Aufgabe 1)

Es seien $a_{11}, \dots, a_{1n}$ teilerfremde Elemente eines Hauptideal-rings R. ($ggT(a_{11}, \dots, a_{1n}) = 1$). Man zeige, es gibt Elemente $a_{ij} \in R$, $i = 2, \dots, n$, $j = 1, \dots, n$, so dass die Matrix $(a_{ij})_{i,j=1,\dots,n}$ in $R^{n\times n}$ invertierbar ist.

Lösung:

Lemma:

Es sei R ein Hauptidealring und $A = (\alpha_{ij}) \in R^{m\times n}$ eine Matrix mit Koeffizienten aus R. Dann gibt es invertierbare Matrizen $S \in R^{m\times m}$ & $T \in R^{n\times n}$ mit

$$S \cdot A \cdot T = \begin{pmatrix} \alpha_1 & 0 & & & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & & & 0 & 0 & \cdots & 0 \\ & & \ddots & & \vdots & & & \\ 0 & 0 & \cdots & & \alpha_s & 0 & \cdots & 0 \\ 0 & 0 & \cdots & & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & & 0 & 0 & \cdots & 0 \end{pmatrix}$$

und mit Koeffizienten $\alpha_1, \dots, \alpha_s \in R - \{0\}$ (wobei $0 \leq s \leq \min(m,n)$ gilt), die für $1 \leq i < s$ die Bedingung $\alpha_i \mid \alpha_{i+1}$ erfüllen.
Dabei sind $\alpha_1, \dots, \alpha_s$ bis auf Assoziiertheit eindeutig bestimmt; man nennt sie die Elementarteiler der Matrix A.

Idee)

- Wir betrachten die Elementarteiler von $A_1 = (a_{11}, \dots, a_{1n})$ wobei $A_1 \in R^{1\times n}$

- Lemma $\Longrightarrow$ A_1 lässt sich ~~mittels~~ mittels Multiplikation mit invertierbaren Matrizen aus $R^{n\times n}$ von ~~Rechts~~ rechts in die Gestalt $(\alpha, 0, \dots, 0)$ ~~bringen~~ bringen. $(\alpha \in R)$

- α ist der erste (und einzige) Elementarteiler von A_1.

$\Rightarrow \exists\, T \in R^{n\times n}$, sodass T invertierbar &

$$A_1 \cdot T = (\alpha, 0, \dots, 0)$$

- $\Rightarrow$ $A_1 = (\alpha, 0, \dots, 0) \cdot T^{-1}$ & α ist ein gemeinsamer Teiler von $a_{11}, \dots, a_{1n}$

$\Rightarrow$ α ist die Einheit

- $\Rightarrow$ A_1 kann ~~mittels mittels~~ mittels geeigneter invertierbarer Matrix in den Zeilenvektor $(1, 0, \dots, 0) \in R^{1\times n}$ transformiert werden.

- Wir betrachten diese Zeile als erste Zeile der Einheitsmatrix $E \in R^{n\times n}$ und wenden die zuvor betraeteten Matrix invertiert auf E.

$\Rightarrow$ ~~Es~~ wir gelangen zu einer Matrix A, die das Gewünschte leistet.

Lösungsweg:

- Sei $F = R^n$ der freie R-Modul aller n-Tupel von Elementen aus R (die wir wie üblich als Spaltenvektoren interpretieren.)
- Sei M der von der Spalte $(a_{11}, \ldots, a_{1n})^t$ erzeugte R-Untermodul.

$\Rightarrow$ Elementarteilersatz &

Korollar:
Es sei R ein Hauptidealring und F ein endlicher freier R-Modul. Dann besitzen je zwei Basen von F gleiche Länge. Diese Länge wird als der Rang von F bezeichnet.

$\Rightarrow$ Es gibt eine Basis $X = (x_1, \ldots, x_n)$ von F mit $M = R \cdot \alpha x_1$ für eine geeignete Konstante $\alpha \in R$.

$\rightsquigarrow$ $ggT(\alpha_{11}, \ldots, \alpha_{1n}) = 1$ & α muss alle Elemente α_{1j} teilen $\Rightarrow \alpha = 1$ & $x_1 = (\alpha_{11}, \ldots, \alpha_{1n})^t$.

Für die kanonische Basis e von R^n betrachten wir nun die Basiswechselmatrix $A_{id,X,e}$.

- $A_{id,X,e}$ ist invertierbar & besitzt $(\alpha_{11}, \ldots, \alpha_{1n})^t$ als erste Spalte.

$\Rightarrow (A_{id,X,e})^t$ ist invertierbar in $R^{n \times n}$, die $(a_{11}, \ldots, a_{1n})$ als erste Zeile besitzt.

Frage:

Warum ist die Charakteristik eines endlichen Körpers stets eine Primzahl?

Antwort:

Sei $\mathrm{Char}(K) = n = pq$ eine zusammengesetzte Zahl mit $1 < p,$ $q < n$.

Definitionsgemäß ist dann n die kleinste natürliche Zahl mit ~~$n1_K = 0$~~ $n\,1_K = 0$. Aufgrund des Distributivgesetzes gilt

$$(p\,1_K)\cdot(q\,1_K) = \underbrace{(1_K + \dots + 1_K)}_{p\text{-mal}} \cdot \underbrace{(1_K + \dots + 1_K)}_{q\text{-mal}}$$

$$= (pq)\,1_K = n\,1_K = 0$$

Nach Voraussetzung ist $q\,1_K \neq 0$, also existiert ein Inverses $(q\,1_K)^{-1}$, und es folgt

$$p\,1_K = (p\,1_K)(q\,1_K)(q\,1_K)^{-1} = 0\,(q\,1_K)^{-1} = 0 \quad ↯$$

Frage:

Ist ein Ideal $\mathfrak{a} \subset R$ stets auch ein Unterring von R?

Antwort:

Nein, denn im Allgemeinen ist $1 \notin \mathfrak{a}$. Genauer folgt aus $1 \in \mathfrak{a}$ bereits $\mathfrak{a} = R$, da für jedes $r \in R$ gilt $r = 1 \cdot r \in \mathfrak{a}$

Aufgabe 2)

Es sei M ein endlich erzeugter R-Modul, der zudem frei ist. Man zeige

(i) M besitzt eine endliche Basis

(ii) Je zwei Basen von M bestehen aus gleich viel Elementen.

Lösung:

Strategie:

$M = 0$ ist trivial ⇝ wir ~~neh~~ nehmen $M \neq 0$ und damit insbesondere auch $R \neq 0$ an.

Seien $X = (x_i)_{i \in I}$ ein freies Erzeugendensystem und Y ein endliches Erzeugendensystem von M

$\Rightarrow$ $y \in Y$ ist eine Linearkombination von endlich vielen der Erzeugenden x_i

$\Rightarrow$ M von einem endlichen Teilsystem von X erzeugt wird

& X freies Erzeugendensystem $\Rightarrow X$ endlich.

Seien nun $X = (x_1, \dots, x_m)$ & $Y = (y_1, \dots, y_n)$ ~~zwei~~ zwei (endliche) freie Erzeugendensysteme von M

$z \in M$ & z_X (bzw. z_Y) der zugehörige Koordinatenspaltenvektor bezüglich der Basen X (bzw. Y).

⇒ ⇝ ~~Tungebenmisch~~ Isomorphismen von R-Moduln

$$M \xrightarrow{\sim} R^m \ \& \ M \xrightarrow{\sim} R^n.$$

⇒ Man erhält $\varphi : R^m \xrightarrow{\sim} R^n$.

Z.Z: Solcher Iso. kann nur im Fall $m=n$ bestehen.

R ein Körper ⇝ $m=n$ folgt ~~aus~~ aufgrund von ~~Dimension~~ Dimensiontheorie.

R kein Körper, aber immerhin noch ein Hauptidealring

⇝ wähle ein Primelement $p \in R$ &

$$\varphi_p : (R/_{pR})^m \xrightarrow{\sim} (R/_{pR})^n$$ (induzierter Iso. von φ)

$R/_{pR}$ ist ein Körper ⇒ $n=m$.

~~⇒~~ ⇝ Dasselbe Argument funktioniert für allgemeine kommutative Ringe R mit 1, sofern wir in R ein Ideal $\mathfrak{m}$ finden können, derart dass der Restklassenring $R/_{\mathfrak{m}}$ ein Körper ist.

$\Rightarrow$ Es genügt dann, wie bereits erläutert, ein Ideal $\mathfrak{m} \subset R$ zu konstruieren, derart dass $R/\mathfrak{m}$ ein Körper ist.

- ~~Wir betrachten di~~ Wir betrachten
  $A = \{\mathfrak{a} \text{ Ideal } \& \ \mathfrak{a} \subsetneq R\}$ mit der durch Inklusion gegebenen teilweisen Ordnung.

Zorn'sches Lemma $\Rightarrow$ A besitzt ein maximales Element $\mathfrak{m}$, sodass

$$\forall\, \mathfrak{a} \subset R \text{ Ideal mit } \mathfrak{m} \subset \mathfrak{a} \Rightarrow \text{folgt} \begin{cases} \mathfrak{m} = \mathfrak{a} \\ \text{oder} \\ \mathfrak{a} = R \end{cases}$$

Behauptung: $R/\mathfrak{m}$ ein Körper ist, und zeigen hierfür dass jedes von Null verschiedene Element $\bar{\alpha} \in R/\mathfrak{m}$ eine Einheit ist.

Sei $R \xrightarrow{p} R/\mathfrak{m}$ die kanonische ~~Proj~~ Proj.

$\Rightarrow$ das Urbild des Hauptideals $(\bar{\alpha}) \subset R/\mathfrak{m}$ unter p ergibt ein Ideal $\mathfrak{a} \subset R$ mit $\mathfrak{m} \subsetneq \mathfrak{a}$

$\Rightarrow$ $R = \mathfrak{a}$. $\Rightarrow$ $(\bar{\alpha}) = R/\mathfrak{m}$

$\Rightarrow$ $\bar{\alpha}$ ist eine Einheit in $R/\mathfrak{m}$.

$$\varphi_{\mathfrak{m}} : (R/\mathfrak{m})^m \xrightarrow{\sim} (R/\mathfrak{m})^n \rightsquigarrow n = m$$

Isomorphie von $(R/\mathfrak{m})$-Vektorräume.