# Exercises to Algebra 2, WS 2020/21

*Christoph Baxa*

**Definition:** Let $(M, \cdot)$ be a monoid with identity element $e$ and $a \in M$. An $x \in M$ is called left inverse (resp. right inverse) element of $a$ if $x \cdot a = e$ (resp. $a \cdot x = e$).

The following lemma actually already been proved in Algebra 1 in Satz 3 but was not stated there as it is here.

**Lemma:** Let $(M, \cdot)$ be a monoid with identity element $e$ and $x, y \in M$ a left inverse and a right inverse element of $a \in M$ (i.e., $x \cdot a = a \cdot y = e$). Then $x = y$.

**Proof:** $x = x \cdot e = x \cdot (a \cdot y) = (x \cdot a) \cdot y = e \cdot y = y$

**66)** Let $V$ be the (real) vector space of real sequences $(a_n)_{n\geq 1}$ (with $(a_n)_{n\geq 1} + (b_n)_{n\geq 1} := (a_n + b_n)_{n\geq 1}$ and $\alpha \cdot (a_n)_{n\geq 1} := (\alpha a_n)_{n\geq 1}$) and let $R$ be the ring of endomorphisms of $V$. Let $\varphi : V \to V$ and $\psi : V \to V$ denote the maps

$$\varphi(a_1, a_2, a_3, \dots) = (0, a_1, a_2, \dots) \quad \text{and} \quad \psi(a_1, a_2, a_3, \dots) = (a_2, a_3, a_4, \dots).$$

Prove the following:

a) $\varphi$ and $\psi$ are in $R$ (i.e., they are $\mathbb{R}$-linear maps),
b) There is a left inverse element of $\varphi$ in $R$ but there is no right inverse element of $\varphi$,
c) There is a right inverse element of $\psi$ in $R$ but there is no left inverse element of $\psi$.

**67)** Prove the following (using the notations of the previous exercise):

a) $\varphi$ is a right zero divisor but not a left zero divisor of $R$,
b) $\psi$ is a left zero divisor but not a right zero divisor of $R$.

Are left inverse elements resp. right inverse elements uniquely determined (in $R$)?

**68)** a) Let $p$ be a prime. Prove without using the results of Chapter 11 that $\{a/p^n \mid a, n \in \mathbb{Z}, n \geq 0\}$ is a subring of $(\mathbb{Q}, +, \cdot)$. Is it even an ideal?
b) Let $p$ be a prime. Prove without using the results of Chapter 11 that $\{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}$ is a subring of $(\mathbb{Q}, +, \cdot)$ ist. Is it even an ideal?

**69)** Let $R_1, \dots, R_n$ be rings. Let addition and multiplication on $R_1 \times \cdots \times R_n$ be defined as in Ex. 65. Prove the following:

a) If $S_i$ is a subring of $R_i$ for $1 \leq i \leq n$, then $S_1 \times \cdots \times S_n$ is a subring of $R_1 \times \cdots \times R_n$.
b) If $I_i$ is an ideal of $R_i$ for $1 \leq i \leq n$, then $I_1 \times \cdots \times I_n$ is an ideal of $R_1 \times \cdots \times R_n$.

**Definition:** Let $R$ be a ring. The center $Z(R)$ of $R$ is defined as

$$Z(R) := \{a \in R \mid ax = xa \text{ for all } x \in R\}.$$

**70)** a) Let $R$ be a ring. Prove that $Z(R)$ is a subring of $R$.
b) Let $R_1, \dots, R_n$ be rings. Prove $Z(R_1 \times \cdots \times R_n) = Z(R_1) \times \cdots \times Z(R_n)$.

**71)** Let $K$ be a field. Prove the following:

a) $Z\big(M_2(K)\big) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \,\middle|\, a \in K \right\}$,

b) $Z\big(M_2(K)\big)$ is neither a left ideal nor a right ideal of $M_2(K)$.

**Definition.** Let $R$ be a ring. An element $a \in R$ is called nilpotent if there is an $n \in \mathbb{N}\setminus\{0\}$ such that $a^n = 0$. The set of all nilpotent elements of $R$ will be denoted by $\mathrm{Nil}(R)$.

**72)** Let $R \neq \{0\}$ be a commutative ring with identity. Prove the following:

a) Every $a \in \mathrm{Nil}(R)$ is a zero divisor,
b) If $a, b \in \mathrm{Nil}(R)$ then $a + b \in \mathrm{Nil}(R)$,
c) $\mathrm{Nil}(R)$ is an ideal of $R$,
d) If $u \in R^*$ and $a \in \mathrm{Nil}(R)$ then $u + a \in R^*$ (*Hint:* geometric series).

**73)** Let $K$ be a field and $1 \leq k \leq n$.

a) Set $I_k := \{(a_{ij})_{1\leq i,j\leq n} \in M_n(K) \mid a_{ij} = 0 \text{ for } j \neq k\}$, i.e., the set of all $n \times n$-matrices with entries in $K$ such that only the $k$-th column may contain entries $\neq 0$. Prove that $I_k$ is a left ideal of $M_n(K)$ but that it is not a right ideal if $n \geq 2$.

b) Set $J_k := \{(a_{ij})_{1\leq i,j\leq n} \in M_n(K) \mid a_{ij} = 0 \text{ for } i \neq k\}$, i.e., the set of all $n \times n$-matrices with entries in $K$ such that only the $k$-th row may contain entries $\neq 0$. Prove that $J_k$ is a right ideal of $M_n(K)$ but that it is not a left ideal if $n \geq 2$.

**74)** Let $K$ be a field. Prove that $M_n(K)$ has only the ideals $\{0\}$ and $M_n(K)$. (*Hint:* Let $E_{ij} = (x_{st})_{1\leq s,t\leq n} \in M_n(K)$ be defined by $x_{ij} = 1$ and $x_{st} = 0$ if $(s,t) \neq (i,j)$. Let $I \neq \{0\}$ be an ideal of $M_n(K)$. Then there is an $A = (a_{ij})_{1\leq i,j\leq n} \in I \setminus \{0\}$. Therefore there are $k, \ell \in \{1, \dots, n\}$ such that $a_{k\ell} \neq 0$. Prove $E_{tk} \cdot A \cdot E_{\ell t} = a_{k\ell} E_{tt}$ for $1 \leq t \leq n$. Deduce $a_{k\ell} E_{tt} \in I$, $a_{k\ell} E_{tt} \cdot a_{k\ell}^{-1} E_{tt} = E_{tt} \in I$ and $I_n = E_{11} + \cdots + E_{nn} \in I$.) Why can this exercise not be used to prove that $M_n(K)$ is a skew field for $n \geq 2$ because of Satz 60 (ii)?

**75)** Let $R$ be a ring and $X \subseteq R$. Prove

$$(X) = \left\{ \sum_{i=1}^{I} \alpha_i x_i \beta_i + \sum_{j=1}^{J} \gamma_j y_j + \sum_{k=1}^{K} u_k \delta_k + \sum_{\ell=1}^{L} n_\ell v_\ell \;\middle|\; \begin{array}{l} \alpha_i, \beta_i \in R \text{ and } x_i \in X \text{ for } 1 \leq i \leq I, \\ \gamma_j \in R \text{ and } y_j \in X \text{ for } 1 \leq j \leq J, \\ \delta_k \in R \text{ and } u_k \in X \text{ for } 1 \leq k \leq K, \\ n_\ell \in \mathbb{Z} \text{ and } v_\ell \in X \text{ for } 1 \leq \ell \leq L \end{array} \right\}.$$

**76)** a) Let $R$ be a commutative ring and $X \subseteq R$. Prove

$$(X) = \left\{ \sum_{i=1}^{I} \alpha_i x_i + \sum_{j=1}^{J} n_j y_j \;\middle|\; \begin{array}{l} \alpha_i \in R \text{ and } x_i \in X \text{ for } 1 \leq i \leq I, \\ n_j \in \mathbb{Z} \text{ and } y_j \in X \text{ for } 1 \leq j \leq J \end{array} \right\}.$$

b) Let $R$ be a ring with identity and $X \subseteq R$. Prove

$$(X) = \left\{ \sum_{i=1}^{n} \alpha_i x_i \beta_i \;\middle|\; \alpha_i, \beta_i \in R \text{ and } x_i \in X \text{ for } 1 \leq i \leq n \right\}.$$

c) Let $R$ be a commutative ring with identity and $X \subseteq R$. Prove

$$(X) = \left\{ \sum_{i=1}^{n} \alpha_i x_i \;\middle|\; \alpha_i \in R \text{ and } x_i \in X \text{ for } 1 \leq i \leq n \right\}.$$

**Definition:** Let $R$ be a ring and $I$ and $J$ ideals of $R$. The product $I \cdot J$ of the ideals $I$ and $J$ is defined as

$$I \cdot J := \{x_1 y_1 + \cdots + x_n y_n \mid n \geq 0, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}.$$

**77)** Let $R$ be a ring and $I$ and $J$ ideals of $R$. Prove the following:

a) $I \cdot J$ is an ideal of $R$,

b) $I \cdot J$ is the ideal generated by the set $\{xy \mid x \in I, y \in J\}$,

c) If $R$ is a commutative ring with identity and $a, b \in R$ then $(a) \cdot (b) = (ab)$.

**78)** Prove that the following maps are ring isomorphisms:

a) $\varphi : \mathbb{C} \to \mathbb{C}$, $\varphi(z) = \overline{z}$,

b) $\varphi : \mathbb{C} \to \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$, $\varphi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ (with $a, b \in \mathbb{R}$),

c) Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be squarefree, $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ and $\varphi : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$, $\varphi(a + b\sqrt{d}) = a - b\sqrt{d}$ (where $a, b \in \mathbb{Z}$).

**79)** Prove that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ and $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ are isomorphic as abelian groups but not as rings. I.e., the abelian groups $\big(\mathbb{Z}[i], +\big)$ and $\big(\mathbb{Z}[\sqrt{2}], +\big)$ are isomorphic, however, the rings $\big(\mathbb{Z}[i], +, \cdot\big)$ and $\big(\mathbb{Z}[\sqrt{2}], +, \cdot\big)$ are not.

**80)** Let $p$ be a prime. Prove, using the definition of a prime ideal, that

$$P = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, p \mid a, p \nmid b \right\}$$

is a prime ideal of the ring

$$R = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, p \nmid b \right\}$$

(as in exercise 68b).

**81)** Let $R\big(\neq \{0\}\big)$ be a commutative ring with identity and $P(\neq R)$ an ideal of $R$. Prove that the following are equivalent:

(i) $P$ is a prime ideal,

(ii) If $I, J$ are ideals and $I \cdot J \subseteq P$ then $I \subseteq P$ or $J \subseteq P$.

**Remarks:** 1) Property (ii) in exercise 81 is used as the definition of a prime ideal in general (i.e., not necessarily commutative) rings.

2) Let $R\big(\neq \{0\}\big)$ be a commutative ring with identity and $P$ an ideal of $R$. We have proved in Satz 75, Satz 76 and exercise 81 that the following four conditions are equivalent (and therefore characterize prime ideals).

(i) $P \neq R$ and $ab \in P$ implies $a \in P$ or $b \in R$ (with $a, b \in R$),

(ii) $R \setminus P$ is a multiplicative subset of $R$,

(iii) $P \neq R$ and $I \cdot J \subseteq P$ implies $I \subseteq P$ or $J \subseteq P$ (where $I, J$ are ideals of $R$),

(iv) $R/P$ is an integral domain.

**82)** Let $R$ and $S$ be commutative rings and $\varphi : R \to S$ an epimorphism of rings. Prove the following:

a) If $P$ is a prime ideal of $R$ and $\ker\varphi \subseteq P$ then $\varphi(P)$ is a prime ideal of $S$.
b) If $Q$ is a prime ideal of $S$ then $\varphi^{-1}(Q)$ is a prime ideal of $R$ and $\ker\varphi \subseteq \varphi^{-1}(Q)$.
c) There is an order preserving bijection between the set of prime ideals of $R$ that contain $\ker\varphi$ and the set of prime ideals of $S$.
d) If $I$ is an ideal of $R$ then every prime ideal of the factor ring $R/I$ has shape $P/I$, where $P$ is a prime ideal of $R$ satisfying $I \subseteq P$.

**83)** Let $R$ be a commutative ring with identity and $M \neq R$ an ideal of $R$. Prove that the following are equivalent:

(i) $M$ is a maximal ideal of $R$,
(ii) $\forall\ x \in R \setminus M\ \ \exists\ y \in R : 1_R - xy \in M$.

**84)** Let $p$ be a prime. Prove, using the definition of a maximal ideal, that

$$M = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, p \mid a, p \nmid b \right\}$$

is a maximal ideal of the ring

$$R = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z}, p \nmid b \right\}$$

(as in exercise 68b).

**85)** Let $R = 2\mathbb{Z}$ (i.e., $R$ denotes the ring of even integers with the usual addition and multiplication) and $M = 4\mathbb{Z}$. Prove the following:

a) $M$ is a maximal ideal but not a prime ideal of $R$,
b) $R/M$ is not a field.

**86)** Let $R$ be an integral domain and $S$ a multiplicative subset of $R$ with the property $0 \notin S$. Prove the following:

a) If $I$ is an ideal of $R$ then $S^{-1}I := \{a/s \mid a \in I, s \in S\}$ is an ideal of $S^{-1}R$.
b) If $I$ is an ideal of $R$ and $S \cap I \neq \varnothing$ then $S^{-1}I = S^{-1}R$.

**87)** Let $G_1, \ldots, G_n$ be groups. Prove the following: If $\sigma \in S_n$ then

$$G_{\sigma(1)} \times \cdots \times G_{\sigma(n)} \cong G_1 \times \cdots \times G_n.$$

**88)** Let $I \neq \varnothing$ be a (index) set and $G_i$ a group for all $i \in I$. Let $e_i$ denote the identity element of the group $G_i$ and

$$\prod_{i\in I}^{w} G_i := \left\{ (x_i)_{i\in I} \,\middle|\, x_i \in G_i \text{ for all } i \in I \text{ and } x_i = e_i \text{ for all but a finite number of } i \right\}.$$

Prove (with componentwise composition as in Satz 93)

$$\prod_{i\in I}^{w} G_i \trianglelefteq \prod_{i\in I} G_i.$$

**89)** Prove the following: If the group $G$ is the internal direct product of its two normal subgroups $N_1$ and $N_2$ then $G/N_1 \cong N_2$ and $G/N_2 \cong N_1$.

**90)** Is the group $S_3$ the internal direct product of two of its subgroups $N_1, N_2$ (satisfying $N_1, N_2 \neq \{\varepsilon\}$ and $N_1, N_2 \neq S_3$)?

**91)** Find groups $G_1, G_2, H_1$ and $H_2$ such that $G_1 \times G_2 \cong H_1 \times H_2$ but $G_i \ncong H_j$ for $i, j \in \{1, 2\}$.

**Definition:** Let $G$ be a group, $N \trianglelefteq G$ and $H \leq G$. The group $G$ is said to be the (internal) semidirect product of $N$ and $H$ if $G = NH$ and $N \cap H = \{e\}$. This is written as $G = N \rtimes H$.

**92)** Let the group $G$ be the semidirect product of $N \trianglelefteq G$ and $H \leq G$. Prove the following:

a) For every $a \in G$ the elements $n \in N$ and $h \in H$ with the property $a = nh$ are uniquely determined (i.e., the map $N \times H \to G$, $(n, h) \mapsto nh$ is bijective).

b) The map $\theta : H \to \mathrm{Aut}(N)$, $h \mapsto \theta_h$ is a homomorphism, where $\theta_h : N \to N$ is defined as $\theta_h(n) = hnh^{-1}$.

**93)** Prove the following: For $n \geq 3$ the symmetric group $S_n$ is the semidirect product of

$$A_n (\trianglelefteq S_n) \text{ and } \{\varepsilon, (12)\} (\leq S_n).$$

(As $\{\varepsilon, (12)\} \cong \mathbb{Z}_2$ this can be written is $S_n = A_n \rtimes \mathbb{Z}_2$.)

**94)** Prove the following: For $n \geq 3$ the dihedral group $D_n$ is the semidirect product of

$$\langle \alpha \rangle (\trianglelefteq D_n) \text{ and } \{\varepsilon, \beta\} (\leq D_n).$$

Here $\alpha$ and $\beta$ denote the same permutations as in Satz 47, compare also with exercise 56 from Algebra 1 (summer semester 2020). (As $\langle \alpha \rangle \cong \mathbb{Z}_n$ and $\{\varepsilon, \beta\} \cong \mathbb{Z}_2$ this can be written as $D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2$.)

**95)** Let $K$ be a field. Prove the following: The General Linear Group $\mathrm{GL}_n(K)$ is the semidirect product of the Special Linear Group $\mathrm{SL}_n(K)(\trianglelefteq \mathrm{GL}_n(K))$ and the group

$$H := \{\mathrm{diag}(a, 1, \dots, 1) \mid a \in K^*\}(\leq \mathrm{GL}_n(K)),$$

where $\mathrm{diag}(a_1, \dots, a_n)$ denotes the diagonal matrix with entries $a_1, \dots, a_n \in K$. (As $H \cong K^*$ this can be written as $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes K^*$.)

**Remarks:** 1) Because of Korollar 98 the (internal) direct product is a special case of the (internal) semidirect product. (I.e., if the group $G$ is the internal direct product of its normal subgroups $N_1$ and $N_2$ then $G$ is also the semidirect product of $N_1$ and $N_2$.)

2) It is possible that two groups $G$ and $H$ are semidirect products of isomorphic normal subgroups and isomorphic subgroups but are not isomorphic themselves.
I.e., it is possible that $G_1 = N_1 \rtimes H_1$, $G_2 = N_2 \rtimes H_2$, $N_1 \cong N_2$ and $H_1 \cong H_2$ but $G_1 \ncong G_2$. E.g., $\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$ (because of Satz 101) and $\mathbb{Z}_6$ is therefore (because of the remark above) also the semidirect product of $\mathbb{Z}_3$ and $\mathbb{Z}_2$. However, in exercise 94 it was proved that $D_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ as well. As $\mathbb{Z}_6$ is abelian but $D_3$ is not, they are not isomorphic. This phenomenon can be understood by regarding the maps $\theta$ (as described in exercise 92) which are different in both cases.

**96)** Let $I : \mathbb{R}^2 \to \mathbb{R}^2$, $I(x, y) = (x, y)$ and $S : \mathbb{R}^2 \to \mathbb{R}^2$, $S(x, y) = (x, -y)$. Let the group $G = (\{I, S\}, \circ)$ act on $M = \mathbb{R}^2$. Determine the orbits and isotropy groups of all $(x, y) \in \mathbb{R}^2$ as well as the fixed points of this group action.

**97)** Let the group $\mathrm{SO}(2)$ act on $\mathbb{R}^2$ by matrix multiplication $(A, x) \mapsto A \cdot x$. Determine the orbits and the isotropy groups of all $x \in \mathbb{R}^2$ as well as the fixed points of this group action.

**98)** Prove the following: The group $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half-plane of the complex plane (i.e., on $H = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$) via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}.$$

**99)** Prove the following: The isotropy group of $i$ for the action of the group $\mathrm{SL}_2(\mathbb{R})$ on the upper half-plane $H$ (as in the preceding exercise) is the group $\mathrm{SO}(2)$.

**100)** Let the group $G$ act on the set $M$. Prove the equation $G_{a \cdot x} = a \cdot G_x \cdot a^{-1}$ for all $x \in M$ and all $a \in G$, i.e., the isotropy groups of $x \in M$ and $a \cdot x \in M$ are conjugate.

**101)** Let $G$ be a group, $\varphi \in \mathrm{Aut}(G)$ and $C$ a conjugacy class of elements of $G$. Prove the following:

a) $\varphi(C)$ is also a conjugacy class,
b) If $\varphi \in \mathrm{Inn}(G)$ then $\varphi(C) = C$.

**102)** For a permutation $\sigma \in S_n$ and $r \in \{1, \dots, n\}$ let $z_r(\sigma)$ be the number of cycles of length $r$ in the decomposition of $\sigma$ into disjoint cycles. Prove that $\sigma, \tau \in S_n$ are conjugate if and only if $z_r(\sigma) = z_r(\tau)$ for all $r \in \{1, \dots, n\}$.

**103)** Let a group $G$ of order $|G| = 55$ act on a set $M$ with $|M| = 39$ elements. Prove that there has to exist a fixed point of this group action.

**104)** Determine the number and the elements of the Sylow 2-subgroups of the group $S_4$.

**105)** Determine the number and the elements of the Sylow 5-subgroups of the group $S_5$.

**106)** Let $G$ be a finite simple group of order $|G| = 168$. Determine the number of $a \in G$ of order $\mathrm{ord}(a) = 7$.

**Remark:** It can be proved that the group $\mathrm{SL}_3(\mathbb{Z}_2)$ is simple and of order 168.

**107)** Prove that the group $A_5$ contains no subgroup of order 15.

**Theorem (Fermat):** Let $p$ be a prime number (in $\mathbb{Z}$). Then the following are equivalent:

(i) There are $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$,
(ii) $p = 2$ or $p \equiv 1 \pmod 4$.

**Proof:** (i) $\Rightarrow$ (ii) If $2 \mid x$ then $x^2 \equiv 0 \pmod 4$. If $2 \nmid x$ then $x^2 \equiv 1 \pmod 4$. This implies $p = x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. It is impossible that $p \equiv 0 \pmod 4$ and $p \equiv 2 \pmod 4$ is possible only if $p = 2$.
(ii) $\Rightarrow$ (i) (Heath-Brown) As $2 = 1^2 + 1^2$ we can from now on assume $p \equiv 1 \pmod 4$. Let

$$S := \{(x, y, z) \in \mathbb{Z}^3 \mid x, y \geq 1, 4xy + z^2 = p\}.$$

The set $S$ is not empty (as $((p-1)/4, 1, 1) \in S$) and finite as $(x, y, z) \in S$ implies $x, y \leq p/4$ and for fixed $x, y$ there are at most two possible values for $z$. We will make use of the map $f : S \to S$, $(x, y, z) \mapsto (y, x, -z)$. It is an involution (i.e., $f \circ f = \mathrm{id}_S$) and has no fixed points (as $f(x, y, z) = (x, y, z)$ is the same as $(y, x, -z) = (x, y, z)$ which implies $z = 0$ and

therefore $p = 4xy$, which is impossible). Clearly $f$ maps the set $T := \{(x, y, z) \in S \mid z > 0\}$ bijectively onto $S \setminus T$. There is no $(x, y, z) \in S$ satisfying $x - y + z = 0$, as this would imply $p = 4xy + z^2 = 4xy + (x - y)^2 = (x + y)^2$. Setting $U := \{(x, y, z) \in S \mid x - y + z > 0\}$, the set $U$ is mapped bijectively onto $S \setminus U$ by $f$. This shows $|T| = |S|/2 = |U|$. Now consider the map

$$g : U \to U, \quad (x, y, z) \mapsto (x - y + z, y, 2y - z).$$

We first check that $g$ is well-defined. If $(x, y, z) \in U$ then $x - y + z > 0$ and $y > 0$ and therefore

$$4(x - y + z)y + (2y - z)^2 = 4xy - 4y^2 + 4yz + 4y^2 - 4yz + z^2 = 4xy + z^2 = p,$$

i.e., $g(x, y, z) \in S$. As $x - y + z - y + 2y - z = x > 0$ we have $g(x, y, z) \in U$. Furthermore, $g$ is also an involution as

$$(g \circ g)(x, y, z) = g(x - y + z, y, 2y - z) = (x - y + z - y + 2y - z, y, 2y - 2y + z) = (x, y, z)$$

and it is easy to see that $g$ has exactly one fixed point as $g(x, y, z) = (x, y, z)$ is the same as $(x - y + z, y, 2y - z) = (x, y, z)$, whence $y = z$ and thus $p = 4xy + y^2 = (4x + y)y$. This is only possible if $y = z = 1$ and $x = (p - 1)/4$. This shows $|U| \equiv 1 \pmod 2$ and therefore $|T| \equiv 1 \pmod 2$. Finally let $h : T \to T$, $(x, y, z) \mapsto (y, x, z)$. Then $h$ is clearly well-definied and an involution. As $|T| \equiv 1 \pmod 2$, the map $h$ has to have a fixed point, i.e., there is a $(x, y, z) \in T$ with the property $x = y$ and therefore $p = 4x^2 + z^2 = (2x)^2 + z^2$.

**Definition:** For $a \in \mathbb{Z}[i]$ the norm $N(a)$ is defined as $N(a) := a \cdot \overline{a} = |a|^2$ (i.e., if $a = x + iy$ with $x, y \in \mathbb{Z}$ then $N(x + iy) = x^2 + y^2$).

**108)** Let $a, b \in \mathbb{Z}[i]$. Prove the following:

a) $N(a \cdot b) = N(a) \cdot N(b)$,
b) If $a \mid b$ (divisibility in $\mathbb{Z}[i]$) then $N(a) \mid N(b)$ (divisibility in $\mathbb{Z}$),

**109)** Let $a \in \mathbb{Z}[i]$. Prove the following:

a) $a \in \mathbb{Z}[i]^* \Leftrightarrow N(a) = 1 \Leftrightarrow a \in \{1, -1, i, -i\}$,
b) If $N(a)$ is a prime number then $a$ is an irreducible element of $\mathbb{Z}[i]$ (and thus prime).

**110)** Prove the following properties of the unique factorization domain $\mathbb{Z}[i]$:
*Hint.* Use Fermat's result above and the preceding exercise.

a) $1+i$ is an irreducible element of $\mathbb{Z}[i]$ (and $2 = -i \cdot (1+i)^2$, i.e., 2 is *ramified*),
b) If $p \equiv 1 \pmod 4$ is a prime number and $x, y \in \mathbb{Z}$, $x > y > 0$ such that $p = x^2 + y^2$ then both $x + iy$ and $x - iy$ are irreducible elements of $\mathbb{Z}[i]$ and are not associates (and $p = (x+iy)(x-iy)$, i.e., $p$ *splits*),
c) If $p \equiv 3 \pmod 4$ is a prime number then $p$ is also an irreducible element of $\mathbb{Z}[i]$ (i.e., $p$ is *inert*).

**111)** Let $R$ be a Euclidean domain whose function $\varphi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ satisfies the additional condition $\varphi(ab) \geq \varphi(a)\ \forall a, b \in R \setminus \{0\}$.

a) Which of the Euclidean domains we discussed so far satisfy this condition?
b) Prove for all $a, b \in R \setminus \{0\}$: If $a$ and $b$ are associates then $\varphi(a) = \varphi(b)$,
c) Prove for all $a, b \in R \setminus \{0\}$: If $\varphi(a) = \varphi(b)$ and $a \mid b$ then $a$ and $b$ are associates,
d) Prove for all $a \in R \setminus \{0\}$: $a \in R^* \Leftrightarrow \varphi(a) = \varphi(1_R)$.

**112)** Let $R$ be a unique factorization domain and $a \in R \setminus \{0\}$. Prove that the ideal $(a)$ is contained in only finitely many prinicipal ideals of $R$.

**113)** Let $R(\neq \{0\})$ be a commutative ring with identity and

$$p(X) = a_0 + a_1 X + \cdots + a_n X^n \in R[X].$$

a) Prove

$$p \in R[X]^* \quad \Longleftrightarrow \quad a_0 \in R^* \text{ and } a_1, \ldots, a_n \in \operatorname{Nil}(R).$$

*Hint:* Let $p(X) \cdot q(X) = 1$ with $q(X) = b_0 + b_1 X + \cdots + b_m X^m \in R[X]$. Use induction on $r$ to show $a_n^{r+1} b_{m-r} = 0$. Deduce that $a_n$ is nilpotent and use exercise 72.
b) Find $\left(\overline{2}X + \overline{3}\right)^{-1} \in \mathbb{Z}_8[X]$.

**114)** Perform the division algorithm for polynomials for the following $f, g \in \mathbb{Q}[X]$, i.e., find polynomials $q, r \in \mathbb{Q}[X]$ such that $f = qg + r$ and $\operatorname{grad} r < \operatorname{grad} g$:

a) $f(X) = X^6 + X^5 - X^4 - 4X^3 - 2X^2 + 2X - 4$,
   $g(X) = X^5 + 2X^4 - 2X^3 - 5X^2 - 5X + 2$
b) $f(X) = X^5 - 2X^4 + 3X^3 - 6X^2 + 2X - 4$, $g(X) = X^4 + X^3 - 5X^2 + X - 6$
c) $f(X) = X^8 - 1$, $g(X) = X^2 - 1$

**115)** Find the greatest common divisors of the polynomials

$$p(X) = X^3 - 2X^2 - X + 2 \quad \text{and} \quad q(X) = X^3 - 4X^2 + 3X$$

in the ring of polynomials $\mathbb{Q}[X]$ using the Euclidean algorithm. Determine polynomials $f_1, f_2 \in \mathbb{Q}[X]$ such that $f_1 p + f_2 q = g$, where $g \in \mathbb{Q}[X]$ denotes the uniquely determined monic greatest common divisor of $p$ and $q$.

**116)** Show that $\mathbb{Z}[X]$ is not a principal ideal domain by proving that the ideal $I := (2, X)$ is not a principal ideal.

**117)** Let $R$ be an infinite integral domain. Prove that the map, which assigns to each $p \in R[X]$ the polynomial function $f_p : R \to R$, $\alpha \mapsto p(\alpha)$, is injective.

**118)** Let $K$ be a field with $\operatorname{char} K = p > 0$ and $f \in K[X]$ with $\operatorname{grad} f \geq 1$. Prove that $f' = 0$ if and only if there exists a $g \in K[X]$ such that $f(X) = g(X^p)$.

**119)** Apply Eisenstein's criterion to prove that the following polynomials are irreducible in $\mathbb{Q}[X]$:

a) $X^3 + 6X + 2$
b) $3X^4 + 15X^2 + 10$
c) $2X^5 - 6X^3 + 9X^2 - 15$
d) $X^{11} - 7X^6 + 21X^5 + 49X - 56$

**120)** Let $p$ be a prime. The $p$-th cyclotomic polynomial $\Phi_p(X)$ is

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Apply Eisenstein's criterion to show that $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$.
*Hint.* Use $\Phi_p(X) = (X^p - 1)/(X - 1)$, consider $\Phi_p(X + 1)$ and apply the binomial theorem.

**121)** Let $K$ be a field and $n \in \mathbb{N} \setminus \{0\}$. Prove that $E_n := \{a \in K \mid a^n = 1\}$ is a finite cyclic subgroup of $(K^*, \cdot)$.

**122)** Let $p$ be a prime and let $L/K$ be a field extension with $[L : K] = p$. Prove $L = K(a)$ for all $a \in L \setminus K$.

**123)** Determine the minimal polynomial $m_{a,K}$ of $a$ over $K$ for the field extension $L/K$ and $a \in L$.

a) $L = \mathbb{C}$, $K = \mathbb{R}$, $a = \sqrt{7}$,
b) $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = \sqrt{7}$,
c) $L = \mathbb{C}$, $K = \mathbb{Q}$, $a = \big(1 + \sqrt{5}\big)/2$.

**124)** Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ are isomorphic as vector spaces over $\mathbb{Q}$ but not as rings.

**125)** Let $L/K$ be a field extension and let $a \in L$ be algebraic over $K$. Prove the following: If $\operatorname{grad} m_{a,K}$ is odd then $K(a^2) = K(a)$. Is this also true if $\operatorname{grad} m_{a,K}$ is even? Deduce $\mathbb{Q}\big(\sqrt[3]{2}\big) = \mathbb{Q}\big(\sqrt[3]{4}\big)$.