cschneid@risc.jku.at

# Exercises

## Lecture for March 7, 2023

**HW 1.** Let $M$ be a nonempty set. Show that the following statements are equivalent:

1. $M$ is an abelian group.
2. $M$ is a $\mathbb{Z}$-module.

## Lecture from March 14, 2023

**HW 2.** Let $V$ be a left $R$-module. Show (using only module axioms) that for all $r \in R$ and $v \in V$ the following holds:

1. $r * 0_M = 0_M$
2. $0_R * v = 0_M$
3. $(-r) * v = -(r * v)$
4. If $r \in R^*$ and $r * v = 0_M$ then $v = 0_M$

**HW 3.** Let $M$ be a left $R$-module and $X \subseteq M$. Show: $\langle X \rangle$ is a submodule of $M$. Further, any submodule $N$ of $M$ with $X \subseteq N$ contains $\langle X \rangle$.

**HW 4.** Let $N$ be a submodule of a left $R$-module $M$ with the scalar multiplication $*_M$. Show: the quotient group $M/N$ turns to a left $R$-module with the (properly defined?) scalar multiplication

$$r * (N + a) := N + (r *_M a).$$

## Lecture from March 21, 2023

**HW 5.** Consider the non-commutative ring $R = \operatorname{End}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}) = \{f : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}^{\mathbb{N}} \mid f \text{ is a linear map}\}$ where the multiplication is the composition of linear maps. Define the maps $\phi_i, \psi_i \in R$ with

$$\begin{aligned}
\phi_1((a_0, a_1, a_2, a_3 \dots)) &= (a_0, a_2, \dots) \\
\phi_2((a_0, a_1, a_2, a_3 \dots)) &= (a_1, a_3, \dots) \\
\psi_1((a_0, a_1, a_2, a_3 \dots)) &= (a_0, 0, a_1, 0, \dots) \\
\psi_2((a_0, a_1, a_2, a_3 \dots)) &= (0, a_0, 0, a_1, 0, \dots)
\end{aligned}$$

1. Show that $\phi_1\,\psi_1 = \phi_2\,\psi_2 = 1$, $\phi_1\,\psi_2 = \phi_2\,\psi_1 = 0$ and $\psi_1\,\phi_1 + \psi_2\,\phi_2 = 1$.
2. Using these relations show that $\langle \phi_1, \phi_2 \rangle = R$.

**HW 6.** [S-Lemma] Let $R$ be a ring and $A \in R^{l \times m}$, $B \in R^{m \times n}$. Show:

1. $S_R(A\,B) \subseteq S_R(B)$.
2. If $l = m$ and $A \in \mathrm{GL}_m(A)$, then
$$S_R(A\,B) = S_R(B).$$
3. If $C \in R^{k \times n}$ with $S_R(C) \subseteq S_R(B)$ then there is a $D \in R^{k \times m}$ with
$$C = D\,B.$$

## Lecture from March 28, 2023

**BP 1.** Let $R$ be a commutative ring and let $A \in \mathrm{M}_n(R)$. Show:

$$\mathrm{adj}(A)\,A = A\,\mathrm{adj}(A) = \det(A)\,I_n$$

(e.g., by lifting the result from the field to the ring version.)

**HW 7.** Let $R$ be a commutative ring. Show: If $A \in \mathrm{M}_n(R)$ has a left-inverse (resp. right-inverse) $B \in \mathrm{M}_n(R)$, then $B$ is also a right-inverse (resp. left-inverse) of $A$.

**HW 8.** Let $M$ and $N$ be isomorphic $R$-modules with $M \overset{f}{\simeq} N$, and let $x_1, \ldots, x_n$ be a basis of $M$. Show: $f(x_1), \ldots, f(x_n)$ is a basis of $R$.

**HW 9.** There is no infinite basis of $R^n$.

**HW 10.** Let $R$ be a commutative ring. Let $M$ be an $R$-module which is free (i.e., has a basis) and which is finitely generated. Then $M$ has a finite basis and any other basis has the same number of elements.

**HW 11.** Let $M$ be an $R$-module with the basis $x_1, \ldots, x_m$. If $A \in \mathrm{GL}_m(R)$, then $y_1, \ldots, y_m$ with

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = P \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

is also a basis of $M$.

## Lecture from April 18, 2023

**HW 12.** Let $R$ be a commutative ring and $U$ be a submodule of $R^m$. Define

$$U_i = U \cap \left(\{0\}^{i-1} \times R^{m-i+1}\right)$$
$$S_i = \{a \mid (\underbrace{0,\dots,0}_{i-1 \text{ zeroes}}, a, \dots) \in U_i\}$$

Show:

1. $U_i$ is a submodule of $U_{i-1}$ over $R$.
2. $S_i$ is an ideal in $R$.

**HW 13.** Let $R$ be a PID. Show: Every submodule of a free $R$-module with rank $m$ is free and has rank $\leq m$.

**HW 14.** Let

$$A = \begin{pmatrix} 1 & -1 & 3 & 0 \\ 0 & 2 & 4 & -2 \\ 0 & 0 & 0 & 3 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 5 & -7 & 11 & 5 \\ 6 & -4 & 22 & -2 \\ 10 & -10 & 30 & 3 \end{pmatrix}.$$

Check if $S_{\mathbb{Z}}(A) = S_{\mathbb{Z}}(B)$ holds.

## Lecture from April 25, 2023

**HW 15.** Let $R$ be a ring, and let $A, B \in R^{n\times m}$ be row equivalent. Show:

1. $S_R(A) = S_R(B) =: U$
2. The rows of $A$ form a basis of $U$ if and only if the rows of $B$ form a basis of $U$.

**HW 16.** Let $R$ be an Euclidean domain. Show:

1. For all $a \in R$: $N(a) \geq N(1)$.
2. For all $a, b \in R^+$: $N(a\,b) = N(a)$ if and only if $b \in R^*$.

**HW 17.** Compute the row echelon form of

1. $\begin{pmatrix} 5 & -7 & 11 & 5 \\ 6 & -4 & 22 & -2 \\ 10 & -10 & 30 & 3 \end{pmatrix}$ in $\mathbb{Z}$.
2. $\begin{pmatrix} x+x^2 & x+x^2 & 1 \\ x^3 & 1 & x+1 \\ x^2 & 1 & 1 \end{pmatrix}$ in $\mathbb{Z}_2[x]$.

**HW 18.** Complete the proof of Theorem CHAR.

**HW 19.** Compute the inverse of

$$\begin{pmatrix} 1 & 1 & 3 \\ 3 & 2 & 11 \\ -1 & 1 & -6 \end{pmatrix} \qquad \text{in } \mathbb{Z}.$$

## Lecture from May 2, 2023

**HW 20.** Compute the Smith normal form of

$$\begin{pmatrix} -7 & 15 & -7 \\ 4 & 8 & -2 \\ -5 & 11 & -5 \end{pmatrix} \qquad \text{in } \mathbb{Z}.$$

**HW 21.** Let $R$ be a commutative ring, $A \in R^{m\times n}$, $b \in R^m$ and $Q \in \mathrm{GL}_n(R)$. Define

$$\begin{aligned} S_1 &= \{x \in R^n \mid A\,x = b\}, \\ S_2 &= \{x \in R^n \mid A\,Q\,x = b\}. \end{aligned}$$

Show: $S_1$ and $S_2$ are in $1-1$ correspondence with $f : S_1 \to S_2$ where $f(x) = Q^{-1}\,x$ and $f^{-1}(x) = Q\,x$.

**HW 22.** Let $R$ be a commutative ring, $A \in R^{m\times n}$, $b \in R^m$ and $P \in \mathrm{GL}_m(R)$. Define

$$\begin{aligned} S_1 &= \{x \in R^n \mid A\,x = b\}, \\ S_2 &= \{x \in R^n \mid P\,A\,x = b\}. \end{aligned}$$

Show: $S_1 = S_2$.

**HW 23.** Solve the following linear system over $\mathbb{Z}$:

$$\begin{aligned} -5x + 2y + 4z + w &= 8 \\ 27x + 10y + 2z + 7w &= 6 \\ -20x - 6y - 4w &= -10. \end{aligned}$$

## Lecture from May 9, 2023

**HW 24.** Let $N$ be a submodule of an $R$-module $M$ and let $f : M \to M$ be an $R$-isomorphism. Then $f(N)$ is a submodule of $M$. Show:

$$M/f(N) \simeq M/N.$$

**HW 25.** Let $R$ be a ring, $A \in R^{m\times n}$ and $Q \in \mathrm{GL}_n(R)$. Show: $f : R^n \to R^n$ with

$$f(x) = x\,Q$$

is a bijective map with

$$S_R(A\,Q) = f(S_R(A)).$$

**HW 26.** Let $A = \begin{pmatrix} 2 & -1 & 3 \\ 4 & 3 & -5 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & -2 \\ 0 & 1 \end{pmatrix}$. Does

$$\mathbb{Z}^3/S_{\mathbb{Z}}(A) \simeq \mathbb{Z}^2/S_{\mathbb{Z}}(B)$$

hold?

**HW 27.** Why are $\mathbb{Z}_{24}$, $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$ are not isomorphic?

## Lecture from May 16, 2023

**HW 28.** Let $M$ be an $R$-module over an Euclidean domain, suppose that

$$M \simeq R/Rd_1 \times \cdots \times R/Rd_r \times R^{n-r}$$

and let $y_1, \ldots, y_n \in M$ as defined in the lecture such that

$$M = Ry_1 \oplus \cdots \oplus Ry_n.$$

Show that

$$Ry_i \simeq \begin{cases} R/Rd_i & \text{if } 1 \leq i \leq r \\ R & \text{if } i > r. \end{cases}$$

**HW 29.** Let $R$ be an Euclidean domain and $A \in R^{m \times n}$. Show:

1. The ranks of $A$ and $A^t$ are the same and the elementary divisors are the same up to units.
2. The rank, row rank and column rank of $A$ are all equal.

## Lecture from May 23, 2023

**HW 30.** Let $\mathbb{F}$ be a field and $A \in V = \mathrm{M}_n(\mathbb{F})$. Show that $a = (A^n)_{n \geq 0} \in V^{\mathbb{N}}$ is $c$-finite. What is the characteristic polynomial of $a$?

**HW 31.** Let $V$ be an $\mathbb{F}$-vector space. Define the operation $\circ : \mathbb{F}[x] \times V^{\mathbb{N}} \to V^{\mathbb{N}}$ by linear continuation of

$$\begin{aligned} x \circ \langle a_0, a_1, \ldots \rangle &\mapsto \langle a_1, a_2, \ldots \rangle \\ c \circ \langle a_0, a_1, \ldots \rangle &\mapsto \langle c\, a_0, c\, a_1, \ldots \rangle, \quad c \in \mathbb{F}. \end{aligned}$$

Show that $V^{\mathbb{N}}$ is an $\mathbb{F}[x]$-module.

**HW 32.** Let $a \in V^{\mathbb{N}}$. Show that

$$\mathrm{Ann}(a) = \{f \in \mathbb{F}[x] \mid f \circ a = 0\}$$

is an ideal in $\mathbb{F}[x]$.

**HW 33.** Let $f, g \in \mathbb{F}[x] \setminus \{0\}$. Show

a $(f\, g)^* = f^* g^*$;

b If $f \mid g$ then $f^* \mid g^*$;

c $\gcd(f^*, g^*) = \gcd(f, g)^*$.

## Lecture from June 6, 2023

**HW 34.** Let $a = (a_n)_{n\geq 0} \in \mathbb{F}^{\mathbb{N}}$ be a sequence which satisfies a $C$-finite recurrence of order $m$. Define

$$A_d = -\begin{pmatrix} a_0 & a_1 & \dots & a_{d-1} \\ a_1 & a_2 & \dots & a_d \\ \vdots & & & \\ a_{d-1} & a_d & \dots & a_{2d-1} \end{pmatrix} \in \mathbb{F}^{d\times d}$$

for $d \in \mathbb{N}^+$. Show that

$$\deg(\mu_a) = \max\{0 \leq i \leq m \mid \det A_i \neq 0\}.$$

## Lecture from June 13, 2023

**HW 35.** Let $a, b, s, t, r \in \mathbb{F}[x]$ with $\deg(a) > \deg(b)$, $\deg(a) > \deg(t) + \deg(r)$ and $s\,a + t\,b = r$. Let $((r_i, s_i, t_i))_{-1\leq i\leq r}$ be the extended polynomial remainder sequences of $a$ and $b$ . Then we have shown that for $j$ with $\deg(r_j) \leq \deg(r) \leq \deg(r_{j-1})$ there is an $h \in \mathbb{F}[x]$ such that $s = h\,s_j$, $t = h\,t_j$ and $r = h\,r_j$. Show: If $\deg(t) \leq m$ then the $j$ is also determined by the the XPRS, i.e., by

$$\deg(r_j) < m \leq \deg(r_{j-1}).$$

**BP 2.** Apply the above result to link it to Padé approximation. More precisely, how can Padé approximation be solved with the extended Eucliden algorithm and can one check if there exists such a solution?

**HW 36.** Prove the Cayley-Hamilton theorem: let $A \in \mathrm{M}_n(\mathbb{F})$ and define the polynomial $c_A(x) = \det(I_n\,x - A) = \sum_{i=0}^{n} f_i\,x^i \in \mathbb{F}[x]$. Show that $C_A(A) = \sum_{i=0}^{n} f_i\,A^i = 0$.

**HW 37.** Let $A \in \mathrm{M}_n(\mathbb{F}) =: V$ and $a = (A^i)_{i\geq 0} \in V^{\mathbb{N}}$. Let $c_A$ be the characteristic polynomial of $A$ (see the HW above), i.e., the characteristic polynomial of $a$. Let $v \in \mathbb{F}^n =: V'$ and define $a' := (A^i v)_{i\geq 0} \in V'^{\mathbb{N}}$. Further let $v \in \mathbb{F}^n$ and define $a'' := (bA^i v)_{i\geq 0} \in \mathbb{F}^{\mathbb{N}}$. Let $\mu_a$, $\mu_{a'}$ and $\mu_{a''}$ be the minimal polynomials of $a$, $a'$ and $a''$, respectively. Show:

1. $\mu_a$ is a characteristic polynomial of $a'$ and we have $\mu_{a'} \mid \mu_a \mid c_A$.
2. $\mu_{a'}$ is a characteristic polynomial of $a''$ and we have $\mu_{a''} \mid \mu_{a'}$.

## Lecture from June 20, 2023

**HW 38.** Given

$$A \in \begin{pmatrix} 1 & 4 & 4 \\ 4 & 0 & 3 \\ 1 & 2 & 4 \end{pmatrix} \in \mathbb{F}_5^{3\times 3} \quad \text{and} \quad b = \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} \in \mathbb{F}_5^3.$$

Find $y \in \mathbb{F}_5^3$ with $A\,y = b$ by choosing $u = (1, 2, 0)$ in Wiedemann's algorithm.

**HW 39.** Show that
$$M_f = \{a \in \mathbb{F}^{\mathbb{N}} \mid f \circ a = 0\}$$
for $f \in \mathbb{F}[x]$ is an $\mathbb{F}[x]$-module.

**HW 40.** Let $c = (c_n)_{n\geq 0} \in \mathbb{F}^{\mathbb{N}}$ with $(c_0, c_1, \ldots, c_{d-1}) = (0, \ldots, 0, 1)$ and $f \circ c = 0$. Define $\tau : \mathbb{F}[x] \to \mathbb{F}[x] \circ c = \langle c \rangle_{\mathbb{F}[x]}$ with $\tau(h) = h \circ c$. Show that $\ker(\tau) = \langle f \rangle = \mathbb{F}[x]\, f$.

**HW 41.** Consider $\psi : \mathbb{F}^n \to \mathbb{F}[x]/\langle f \rangle$ as given in the lecture. Show for $u \in \mathbb{F}^n$: $\psi(u)$ is not a zero divisor if and only if $\psi(u)$ is a unit in $\mathbb{F}[x]/\langle f \rangle$.

**HW 42.** Let $f, g \in \mathbb{F}[x] \setminus \{0\}$. Show: $\gcd(f, g) \neq 1$ if and only if there are $s, g \in \mathbb{F}[x] \setminus \{0\}$ with $\deg(s) < \deg(g)$, $\deg(t) < \deg(f)$ and $s\, f + t\, g = 0$.