16.1 Problem Sheet: Navigation

1. Why should the symbols $\subset$, $\forall$, $\exists$ be banned? What should they be replaced by?
2. Why should the phrase "Let $a > 7$" be banned? What should it be replaced by?
3. What does the symbol $\mapsto$ mean and how should it be used?
4. What comes at the end of a sentence? and at the end of an equation that ends a sentence?
5. Why should the phrases 'for all', 'for every', 'for each', and 'for some' be banned? What should they be replaced by?
6. Why is it bad style to start a sentence with a mathematical symbol? What should be written instead?
7. Why do we never use a comma in place of the word 'then' in mathematical writing?
8. What are the symbols for "subset of", "proper subset of"? "element of" and "equal"?
9. What is the form of a mathematical definition (for a noun)?
10. What is the form of a mathematical definition (for an adjective)?
11. What is the definition of equal sets?
12. What is the defnition of equal functions?
13. What is the definition of a function?
14. What is Proof type I? How does proof type I proceed?
15. What is proof type II? How does proof type II proceed?
16. What is proof type III? How does proof type III proceed?
17. What is proof by contrapositive? How does a proof by contrapositive proceed?
18. How do proofs of uniqueness proceed?
19. What is the underlying source of proof by induction? How does proof by induction proceed?
20. Why should proof by contradiction be banned? What should it be replaced by?
21. What is the structure of a universal property? What property 'in English' is a universal property capturing? Give an explicit example of something that is defined by a universal property and state the definition carefully and completely.
22. What property is "there exists" capturing? What property is "there exists a unique" capturing?
23. Prove that if $x^2 < y^2$ then $x < y$. (Correct the statement as necessary before proving it.)
24. Prove that if a^2 is divisible by 2 then a^2 is divisible by 4. (Correct the statement as necessary before proving it.)
25. Prove that a function is invertible if and only if it is bijective. (Correct the statement as necessary before proving it.)

26. When is it appropriate to use the symbols $\Longrightarrow$, $\Longleftrightarrow$, $\longrightarrow$ and when is it not? When they should not be used, what should they be replaced by?
27. Carefully define a field.
28. Carefully define a vector space.
29. Carefully define $\mathrm{span}(S)$.
30. Carefully define linearly independent.
31. Carefully define basis.
32. Carefully define $\mathbb{Q}$ and prove that it is a field.
33. Carefully define $\mathbb{C}$ and prove that it is a field.
34. Let $m \in \mathbb{Z}_{>0}$. Carefully define $\mathbb{Z}/m\mathbb{Z}$.
35. Let $p \in \mathbb{Z}_{>0}$. Show that $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime.
36. Show that $3 \cdot 6 = 1 \cdot 6$ in $\mathbb{Z}/12\mathbb{Z}$.
37. Let $m \in \mathbb{Z}_{>1}$. Show that if m is not prime then there exist $a, b, c \in \mathbb{Z}/m\mathbb{Z}$ such that $ac = bc$ and $c \neq 0$ and $a \neq b$.
38. Let $\mathbb{F}$ be a field. Show that if $a, b, c \in \mathbb{F}$ and $ac = bc$ and $c \neq 0$ then $a = b$.
39. Show that if $a, b, c \in \mathbb{Z}$ and $ac = bc$ and $c \neq 0$ then $a = b$.
40. Carefully define $\mathbb{R}[x]$ and determine which of the axioms of a field it satisfies and which axioms of a field it does not satisfy.
41. Show that if $a, b, c \in \mathbb{R}[x]$ and $ac = bc$ and $c \neq 0$ then $a = b$.
42. Show that the $\mathbb{R}$-subspace of $\mathbb{C}$ with $\mathbb{R}$-basis $\{1, i\}$ is a field.
43. Show that the $\mathbb{Q}$-subspace of $\mathbb{C}$ with $\mathbb{Q}$-basis $\{1, i\}$ is a field.
44. Let $2^{1/3} \in \mathbb{R}_{\geq 0}$. Show that the $\mathbb{Q}$-subspace of $\mathbb{C}$ with $\mathbb{Q}$-basis $\{1, 2^{1/3}, 2^{2/3}\}$ is a field.
45. Let $\zeta = e^{2\pi i/3}$. Show that $\zeta^2 = -1 - \zeta$ and that the $\mathbb{Q}$-subspace of $\mathbb{C}$ with $\mathbb{Q}$-basis $\{1, \zeta, \}$ is a field.
46. Let $\zeta = e^{2\pi i/3}$. Show that $\zeta^2 = -1 - \zeta$ and that the $\mathbb{R}$-subspace of $\mathbb{C}$ with $\mathbb{R}$-basis $\{1, \zeta\}$ is a field.
47. Let $2^{1/3} \in \mathbb{R}_{\geq 0}$ and $\zeta = e^{2\pi i/3}$. Show that the $\mathbb{Q}$-subspace of $\mathbb{C}$ with $\mathbb{Q}$-basis $\{1, \zeta, 2^{1/3}, 2^{1/3}\zeta, 2^{2/3}, 2^{2/3}\zeta\}$ is a field.
48. Let $2^{1/3} \in \mathbb{R}_{\geq 0}$ and $\zeta = e^{2\pi i/3}$. Find a $\mathbb{Q}$-basis of the smallest field contained in $\mathbb{C}$ that contains $\mathbb{Q}$ and $2^{\frac{1}{3}}\zeta$.
49. Carefully define the following
    (a) group
    (b) abeliangroup

   (c) ring
   (d) $\mathbb{Z}$-algebra
   (d) $\mathbb{F}$-algebra
   (d) R-algebra
   (e) commutativering
   (f) field

50. Carefully define the following
   (a) G-set
   (b) $\mathbb{Z}$-module
   (c) R-module
   (d) $\mathbb{F}$-module
   (e) $\mathbb{F}$-vector space

51. Carefully define the following
   (a) subgroup
   (b) subabeliangroup
   (c) subring
   (d) $\mathbb{Z}$-subalgebra
   (d) $\mathbb{F}$-subalgebra
   (d) R-subalgebra
   (e) subcommutativering
   (f) subfield

52. Carefully define the following
   (a) sub G-set
   (b) $\mathbb{Z}$-submodule
   (c) R-submodule
   (d) $\mathbb{F}$-submodule
   (e) $\mathbb{F}$-subspace

53. Carefully define the following
   (a) group morphism
   (b) abeliangroup morphism
   (c) ring morphism
   (d) $\mathbb{Z}$-algebra morphism
   (d) $\mathbb{F}$-algebra morphism
   (d) R-algebra morphism
   (e) commutativering morphism
   (f) field morphism

54. Carefully define the following

   (a) G-set morphism
   (b) $\mathbb{Z}$-module morphism
   (c) R-module morphism
   (d) $\mathbb{F}$-module morphism
   (e) $\mathbb{F}$-linear transformation

55. Carefully define the following

(a) group isomorphism
(b) abeliangroup isomorphism
(c) ring isomorphism
(d) $\mathbb{Z}$-algebra isomorphism
(d) $\mathbb{F}$-algebra isomorphism
(d) R-algebra isomorphism
(e) commutativering isomorphism
(f) field isomorphism

56. Carefully define the following
    (a) G-set isomorphism
    (b) $\mathbb{Z}$-module isomorphism
    (c) R-module isomorphism
    (d) $\mathbb{F}$-module isomorphism
    (e) $\mathbb{F}$-vector space isomorpihsm

57. Carefully define the following
    (a) group automorphism
    (b) abeliangroup automorphism
    (c) ring automorphism
    (d) $\mathbb{Z}$-algebra automorphism
    (d) $\mathbb{F}$-algebra automorphism
    (d) R-algebra automorphism
    (e) commutativering automorphism
    (f) field automorphism

58. Carefully define the following
    (a) G-set automorphism
    (b) $\mathbb{Z}$-module automorphism
    (c) R-module automorphism
    (d) $\mathbb{F}$-module automorphism
    (e) $\mathbb{F}$-vector space automorpihsm

59. Carefully define the following
    (a) kernel and image of a group morphism
    (b) kernel and image of an abeliangroup morphism
    (c) kernel and image of a ring morphism
    (d) kernel and image of a $\mathbb{Z}$-algebra morphism
    (d) kernel and image of a $\mathbb{F}$-algebra morphism
    (d) kernel and image of a R-algebra morphism
    (e) kernel and image of a commutativering morphism
    (f) kernel and image of a field morphism

60. (a) Let G be a group and let K be a subgroup of G. Show that

$$K \text{ is a normal subgroup of } G \qquad \text{if and only if} \qquad \begin{matrix}\text{there exists a group morphism} \\ \varphi\colon G \to H \text{ such that } \ker\varphi = K.\end{matrix}$$

    (b) Let R be a ring and let I be a subabeliangroup of R. Show that

$$I \text{ is an ideal of } R \qquad \text{if and only if} \qquad \begin{matrix}\text{there exists a ring morphism} \\ \varphi\colon R \to S \text{ such that } \ker\varphi = I.\end{matrix}$$

(b) Let A be an R-algebra and let B be an R-submodule of A. Show that

$$B \text{ is an ideal of } A \qquad \text{if and only if} \qquad \begin{matrix}\text{there exists an } R\text{-algebra morphism} \\ \varphi\colon A \to C \text{ such that } \ker(\varphi) = B.\end{matrix}$$

(c) Let M be an R-module and let N be an R-submodule of M. Show that

$$N \text{ is an } R\text{-submodule of } M \qquad \text{if and only if} \qquad \begin{matrix}\text{there exists an } R\text{-module morphism} \\ \varphi\colon M \to P \quad \text{such that} \quad \ker(\varphi) = N.\end{matrix}$$

(d) Let V be an $\mathbb{F}$-vector space and let W be an $\mathbb{F}$-subspace of V. Show that

$$W \text{ is an } \mathbb{F}\text{-subspace of } V \qquad \text{if and only if} \qquad \begin{matrix}\text{there exists an } \mathbb{F}\text{-linear transformation} \\ \varphi\colon V \to P \quad \text{such that} \quad \ker(\varphi) = W.\end{matrix}$$

61. (a) Let $\varphi\colon G \to H$ be a group morphism. Show that

$$\frac{G}{\ker(\varphi)} \cong \mathrm{im}(\varphi) \qquad \text{as groups.}$$

(b) Let $\varphi\colon R \to S$ be a ring morphism. Show that

$$\frac{R}{\ker(\varphi)} \cong \mathrm{im}(\varphi) \qquad \text{as rings.}$$

(c) Let $\varphi\colon A \to B$ be an R-algebra morphism. Show that

$$\frac{A}{\ker(\varphi)} \cong \mathrm{im}(\varphi) \qquad \text{as } R\text{-algebras.}$$

(d) Let $\varphi\colon M \to N$ be an R-module morphism. Show that

$$\frac{M}{\ker(\varphi)} \cong \mathrm{im}(\varphi) \qquad \text{as } R\text{-modules.}$$

(e) Let $\varphi\colon V \to V$ be an $\mathbb{F}$-linear transformation. Show that

$$\frac{V}{\ker(\varphi)} \cong \mathrm{im}(\varphi) \qquad \text{as } \mathbb{F}\text{-vector spaces.}$$

62. (a) Let $\varphi\colon G \to H$ be a group morphism. Show that $\ker\varphi$ is a normal subgroup of G.
(b) Give an example of a group morphism $\varphi\colon G \to H$ such that $\mathrm{im}(\varphi)$ is a subgroup of H.
(c) Give an example of a group morphism $\varphi\colon G \to H$ such that $\mathrm{im}(\varphi)$ is not a subgroup of H.
(d) Let $\varphi\colon G \to H$ be a ring morphism. Explain how to use φ to make H into a G-set and show that $\mathrm{im}(\varphi)$ is an G-subset of H.

63. (a) Let $\varphi\colon R \to S$ be a ring morphism. Show that $\ker\varphi$ is an ideal of R.
(b) Give an example of a ring morphism $\varphi\colon R \to S$ such that $\mathrm{im}(\varphi)$ is an S-submodule of S.
(c) Give an example of a ring morphism $\varphi\colon R \to S$ such that $\mathrm{im}(\varphi)$ is not an S-submodule S.
(d) Let $\varphi\colon R \to S$ be a ring morphism. Explain how to use φ to make S into an R-module and show that $\mathrm{im}(\varphi)$ is an R-submodule of S.

64. Let R be a ring.

(a) Let $\varphi\colon A \to B$ be an R-algebra morphism. Show that $\ker\varphi$ is an ideal of A.
(b) Give an example of an R-algebra morphism $\varphi\colon A \to B$ such that $\mathrm{im}(\varphi)$ is a B-submodule of B.
(c) Give an example of a R-algebra morphism $\varphi\colon A \to B$ such that $\mathrm{im}(\varphi)$ is not an B-submodule B.
(d) Let $\varphi\colon A \to B$ be an R-algebra morphism. Explain how to use φ to make B into an A-module and show that $\mathrm{im}(\varphi)$ is an A-submodule of B.

65. Let $\mathbb{F}$ be a field. Show that an $\mathbb{F}$-vector space is the same thing as an $\mathbb{F}$-module.

66. Show that a ring is the same thing as a $\mathbb{Z}$-algebra.

67. Show that an abeliangroup is the same thing as a $\mathbb{Z}$-module.

68. Let R be a ring. Explain how R is an R-module. Show that an ideal of R is the same thing as an R-submodule of R.

69. Let A be an R-algebra. Explain how A is an A-module. Show that an ideal of A is the same thing as an A-submodule of A.

70. (a) Let G be a group. Show that a subgroup of G is the same as an injective group morphism $\varphi\colon H \to G$.
(b) Let R be a ring. Show that a subring of R is the same as an injective ring morphism $\varphi\colon S \to R$.
(c) Let A be an R-algebra. Show that an R-subalgebra A is the same as an injective R-algebra morphism $\varphi\colon C \to A$.
(d) Let $\mathbb{K}$ be a field. Show that a subfield of $\mathbb{K}$ is the same as an injective field morphism $\varphi\colon \mathbb{F} \to \mathbb{K}$.
(e) Let R be a ring and let M be an R-module. Show that an R-submodule of M is the same as an injective R-module morphism $\varphi\colon N \to M$.
(f) Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. Show that an $\mathbb{F}$-subspace of V is the same as an injective $\mathbb{F}$-linear transformation $\varphi\colon W \to V$.

71. Show that the symmetric group S_n is presented by generators $s_1, \ldots, s_{n-1}$ and relations

$$s_j^2 = 1, \qquad s_k s_\ell = s_\ell s_k, \qquad s_i, s_{i+1} s_i = s_{i+1} s_i s_{i+1},$$

for $j \in \{1, \ldots, n-1\}$, $j, k \in \{1, \ldots n-1$ with $k \notin \{k+1, k-1\}$ and $i \in \{1, \ldots, n-2\}$.

72. Show that the dihedral group D_n is presented by generators s, r with relations

$$s^2 = 1, \qquad r^n = 1, \qquad sr = r^{-1}s.$$

73. Show that the cyclic group μ_n is presented by a single generator ζ with relation $\zeta^n = 1$.

74. Show that the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is presented by a single generator 1 with relation $n = 0$.

75. Show that the dihedral group D_n is presented by generators s_1, s_2 with

$$s_1^2 = 1, \qquad s_2^2 = 1, \qquad (s_1 s_2)^n = 1.$$

76. Carefully define permutation matrix. Show that the symmetric group S_n is (isomorphic to) the group of $n \times n$ permutation matrices.

77. Carefully define cyclic matrix. Show that the cyclic group μ_n is (isomorphic to) the group of $n \times n$ cyclic matrices.

78. Carefully define dihedral matrices. Show that the dihedral group D_n is (isomorphic to) the group of $n \times n$ dihedral matrices.

79. Show that the symmetric group S_n is (isomorphic to) $\mathrm{Aut}(\{1, \ldots, n\})$.

80. Determine the subgroup lattice of $\mathbb{Z}/2\mathbb{Z}$.

81. Determine the subgroup lattice of $\mathbb{Z}/3\mathbb{Z}$.

82. Determine the subgroup lattice of $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

83. Determine the subgroup lattice of $\mathbb{Z}/5\mathbb{Z}$.

84. Show that $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

85. Determine the subgroup lattice of $\mathbb{Z}/6\mathbb{Z}$.

86. Show that $S_3 \cong D_3$.

87. Carefully define the quaternion group and determine its subgroup lattice.

88. Show that $\mathbb{C}$ is the $\mathbb{R}$-algebra presented by a single generator i and the relation $i^2 = 1$.

89. Show that $\mathbb{R}[x]$ is the $\mathbb{R}$-algebra presented by a single generator x (and no relations).

90. Show that $\mathbb{Z}$ is the group generated by single generator 1 (and no relations).

91. Show that $\mathbb{R}[x, x^{-1}]$ is the $\mathbb{R}$-algebra presented by a generators x, y with relation $xy = 1$.

92. Show that $\mathbb{F}_4$ is the $\mathbb{F}_2$-algebra presented by a single generator τ with relation $\tau^2 + \tau + 1 = 0$.

93. Let I be an ideal of $\mathbb{Z}$. Let $m \in \mathbb{Z}_{>0}$ be minimal such that $m \in I$. Show that $m\mathbb{Z} = I$.

94. Show that if I is an ideal of $\mathbb{Z}$ then there exists $m \in \mathbb{Z}_{>0}$ such that $m\mathbb{Z} = I$.

95. Show that $\mathbb{Z}_{>0}$ indexes the ideals of $\mathbb{Z}$.

96. Show that $p \in \mathbb{Z}_{>0}$ is prime if and only if there does not exist $c \in \mathbb{Z}_{>1}$ such that $p\mathbb{Z} \subsetneq c\mathbb{Z} \subsetneq \mathbb{Z}$.

97. Let $m, n \in \mathbb{Z}_{>0}$. Show that n is divisible by m if and only if $n\mathbb{Z} \subseteq m\mathbb{Z}$.

98. Show that $p \in \mathbb{Z}_{>0}$ is prime if and only if $\mathbb{Z}/p\mathbb{Z}$ is a simple $\mathbb{Z}$-module.

99. Let $m, n, \ell \in \mathbb{Z}_{>0}$ and assume that $m\ell = n$. Show that ℓ is prime if and only if $m\mathbb{Z}/n\mathbb{Z}$ is a simple $\mathbb{Z}$-module.

100. Let $n \in \mathbb{Z}_{>1}$. Show that there does not exist an infinite sequence $n > m_1 > m_2 > \cdots > 1$ such that $n\mathbb{Z} \subsetneq m_1\mathbb{Z} \subsetneq m_2\mathbb{Z} \subsetneq \cdots \subsetneq \mathbb{Z}$.

101. Show that if M is a $\mathbb{Z}$-module and $N \subseteq M$ is a $\mathbb{Z}$-submodule of M and M/N is not simple then there exists a $\mathbb{Z}$-module M' such that $N \subsetneq M' \subsetneq M$.

102. Assume that $k \in \mathbb{Z}_{>0}$ and $p_1, \ldots, p_k \in \mathbb{Z}_{>0}$ are prime. Let

$$n = p_1 \cdots p_k, \quad m_1 = p_2 \cdots p_k, \quad \ldots, \quad m_{k-1} = p_k.$$

Show that $n\mathbb{Z} \subsetneq m_1\mathbb{Z} \subsetneq \cdots \subsetneq m_{k-1}\mathbb{Z} \subsetneq \mathbb{Z}$ and that Let $m_0 = n$ and $m_k = 1$. Show that if $j \in \{1 \ldots, k\}$ then $m_j\mathbb{Z}/m_{j-1}\mathbb{Z}$ is a simple $\mathbb{Z}$-module.

103. Let $n \in \mathbb{Z}_{>0}$. Show that there exist $k \in \mathbb{Z}_{>0}$ and primes $p_1, \ldots, p_k \in \mathbb{Z}_{>0}$ such that $n = p_1 \cdots p_k$.

104. (Eisenstein criterion) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and let $p \in \mathbb{Z}_{>0}$ be a prime integer.
Assume that

(a) p does not divide a_n,

(b) p divides each of $a_{n-1}, a_{n-2}, \ldots, a_0$,

(c) p^2 does not divide a_0.

Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

105. Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and let p be a prime integer such that p does not divide a_n. Let

$$\begin{array}{rccc} \pi_p\colon & \mathbb{Z}[x] & \to & \mathbb{Z}/p\mathbb{Z}[x] \\ & a_n x^n + \cdots + a_0 & \mapsto & \bar{a}_n x^n + \cdots + \bar{a}_0, \end{array} \qquad \text{where } \bar{a} \text{ denotes } a \bmod p.$$

Show that if $\pi_p\big(f(x)\big)$ is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

106. Show that if $f(x) \in \mathbb{Z}[x]$, $\deg\big(f(x)\big) > 0$, and $f(x)$ is irreducible in $\mathbb{Z}[x]$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

107. Let $f(x) \in \mathbb{Z}[x]$. Show that $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if

$$\begin{array}{rl} & \text{either } f(x) = \pm p, \text{ where } p \text{ is a prime integer,} \\ \text{or} & f(x) \text{ is a primitive polynomial and } f(x) \text{ is irreducible in } \mathbb{Q}[x]. \end{array}$$

108. Carefully define field, field morphism, subfield, field automorphism, and field extension.

109. Show that $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

110. Show that $\mathbb{C}(x)$ and $\mathbb{C}((x))$ are fields.

111. Show that $\mathbb{Z}$ and $\mathbb{C}[x]$ and $\mathbb{C}[x, x^{-1}]$ and $\mathbb{C}[[x]$ are not fields.

112. Let $\mathbb{E}/\mathbb{F}$ be a field extension. Show that $\mathbb{E}$ is an $\mathbb{F}$-vector space.

113. Give an example of fields $\mathbb{F} \subseteq \mathbb{E}$ such that $\dim_{\mathbb{F}}(\mathbb{E})$ finite.

114. Give an example of fields $\mathbb{F} \subseteq \mathbb{E}$ such that $\dim_{\mathbb{F}}(\mathbb{E})$ is infinite.

115. Show that if $\varphi\colon \mathbb{E} \to \mathbb{F}$ is a field morphism then φ is injective.

116. Give an example of a field morphism $\varphi\colon \mathbb{F} \to \mathbb{F}$ that is not surjective.

117. Carefully define $\mathbb{F}$-module and $\mathbb{F}$-algebra.

118. Let $\mathbb{E}/\mathbb{F}$ be a field extension. Show that $\mathbb{E}$ is an $\mathbb{F}$-algebra.

119. Let $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$ be inclusions of fields. Show that $[\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}] = [\mathbb{E} : \mathbb{F}]$.

120. Let $\mathbb{F}$ be a field. Show that $\mathrm{Aut}(\mathbb{F})$ is a group.

121. Let $\mathbb{F}$ be a finite field of characteristic 2. Show that the map

$$\begin{matrix} \mathbb{F} & \to & \mathbb{F} \\ x & \mapsto & x^2 \end{matrix} \qquad \text{is a bijection.}$$

122. Let $\mathbb{F}$ be a field of characteristic 2. Show that the map

$$\begin{matrix} \mathbb{F} & \to & \mathbb{F} \\ x & \mapsto & x^2 \end{matrix} \qquad \text{is a bijection.}$$

123. Give an example of a field of characteristic p such that the Frobenius map is not an automorphism.

124. Determine $\mathrm{Aut}(\mathbb{Q})$, $\mathrm{Aut}(\mathbb{R})$ and $\mathrm{Aut}(\mathbb{C})$ and $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ and $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$.

125. Carefully define $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ and $\mathrm{Fix}(H)$.

126. Show that if $\mathbb{F} \subseteq \mathbb{E}$ is an inclusion of fields then $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is a subgroup of $\mathrm{Aut}(\mathbb{E})$.

127. Show that if $\mathbb{F} \subseteq \mathbb{E}$ is an inclusion of fields and $\dim_{\mathbb{F}}(\mathbb{E})$ is finite then $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$.

128. Show that if H is a subgroup of $\mathrm{Aut}(\mathbb{E})$ then $\mathrm{Fix}(H)$ is a subfield of $\mathbb{E}$.

129. Show that if H is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$ then $\mathbb{F} = \mathrm{Fix}(H)$ is a subfield of $\mathbb{E}$ and $\dim_{\mathbb{F}}(\mathbb{E})$ is finite.

130. Show that if $\mathbb{F}$ is a subfield of $\mathbb{E}$ then $\mathrm{Fix}(\mathrm{Gal}(\mathbb{E}/\mathbb{F})) \supseteq \mathbb{F}$.

131. Show that if H is a subgroup of $\mathrm{Aut}(\mathbb{E})$ then $\mathrm{Gal}(\mathbb{E}/\mathrm{Fix}(H)) \supseteq H$,

132. Show that if $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ are inclusions of fields then $\mathrm{Gal}(\mathbb{E}/\mathbb{K}) \supseteq \mathrm{Gal}(\mathbb{E}/\mathbb{F})$,

133. Show that if $H \subseteq G \subseteq \mathrm{Aut}(\mathbb{E})$ are inclusions of groups then $\mathrm{Fix}(H) \supseteq \mathrm{Fix}(G)$.

134. Show that if $\mathbb{E}$ is a field and H is a subgroup of $\mathrm{Aut}(\mathbb{E})$ then $\mathrm{Fix}(\mathrm{Gal}(\mathbb{E}/\mathrm{Fix}(H))) = \mathrm{Fix}(H)$.

135. Show that if $\mathbb{F} \subseteq \mathbb{E}$ is an inclusion of fields then $\mathrm{Gal}(\mathbb{E}/\mathrm{Fix}(\mathrm{Gal}(\mathbb{E}/\mathbb{F}))) = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

136. Show that if $\sigma \in \mathrm{Aut}(\mathbb{E})$ and $\mathbb{F} \subseteq \mathbb{E}$ is an inclusion of fields then $\sigma\mathbb{F}$ is a subfield of $\mathbb{E}$.

137. Show that if $\sigma \in \mathrm{Aut}(\mathbb{E})$ and $\mathbb{F} \subseteq \mathbb{E}$ is an inclusion of fields then $\mathrm{Gal}(\sigma\mathbb{F}) = \sigma\mathrm{Gal}(\mathbb{F})\sigma^{-1}$.

138. Show that if $\sigma \in \mathrm{Aut}(\mathbb{E})$ and H is a subgroup of $\mathrm{Aut}(\mathbb{E})$ then $\mathrm{Fix}(\sigma H\sigma^{-1}) = \sigma\mathrm{Fix}(H)$.

139. Show that if H is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$ then $[\mathbb{E}\colon \mathrm{Fix}(H)] = |H|$.

140. Show that if H is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$ then $[\mathrm{Gal}(\mathrm{Fix}(H)) = H$.

141. Draw the subgroup lattice of S_2 and determine which subgroups are normal.

142. Draw the subgroup lattice of $\mathbb{Z}/3\mathbb{Z}$ and determine which subgroups are normal.

143. Draw the subgroup lattice of $\mathbb{Z}/4\mathbb{Z}$ and determine which subgroups are normal.

144. Draw the subgroup lattice of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and determine which subgroups are normal.

145. Draw the subgroup lattice of $\mathbb{Z}/5\mathbb{Z}$ and determine which subgroups are normal.

146. Draw the subgroup lattice of S_3 and determine which subgroups are normal.

147. Carefully define $\mathbb{F}(\alpha)$ and $\mathbb{F}[\alpha]$.

148. Define $\mathbb{F}[x]$ and $\mathrm{ev}_\alpha \colon \mathbb{F}[x] \to \mathbb{F}$ and show that ev_α is a ring homomorphism.

149. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that there exists a unique monic polynomial $m(x) \in \mathbb{F}[x]$ such that $\ker(\mathrm{ev}_\alpha) = m(x)\mathbb{F}[x]$.

150. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Let $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$ be the minimal poylnomial of α over $\mathbb{F}$. Show that $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$ is irreducible.

151. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if α is algebraic over $\mathbb{F}$ then $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$.

152. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if $n \in \mathbb{Z}_{>0}$ and $\deg(m_{\alpha,\mathbb{F}}(x)) = n$ then $[\mathbb{F}(\alpha) : \mathbb{F}] = n$.

153. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if $n \in \mathbb{Z}_{>0}$ and $\deg(m_{\alpha,\mathbb{F}}(x)) = n$ then the $\mathbb{F}$-vector space $\mathbb{F}(\alpha)$ has basis $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$.

154. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$.
    (a) Carefully define what it means for α to be algebraic over $\mathbb{F}$.
    (b) Carefully define what it means for α to be transcendental over $\mathbb{F}$.
    (c) Carefully define what it means for α to be separable over $\mathbb{F}$.
    (d) Carefully define what it means for α to be normal over $\mathbb{F}$.
    (e) Carefully define what it means for α to be Galois over $\mathbb{F}$.

155. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if α is algebraic over $\mathbb{F}$ then $\mathbb{F}(\alpha)$ is a finite extension of $\mathbb{F}$.

156. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if α is transcendental over $\mathbb{F}$ then $\mathbb{F}(\alpha)$ is not a finite extension of $\mathbb{F}$.

157. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if α is transcendental over $\mathbb{F}$ then $\mathbb{F}(\alpha) \cong \mathbb{F}(x)$, where $\mathbb{F}(x)$ is the fraction field of the polynomial ring $\mathbb{F}[x]$.

158. Show that $\alpha = 2\pi i$ is algebraic over $\mathbb{R}$ and transcendental over $\mathbb{Q}$.

159. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields. Let $\alpha \in \mathbb{E}$ and let $m_\alpha(x) \in \mathbb{F}[x]$ be the minimal polynomial of α over $\mathbb{F}$. Show that all roots of $m_\alpha(x)$ have the same multiplicity.

160. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if $\mathrm{char}(\mathbb{F}) = 0$ then all elements of $\mathbb{E}$ are separable.

161. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$. Show that if $\mathbb{F}$ is finite then all elements of $\mathbb{E}$ are separable.

162. Show that if $\mathbb{E}/\mathbb{F}$ is a finite separable extension of $\mathbb{F}$ then there exists $\theta \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{F}(\theta)$.

163. Let $\mathbb{E} \supseteq \mathbb{F}$ be a finite extension. Show that there exists $\theta \in \mathbb{E}$ such that $\mathbb{E} = \mathbb{F}(\theta)$ if and only if there are only a finite number of fields $\mathbb{K}$ with $\mathbb{E} \supseteq \mathbb{K} \supseteq \mathbb{F}$.

164. Carefully define the finite field $\mathbb{F}_{p^k}$.

165. Provide the addition and multiplication tables for $\mathbb{F}_2$ and $\mathbb{F}_4$ and $\mathbb{F}_3$ and $\mathbb{F}_9$.

166. Prove that there does not exist a field with 6 elements.

167. Show that the function

$$\begin{array}{ccc} \{\text{finite fields}\} & \longrightarrow & \{p^k \mid p \in \mathbb{Z}_{>0} \text{ is prime, } k \in \mathbb{Z}_{>0}\} \\ \mathbb{F} & \longmapsto & \mathrm{Card}(\mathbb{F}) \end{array} \qquad \text{is a bijection.}$$

168. Show that the finite field $\mathbb{F}_{p^k}$ with p^k elements is given by

$$\mathbb{F}_{p^k} \text{ is the extension of } \mathbb{F}_p \text{ of degree } k, \qquad \mathbb{F}_{p^k} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^k} - \alpha = 0\}, \qquad \mathbb{F}_{p^k} = (\overline{\mathbb{F}_p})^{F^k},$$

where

$$F\colon \begin{array}{ccc} \overline{\mathbb{F}_p} & \to & \overline{\mathbb{F}_p} \\ \alpha & \mapsto & \alpha^p \end{array} \qquad \text{is the Frobenius map.}$$

169. Show that

$$\overline{\mathbb{F}_p} = \bigcup_{r \in \mathbb{Z}_{>0}} \mathbb{F}_{p^r}.$$

170. Determine $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$.

171. Determine $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

172. Show that $\overline{\mathbb{F}_{p^r}} = \overline{\mathbb{F}_p}$. Determine $\mathrm{Gal}(\overline{\mathbb{F}_{p^r}}/\mathbb{F}_{p^r})$.

173. Determine $\mathrm{Gal}(\overline{\mathbb{C}}/\mathbb{C})$.

174. Determine $\mathrm{Gal}(\overline{\mathbb{R}}/\mathbb{R})$.

175. Determine $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

176. Carefully define the cyclotomic field $\mathbb{Q}(\omega)$.

177. Carefully define primitive nth root of unity, nth cyclotomic polynomial and the Euler ϕ function.

178. Let $\Phi_n(x)$ be the nth cyclotomic polynomial. Show that $\Phi_n(x) \in \mathbb{Z}[x]$.

179. Let $\Phi_n(x)$ be the nth cyclotomic polynomial. Show that $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$.

180. Let $\Phi_n(x)$ be the nth cyclotomic polynomial. Show that

$$\phi(n) = \deg(\Phi_n(x)) = \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^\times) = (\text{the number of primitive } n\text{th roots of unity}).$$

181. Let ω be a primitive nth root of unity. Show that $\mathbb{Q}(\omega)$ is the splitting field of $x^n - 1 \in \mathbb{Q}[x]$.

182. Let ω be a primitive nth root of unity. Show that $\mathbb{Q}(\omega)$ is the splitting field of $\Phi_n(x) \in \mathbb{Q}[x]$.

183. Let ω be a primitive nth root of unity. Show that $x^n - 1 \neq m_{\omega,\mathbb{Q}}(x)$ and $\Phi_n(x) = m_{\omega,\mathbb{Q}}(x)$.

184. Let ω be a primitive nth root of unity. Show that $\mathbb{Q}(\omega))/\mathbb{Q}$ is a Galois extension.

185. Let ω be a primitive nth root of unity. Show that $\mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

186. Let ω be a primitive nth root of unity. Show that

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\omega))/\mathbb{Q}) = |\phi(n).$$

187. Let $p \in \mathbb{Z}_{>0}$ be prime. Give a formula for $\Phi_p(x)$.

188. Let $p \in \mathbb{Z}_{>0}$ be prime and let $r \in \mathbb{Z}_{>0}$. Give a formula for $\Phi_{p^r}(x)$.

189. Let $n \in \mathbb{Z}_{>0}$. Show that $\prod_{d|n} \Phi_d(x) = x^n - 1$.

190. Let $n \in \mathbb{Z}_{>0}$. Show that $\Phi_n(x) \in \mathbb{Q}[x]$.

191. Let $n \in \mathbb{Z}_{>0}$. Show that $\Phi_n(x) \in \mathbb{Z}[x]$.

192. Factor $\Phi_{12}(x)$ into irreducibles in $\mathbb{R}[x]$.

193. Prove that $\Phi_{12}(x)$ is irreducible in $\mathbb{Q}[x]$.

194. Let $n \in \mathbb{Z}_{>0}$. Show that $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

195. Let $n \in \mathbb{Z}_{>0}$. Let $p \in \mathbb{Z}_{>0}$ such that p is prime and $p = 1 \bmod n$. Show that $\Phi_n(x)$ factors into linear factors in $\mathbb{F}_p[x]$.

196. Let $\mathbb{F}$ be the splitting fiield of $\Phi_{12}(x)$ over $\mathbb{Q}$. Show that the Galois group $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

197. Let $p \in \mathbb{Z}_{>0}$. Show that

$$p \text{ is prime} \qquad \text{if and only if} \qquad \frac{\mathbb{Z}}{p\mathbb{Z}} \text{ is a field.}$$

198. Let $p \in \mathbb{Z}_{>0}$. Show that

$$p \text{ is prime} \qquad \text{if and only if} \qquad \frac{\mathbb{Z}}{p\mathbb{Z}} \text{ is an integral domain.}$$

199. Let $\mathbb{F}$ be a field and let $m(x) \in \mathbb{F}[x]$. Show that

$$m(x) \text{ is irreducible in } \mathbb{F}[x] \qquad \text{if and only if} \qquad \frac{\mathbb{F}[x]}{(m(x))} \text{ is a field.}$$

200. Let $\mathbb{F}$ be a field and let $m(x) \in \mathbb{F}[x]$. Show that

$$m(x) \text{ is irreducible in } \mathbb{F}[x] \qquad \text{if and only if} \qquad \frac{\mathbb{F}[x]}{(m(x))} \text{ is an integral domain.}$$

201. Show that $x^2 - 12$ is irreducible in $\mathbb{Q}[x]$.

202. Show that $8x^3 + 4399x^2 - 9x + 2$ is irreducible in $\mathbb{Q}[x]$.

203. Show that $2x^{10} - 25x^3 + 10x^2 - 30$ is irreducible in $\mathbb{Q}[x]$.

204. Determine all irreducible polynomials of degree ≤ 4 in $\mathbb{F}_2[x]$.

205. List all monic polynomials of degree ≤ 2 in $\mathbb{F}_3[x]$. Determine which of these are irreducible.

206. What is the difference between $\mathbb{Q}[5^{\frac{1}{3}}]$ and $Q(5^{\frac{1}{3}})$?

207. Show that $x^3 - 5$ does not factor into linear polynomials with coefficients in $\mathbb{Q}[5^{\frac{1}{3}}]$. Show that $\mathbb{Q}(5^{\frac{1}{3}}) = \mathbb{Q}[5^{\frac{1}{3}}]$ and has $\mathbb{Q}$-basis $\{1, 5^{\frac{1}{3}}, 5^{\frac{2}{3}}\}$. Let ζ be a primitve cube root of 1 and show that the splitting field of $x^3 - 5$ is $\mathbb{Q}(5^{\frac{1}{3}}, \zeta)$ and is dimension 9 as a $\mathbb{Q}$-vector space.

208. Let $\alpha = \sqrt{2} + \sqrt{3}$ in $\mathbb{R}_{\ge 0}$.

    (a) Find $f(x) \in \mathbb{Q}[x]$ such that $\deg(f(x)) = 4$ and $f(\alpha) = 0$.
    (b) Factor $f(x)$ in $\mathbb{C}[x]$.
    (c) Find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

209. Let $f(x) = x^3 - x + 4$ and let $\alpha \in \mathbb{C}$ be such that $f(\alpha) = 0$. Find the inverse of $\alpha^2 + \alpha + 1$ in $\mathbb{Q}(\alpha)$. More precisely, find $a, b, c \in \mathbb{Q}$ such that

$$(\alpha^2 + \alpha + 1)^{-1} = a + b\alpha + c\alpha^2.$$

210. Let $\mathbb{F} \subseteq R$ be a inclusion of rings and assume that $\mathbb{F}$ is a field and R is an integral domain and $\dim_{\mathbb{F}}(R)$ is finite. Show that R is a field.

211. Let $\mathbb{F}$ be a field and let $\alpha \in \overline{\mathbb{F}}$ such that $[\mathbb{F}(\alpha) : \mathbb{F}] = 5$. Show that $\mathbb{F}(\alpha^2) = \mathbb{F}(\alpha)$.

212. Let $\alpha \in \mathbb{C}$ be a root of $x^3 - x + 1$. Determine the minimal polynomial of $\beta = \alpha^2 + 1$ over $\mathbb{Q}$.

213. Let $\mathbb{F} = \mathbb{C}(u)$. Let $f(x) = x^4 - 4x^2 + 2 - u \in \mathbb{F}[x]$.

    (a) Carefully state Gauss' lemma.
    (b) Prove that $f(x)$ is irreducible in $\mathbb{F}[x]$.
    (c) Show that the $\mathbb{C}$-algebra homomorphism given by

$$\begin{matrix} \mathbb{C}(v)[x] & \to & \mathbb{C}(t)[x] \\ v & \mapsto & t^4 + t^{-4} \\ x & \mapsto & x \end{matrix} \qquad \text{has kernel} \qquad (f(x)).$$

    (c) Let

$$\mathbb{K} = \frac{\mathbb{F}[x]}{(f(x))}.$$

    Prove that $\mathbb{K}$ is not a splitting field of $f(x)$.

214. Show that if $\mathbb{F}$ is a finite field then there exists $p \in \mathbb{Z}_{>0}$ prime and $r \in \mathbb{Z}_{>0}$ such that

$$\mathrm{Card}(\mathbb{F}) = p^r.$$

215. Let $n \in \mathbb{Z}_{>0}$. Show that the set

$$\{p(x) \in \mathbb{Q}[x] \mid \deg(p(x)) = n \text{ and } p(x) \text{ is irreducible}\} \qquad \text{is infinite.}$$

216. Let $p \in \mathbb{Z}_{>0}$ and let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) = p$. Let $r \in \mathbb{Z}_{>0}$. Show that

$$\mathbb{K} = \{x \in \mathbb{F} \mid x^{p^r} = x\} \qquad \text{is a subfield of } \mathbb{F}.$$

217. Let $\mathbb{E}$ be a field and let H be a subgroup of $\mathrm{Aut}(\mathbb{E})$. Show that

$$\mathbb{E}^H = \{x \in \mathbb{E} \mid \text{if } h \in H \text{ then } h(\alpha) = \alpha\} \qquad \text{is a subfield of } \mathbb{E}.$$

218. Let $\mathbb{K}$ be a field. Let G be a subgroup of $\mathrm{Aut}(\mathbb{K}$ and let N be a normal subgroup of G. Then

$$N \subseteq G \subseteq \mathrm{Aut}(\mathbb{K}) \qquad \text{so that} \qquad \mathbb{K}^G \subseteq \mathbb{K}^N.$$

Define an injective homomorphism

$$G/N \to \mathrm{Aut}_{\mathbb{K}^G}(\mathbb{K}^N)$$

Is this an isomorphism?

219. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields and let $\alpha \in \mathbb{E}$.

   (a) Carefully define what it means for α to be algebraic over $\mathbb{F}$.
   (b) Carefully define what it means for α to be transcendental over $\mathbb{F}$.
   (c) Carefully define what it means for α to be separable over $\mathbb{F}$.
   (d) Carefully define what it means for α to be normal over $\mathbb{F}$.
   (e) Carefully define what it means for α to be Galois over $\mathbb{F}$.

220. Let $\mathbb{E} \supseteq \mathbb{F}$ be an inclusion of fields.

   (a) Carefully define what it means for $\mathbb{E}$ to be a finite extension of $\mathbb{F}$.
   (b) Carefully define what it means for $\mathbb{E}$ to be an algebraic extension of $\mathbb{F}$.
   (c) Carefully define what it means for $\mathbb{E}$ to be a separable extension of $\mathbb{F}$.
   (d) Carefully define what it means for $\mathbb{E}$ to be a normal extension of $\mathbb{F}$.
   (e) Carefully define what it means for $\mathbb{E}$ to be a Galois extension of $\mathbb{F}$.

221. Determine which properties $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$ and $\mathbb{R}/\mathbb{Q}$ have (finite, algebraic, separable, normal, Galois).

222. Show that $\mathbb{E}/\mathbb{F}$ is a Galois extension if and only if $[\mathbb{E};\mathbb{F}]$ is finite and $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = [\mathbb{E} : \mathbb{F}]$.

223. Show that if $\mathbb{E}$ is a Galois extension of $\mathbb{F}$ then $\mathrm{Fix}(\mathrm{Gal}(\mathbb{E}/\mathbb{F})) = \mathbb{F}$.

224. Show that if $\mathbb{E}$ is a Galois extension of $\mathbb{F}$ then $[\mathbb{E} : \mathbb{F}] = |\mathrm{Gal}(\mathbb{E}/\mathbb{F})|$.

225. Show that if $\mathbb{E}/\mathbb{K}$ is Galois and $\mathbb{E} \supseteq \mathbb{F} \supseteq \mathbb{K}$ are field inclusions then $\mathbb{E}/\mathbb{F}$ is Galois.

226. Show that if $\mathbb{E}/\mathbb{K}$ is Galois and $\mathbb{E} \supseteq \mathbb{F} \supseteq \mathbb{K}$ are field inclusions then $\mathbb{F}/\mathbb{K}$ is Galois if and only if $\mathbb{F}$ satisfies

$$\text{if } \sigma \in \mathrm{Gal}(\mathbb{E}/\mathbb{K}) \text{ then } \sigma\mathbb{F} = \mathbb{F}.$$

227. Show that if $\mathbb{E}/\mathbb{K}$ is Galois and $\mathbb{E} \supseteq \mathbb{F} \supseteq \mathbb{K}$ are field inclusions then $\mathbb{F}/\mathbb{K}$ is Galois if and only if $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$ is a normal subgroup of $\mathrm{Gal}(\mathbb{E}/\mathbb{K})$.

228. Show that if $\mathbb{E}/\mathbb{K}$ is Galois and $\mathbb{E} \supseteq \mathbb{F} \supseteq \mathbb{K}$ are field inclusions then

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{E}/\mathbb{K}) & \to & \mathrm{Gal}(\mathbb{F}/\mathbb{K}) \\ \sigma & \mapsto & \sigma|_H \end{array} \qquad \text{is a group homomorphism with kernel } \mathrm{Gal}(\mathbb{E}/\mathbb{F}).$$

229. Show that $\mathbb{F} \supseteq \mathbb{K}$ is a finite separable extension then there exists a finite extension $\mathbb{E} \supseteq \mathbb{F} \supseteq \mathbb{K}$ such that $\mathbb{E}/\mathbb{K}$ is Galois.

230. Show that the monic polynomials in $\mathbb{F}[x]$ index the ideals of $\mathbb{F}[x]$.

231. Let B be an $\mathbb{F}$-algebra. Show that $\mathrm{Hom}_{\mathbb{F}}(\mathbb{F}[x], B) \cong B$.

232. Show that the $\mathbb{R}$-algebra morphisms given by

$$\begin{array}{ccc} \frac{\mathbb{R}[x]}{(x^2+1)} & \to & \mathbb{C} \\ x & \mapsto & i \end{array} \qquad \text{anc} \qquad \begin{array}{ccc} \frac{\mathbb{R}[x]}{(x^2+1)} & \to & \mathbb{C} \\ x & \mapsto & -i \end{array}$$

are both isormorphisms.

233. Show that $\mathbb{C}$ and $\mathbb{R}^2$ are not isomorphic are $\mathbb{R}$-algebras.

234. Give an $\mathbb{R}$-algebra isomorphism from $\mathbb{R}[x]/(x^2+x+1)$ and $\mathbb{C}$.

235. Give an $\mathbb{R}$-algebra isomorphism from $\mathbb{R}[x]/(x(x+1))$ and $\mathbb{R}^2$.

236. Show that $[\mathbb{C} : \mathbb{R}] = 2$.

237. Show that $[\mathbb{R} : \mathbb{Q}] = \infty$.

238. Let $f \in \mathbb{F}[x]$. Show that if $[\mathbb{F}[x]/(f) : \mathbb{F}] = \deg(f)$.

239. Let $A \subseteq B$ be an inclusion of k-algebras. Assume that B has a A-basis $\{b_1, \ldots, b_m\}$. Let $\{a_1, \ldots, a_n\}$ be a k-basis of A. Show that B has k-basis $\{a_i b_j \mid i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}$.

240. Show that $\mathrm{Card}(\overline{Q}) = \mathrm{Card}(\mathbb{Q}) = \mathrm{Card}(\mathbb{Z}) = \mathrm{Card}(\mathbb{Z}_{>0})$.

241. Prove that

$$\sum_{n \in \mathbb{Z}_{>\geq 0}} 10^{-n!} \qquad \text{is transcendental over } \mathbb{Q}.$$

242. Prove that e is transcendental over $\mathbb{Q}$.

243. Prove that π is transcendental over $\mathbb{Q}$.

244. Let $\mathbb{K} \supseteq \mathbb{F}$ be an extension. Show that the set of elements of $\mathbb{K}$ that are algebraic over $\mathbb{F}$ is a subfield of $\mathbb{K}$.

245. Let $\mathbb{F}$ be a field. Show that if α is algebraic over $\mathbb{F}$ then $\mathbb{F}[\alpha]$ is a field.

246. Let $\mathbb{K} \supseteq \mathbb{F}$ be a field extension and let $\alpha \in \mathbb{K}$. Let $f \in \mathbb{F}[x]$ be the minimal polynomial of α. Show that f is irreducible, that $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$ and that $\mathbb{F}(\alpha)$ has $\mathbb{F}$-basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$, where $n = \deg(f)$.

247. The "Theorem of Louiville" states that if $f \colon \mathbb{C} \to \mathbb{C}$ is holomorphic and bounded then f is constant. Use Louiville's theorem to prove that $\mathbb{C}$ is algebraically closed. (Be sure to give a careful definition of $\mathbb{C}$.)

248. Let $\mathbb{F}$ be a field. Carefully define *algebraically closed* and *the algebraic closure of* $\mathbb{F}$. Show that the algebraic closure of $\mathbb{F}$ exists, is unique, is algebraic over $\mathbb{F}$ and is algebraically closed.

249. Show that $\overline{\mathbb{Q}} \neq \mathbb{C}$.

250. Let $\mathbb{F}$ be a field and let $J \subseteq \mathbb{F}[x]$. Carefully define *the splitting field of* J *over* $\mathbb{F}$. Show that the splitting field of J over $\mathbb{F}$ exists, is unique, and is algebraic over $\mathbb{F}$.

251. Let $\mathbb{F}$ be a field. Show that a finite dimensional $\mathbb{F}$-vector space is the same as a finitely generated $\mathbb{F}$-module.

252. Let $\mathbb{F}$ be a field and let V be a finite dimensional $\mathbb{F}$-vector space. Explain why a linear transformation $T: V \to V$ is the same data as an $\mathbb{F}[x]$-module structure on V.

253. Let R be a ring and let $n \in \mathbb{Z}_{>0}$. Show that an element of $GL_n(R)$ is the same data as an R-module isomorphism $\varphi: R^n \to R^n$.

254. Let R be a Euclidean domain. For $i \in \{1, \ldots, n-1\}$, $j \in \{1, \ldots, n\}$, $c \in R$ and $d \in R^\times$ let

$$x_{i,i+1}(c) = 1 + cE_{ij}, \qquad x_{i+1,i}(c) = 1 + cE_{i+1,i}, \qquad h_j(d) = 1 + (d-1)E_{jj}.$$

Show that $GL_n(R)$ is generated by the matrices

$$x_{i,i+1}(c), \qquad x_{i+1,i}(c), \qquad h_j(d), \qquad \text{with} \quad c \in R, d \in R^\times$$

and $i \in \{1, \ldots, n-1\}$ and $j \in \{1, \ldots, n\}$.

255. Let R be a PID. For $i \in \{1, \ldots, n-1\}$, $j \in \{1, \ldots, n\}$, $d \in R^\times$ and $r, s, p, q \in R$ with $rq - ps = 1$, let

$$y_i \begin{pmatrix} r & s \\ p & q \end{pmatrix} = 1 + (r-1)E_{ii} + sE_{i,i+1} + pE_{i+1,i} + (q-1)E_{i+1,i+1}, \qquad h_j(d) = 1 + (d-1)E_{jj}.$$

Show that $GL_n(R)$ is generated by the matrices

$$y_i \begin{pmatrix} r & s \\ p & q \end{pmatrix} \quad \text{and} \quad h_j(d), \qquad \text{with} \quad d \in R^\times \text{ and } r, s, p, q \in R \text{ such that } rq - ps = 1,$$

and $i \in \{1, \ldots, n-1\{$ and $j \in \{1, \ldots, n\}$.

256. Show that a Euclidean domain is a PID.

257. Show that a PID is a UFD.

258. Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(\mathbb{Z})$. Show that there exist $P \in GL_t(\mathbb{Z})$ and $Q \in GL_s(\mathbb{Z})$ such that PAQ is diagonal.

259. Let $\mathbb{F}$ be a field. Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(\mathbb{F}[x])$. Show that there exist $P \in GL_t(\mathbb{F}[x])$ and $Q \in GL_s(\mathbb{F}[x])$ such that PAQ is diagonal.

260. Let R be a Euclidean domain. Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(R)$. Show that there exist $P \in GL_t(R)$ and $Q \in GL_s(R)$ such that PAQ is diagonal.

261. Let R be a PID. Let $s, t \in \mathbb{Z}_{>0}$ and let $A \in M_{t \times s}(R)$. Show that there exist $P \in GL_t(R)$ and $Q \in GL_s(R)$ such that PAQ is diagonal.

262. Let $p_1, p_2 \in \mathbb{Z}_{>0}$ be prime. Show that

$$\frac{\mathbb{Z}}{p_1p_2\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{p_2\mathbb{Z}}.$$

263. Let $m, n \in \mathbb{Z}_{>0}$ with $\gcd(m, n) = 1$. Show that

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

264. Let $\mathbb{F}$ be a field and let $a_1, a_2 \in \mathbb{F}$ with $a_1 \neq a_2$. Let $r, s \in \mathbb{Z}_{>0}$. Show that

$$\frac{\mathbb{F}[x]}{(x-a_1)^r(x-a_2)^s\mathbb{F}[x]} \cong \frac{\mathbb{F}[x]}{(x-a_1)^r\mathbb{F}[x]} \oplus \frac{\mathbb{F}[x]}{(x-a_2)^s\mathbb{F}[x]}.$$

265. Let $\mathbb{F}$ be a field and let $p(x), q(x) \in \mathbb{F}[x]$ with $\gcd(p(x), q(x)) = 1$. Show that

$$\frac{\mathbb{F}[x]}{p(x)q(x)\mathbb{F}[x]} \cong \frac{\mathbb{F}[x]}{p(x)\mathbb{F}[x]} \oplus \frac{\mathbb{F}[x]}{q(x)\mathbb{F}[x]}.$$

266. Let R be a.PID and let $p, q \in R$ with $\gcd(p, q) = 1$. Show that

$$\frac{R}{pqR} \cong \frac{R}{pR} \oplus \frac{R}{qR}.$$

267. Compute the matrix of the action of x on

$$\frac{\mathbb{F}[x]}{(x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0)\mathbb{F}[x]} \quad \text{with respect to the } \mathbb{F}\text{-basis} \qquad \{1, x, \ldots, x^{r-1}\}.$$

268. Let $\lambda \in \mathbb{F}$. Compute the matrix of the action of x on

$$\frac{\mathbb{F}[x]}{(x-\lambda)^d\mathbb{F}[x]} \quad \text{with respect to the } \mathbb{F}\text{-basis} \qquad \{1, x-\lambda, \ldots, (x-\lambda)^{d-1}\}.$$

269. Let $p(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1x + a_0 \in \mathbb{F}[x]$. Compute the matrix of the action of x on

$$\frac{\mathbb{F}[x]}{p(x)^d\mathbb{F}[x]}$$

with respect to the $\mathbb{F}$-basis

$$\{1, x, \ldots, x^{r-1}\} \cup \{p(x), xp(x), \ldots, x^{r-1}p(x)\} \cup \cdots \cup \{p(x)^{d-1}, xp(x)^{d-1}, \ldots, x^{r-1}p(x)^{d-1}\}.$$

270. Let $n \in \mathbb{Z}_{>0}$. Let $\mathbb{F}$ be a field and let $A \in M_n(\mathbb{F})$. Prove that there exists $P \in GL_n(\mathbb{F})$ such that PAP^{-1} is in Jordan normal form.