.

$\diamond$ **9.22** Prove that the Frobenius mapping (see 9.18c)) $\Phi : \mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$ is an isomorphism.

$\diamond$ **9.23** Let $P(x)$ be a degree n irreducible polynomial in $\mathbb{F}_p[x]$. Let $\mathbb{F}_p[\alpha]=\mathbb{F}_p[x]/(P(x))$ be the field obtained from $\mathbb{F}_p$ by adjoining a root α of the irreducible polynomial $P(x)$. Prove that $\mathbb{F}_p[\alpha]\cong\mathbb{F}_{p^n}$. Prove that $P(x)$ has exactly n roots in $\mathbb{F}_p[\alpha]$ and that those roots are: $\alpha,\Phi(\alpha),\Phi^2(\alpha),\dots,\Phi^{n-1}(\alpha)$. ($\Phi$ is the Frobenius mapping, see 9.18c).)

$\diamond$ **9.24** Give an example of (an infinite) characteristic p field K such that the Frobenius mapping is not surjective.

$\diamond$ **9.25** Prove that $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \Leftrightarrow m \mid n$. Hint:

(1) "$\Rightarrow$": $\mathbb{F}_{p^n}$ is a r-dimensional vector space over $\mathbb{F}_{p^m}$, therefore $|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^r$

(2) "$\Leftarrow$": Prove that if $m \mid n$ then $x^{p^m-1} - 1 \mid x^{p^n-1} - 1$, therefore the equation $x^{p^m} - x = 0$ has exactly p^m roots in $\mathbb{F}_{p^n}$.

$\diamond$ **9.26** Prove that $\mathbb{F}_{p^m} = \{a \in \mathbb{F}_{p^{rm}}, \quad \Phi^m(a) = a\} \subset \mathbb{F}_{p^{rm}}$

$\diamond$ **9.27** Let $a \in \mathbb{F}_{p^n}$ be a generator of the cyclic group $\mathbb{F}^*_{p^n}$. Prove that $\mathbb{F}_{p^n} = \mathbb{F}_p[a]$ and therefore the minimal polynomial of a is an irreducible degree n polynomial in $\mathbb{F}_p[x]$. Thus $\forall n > 1$ irreducible degree n polynomials in $\mathbb{F}_p[x]$ exist.

$\diamond$ **9.28** Let $a \in \mathbb{F}_{p^n}$, let $P_a(x)$ be the minimal polynomial of a. Prove that $P_a(x) \mid x^{p^n} - x$ and $\deg P_a(x) \mid n$.

$\diamond$ **9.29** Let $P(x)$ be a degree n irreducible polynomial in $\mathbb{F}_p[x]$. Prove that $P(x) \mid x^{p^n} - x$.

$\diamond$ **9.30** Prove that

$$x^{p^n} - x = \prod_{\substack{\text{All irreducible} \\ \text{polynomials} \\ P(x) \in \mathbb{F}_p[x], \\ \deg P(x) \mid n}} P(x)$$

and

$$\left(x^{p^n} - x\right) / \left(\mathrm{LCM}_{m|n}(x^{p^m} - x)\right) = \prod_{\substack{\text{All irreducible} \\ \text{polynomials} \\ P(x) \in \mathbb{F}_p[x], \\ \deg P(x) = n}} P(x)$$

$\diamond$ **9.31** Use 9.30 to list all irreducible polynomials of degree 2, 3 and 4 over $\mathbb{F}_2$ and of degree 2 and 3 over $\mathbb{F}_3$.

$\diamond$ **9.32** Prove that $P(x) = x^4 + x + 1$ is irreducible over $\mathbb{F}_2$. Let α be a root of $P(x)$ in $\mathbb{F}_{16}$. Find the order of α as an element of $\mathbb{F}^*_{16}$. Find the other three roots of $P(x)$. List all the four elements of $\mathbb{F}_4 \subset \mathbb{F}_{16}$. Find the four elements of order 5 in $\mathbb{F}^*_{16}$ and their minimal polynomial. (Hint: all the elements of $\mathbb{F}_{16}$ may be expressed explicitly as $a + b\alpha + c\alpha^2 + d\alpha^3$ where $a, b, c, d \in \mathbb{F}_2$. $\mathbb{F}_{16}$ is four-dimensional vector space over $\mathbb{F}_2$ with the basis $1, \alpha, \alpha^2, \alpha^3$; the Frobenius mapping is a linear operator whose matrix can be easily written. Then use 9.23 and 9.26 .)