

Algebra 3 2006

All exercises

This is the collection of all exercises for the exercise classes.

At the end you find exercises which were used in some tests last year.

Exercises marked with * are particularly recommended.

Exercise (1.1)*: Discuss the Exercises 1.9, 1.19 and 1.23 in Chapter I of the notes.

Exercise (1.2): Show that an infinite group G has to contain a non-trivial subgroup, ie. a subgroup $\neq G, \{e\}$.

Exercise (1.3): Give examples of the following:

- (1) An infinite group G with a subgroup $H \neq G$ and $|G : H|$ finite.
- (2) An infinite group G with a subgroup $H \neq \{e\}$ and $|H|$ finite.

Exercise (1.4)*: Show that

$$\langle (1, 2, 3, 4), (1, 2) \rangle = S_4$$

Exercise (1.5):

(1) Let a and b be commuting elements in G of finite orders m and n , respectively. Show that $(ab)^{mn} = e$.

(2) Suppose in addition that n and m are relatively prime. Prove that if a power a^i of a equals a power b^j of b , then $a^i = b^j = e$. Use this to prove that the order of ab is nm .

Exercise (1.6):

Show that the elements of finite order in an *abelian* group G form a subgroup of G .

Exercise (1.7): Let a, b and c be elements in a group G .

- (1) Show that a and a^{-1} have the same order.
- (2) Show that ab and ba have the same order.

(3) Show that abc and bca have the same order. (Try to generalize this to a general theorem.)

(4) Find three elements a, b, c in the symmetric group S_3 , such that abc and bac have *different* orders.

Exercise (1.8): Consider the group $(\mathbb{Q}, +)$ and its subgroup $(\mathbb{Z}, +)$. Let p, q be two different prime numbers. Show that the cosets $\frac{1}{p} + \mathbb{Z}$ and $\frac{1}{q} + \mathbb{Z}$ in \mathbb{Q} are different. Show that the index $|\mathbb{Q} : \mathbb{Z}|$ is infinite.

Exercise (1.9): Let S be a subgroup of the group G . Suppose that $a, b \in G$ satisfies $Sa = bS$. Thus the left coset of S containing a equals the right coset of S containing b . Show that $Sa = aS = bS = Sb$.

Exercise (1.10): It is wellknown that the subgroups of the group $(\mathbb{Z}, +)$ are exactly those on the form $(m\mathbb{Z}, +)$ for some $m \in \mathbb{Z}$, $m \geq 0$. Let $n_1, n_2 \in \mathbb{Z} \setminus \{0\}$ have greatest common divisor n . Show that the smallest subgroup of \mathbb{Z} which contains n_1 and n_2 is $n\mathbb{Z}$.

Exercise (1.11): Define an equivalence relation on the elements of the group G by

$$a \sim_c b \iff \langle a \rangle = \langle b \rangle.$$

Here $\langle a \rangle$ is the cyclic subgroup of G generated by a . Show that the \sim_c -equivalence class of a is always finite.

Exercise (1.12)*: Let G be a finite group.

(1) Show that if $|G|$ is even then the number of elements of order 2 in G is *odd*. (Consider the mapping $x \mapsto x^{-1}$. Which elements are the fixed points of this map?)

(2) Show that the number of elements of order 3 in G is *even* (possibly 0).

(3) Show that the number of elements of order 4 in G is *even* (possibly 0).

Exercise (1.13): Suppose that $H \triangleleft G$ and that $|G : H| = p$, where p is a prime number. Let K be a subgroup of G . Show that either $K \subseteq H$ or $G = HK$, $|K : K \cap H| = p$.

Exercise (2.1)*: Find all subgroups of the dihedral group D_4 and draw a diagram illustrating their mutual positions. Find all normal subgroups of D_4 .

Exercise (2.2)*: Discuss the Exercises 1.28, 1.46 and 1.48 in Chapter 1.

Exercise (2.3): Suppose that N_1 and N_2 are normal subgroups in the finite group G . Are the following claims *true or false*? (Please give either a proof or a counterexample.)

- (i) If $N_1 \simeq N_2$, then $G/N_1 \simeq G/N_2$.
- (ii) If $G/N_1 \simeq G/N_2$, then $N_1 \simeq N_2$.

Exercise (2.4)*: Discuss the Exercises 1.64, 1.74 and 1.87 in Chapter 1.

Exercise (2.5): Suppose that $S \triangleleft G$, that G is finite and that $\kappa : G \rightarrow \overline{G} = G/S$ is the canonical epimorphism. Suppose that $g \in G$ has an order, which is relatively prime to $|S|$. Show that $|g| = |\kappa(g)|$.

Exercise (2.6)*: Let G be a finite p -group (p a prime). Suppose $N \triangleleft G$, $N \neq \{e\}$.

- (1) Show that

$$N \cap Z(P) \neq \{e\}.$$

Hint: It is possible to modify the proof of Theorem 1.93 in the notes. Note that N is a union of conjugacy classes of G .

- (2) Show that if $|N| = p$, then $N \subseteq Z(P)$.

Exercise (2.7): Let G be a p -group. Suppose that $H \neq G$ is a subgroup. Show that $H \subset N_G(H)$, ie. $N_G(H)$ contains H properly.

Exercise (2.8): Solve Exercise 1.56 in Chapter 1 and answer the following additional questions:

- (1) Show that if ϕ is injective (ie. $\ker(\phi) = \{e\}$), then $|\phi(a)| = |a|$.
- (2) If $G^{(1)}$ and $H^{(1)}$ are the commutator subgroups of G and H respectively show that $\phi(G^{(1)}) \subseteq H^{(1)}$.

Suppose now in the rest of this exercise that ϕ is an *epimorphism*.

- (3) Show that $\phi(G^{(1)}) = H^{(1)}$.
- (4) Show that $|H : H^{(1)}|$ divides $|G : G^{(1)}|$.

Hint to (4): Let $\psi = \phi \circ \kappa$, where $\kappa : H \rightarrow H/H^{(1)}$ is the canonical epimorphism. Show that $G^{(1)} \subseteq \text{Ker}(\psi)$ and apply the Homomorphism theorem.

Exercise (2.9): Show that the only finite group with 2 conjugacy classes is \mathbb{Z}_2 .

Exercise (2.10)*: Let G be a group. Suppose that $|G : Z(G)| = n$ is finite. Show that any conjugacy class of G contains at most n elements.

Exercise (2.11): Let G be a group. Show that the following subset T of $\text{Aut}(G)$ is a *normal* subgroup in $\text{Aut}(G)$

$$T = \{\alpha \in \text{Aut}(G) \mid \alpha(U) = U \text{ for all subgroups } U \text{ in } G\}$$

Exercise (2.12)*: Discuss the Exercises 1.96, 1.101, 1.119 and 1.120 in Chapter 1.

Exercise (2.13): Show that for any (finite) group G we have:

$$|G| \leq 2 \Leftrightarrow \text{Aut}(G) = \{1_G\}.$$

Exercise (2.14): Let G_4 be the abelian group consisting of all infinite sequences (a_1, a_2, \dots) where each a_i is some element in a cyclic group of order 4.

(1) Define an isomorphism $\phi : G_4 \rightarrow G_4 \times G_4$.

(2) Investigate whether the following subsets of G_4 are subgroups:

$$M_1 = \{(a_1, a_2, \dots) \in G_4 \mid \text{There exists } k \in \mathbb{N} \text{ such that } a_i = e \text{ for all } i \geq k.\}$$

$$M_2 = \{(a_1, a_2, \dots) \in G_4 \mid \text{Only finitely many } a_i\text{'s equal } e\} \cup \{(e, e, \dots)\}.$$

Exercise (2.15): Let G_4 be the same group as in the previous exercise. Consider the (outer) direct product:

$$H_4 = C \times G_4$$

where C is a cyclic group of order 2. Show that G_4 is isomorphic to a proper subgroup of H_4 and that H_4 is isomorphic to a proper subgroup of G_4 . Show that G_4 and H_4 are *not* isomorphic.

(Thus there is no “Bernstein’s equivalence theorem” for groups.)

Exercise (2.16): Show that the matrices

$$\left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in \mathbb{Z}/3\mathbb{Z} \right\}$$

with usual matrix multiplication form a group of order 27, where every element $\neq e$ has order 3.

Use this to find two non-isomorphic finite groups for which for every t the number of elements of order t coincide for the two groups.

Exercise (2.17): Compute the center of the group of order 27 from Exercise (2.16).

Exercise (2.18)*: Describe all the 2-Sylow subgroups and all the 3-Sylow subgroups of D_6 and of $S_3 \times S_3$.

Exercise (2.19): Show that $m_p(D_n) = 1$ for all $n \geq 2$ and all odd primes p .

Exercise (3.0)*: Discuss (again?) the Exercise 1.119 in the notes.

Exercise (3.1)*: Show that a group of order 45 is abelian. Determine the number of isomorphism classes of groups of order 45.

Exercise (3.2)*: Show that if $|G| = 80 = 2^4 \cdot 5$ then either $m_5(G) = 1$ or $m_2(G) = 1$. Is G solvable? Give examples of three non-isomorphic non-abelian groups of order 80, each with a normal 5-Sylow subgroup.

Exercise (3.3): Show that a group of order 200 has a normal 5-Sylow subgroup and that it is solvable.

Exercise (3.4)*: Let G have order $231 = 3 \cdot 7 \cdot 11$. Show that $m_7(G) = m_{11}(G) = 1$. Show that G has a cyclic subgroup of order 33. Show that if $P \in \text{Syl}_{11}(G)$, then $P \subseteq Z(G)$.

Exercise (3.5): Which of the following groups are isomorphic?

$$\mathbb{Z}_{24}, \mathbb{Z}_4 \times \mathbb{Z}_6, S_4, A_4 \times \mathbb{Z}_2, \mathbb{Z}_8 \times \mathbb{Z}_3, D_{12}, D_6 \times \mathbb{Z}_2.$$

Exercise (3.6): Let $n = pa$, where p is a prime and $1 \leq a < p$. Compute the order of a p -Sylow group of the symmetric group S_{pa} . Show that such a group is abelian.

Exercise (3.7): Consider the permutations

$$\alpha = (1, 2, 3) \quad \beta = (1, 4, 7)(2, 5, 8)(3, 6, 9) \in S_9.$$

Show that α and β generate a subgroup of order $81 = 3^4$ in S_9 . Show that this is a non-abelian 3-Sylow subgroup in S_9 .

Exercise (3.8): (*The Frattini argument*). Suppose that $H \triangleleft G$ and that $P \in \text{Syl}_p(H)$. Show that

$$G = HN_G(P).$$

(This result will be presented by the instructor. It is sometimes very useful, for instance in the study of finite solvable groups.)

Exercise (3.9): Show that any group of order $132 = 2^2 \cdot 3 \cdot 11$ contains subgroups of order $33 = 3 \cdot 11$, $44 = 2^2 \cdot 11$ and $12 = 2^2 \cdot 3$. (This is an example of P. Halls generalization of Sylow's theorems for finite *solvable* groups. Ask your instructor!)

Hint: The new Example 1.183 in the *second edition* of the notes discusses groups of order 132. The previous exercise may also be used to show the existence of a subgroup of order 12.

Exercise (3.10)*: Discuss the Exercises 1.155 and 1.156 in the notes.

Exercise (3.11)*: Discuss the Exercise 1.171 in the notes. Determine all higher commutator subgroups of all symmetric groups.

Exercise (3.12): Discuss the Exercise 1.181 in the notes.

Exercise (3.13): Let G be a subgroup of S_n . Suppose that we can find elements $\tau_2, \dots, \tau_n \in G$, such that $\tau_i(1) = i$ for $2 \leq i \leq n$. Show that G is transitive.

Exercise (3.14): Show, eg. using the previous exercise, that for $n \geq 3$ is A_n a transitive subgroup of S_n .

Exercise (3.15)*: For $m \in \mathbb{N}$ let

$$s(m) = \min\{n \in \mathbb{N} \mid m \text{ divides } n!\}.$$

Thus for example if $m = 700 = 2^2 5^2 7$ then $s(m) = 10$. Show that a simple group of order m cannot have a proper subgroup of index $< s(m)$.

Hint: Use Theorem 1.148 in the notes.

Exercise (3.16): Let p be the largest prime number dividing the order of the simple group G . Show that G cannot have a proper subgroup of index $< p$.

Exercise (4.0): Solve Exercises 2.1 and 2.6 in Chapter II of the notes.

Exercise (4.1): 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 (4.2): 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 (4.3): 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 (4.4)*: 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 (4.5): Investigate whether the polynomial $x^3 + 4$ is reducible or irreducible in $\mathbb{Q}[x]$. The same question for $x^4 + 4$.

Exercise (4.6)*: 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 (4.7): 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 (4.8)*: 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 (4.9): 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 $\mathbb{Q}[x]$. (The proof is similar to that of the previous exercise, but a little harder.)

Exercise (4.10): Is $x^4 - 10x^2 + 1$ reducible or irreducible in $\mathbb{Q}[x]$?

Exercise (4.11): 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 (4.12)*: 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 (4.13): 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 (4.14)*: 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 (4.15): 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 (4.16): 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 (5.1)*: 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 (5.2): 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 (5.3)*: 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 (5.4)*: 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 4.14 from last week.)

Exercise (5.5): 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 (5.6): 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 (5.7)*: 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 (5.8)*: 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 (5.9): 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 (5.10): 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 (5.11)*: 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 (5.12): 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 (6.1): 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 (6.2): 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, discussed in the lecture on 29. September.

Exercise (6.3)*: Let $f(x) = x^4 + ax^2 + 1$ be an irreducible polynomial in $\mathbb{Q}(x)$. Let α be a root of $f(x)$.
Prove that all the roots of $f(x)$ are $\alpha, -\alpha, 1/\alpha$ and $-1/\alpha$.
Prove that the splitting field M over \mathbb{Q} is a normal extension of \mathbb{Q} and find the Galois group $\text{Gal}(M/\mathbb{Q})$.

Exercise (6.4)*: Let M be the splitting field over \mathbb{Q} for $x^3 - 2$.
Prove that M/\mathbb{Q} is a normal extension.
Determine the Galois group G for M over \mathbb{Q} .
Find all subfields of M and the corresponding subgroups of G .

Exercise (6.5)*: Let M be the splitting field over \mathbb{Q} for $x^6 - 2$.
Find $[M : \mathbb{Q}]$.
Show that M/\mathbb{Q} is a normal extension.
Determine the Galois group G for M over \mathbb{Q} .
Decide if the G is abelian or not.
Decide if G is solvable or not.

Exercise (6.6): Let M be the splitting field over \mathbb{Q} for $x^8 - 2$.
Find $[M : \mathbb{Q}]$.
Show that M/\mathbb{Q} is a normal extension.
Decide if the G is abelian or not.
Decide if G is solvable or not.

Exercise (6.7)*: 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 (6.8): 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 (6.9): 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 (6.10): Solve Exercise 3.35 - 3.37 in the notes.

Exercise (6.11): 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 (7.1): Discuss Example 3.50 and Exercise 3.51 in the notes. (Please note that there is a misprint in Exercise 3.51: in the third line from below b should be replaced by ib !)

Exercise (7.2)*: 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 (7.3)*: 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 (7.4)*: 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 (7.5): 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 (7.6): 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 (7.7): 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 (7.8): 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 (7.9)*: 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 (7.10): 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 (7.11): 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 $\text{Gal}(M/\mathbb{Q})$.

Test-exercises from last year.

The questions at the written exam this year are going to be somewhat more advanced, especially since you have much more time to solve them. Also please note that the curriculum was in some points essentially different last year, especially in group theory.

Question 1.2: How many non-isomorphic groups are there of order 22?

Question 1.3: Let $f : G \rightarrow H$ be homomorphism between the groups G and H , not necessarily surjective. Does $K \triangleleft G$ imply $f(K) \triangleleft H$? Please provide a proof or a counterexample.

Question 1.4: Suppose that a, b, c, d are elements in the finite group G . Is it true that the products $abcd$ and $dabc$ have the same order?

Question 1.5: Does the alternating group A_4 of order 12 contain a subgroup of index 3? Does it contain a subgroup of index 2?

Question 1.6: Let B be a subgroup of the *abelian* group A . Show that the factor group A/B is abelian. Give an example of a nontrivial normal subgroup H of a *nonabelian* group G , where the factor group G/H is abelian.

Question 1.7: Show that the subgroup generated by the permutations $\alpha = (1, 2, 3, 4, 5)$ and $\beta = (6, 7, 8)$ in S_8 is a subgroup of the *alternating* group A_8 . Is this subgroup transitive?

Question 1.8: In the class equation for a finite group the conjugacy classes play a rôle. (Classes of conjugate elements, in Danish: Ækvivalensklasser af konjugerede elementer.) Let p be a prime. Show that the number of conjugacy classes in a p -group of order $> p$ is at least $p + 1$. (**Hint:** You may prefer to consider the cases G abelian and G not abelian.)

Question 1.9: Compute the possible numbers of 3-Sylow groups in a group of order 24. Give examples of groups, where these numbers of 3-Sylow groups occur.

Question 1.10: Suppose that the normalizer $N_P = N_G(P)$ of a p -Sylow subgroup P of the finite group G is abelian. Prove, using a theorem from the book, that G has a normal subgroup N such that $G/N \simeq P$.

Question 1.11: Suppose that the group G contains a subgroup H of index $|G : H| = 3$. Show that either H is a *normal* subgroup of G or G contains a *normal* subgroup of index 2.

Question 1.12: Show that a group of order $350 = 2 \cdot 5^2 \cdot 7$ has a normal 5-Sylow subgroup. Show that it has also a normal 7-Sylow subgroup.

Hint for the second part: Use Theorem 40=Exercise 3.15, which states that generally a group of order $2m$, m odd, contains a normal subgroup of order m . Then show that a group of order $175 = \frac{350}{2}$ has a normal 7-Sylow subgroup.

Question 2.1: Consider the field $\mathbb{Q}(\sqrt[3]{2})$. Determine rational numbers q_0 , q_1 and q_2 such that

$$\frac{1}{1 + \sqrt[3]{2}} = q_0 + q_1\sqrt[3]{2} + q_2\sqrt[3]{4}.$$

Question 2.2: Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. Let $k \in \mathbb{Z}$ and define $g(x) = f(x + k)$.

- (1) Show that $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if $g(x)$ is irreducible in $\mathbb{Z}[x]$.
- (2) Let M be a splitting field for $f(x)$ over \mathbb{Q} and let $\alpha \in M$ be a root of $f(x)$. Show that $\alpha - k$ is a root of $g(x)$.
- (3) Is M also a splitting field for $g(x)$ over \mathbb{Q} ?

Question 2.3: Let $L = \text{GF}(16)$ be the finite field with 16 elements.

- (1) Determine the characteristic p of L .

Let $K = \text{GF}(p)$ and consider the polynomial $f(x) = x^3 + x + 1 \in K[x]$.

- (2) Is $f(x)$ irreducible over K ?
- (3) Is $f(x)$ separable over K ?
- (4) Can L be obtained from K by adjoining a root of $f(x)$ over K ?

Question 2.4:

- (1) Is the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ normal?
- (2) Is the extension $\mathbb{Q}(\sqrt[4]{2}i)/\mathbb{Q}$ normal?
- (3) Is the extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ normal?

Question 2.5: Let M be the splitting field over \mathbb{Q} for the polynomial $x^4 - 4x^2 + 2$. Show that M/\mathbb{Q} is a normal extension and determine the Galois group $\text{Gal}(M/\mathbb{Q})$.

Question 2.6:

- (1) Compute explicitly the 16'th cyclotomic polynomial F_{16} .

Let \mathbb{Q}_{16} be the 16'th cyclotomic field.

- (2) What is the order of the Galois group of the extension $\mathbb{Q}_{16}/\mathbb{Q}$?