Lösungen der Klausur
am 01.09.2015 zur Linearen Algebra IIa

1. *(6=3+1+1+1 Punkte)*

   (a) Eine Relation $R \subset M \times M$ ist eine *Äquivalenzrelation*, falls sie folgende drei Eigenschaften erfüllt:

   (i) *Reflexivität:* Für alle $x \in M$ gilt: $(x,x) \in R$.

   (ii) *Symmetrie:* Für alle $x, y \in M$ gilt: $(x,y) \in R \Rightarrow (y,x) \in R$.

   (iii) *Transitivität:* Für alle $x, y, z \in M$ gilt: $(x,y) \in R$ und $(y,z) \in R \Rightarrow (x,z) \in R$.

   (b) U ist genau dann ein Normalteiler von G, wenn $U = aUa^{-1}$ für alle $a \in G$ ist.

   (c) Eine Teilmenge $I \subset R$ ist genau dann ein Ideal, wenn sie eine additive Untergruppe mit

   $$a \in I,\ b \in R \Rightarrow b \cdot a \in I$$

   ist.

   (d) Ein Ideal $I \subset R$ ist genau dann ein maximales Ideal, wenn $I \subsetneqq R$ gilt und wenn kein Ideal $J \subset R$ mit $I \subsetneqq J \subsetneqq R$ existiert.

2. *(6=5+1 Punkte)*

   (a)

$$\begin{array}{l|c|c}
150 = 2 \cdot 55 + 40 & q_1 = 2 & r_2 = 40 \\
55 = 1 \cdot 40 + 15 & q_2 = 1 & r_3 = 15 \\
40 = 2 \cdot 15 + 10 & q_3 = 2 & r_4 = 10 \\
15 = 1 \cdot 10 + 5 & q_4 = 1 & r_5 = 5 \\
10 = 2 \cdot 5 & q_5 = 2 & r_6 = 0
\end{array}$$

i	r_i	q_i	x_i	y_i
0	150	–	1	0
1	55	2	0	1
2	40	1	1	-2
3	15	2	-1	3
4	10	1	3	-8
5	5	2	-4	11
6	0	–	$\frac{r_1}{r_5} = 11$	$-\frac{r_0}{r_5} = -30$

   also $n = 5$, $\quad ggT(r_0, r_1) = r_5 = 5$.

   (b) $n \leq 5 \cdot |\text{Dezimalstellen von } r_1|$.

3. *(6=3+3 Punkte)*

(a) Es ist $x^3 - 1 = \Phi_1 \cdot \Phi_3$ und $\Phi_1 = x - 1$. Daher ist

$$\Phi_3 = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

Es ist $x^9 - 1 = \Phi_1 \cdot \Phi_3 \cdot \Phi_9 = (x^3 - 1) \cdot \Phi_9$. Daher ist

$$\Phi_9 = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1.$$

Es ist $x^{27} - 1 = \Phi_1 \cdot \Phi_3 \cdot \Phi_9 \cdot \Phi_{27} = (x^9 - 1) \cdot \Phi_{27}$. Daher ist

$$\Phi_{27} = \frac{x^{27} - 1}{x^9 - 1} = x^{18} + x^9 + 1.$$

(b) Lösungen zu $b \equiv 4 \bmod 5$ sind $4, 9, 14, 19, 24, ...$ Ihre Reste modulo 7 sind $4, 2, 0, 5, 3, ...$ Also ist $b_0 := 24$ eine Lösung des Gleichungssystems

$$\begin{aligned} b &\equiv 4 \bmod 5 \\ b &\equiv 3 \bmod 7 \end{aligned}$$

Es ist $b_0 \equiv 7 \bmod 17$ und $5 \cdot 7 = 35 \equiv 1 \bmod 17$. Also ist

$$\begin{aligned} b &= 24 + 2 \cdot 35 = 94 \\ \text{mit } b &\equiv 7 + 2 \cdot 1 = 9 \bmod 17 \end{aligned}$$

eine Lösung des Gleichungssystems

$$\begin{aligned} b &\equiv 4 \bmod 5 \\ b &\equiv 3 \bmod 7 \\ b &\equiv 9 \bmod 17 \end{aligned}$$

4. *(6=3+3 Punkte)*

(a) Sei G eine endliche Gruppe, und sei U eine Untergruppe von G.
Dann sind auch U und G/U endlich, und alle Linksnebenklassen (und Rechtsnebenklassen) haben genauso viele Elemente wie U. Daher ist

$$|G| = |U| \cdot |G/U|.$$

Also teilt die Ordnung $|U|$ von U die Ordnung $|G|$ von G.

(b) Es ist $[a] \in \mathbb{Z}/p\mathbb{Z} - \{0\}$, also $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$. Die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ hat Ordnung $p - 1$. Das Element $[a]$ erzeugt eine zyklische Untergruppe $\langle [a] \rangle \subset (\mathbb{Z}/p\mathbb{Z})^*$. Aufgrund des Satzes von Lagrange gilt
$|\langle [a] \rangle| \mid |(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$. Aber die Ordnung von $[a]$ ist gleich $|\langle [a] \rangle|$. Daraus folgt $[a]^{p-1} = [1]$, also $a^{p-1} \equiv 1 \bmod p$. $\square$

5. *(6 Punkte)* Die 4 erzeugenden Elemente sind $b := \alpha+1, \alpha+2, 2\alpha+1$ und $2\alpha+2$. Das folgt aus folgenden Rechnungen:

$$\begin{aligned}
b^0 &= 1, \\
b^1 &= \alpha+1, \\
b^2 &= (\alpha+1)^2 = \alpha^2+2\alpha+1 = 2\alpha, \\
b^3 &= (\alpha+1)\cdot 2\alpha = 2\alpha^2+2\alpha = 2\alpha+1, \\
b^4 &= (\alpha+1)\cdot(2\alpha+1) = 2\alpha^2+3\alpha+1 = 2, \\
b^5 &= (\alpha+1)\cdot 2 = 2b^1 = 2\alpha+2, \\
b^6 &= (\alpha+1)\cdot(2\alpha+2) = 2b^2 = \alpha, \\
b^7 &= (\alpha+1)\cdot\alpha = 2b^3 = \alpha+2.
\end{aligned}$$

6. *(6=2+1+2+1 Punkte)*

   (a) $\Phi_f : K[t] \to \mathrm{End}(V)$ bildet $\sum_{j=0}^m a_j t^j$ auf $\sum_{j=0}^m a_j f^j$ ab. Φ_f ist ein Ringhomomorphismus und ein K-Vektorraumhomomorphismus.

   (b) Sei $f : V \to V$ ein Endomorphismus eines K-Vektorraums V mit $\dim_K V = n \in \mathbb{N}$. Es ist
   $$P_f(f) = 0 \in \mathrm{End}(V).$$

   (c) Der Kern der Abbildung Φ_f oben enthält ein eindeutiges unitäres Polynom mit kleinstem positiven Grad. Es ist das Minimalpolynom $M_f(t)$ von f.

   (d) $P_f(t) = (t-\alpha)^9\cdot(t-\beta)^5\cdot(t-\gamma)^7$.
   $M_f(t) = (t-\alpha)^5\cdot(t-\beta)^2\cdot(t-\gamma)^3$.

7. *(6 Punkte)* $\Rightarrow$: Sei R/I ein Körper. Wegen Lemma 11.19 (c) reicht es zu zeigen, dass für jedes $a \in R-I$ gilt: $(a)+I = R$. Sei $a \in R-I$. Dann ist $[a] \in R/I - \{0\}$. Daher ist $[a]$ invertierbar. Also gibt es ein $b \in R$ mit $[a][b] = 1_{R/I} = [1_R]$. Daher ist $1_R \in ab + I \subset (a)+I$. Daher ist $R = (a)+I$.

   $\Leftarrow$: Sei I ein maximales Ideal. R/I ist ein kommutativer Ring mit Einselement $1_{R/I} = [1_R]$. Zu zeigen ist, dass jedes Element $[a] \in R/I - \{0\}$ invertierbar ist. Sei $[a] \in R/I - \{0\}$. Dann ist $a \in R - I$. Weil I ein maximales Ideal ist, ist $(a)+I = R$. Also gibt es es ein $b \in R$ und ein $u \in I$ mit $ab + u = 1_R$. Es folgt $[a][b] = [1_R] = 1_{R/I}$. Also ist $[a]$ invertierbar, und das Inverse ist $[b]$. $\square$

8. *(6 Punkte)* (Spektralsatz für hermitesche Matrizen) Sei $A \in M(n\times n, \mathbb{C})$ eine hermitesche Matrix, also $\overline{A} = A^{tr}$.

   Sei $\lambda \in \mathbb{C}$ ein Eigenwert von A als komplexer Matrix, und sei $v = (v_1, ..., v_n)^{tr} \in M(n\times 1, \mathbb{C}) - \{0\}$ ein Eigenvektor mit Eigenwert λ, also $M\cdot v = \lambda\cdot v$. Es ist $v^{tr}\cdot\overline{v} > 0$ wegen $v \neq 0$. Es ist

$$\begin{aligned}
\lambda\cdot(v^{tr}\cdot\overline{v}) &= (\lambda\cdot v)^{tr}\cdot\overline{v} = (A\cdot v)^{tr}\cdot\overline{v} \\
&= v^{tr}\cdot A^{tr}\cdot\overline{v} = v^{tr}\cdot\overline{A}\cdot\overline{v} = v^{tr}\cdot\overline{A\cdot v} \\
&= v^{tr}\cdot\overline{\lambda\cdot v} = \overline{\lambda}\cdot(v^{tr}\cdot\overline{v}).
\end{aligned}$$

   Daher ist $\lambda = \overline{\lambda}$, also $\lambda \in \mathbb{R}$.

Es gibt eine Basis $b_1, , , .b_n$ von $M(n \times 1, \mathbb{R})$, so dass mit $B := (b_1 ... b_n) \in GL(n, \mathbb{R})$ die Matrix $B^{-1}AB$ in Jordannormalform ist.

Nun Indirekter Beweis. **Annahme:** *A ist nicht diagonalisierbar.*

Dann gibt es einen Eigenwert λ, so dass die Matrix $B^{-1}AB$ einen Jordanblock der Größe ≥ 2 zum Eigenwert λ hat. Also gibt es Vektoren b_j und b_{j+1} in der Basis oben mit

$$A \cdot b_j = \lambda \cdot b_j \quad \text{und} \quad A \cdot b_{j+1} = \lambda \cdot b_{j+1} + b_j.$$

Aber dann ist (wegen $\overline{A} = A^{tr}$)

$$\begin{aligned}
\lambda \cdot \overline{b_j}^{tr} \cdot b_{j+1} + \overline{b_j}^{tr} \cdot b_j &= \overline{b_j}^{tr} \cdot (\lambda \cdot b_{j+1} + b_j) = \overline{b_j}^{tr} \cdot (A \cdot b_{j+1}) \\
&= (\overline{b_j}^{tr} \cdot A) \cdot b_{j+1} = (\overline{b_j}^{tr} \cdot \overline{A}^{tr}) \cdot b_{j+1} = (\overline{A} \cdot \overline{b_j})^{tr} \cdot b_{j+1} \\
&= (\overline{A \cdot b_j})^{tr} \cdot b_{j+1} = \overline{\lambda \cdot b_j}^{tr} \cdot b_{j+1} = \lambda \cdot \overline{b_j}^{tr} \cdot b_{j+1} \\
\text{also} \qquad \overline{b_j}^{tr} \cdot b_j &= 0.
\end{aligned}$$

Aber das ist wegen $b_j \neq 0$ unmöglich. Also war die Annahme oben falsch.