

Algebra 3

Exercises for Chapters II-V

Some exercises are particularly recommended. They are marked by a *.

Exercise (2.1)*: Solve Exercises 2.1 and 2.6 in Chapter II of the notes.

Exercise (2.2): Discuss the Examples 2.9 and 2.18 in the notes in detail.

Exercise (2.3): Let $\varphi : R \rightarrow R^*$ be a ring homomorphism and $\Phi : R[x] \rightarrow R^*[x]$ the corresponding homomorphism between the polynomial rings. Discuss the relation between the kernels of φ and Φ . Consider especially the case $R = \mathbb{Z}$, $R^* = \mathbb{Z}_p$, p a prime.

Exercise (2.4): Suppose that $k \in \mathbb{Z}$. For which values of k is the polynomial $x^2 - k \in \mathbb{Q}[x]$ irreducible in $\mathbb{Q}[x]$?

Exercise (2.5)*: Prove that the polynomials $x^n - a$, $n \in \mathbb{N}$, $a \in \mathbb{Z}$ are irreducible in $\mathbb{Q}[x]$, if there exists a prime number p such that p but not p^2 divides a .

Exercise (2.6): Show that the polynomials $x^4 - 4x^3 + 6$ and $x^4 + 4x^3 + 6x^2 + 2x + 1$ in $\mathbb{Q}[x]$ are irreducible. (In the second polynomial you may try to substitute $x - 1$ for x . Why is this allowed?)

Exercise (2.7)*: Investigate whether the polynomial $x^3 + 4$ is reducible or irreducible in $\mathbb{Q}[x]$. The same question for $x^4 + 4$.

Exercise (2.8)*: Let R be an integral domain. Let $f(x) \in R[x]$ be a monic polynomial of degree 2 or 3. Show that $f(x)$ is irreducible in $R[x]$ if and only if $f(r) \neq 0$ for all $r \in R$.

Exercise (2.9)*: If p is a prime, let \mathbb{Z}_p be the field with p elements.

(1) Explain why the number of polynomials of a given degree n in $\mathbb{Z}_p[x]$ is finite.

(2) Write down explicitly a list of monic irreducible polynomials of degree 2 and 3 in $\mathbb{Z}_p[x]$, in the cases where $p = 2$ or $p = 3$.

Exercise (2.10): Let a_1, \dots, a_n be n distinct integers. Show that $f(x) = \prod_{i=1}^n (x - a_i) - 1$ is irreducible in $\mathbb{Q}[x]$. (This is Exercise 2.40 in the lecture notes.) (Hint: Assume $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are monic polynomials in $\mathbb{Z}[x]$ of degree $< n$. Consider $g(a_i) + h(a_i)$ for $i = 1, \dots, n$.)

Exercise (2.11): Let a_1, \dots, a_n be n distinct integers. Show that $f(x) = \prod_{i=1}^n (x - a_i)^2 + 1$ is irreducible in $\mathbb{Q}[x]$. (Hint: The proof is similar to that of the previous exercise, but a little harder.)

Exercise (2.12): Is $x^4 - 10x^2 + 1$ reducible or irreducible in $\mathbb{Q}[x]$?

Exercise (2.13): Show that $x^n + 5x^{n-1} + 3$ is irreducible in $\mathbb{Z}[x]$ (and thereby also in $\mathbb{Q}[x]$) for every natural number $n > 1$. (This problem, which is not easy, was posed at the international mathematics olympiad in July 1993.)

Exercise (2.14)*: The field $\mathbb{Q}(\sqrt{2})$ consists of all numbers on the form $q_0 + q_1\sqrt{2}$, where q_0 and q_1 are rational numbers. Thus $1/(4 + 3\sqrt{2})$ lies in $\mathbb{Q}(\sqrt{2})$. Find rational numbers q_0 and q_1 , such that $1/(4 + 3\sqrt{2}) = q_0 + q_1\sqrt{2}$.

Exercise (2.15): The field $\mathbb{Q}(\sqrt[3]{2})$ consists of all numbers of the form $q_0 + q_1\sqrt[3]{2} + q_2(\sqrt[3]{2})^2$, where q_0, q_1 and q_2 are rational numbers. Thus $\alpha := 1/(2 + \sqrt[3]{2} - \sqrt[3]{4})$ lies in $\mathbb{Q}(\sqrt[3]{2})$. Find rational numbers q_0, q_1 and q_2 , such that $\alpha = q_0 + q_1\sqrt[3]{2} + q_2(\sqrt[3]{2})^2$.

Exercise (2.16)*: Let $L \supset K$ be fields and α and β elements in L that are algebraic over K . Assume that the degree of α over K is m and the degree of β over K is n . Thus $[K(\alpha) : K] = m$ and $[K(\beta) : K] = n$.

- (1) Show that $[K(\alpha, \beta) : K] \leq m \cdot n$.
- (2) Show that $[K(\alpha, \beta) : K]$ is divisible by m and by n .
- (3) Show that $[K(\alpha, \beta) : K] = m \cdot n$ if m and n are relatively prime.

Exercise (2.17): Let α and β be complex numbers that are algebraic over \mathbb{Q} of degree p resp. q , where p and q are distinct prime numbers. Show that $\alpha + \beta$ is algebraic over \mathbb{Q} of degree $p \cdot q$. (Hint: Use the previous exercise and prove by way of contradiction that the degree of $\alpha + \beta$ cannot be 1, p or q .)

Exercise (2.18)*: Let α be an algebraic number. Prove that $\mathbb{Q}(q_0 + q_1\alpha) = \mathbb{Q}(\alpha)$ for all rational numbers q_0 and q_1 , ($q_1 \neq 0$). In particular, the degree of α with respect to \mathbb{Q} is equal to the degree of $q_0 + q_1\alpha$ with respect to \mathbb{Q} .

Exercise (2.19)*: Let a and b be non-zero elements in a field K of characteristic 0.

- (1) Prove that $K(\sqrt{a}) = K(\sqrt{b})$ if and only if $a \cdot b$ is the square of an element in K .
- (2) Find $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.
- (3) Is $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Exercise (2.20): Let p be a prime number and $\alpha = \sqrt[p]{2}$. Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^t)$ for every integer t , $1 \leq t \leq p - 1$.

Exercise (2.21)*: Let p be a prime number and $\varepsilon := e^{\frac{2\pi i}{p}}$ a p -th root of unity. Prove that $\mathbb{Q}(\varepsilon)$ is the splitting field of the polynomial $x^p - 1$ over \mathbb{Q} . Show that $\text{Irr}(\varepsilon, \mathbb{Q}) = x^{p-1} + \cdots + x + 1$. Determine $[\mathbb{Q}(\varepsilon) : \mathbb{Q}]$. (Hint: Use for instance Example 2.34 in the notes.)

Exercise (2.22)*: Prove that $\mathbb{Q}(\sqrt[p]{2}, e^{\frac{2\pi i}{p}})$ is the splitting field of $x^p - 2$ over \mathbb{Q} . Determine the dimension over \mathbb{Q} of this splitting field. (Hint: Use the previous exercise and Exercise (5.1).)

Exercise (2.23): Can it happen that the difference between two distinct roots of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ is rational?

(*Hint:* Consider what happens when $f(x)$ and $f(x+q)$ have a common root for some $q \in \mathbb{Q}$.)

Can it happen that the sum of two distinct roots of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ is rational?

Exercise (2.24): Prove that the polynomial $f(x) = x^3 - x^2 + 1$ is irreducible over \mathbb{Q} and let α be a root of $f(x)$.

Find $[\mathbb{Q}(\sqrt{2}, \alpha) : \mathbb{Q}]$ and show that $\mathbb{Q}(\sqrt{2}, \alpha) = \mathbb{Q}(\alpha\sqrt{2})$.

[Prove and use, that $\alpha = -\alpha^4 + \alpha^2 - 1 \in \mathbb{Q}(\alpha\sqrt{2})$.]

Is $\mathbb{Q}(\sqrt{2}, \alpha) = \mathbb{Q}(\sqrt{2} + \alpha)$?

Exercise (2.25)*: Determine the splitting fields (viewed as subfields of the complex number field) over \mathbb{Q} for each of the following polynomials $x^4 + 4$, $x^8 - 2$, $x^4 - 10$, $x^3 - 2$ and $x^3 - 4$ and find the dimension of the splitting fields over \mathbb{Q} .

Exercise (2.26)*: Determine $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$. Prove that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

Let $\varepsilon = e^{\frac{2\pi i}{3}} = (-1 + i\sqrt{3})/2$.

Determine $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt[3]{2}\varepsilon) : \mathbb{Q}]$ and $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\varepsilon) : \mathbb{Q}]$.

Exercise (2.27): Let $f(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$ of the form $f(x) = x^4 + ax^2 + b$, a and b rational numbers. Let M be the splitting field of $f(x)$ over \mathbb{Q} . Prove that $[M : \mathbb{Q}]$ is 4 or 8. (Notice that $f(\alpha) = 0 \Rightarrow f(-\alpha) = 0$.)

Let M_1 , resp. M_2 be the splitting field of

$$f_1(x) = x^4 - 4x^2 + 2, \quad \text{resp.} \quad f_2(x) = x^4 - 10x^2 + 1.$$

Find $[M_1 : \mathbb{Q}]$ and $[M_2 : \mathbb{Q}]$.

Exercise (2.28): Considering the “Comforting remark” on page 2.21 does there exist a field K such that $\mathbb{C} \subset K$ and such that $[K : \mathbb{C}] \neq 1$ is finite?

Exercise (2.29)*: Let M_1, M_2, M_3 and M_4 be the splitting fields of $x^4 - 2, x^4 + 2, x^3 - 3, x^3 + 3$.

Find $[M_1 : \mathbb{Q}], [M_2 : \mathbb{Q}], [M_3 : \mathbb{Q}]$ and $[M_4 : \mathbb{Q}]$.

Exercise (2.30): Let $P(x), Q(x), R(x)$ and $S(x)$ be polynomials with real coefficients such that

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (1 + x + x^2 + x^3 + x^4)S(x).$$

Prove that $x - 1$ divides $P(x)$. (This problem was posed at a mathematics olympiad in USA in 1993.)

Exercise (2.31): Let $L = \mathbb{R}(x)$ be the field of rational functions over \mathbb{R} . Thus the elements of L are quotients $\frac{f(x)}{g(x)}$ where f and g are real polynomials and $g \neq 0$. (See the Example 3.10 in the notes.)

(1) Show that the map τ defined by

$$\tau\left(\frac{f(x)}{g(x)}\right) = \frac{f(-x)}{g(-x)}$$

generates a subgroup H of order 2 in $\text{Aut}(L/\mathbb{R})$.

(2) Determine the subfield $\mathcal{F}(H)$ of L .

Exercise (2.32): Find $\text{Aut}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$.

Is $\mathbb{Q}(\sqrt[4]{2})$ a normal extension of \mathbb{Q} ?

Remark: This exercise is related to the example 3.44 in the notes.

Exercise (2.33)*: Let $f(x) = x^4 + ax^2 + 1$ be an irreducible polynomial in $\mathbb{Q}[x]$. Let α be a root of $f(x)$.

(1) Prove that all the roots of $f(x)$ are $\alpha, -\alpha, 1/\alpha$ and $-1/\alpha$.

(2) Prove that the splitting field M of f over \mathbb{Q} is a normal extension of \mathbb{Q} and find the Galois group $\text{Gal}(M/\mathbb{Q})$.

Exercise (2.34)*: Let M be the splitting field over \mathbb{Q} for $x^3 - 2$.

(1) Prove that M/\mathbb{Q} is a normal extension.

(2) Determine the Galois group G for M over \mathbb{Q} .

(3) Find all subfields of M and the corresponding subgroups of G .

Exercise (2.35)*: Let M be the splitting field over \mathbb{Q} for $x^6 - 2$.

- (1) Find $[M : \mathbb{Q}]$.
- (2) Show that M/\mathbb{Q} is a normal extension.
- (3) Determine the Galois group G for M over \mathbb{Q} .
- (4) Decide if G is abelian or not.
- (5) Decide if G is solvable or not.

Exercise (2.36): Let M be the splitting field over \mathbb{Q} for $x^8 - 2$.

- (1) Find $[M : \mathbb{Q}]$.
- (2) Show that M/\mathbb{Q} is a normal extension.
- (3) Decide if Galois group G for M over \mathbb{Q} is abelian or not.
- (4) Decide if G is solvable or not.

Exercise (2.37)*: Let $f(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$ of degree n and let M be the splitting field of $f(x)$ over \mathbb{Q} .

Show that $[M : \mathbb{Q}] = n$ if the Galois group $\text{Gal}(M/\mathbb{Q})$ is abelian. (Notice that $\text{Gal}(M/\mathbb{Q})$ is abelian implies that every subgroup of $\text{Gal}(M/\mathbb{Q})$ is normal.)

Can the above statement be reversed? In other words, can it happen that $[M : \mathbb{Q}] = n$ but $\text{Gal}(M/\mathbb{Q})$ is not abelian?

Exercise (2.38): Let M/K be a finite normal extension.

Prove that an element $\alpha \in M$ is a primitive element for M/K if and only if $\sigma(\alpha) \neq \alpha$ for every $\sigma \in \text{Gal}(M/K)$, σ not the identity automorphism of M/K .

Exercise (2.39): Let M/K be a finite normal extension with Galois group G .

Prove that M is the splitting field over K for some irreducible polynomial in $K[x]$ of degree n if and only if there exists a subgroup H in G of index n and such that no subgroup (except $\{e\}$) in H is a normal subgroup of G .

Exercise (2.40): Solve Exercise 3.35 - 3.37 in the notes.

Exercise (2.41): Let M/K be a finite normal extension with Galois group G . Let L be an intermediate field between K and M . Let H be the subgroup of G consisting of those automorphisms σ in G for which $\sigma(L) = L$. Prove that H is the normalizer of $T(L)$ in G .

Exercise (2.42): Discuss Example 3.50 and Exercise 3.51 in the notes.

Exercise (2.43): Let M be the splitting field over \mathbb{Q} for the polynomial $x^4 - 10x^2 + 20$. Show that M/\mathbb{Q} is a normal extension and determine the Galois group $\text{Gal}(M/\mathbb{Q})$.

Exercise (2.44)*: Let M_1 be the splitting field over \mathbb{Q} for $x^4 - 3$ and M_2 the splitting field over \mathbb{Q} for $x^4 + 3$.

(1) Show that M_1 is a normal extension over \mathbb{Q} and determine the Galois group $\text{Gal}(M_1/\mathbb{Q})$. Find all subfields of M_1 whose dimension over \mathbb{Q} is 2.

(2) Show that M_2 is a normal extension of \mathbb{Q} containing $\mathbb{Q}(i)$ and prove that $x^4 + 3$ is irreducible over $\mathbb{Q}(i)$.

(3) Find the dimension $[M_2 : \mathbb{Q}]$ and the Galois group $\text{Gal}(M_2/\mathbb{Q})$.

(4) Find all subfields of M_2 whose dimension over \mathbb{Q} is 2.

(5) Find the dimension of $M_1 \cap M_2$ over \mathbb{Q} and the dimension of the compositum M_1M_2 over \mathbb{Q} .

(6) Show that there exists a rational number a , such that $M_1M_2 = M_1(\sqrt{a})$ and use this to determine the Galois group $\text{Gal}(M_1M_2/\mathbb{Q})$.

Exercise (2.45)*: Let $f(x)$ be an irreducible polynomial in $\mathbb{Q}[x]$ of degree n . Assume that the number r of real roots of $f(x)$ satisfies $0 < r < n$. Let M be the splitting field for $f(x)$ over \mathbb{Q} (viewed as a subfield of the complex number field \mathbb{C}). Show that $L = M \cap \mathbb{R}$ is a non-normal extension of \mathbb{Q} and that $[L : \mathbb{Q}] \geq n$.

(1) Show that $[M : \mathbb{Q}] \geq 2n$.

Now let $f(x)$ be $x^4 - 2x^3 - 2x + 1$.

(2) Show that $f(x) = x^4 - 2x^3 - 2x + 1$ is irreducible over \mathbb{Q} (consider $f(x+1)$).

(3) Show that $f(x)$ has exactly 2 real roots.

(4) Let M be the splitting field for $f(x)$ over \mathbb{Q} . Find $[M : \mathbb{Q}]$ and $\text{Gal}(M/\mathbb{Q})$. (Hint: Observe that a number α is a root of $f(x)$ if and only if $1/\alpha$ is a root of $f(x)$. Hence the roots of $f(x)$ have the form $\alpha, 1/\alpha, \beta, 1/\beta$ for suitable numbers α and β .)

Exercise (2.46)*: Let M/\mathbb{Q} be a normal extension whose Galois group is cyclic of order 4. Show that M cannot contain $i = \sqrt{-1}$. (Notice that a cyclic group of order 4 has exactly one element of order 2 and complex conjugation is an automorphism of order 2.)

Exercise (2.47): Let K/\mathbb{Q} be a finite extension.

(1) Show that K contains only finitely many roots of unity. (Hint: It can be shown that $\varphi(n) \geq \sqrt{n}/2$, where φ is Euler's function.)

(2) Suppose n is odd and that K contains a primitive n 'th root of unity. Show that K contains also a primitive $(2n)$ 'th root of unity.

Exercise (2.48): Let $F_n(x)$ be the n 'th cyclotomic polynomial. Show that if $n > 1$ is *odd* then $F_{2n}(x) = F_n(-x)$.

Exercise (2.49): For $n \in \mathbb{N}$ let M_n be the splitting field for the polynomial $x^n + 1$ over \mathbb{Q} . Determine the Galois group $\text{Gal}(M_n/\mathbb{Q})$.

Exercise (2.50): Are the Galois groups of the following extensions isomorphic?

- (1) \mathbb{Q}_5/\mathbb{Q} and \mathbb{Q}_8/\mathbb{Q} .
- (2) $\mathbb{Q}_{20}/\mathbb{Q}$ and $\mathbb{Q}_{16}/\mathbb{Q}$.

Exercise (2.51): Let M be the splitting field over \mathbb{Q} for the polynomial $x^4 + 5x^2 + 5$. Investigate whether $M = \mathbb{Q}_5$, the fifth cyclotomic field.

Exercise (2.52): Let ε_{17} be a primitive 17-th root of unity. Let

$$M = \mathbb{Q}(\varepsilon_{17} + \varepsilon_{17}^{-1}).$$

Show that M/\mathbb{Q} is normal and determine $\text{Gal}(M/\mathbb{Q})$.