Algebra Blatt 6.

Christian Merten Zichu Li

A1	A2	A3	A4	A5	Σ

A1) Bezeichne $\mathbb{Z}/_n := \mathbb{Z}/n\mathbb{Z}$

(a) $d, n \in \mathbb{N}$, $d \mid n$.

Beh. $\mathbb{Z}/d\mathbb{Z}$ proj. $\mathbb{Z}/n\mathbb{Z}$-Modul $\iff ggT(d, \frac{n}{d}) = 1$.

Bew. "$\Rightarrow$" Sei $\mathbb{Z}/d\mathbb{Z}$ projektiv. Es ist folgende Folge von $\mathbb{Z}/n\mathbb{Z}$-Moduln exakt:

$$0 \longrightarrow \underset{\substack{\cong \\ \mathbb{Z}/\frac{n}{d}\mathbb{Z}}}{d\mathbb{Z}/n\mathbb{Z}} \xhookrightarrow{\text{kan}} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\text{kan}} \underset{\substack{\cong \\ \mathbb{Z}/d\mathbb{Z}}}{\mathbb{Z}/n\mathbb{Z} \big/ d\mathbb{Z}/n\mathbb{Z}} \longrightarrow 0$$

Da $\mathbb{Z}/d\mathbb{Z}$ proj. zerfällt diese Folge und es folgt $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\frac{n}{d}\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$.

Also insbes. ist $\mathbb{Z} \xrightarrow{\text{kan}} \mathbb{Z}/\frac{n}{d}\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z}$ surj. also gilt nach chin. Restsatz:

$d\mathbb{Z} + \frac{n}{d}\mathbb{Z} = 1$ also $ggT(d, \frac{n}{d}) = 1$.

"$\Leftarrow$" Sei $ggT(d, \frac{n}{d}) = 1$. Dann ist $d\mathbb{Z} + \frac{n}{d}\mathbb{Z} = 1$ also

nach chin. Restsatz: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/(n/d)\mathbb{Z}$. Da $\mathbb{Z}/n\mathbb{Z}$ freier $\mathbb{Z}/n\mathbb{Z}$-Modul ist $\mathbb{Z}/d\mathbb{Z}$ direkter Summand in freiem Modul, also projektiv.

$\square$

Beh. Für $n = p_1^{e_1} \cdots p_r^{e_r}$ ist jeder e.e. projektive $\mathbb{Z}/n\mathbb{Z}$-Modul M von der Form

$$M \cong (\mathbb{Z}/p_1^{e_1})^{f_1} \oplus \cdots \oplus (\mathbb{Z}/p_r^{e_r})^{f_r}$$

Bew. Als abelsche Gruppe ist nach Hauptsatz $M \cong \mathbb{Z}^s \oplus \bigoplus_{\substack{p \in \mathbb{N} \\ p \text{ prim}}} (\mathbb{Z}/p^{n_{p,1}} \oplus \cdots \oplus \mathbb{Z}/p^{n_{p,s_p}})$

mit $s \in \mathbb{N}_0$ und $s_p, n_p \in \mathbb{N}_0$ $\forall p \in \mathbb{N}$, p prim und $s_p = 0$ f.f. alle p.

Nun ist M e.e. $\mathbb{Z}/n\mathbb{Z}$-Modul. Da $\mathbb{Z}/n\mathbb{Z}$ endl. folgt damit $s = 0$. Da M $\mathbb{Z}/n\mathbb{Z}$-Modul folgt $p^{n_{p,k}} \mid n$ $\forall p$ Primzahl und $1 \le k \le s_p$. Insbes. folgt

$$M \cong \bigoplus_{i=1}^{r} \mathbb{Z}/p_i^{n_{i,1}} \oplus \cdots \oplus \mathbb{Z}/p_i^{n_{i,s_i}}$$ mit den p_i aus der Primfaktorzerlegung von n.

Da M proj. sind nach VL $\mathbb{Z}/p_i^{n_{i,1}}$ projektiv, also folgt nach Beh 1. $ggT(p_i^{n_{i,k}}, \frac{n}{p_i^{n_{i,k}}}) = 1$

$\forall 1 \le i \le r$ und $1 \le k \le s_i$. Also folgt $n_{i,1} = \ldots = n_{i,s_i} = e_r$. Insgesamt folgt

$$M \cong \bigoplus_{i=1}^{r} \underbrace{\left(\mathbb{Z}/p_i^{e_r} \oplus \cdots \oplus \mathbb{Z}/p_i^{e_r}\right)}_{f_i := s_i \text{ mal}} \cong (\mathbb{Z}/p_1^{e_1})^{f_1} \oplus \cdots \oplus (\mathbb{Z}/p_r^{e_r})^{f_r}.$$

$\square$

(b) Beh. $\mathbb{Z}/n\mathbb{Z}$ kofreier $\mathbb{Z}/n\mathbb{Z}$-Modul.

Bew. Betrachte $\quad (\mathbb{Z}/n\mathbb{Z})^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$

Ein Grp. hom $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z}$ ist bereits eindeutig durch das Bild des Erzeugers $\overline{1}$ der zykl. Gruppe $\mathbb{Z}/n\mathbb{Z}$ festgelegt.

Für $\varphi \in (\mathbb{Z}/n\mathbb{Z})^*$ muss dabei gelten $\quad n \cdot \varphi(\overline{1}) = 0$, d.h.

$n \cdot \varphi(\overline{1}) \in \mathbb{Z}$, d.h. $\varphi(\overline{1}) = \overline{\left(\frac{a}{n}\right)}$ für ein $a \in \mathbb{Z}$.

Weiter gilt $\quad \overline{\left(\frac{a}{n}\right)} = \overline{\left(\frac{b}{n}\right)}$ in $\mathbb{Q}/\mathbb{Z} \iff \frac{a-b}{n} \in \mathbb{Z} \iff a-b \in n\mathbb{Z}$.

Es gilt also $\#(\mathbb{Z}/n\mathbb{Z})^* = n$ und $\varphi_1 : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ mit $\varphi_1(\overline{1}) = \overline{\left(\frac{1}{n}\right)}$ ist Erzeuger von $(\mathbb{Z}/n\mathbb{Z})^*$, insbes. ist $(\mathbb{Z}/n\mathbb{Z})^*$ zyklische Gruppe der Ordnung n.

D.h. der Grp.hom. $\psi: \mathbb{Z}/n\mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$, $\overline{1} \longmapsto \varphi_1$ ist Grp.isom.

b.z.z.: ψ $\mathbb{Z}/n\mathbb{Z}$-Modulhom. Dazu seien $\overline{a}, \overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Dann gilt

$$\psi(\overline{a} \cdot \overline{m})(\overline{1}) = am \cdot \overline{\left(\frac{1}{n}\right)} = m \cdot \overline{\left(\frac{a}{n}\right)} = \varphi_m(\overline{a}) = \varphi_m(\overline{1} \cdot \overline{a}) \underset{\substack{\uparrow \\ \text{Def der} \\ \mathbb{Z}/n\mathbb{Z}\text{-Mod Struktur} \\ \text{von } (\mathbb{Z}/n\mathbb{Z})^*}}{=} \overline{a}\, \varphi_m(\overline{1}) = \overline{a}\, \psi(\overline{m})(\overline{1})$$

Insgesamt folgt $\psi(\overline{a} \cdot \overline{m}) = \overline{a}\, \psi(\overline{m})$. Also $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})^*$ als $\mathbb{Z}/n\mathbb{Z}$-Moduln, also insbes. $\mathbb{Z}/n\mathbb{Z}$ kofreier $\mathbb{Z}/n\mathbb{Z}$-Modul.

Beh. Jeder e.e. proj. $\mathbb{Z}/n\mathbb{Z}$-Modul auch injektiv.

Bew Nach (a) ist jeder e.e. proj. $\mathbb{Z}/n\mathbb{Z}$-Modul M von der Form

$$M \cong (\mathbb{Z}/p_1^{e_1})^{f_1} \oplus \dots \oplus (\mathbb{Z}/p_r^{e_r})^{f_r}$$ mit $n = p_1^{e_1} \cdots p_r^{e_r}$. Da nach chin. Restsatz: $\mathbb{Z}/n \cong \mathbb{Z}/p_1^{e_1} \oplus \dots \oplus \mathbb{Z}/p_r^{e_r}$ ist M direkter Summand in $(\mathbb{Z}/n)^{\max\{f_1,\dots,f_r\}}$ also in einem kofreien $\mathbb{Z}/n\mathbb{Z}$-Mod. Insbes. ist M injektiv.

□

A2 (a) Beh. Jeder inj. Ringhom ist Monomorphismus.

Bew. Sei $f: A \to B$ inj. Ringhom. und seien $g_1, g_2: C \to A$ Ringhoms. mit $f \circ g_1 = f \circ g_2$. Dann ist $\forall c \in C$: $f(g_1(c)) = f(g_2(c))$. Da f injektiv folgt $g_1(c) = g_2(c)$. Also $g_1 = g_2$ und damit f Monom. $\square$

(b) Beh. Jeder Monomorphismus ist injektiv.

Bew. $f: A \to B$ Monom. und $x, y \in A$ mit $f(x) = f(y)$. Dann ex. nach univ. Eig. des Polynomrings $g_1: \mathbb{Z}[X] \to A$ Ringhom mit $g_1(X) = x$ und $g_2: \mathbb{Z}[X] \to A$ Ringhom mit $g_2(X) = y$ und $g_1|_{\mathbb{Z}} = g_2|_{\mathbb{Z}} = (\mathbb{Z} \xrightarrow{\text{kan}} A)$.

Dann gilt $f(g_1(X)) = f(x) = f(y) = f(g_2(X))$.

Nach univ. Eigenschaft d. Polynomrings ex. genau eine Abb. $h: \mathbb{Z}[X] \to B$ mit $h|_{\mathbb{Z}} = f \circ g_1|_{\mathbb{Z}} = f \circ g_2|_{\mathbb{Z}}$ und $h(X) = f(x) = f(y)$. Also folgt $f \circ g_1 = h = f \circ g_2$. Also da f Monom. folgt $g_1 = g_2$, also insbes. $x = g_1(X) = g_2(X) = y$. $\square$

(c) Beh. Jeder surj. Ringhom. ist Epimorphismus.

Bew. Sei $f: A \to B$ surj. und $g_1, g_2: B \to C$ Ringhom. mit $g_1 \circ f = g_2 \circ f$. Dann ist $\forall b \in B: \exists a \in A: f(a) = b$. Also $g_1(b) = g_1(f(a)) = g_2(f(a)) = g_2(b)$. $\square$

(d) Beh. $f: \mathbb{Q} \hookrightarrow \mathbb{Z}$ ist nicht surj. Epimorphismus.

Bew. f nicht surjektiv ist klar. Sei also $g_1, g_2: \mathbb{Z} \to C$ bel. Ringhom's.

Dann ist $g_1(a) = g_1((\pm 1) \cdot \underbrace{(1 + \dots + 1)}_{|a| \text{ mal}}) = g_1(\pm 1) \cdot \underbrace{(g_1(1) + \dots + g_1(1))}_{|a| - \text{mal}}$

$= \pm \underbrace{(1 + \dots + 1)}_{|a| \text{mal}}$

$\overset{\text{analog}}{=} g_2(a)$.

Also $g_1 = g_2$ insbes. gilt $f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$ also f Epim. $\square$

A31 (a) Beh. $(I, \leq)$ Kategorie im eng. Sinn.

Bew. Die Daten sind klar. Das Verknüpfungsgesetz ist wohldefiniert, da $\leq$ transitiv und $\# \mathrm{Mor}_{\mathrm{Kat}(I)}(i,j) \leq 1$.

(A1) gilt nach Konstruktion. (A2) gilt da es für $i,j \in I = \mathrm{ob}(\mathrm{Kat}(I))$ stets maximal ein $f \in \mathrm{Mor}_{\mathrm{Kat}(I)}(i,j)$ gibt. (A3): Existenz folgt aus Reflexivität von $\leq$ und die Neutralität aus $\# \mathrm{Mor}_{\mathrm{Kat}(I)}(i,j) \leq 1$.

□

(b) I gerichtet, R Ring

Beh. Kovariante Funktoren $F: \mathrm{Kat}(I) \to R\text{-Mod}$ sind genau die direkten Systeme von R-Moduln.

Bezeichnung: Für $i \leq j$ bezeichne mit $i \to j$ den Morphismus von i nach j.

Bew. Sei $F: \mathrm{Kat}(I) \to R\text{-Mod}$ (kovar.) Funktor. Bezeichne $M_i := F(i)$ und

$\varphi_{ij} := F(i \to j) \in \mathrm{Hom}_R(M_i, M_j)$ für $i \leq j$ (*).

Dann ist $\varphi_{ii} = F(i \to i) = F(\mathrm{id}_i) = \mathrm{id}_{M_i}$

und für $i \leq j \leq k$ gilt
$$\varphi_{ik} = F(i \to k) = F((j \to k) \circ (i \to j)) = F(j \to k) \circ F(i \to j) = \varphi_{jk} \circ \varphi_{ij}$$

Andersherum liefern $(M_i)_{i \in I}$ und $\varphi_{ij}: M_i \to M_j$ für $i \leq j$ einen Funktor durch Umdrehen der Definitionen in (*). Diese Konstruktionen sind damit auch invers zu einander.

□

Beh. Kontravariante Funktoren $G: \mathrm{Kat}(I) \to R\text{-Mod}$ sind genau die proj. Systeme von R-Moduln.

Bew. Betrachte $F: \mathrm{Kat}(I)^{op} \to R\text{-Mod}$. In $\mathrm{Kat}(I)^{op}$ gilt

dann $i \to j \in \mathrm{Mor}_{\mathrm{Kat}(I)^{op}}(i,j) \iff j \to i \in \mathrm{Mor}_{\mathrm{Kat}(I)}(j,i) \iff j \leq i$.

Es ist also $\mathrm{Kat}(I)^{op} = \mathrm{Kat}(I^{op})$ wobei $I^{op} = (I, \geq)$ mit "$\geq$" die umgekehrte Ordnung von "$\leq$". Dann sind nach (a) die kovar. Funktoren $\mathrm{Kat}(I)^{op} \to R\text{-Mod}$ genau die direkten Systeme von R-Moduln über I^{op}. Also die proj. Systeme über I.

□

A4| $\phi: A \to B$ Ringhom. $\phi^*: \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$, $q \longmapsto \phi^{-1}(q)$

(a) Beh. Für $f \in A$ ist $(\phi^*)^{-1}(D(f)) = D(\phi(f))$

Bew. $(\phi^*)^{-1}(D(f)) = \{ q \in \mathrm{Spec}(B) : \phi^*(q) \in D(f) \}$

$$= \{ q \in \mathrm{Spec}(B) : \phi^{-1}(q) \in D(f) \}$$
$$= \{ q \in \mathrm{Spec}(B) : f \notin \phi^{-1}(q) \}$$
$$= \{ q \in \mathrm{Spec}(B) : \phi(f) \notin q \}$$
$$= \{ q \in \mathrm{Spec}(B) : q \in D(\phi(f)) \}$$
$$= D(\phi(f))$$

$\square$

Beh. ϕ^* stetig

Bew. Sei $U \subseteq \mathrm{Spec}(A)$ offen. Dann ist nach Blatt 4: $U = \bigcup_{i \in I} D(f_i)$ für $f_i \in A$. Dann gilt

$$(\phi^*)^{-1}(U) = (\phi^*)^{-1}\Big(\bigcup_{i \in I} D(f_i)\Big) = \bigcup_{i \in I} (\phi^*)^{-1}(D(f_i))$$
$$\overset{\text{Beh 1}}{=} \bigcup_{i \in I} D(\phi(f_i))$$

offen, da $D(g)$ offen $\forall g \in B$.

$\square$

(b) Beh. $a \subseteq A$ Ideal: $(\phi^*)^{-1}(V(a)) = V(a^e)$

Bew. $(\phi^*)^{-1}(V(a)) = \{ q \in \mathrm{Spec}(B) : \phi^{-1}(q) \in V(a) \}$

$$= \{ q \in \mathrm{Spec}(B) : a \subseteq \phi^{-1}(q) \}$$
$$= \{ q \in \mathrm{Spec}(B) : \phi(a) \subseteq q \}$$
$$= V(\phi(a))$$
$$\overset{B2}{=} V(B\phi(a))$$
$$= V(a^e)$$

$\square$

(c) Beh. $\mathfrak{b} \subseteq B$: $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$

Bew. Sei $\mathfrak{p} \in \phi^*(V(\mathfrak{b}))$. Dann ex. ein $\mathfrak{q} \in V(\mathfrak{b})$ mit $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Da $\mathfrak{b} \subseteq \mathfrak{q}$ folgt
$$\begin{aligned} \mathfrak{b}^c = \phi^{-1}(\mathfrak{b}) &= \{ a \in A : \phi(a) \in \mathfrak{b} \} \\ &\subseteq \{ a \in A : \phi(a) \in \mathfrak{q} \} \\ &= \phi^{-1}(\mathfrak{q}) \\ &= \mathfrak{p}. \end{aligned}$$

Also folgt $\mathfrak{p} \in V(\mathfrak{b}^c)$ und damit $\phi^*(V(\mathfrak{b})) \subseteq V(\mathfrak{b}^c)$.

Sei nun $V(M) \subseteq \mathrm{Spec}(A)$ bel. mit $M \subseteq \mathrm{Spec}(A)$ mit $\phi^*(V(\mathfrak{b})) \subseteq V(M)$. Dann sei $\mathfrak{p} \in V(\mathfrak{b}^c)$ bel. Es bzz. $M \subseteq \mathfrak{p}$. Da $\phi^*(V(\mathfrak{b})) \subseteq V(M)$ gilt für $\mathfrak{q} \in V(\mathfrak{b})$: $\phi^*(\mathfrak{q}) \in V(M)$, d.h. $M \subseteq \phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$. Also $\phi(M) \subseteq \bigcap_{\mathfrak{q} \in V(\mathfrak{b})} \mathfrak{q} = \bigcap_{\substack{\mathfrak{q} \text{ PI} \\ \mathfrak{b} \subseteq \mathfrak{q}}} \mathfrak{q} \overset{\text{VL}}{=} r(\mathfrak{b})$.

Da nach B2 $V(\mathfrak{b}^c) = V(r(\mathfrak{b}^c))$, gilt:
$$M \subseteq \phi^{-1}\Big(\bigcap_{\mathfrak{q} \in V(\mathfrak{b})} \mathfrak{q}\Big) = \phi^{-1}(r(\mathfrak{b})) \overset{\text{df}}{=} r(\mathfrak{b})^c \overset{\text{VL}}{=} r(\mathfrak{b}^c) \subseteq \mathfrak{p}.$$

$\square$

A5 | A HIR, $\mathrm{Proj}(A)^{\cong}$ Menge der Isom.klassen e.e. proj. (= freier) A-Moduln.

$$K(A) := \Big(\bigoplus_{[P] \in \mathrm{Proj}(A)^{\cong}} \mathbb{Z} \cdot [P] \Big) \Big/ \mathrm{Exakt}$$

mit $\mathrm{Exakt} = \langle [P] - [P'] - [P''] \mid 0 \to P' \to P \to P'' \to 0 \text{ exakt} \rangle$

Beh. $\mathrm{rg}: \mathrm{Proj}(A)^{\cong} \to \mathbb{Z}$ induziert Isom. ab Grp. $K(A) \xrightarrow{\sim} \mathbb{Z}$

Bew. Für $[P], [N] \in K(A)$ ist $0 \to P \hookrightarrow P \oplus N \twoheadrightarrow N \to 0$ kurze exakte Folge

also $[P \oplus N] - [P] - [N] = 0 \Rightarrow [P \oplus N] = [P] + [N]$.

Über HIR ist frei und proj. äquivalent, d.h. $[P] = [A^n]$ mit $n = \mathrm{rg}(P)$ für $[P] \in \mathrm{Proj}(A)^{\cong}$.

Nun gilt für $[P] \in K(A)$: $[P] = [A^n] = [A^{n-1}] + [A] = \ldots = n[A]$.

Also folgt für $x \in K(A)$ mit
$$\begin{aligned} x = n_1[P_1] + \ldots + n_r[P_r] &= n_1[A^{m_1}] + \ldots + n_r[A^{m_r}] \\ &= n_1 m_1 [A] + \ldots + n_r m_r [A] \\ &= s \cdot [A] \end{aligned}$$

für ein $s \in \mathbb{Z}$.

Also ist $K(A)$ zyklisch mit Erzeuger $[A]$. Seien nun $n, m \in \mathbb{Z}$ mit $n[A] = m[A]$.
OE $n \geq m$. Dann betrachte $(n-m)[A] = 0$. Da $n-m \in \mathbb{N}_0$ folgt $0 = (n-m)[A] = [A^{n-m}]$.
Da rg wohldef., folgt $n-m=0$ also $n=m$. Also ist $\mathbb{Z} \longrightarrow K(A)$, $s \longmapsto s[A]$ injektiv. Insgesamt folgt $K(A) \cong \mathbb{Z}$.

$\square$