# § 3 Lineare Gruppen

Sei $F$ ein Körper. Untergruppen von $GL_n F$, $n \geq 1$, nennt man lineare Gruppen (über $F$).

Lineare Gruppen sind also Matrizengruppen. Wir benötigen etwas Ringtheorie. Im folgenden sei $A$ stets ein kommutativer Ring mit $1$, z.B. $A = \mathbb{Z}$. Die Einheitengruppe eines (nicht notwendig kommutativen) Ringes $R$ sei $R^*$.

Wir setzen $GL_n A = (A^{n \times n})^*$ (Gruppe der invertierbaren $n \times n$ Matrizen über $A$).

Wie in der Linearen Algebra definieren wir für Matrizen $a \in A^{n \times n}$, $a = (a_{ij})_{i,j=1}^{n}$

$$\det(a) = \sum_{g \in \mathrm{Sym}(n)} \mathrm{sign}(g) \prod_{i=1}^{n} a_{g(i),i} \in A$$

$a^T \in A^{n \times n}$, $(a^T)_{ij} = a_{ji}$ (transponierte Matrix)

$$\mathrm{tr}(a) = \sum_{i=1}^{n} a_{ii}, \quad S_{ij}(a) = \begin{array}{cc} \left(\begin{array}{c|c} \; & \; \\ \hline \; & \; \end{array}\right) & i \\ j & \end{array}$$

Matrix, die man durch Streichen der $i$-ten Zeile und $j$-ten Spalte erhält.

Wir definieren die Komplementärmatrix

$a^\#$ durch $(a^\#)_{ij} = (-1)^{i+j} \det(S_{ji}(a))$

Aus LA wissen wir: $\det(ab) = \det(a)\det(b)$,

$aa^\# = a^\# a = \det(a)\, \mathbb{1}_n$ , falls $a, b \in F^{n \times n}$.

Um zu zeigen, dass die Rechenregeln in beliebigen kommutativen Ringen gelten, benutzen wir einen Trick.

Betrachte den Polynomring $R = \mathbb{Z}[T_{11}, \dots, T_{nn}]$ in $n^2$ Variablen, mit Quotientenkörper $Q = \mathbb{Q}(T_{11}, \dots, T_{nn})$.

Ist $a \in A^{n \times n}$, so erhalten wir den Einsetzungshomomorphismus $\Phi : R \to A$, $f(T_{11}, \dots, T_{nn}) \mapsto f(a_{11}, \dots, a_{nn})$

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[d, "\Phi"] & Q \\
A &
\end{tikzcd}$$

Für die Matrix $X = \begin{pmatrix} T_{11} & \cdots & T_{1n} \\ \vdots & \ddots & \vdots \\ T_{n1} & \cdots & T_{nn} \end{pmatrix} \in R^{n \times n}$

gilt $XX^\# = \det(X)\, \mathbb{1}_n$ (weil $R \subseteq Q$)

Der Eintrag $(X \cdot X^\#)_{ij}$ ist ein Polynom, und es folgt

$$\left.\begin{array}{l}
\Phi\left((X \cdot X^\#)_{ij}\right) = (a \cdot a^\#)_{ij} \\
\qquad \parallel \\
\Phi\left(\det(X)(\mathbb{1}_n)_{ij}\right) = \det(a) \cdot (\mathbb{1}_n)_{ij}
\end{array}\right\} \Rightarrow a \cdot a^\# = \det(a)\, \mathbb{1}_n$$

Ähnlich zeigt man $\det(ab) = \det(a)\cdot\det(b)$ für $a, b \in A^{n\times n}$ (betrachte $R = \mathbb{Z}[T_{11} \dots T_{nn}, S_{11}, \dots, S_{nn}]$

$X = \begin{pmatrix} T_{11} & \cdots & T_{1n} \\ \vdots & & \vdots \\ T_{n1} & \cdots & T_{nn} \end{pmatrix}$ $Y = \begin{pmatrix} S_{11} & \cdots & S_{1n} \\ \vdots & & \vdots \\ S_{n1} & \cdots & S_{nn} \end{pmatrix}$ usw.

1. <u>Lemma</u> Sei $A$ ein kommutativer Ring. Dann gilt für alle $a, b \in A^{n\times n}$, $g \in GL_n(A)$

$$\det(ab) = \det(a)\det(b)$$
$$\det(gag^{-1}) = \det(a) = \det(a^T)$$
$$\operatorname{tr}(gag^{-1}) = \operatorname{tr}(a) \qquad \operatorname{tr}(ab) = \operatorname{tr}(ba)$$
$$a \cdot a^{\#} = a^{\#} \cdot a = \det(a) \cdot \mathbb{1}_n$$

$\square$

<u>Korollar</u> Es gilt $GL_n(A) = \{a \in A^{n\times n} \mid \det(a) \in A^*\}$

Insbesondere $GL_n\mathbb{Z} = \{a \in \mathbb{Z}^{n\times n} \mid \det(a) = \pm 1\}$

Die Gruppe $SL_n(A) = \{a \in A^{n\times n} \mid \det(a) = 1\}$ ist ein Normalteiler in $GL_n(A)$.

<u>Beweis</u> Ist $a \in GL_n(A)$ mit Inversem $b$, so folgt:

$$\left.\begin{aligned} \det(ab) &= \det(a)\cdot\det(b) \\ \| \quad & \\ \det(\mathbb{1}_n) &= 1 \end{aligned}\right\} \Rightarrow \det(a) \in A^*$$

Ist $\delta = \det(a) \in A^*$, so folgt mit $b = a^{\#}\cdot\delta^{-1}$, dass $ab = ba = \mathbb{1}_n$.

Ist $a \in SL_n(A)$, $g \in GL_n(A)$, so folgt

$\det(gag^{-1}) = \det(a) = 1 \Rightarrow gag^{-1} \in SL_n(A)$ $\square$

2. <u>Def</u> Sei $A$ ein kommutativer Ring, sei $X \subseteq A$ eine Teilmenge. Der von <u>$X$ erzeugte Ring</u> ist

$$\langle X \rangle_{\text{Ring}} = \bigcap \{ R \mid R \subseteq A \text{ Teilring}, X \subseteq R, 1 \in R \}$$

(Dahinter ist unsere Konvention: Ringe haben immer ein 1-Element!)

Andere Beschreibung von $\langle X \rangle_{\text{Ring}}$:

$X_0 = X \cup \{1\}$ und rekursiv

$X_{s+1}$ die von den Elementen $\{ab \mid a, b \in X_s\}$ erzeugte Untergruppe von $(A, +)$. Dann gilt:

$$\langle X \rangle_{\text{Ring}} = \bigcup_{s \geq 0} X_s$$

Ein Ring $A$ heißt <u>endlich erzeugt</u>, wenn es eine endliche Menge $X \subseteq A$ gibt mit

$$A = \langle X \rangle_{\text{Ring}}.$$

$\#$

3. Lemma  Ist $A$ endlich erzgt. Ring, so existiert ein surjektiver Homomorphismus

$$\mathbb{Z}[T_1,\dots,T_m] \longrightarrow A \quad , \text{ für ein } m \geq 1.$$

Die endlich erzgt. Ringe sind genau die Quotienten von ganzzahligen Polynomringen in mehreren Variablen.

Beweis  $A = \langle \{x_1,\dots,x_s\} \rangle$, betrachte Einsetzungshomomorphismus $\mathbb{Z}[T_1,\dots,T_s] \xrightarrow{\Phi} A$, $\Phi(T_i) = x_i$.
Dann ist $\Phi(\mathbb{Z}[T_1,\dots,T_s]) \subseteq A$ Teilring, der $X$ enthält. □

4. Beobachtung  Sei $F$ ein Körper, $S \subseteq GL_n(F)$ endliche Teilmenge, $A \subseteq F$ der Teilring von $F$, der von den Einträgen der Matrizen $a \in S \cup S^{-1}$ erzeugt wird,

$$A = \langle X \rangle_{\text{Ring}} \quad , \quad X = \{ a_{ij} \mid a \in S \cup S^{-1} \}$$

Dann gilt $\quad \langle S \rangle \subseteq GL_n(A) \subseteq GL_n(F)$,

denn: $\quad a \in S \Rightarrow a, a^{-1} \in A^{n \times n} \Rightarrow a \in GL_n(A)$

also $\quad S \subseteq GL_n(A) \rightsquigarrow \langle S \rangle \subseteq GL_n(A)$ □

Für die Ringtheorie:  Herstein, Topics in algebra
Jacobson, Basic algebra I

**5. Def** Ein kommutativer Ring $A$ heißt <u>noethersch</u>, wenn er eine der beiden folgenden äquivalenten Bedingungen erfüllt.

(i) Jedes Ideal $I \trianglelefteq A$ ist endlich erzeugt, $I = Ax_1 + \dots + Ax_s = (x_1, \dots, x_s)$

(ii) Jede aufsteigende Kette von Idealen
$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ wird stationär, d.h.
$I_{n+k} = I_n$ für ein $n$, alle $k \geq 0$.

((i) $\Rightarrow$ (ii) klar, $\neg$(i) $\Rightarrow$ $\neg$(ii) klar / ÜA )

**6. Theorem** (Hilberts Basissatz) Ist $A$ noethersch, so ist auch $A[T]$ noethersch.

<u>Beweis</u> Angenommen, das ist falsch. Dann existiert ein Ideal $I \trianglelefteq A[T]$, das nicht endlich erzeugt ist. Wähle $f_0 \in I - \{0\}$ mit minimalem Grad, allgemein $f_{s+1} \in I - f_0 \cdot A[T] + \dots + f_s \cdot A[T]$ mit minimalem Grad.
Sei $n_i = \deg(f_i)$, $a_i$ der Leitkoeffizient von $f_i$, also $f_i = a_i T^{n_i} + \dots$. Es gilt $n_0 \leq n_1 \leq \dots$.
Setze $I_s = a_0 A + \dots + a_s A = (a_0, \dots, a_s)$

<u>Beh:</u> $I_{s+1} \neq I_s$ für alle $s$.

<u>Denn sonst:</u> $a_{s+1} = a_0 b_0 + \dots + a_s b_s$, $b_i \in A$

also $\tilde{f} = f_{s+1} - \underbrace{\left(f_0 \cdot b_0 T^{n_{s+1}-n_0} + \ldots + f_s \cdot b_s T^{n_{s+1}-n_s}\right)}_{\in f_0 A[T] + \ldots + f_s A[T]}$

$\deg(\tilde{f}) < \deg(f_{s+1})$ ↯ nach Wahl von $f_{s+1}$ $\square$

Also ist $A$ nicht noethersch, ein Widerspruch. $\square$

<u>Korollar</u> $A[T_1, \ldots, T_s]$ ist noethersch, wenn $A$ noethersch ist.

7. <u>Lemma</u> Ist $A$ noethersch, $I \trianglelefteq A$, so ist auch $A/_I$ noethersch.

<u>Bew.</u> Ist $J \trianglelefteq A/_I$ Ideal, so ist $\pi^{-1}(J) \trianglelefteq A$ Ideal ($\pi : A \to A/_I$ kanon. Projektion), also $\pi^{-1}(J)$ endlich erzt., also $J = \pi\,\pi^{-1}(J)$ endlich erzeugt.

<u>Korollar</u> Jeder endlich erzt. kommutative Ring $A$ ist noethersch.

<u>Bew.</u> Sei $\{x_1, \ldots, x_s\} \subseteq A$ EZS als Ring. Da $\mathbb{Z}[T_1, \ldots, T_s]$ noethersch ist und der Einsetzungshomomorphismus $\Phi : \mathbb{Z}[T_1, \ldots, T_s] \to A$, $T_i \mapsto x_i$ surjektiv ist, folgt die Beh. $\square$

Sind $J, K \trianglelefteq A$ Ideale, so ist $JK$ definiert als additives Erzeugnis der Menge $\{jk \mid j \in J, k \in K\}$. Es folgt $JK \subseteq J \cap K$ und $JK \trianglelefteq A$.

8. __Theorem__ (__Krulls Durchschnittssatz__) Sei $A$ kommutativer noetherscher Ring, $I \trianglelefteq A$. Sei $b \in \bigcap_{n \geq 1} I^n$. Dann gibt es $i \in I$ mit $(1-i)b = 0$.

__Beweis__ Schreibe $I = (i_1, \dots, i_m)$. Da für jedes $n \geq 1$ gilt $b \in I^n$, gibt es homogene Polynome $P_n \in A[T_1, \dots, T_m]$ mit $b = P_n(i_1, \dots, i_m)$ vom Grad $n$. Setze $J_k = (P_1, \dots, P_k) \trianglelefteq A[T_1, \dots, T_m]$. Da dieser Ring noethersch ist (Hilberts Basissatz, §3.6) gibt es $s$ mit $J_{s+1} = J_s$, also

$$P_{s+1} = P_1 \cdot f_s + \dots + P_s \cdot f_1 \qquad f_j \text{ Polynome}$$

Schreibe $f_t = \underset{\substack{\uparrow \\ \text{homogener Term vom Grad } t}}{Q_t} + \underset{\text{Rest}}{\tilde{f}_t}$

$$\Rightarrow P_{s+1} = P_1 Q_s + \dots + P_s Q_1 + \underbrace{(\text{Terme vom Grad} \neq s+1)}_{=0}$$

damit $b = P_{s+1}(i_1, \dots, i_m) = b \underbrace{Q_s(i_1, \dots, i_m)}_{\in I^n} + \dots + b \underbrace{Q_1(i_1, \dots, i_n)}_{\in I^n}$

$$= b \cdot i \qquad \square$$

**Korollar** Ist $A$ noethersch Integritätsbereich und ist $I \trianglelefteq A$ echtes Ideal (d.h. $1 \notin I$), so gilt

$$\bigcap_{n \geq 1} I^n = \{0\} \qquad \square$$

## 9. Hilberts Nullstellensatz (nach D. Grayson)

Erinnerung: ist $K$ Körper, $R \subseteq K$ Teilring, so heißt $\alpha \in K$ ganz über $R$, wenn es ein normiertes Polynom (Leitkoeffizient 1) $p \in R[T]$ gibt mit $p(\alpha) = 1$.
Äquivalent: es gibt ein $R$-Teilmodul $M \subseteq R$ mit $R[\alpha] \subseteq M$, der über $R$ endlich erzeugt ist. Die Menge aller über $R$ ganzen Elemente in $K$ bilden einen Teilring $S \subseteq K$, $R \subseteq S \subseteq K$. (ÜA)

**Lemma A** Sei $K$ Körper, $R \subseteq K$ Teilring. Wenn jedes $\alpha \in K$ ganz ist über $R$, so ist $R$ ein Körper.

Beweis: Sei $r \in R - \{0\}$ und $p(\frac{1}{r}) = 0$ für
$p = T^n + T^{n-1} a_{n-1} + \ldots + a_0$, $a_i \in R$. Es folgt nach Multiplikation mit $r^{n-1}$, dass

$$\frac{1}{r} + a_{n-1} + \ldots + a_0 r^{n-1} = 0 \Rightarrow \frac{1}{r} \in R \qquad \square$$

<u>Lemma B</u> Sei $K$ Körper, $R \subseteq K$ Teilring, sei $\alpha \in K$ mit $R[\alpha] = K$. Dann existiert $s \in R - \{0\}$ so, dass $F = R[\frac{1}{s}]$ ein Körper ist. Weiter ist $\alpha$ algebraisch (= ganz) über $F$.

<u>Bew.</u> Sei $E \subseteq K$ der Quotientenkörper von $R$ $\Rightarrow$ $E[\alpha] = K$ $\Rightarrow$ $\alpha$ algebraisch über $E$, Nullstelle von $p = T^n + T^{n-1}a_{n-1} + \dots + a_0$ $\quad a_j \in E$. Es gibt $s \in R - \{0\}$ mit $a_0, \dots, a_{n-1} \in R[\frac{1}{s}]$ (Hauptnenner) $\Rightarrow$ $\alpha$ ganz über $R[\frac{1}{s}]$ $\Rightarrow$ $K$ ganz über $R[\frac{1}{s}]$ (nach Eingangsbemerkung!?). Nach Lemma A ist $R[\frac{1}{s}]$ ein Körper. $\square$

<u>Lemma C'</u> Ist $R = \mathbb{Z}$ oder $R = F[T]$, $F$ Körper, so ist für $u \in R - \{0\}$ $R[\frac{1}{u}]$ <u>kein</u> Körper.

$$\left[\, R[\tfrac{1}{u}] = R[S]/(uS-1) \,\right]$$

<u>Bew.</u> Schreibe $u = p_1 \cdots p_s \cdot e$ $\quad$ $e$ Einheit, $p_j$ Primelement.

$\boxed{R \text{ ist ZPE-Ring!}}$

Sei $q \in R$ prim mit $q \nmid u$. Wäre $R[\frac{1}{u}]$ Körper, so gäbe es $a_n, \dots, a_0 \in R$ mit

$$\frac{1}{q} = a_n \frac{1}{u^n} + \dots + a_0 \Rightarrow u^n = q\underbrace{(a_n + \dots + a_0 u^n)}_{\in R}$$

$$\Rightarrow q \mid u^n \quad ↯$$

$\square$

<u>Lemma D</u> Sei $K$ Körper, $F \subseteq K$ Teilkörper, $\alpha \in K$. Sei $u \in F[\alpha] - \{0\}$ mit $F[\alpha, \frac{1}{u}] = K$. Dann gilt schon $F[\alpha] = K$ und $\alpha$ ist algebraisch über $F$.

<u>Beweis</u> Wäre $\alpha$ transzendent über $F$, so wäre $F[\alpha] \cong F[T]$. Dann ist aber $F[\alpha, \frac{1}{u}]$ nach Lemma C kein Körper. Also ist $\alpha$ algebraisch über $F$. Dann ist $F[\alpha]$ Körper, also $\frac{1}{u} \in F[\alpha] \Rightarrow F[\alpha, \frac{1}{u}] = F[\alpha] = K$. $\square$

<u>Lemma E</u> Sei $K$ Körper, $R \subseteq K$ Teilring, $\alpha \in K$. Sei $u \in R[\alpha] - \{0\}$ mit $R[\alpha][\frac{1}{u}] = K$. Dann gibt es $v \in R - \{0\}$ mit $R[\alpha, \frac{1}{v}] = K$. Weiter ist $R[\frac{1}{v}]$ Körper und $\alpha$ algebraisch über $R[\frac{1}{v}]$.

<u>Beweis</u> Sei $F \subseteq K$ der Quotientenkörper von $R$. Nach Lemma D folgt $F[\alpha] = K$ und $\alpha$ ist algebraisch über $F$. Es folgt

$$\frac{1}{u} = a_n \alpha^n + \dots + a_0, \quad a_j \in F \Rightarrow \text{es gibt}$$

$t \in R - \{0\}$ mit $a_n, \dots, a_0 \in R[\frac{1}{t}]$ (Hauptnenner).

Also $R[\alpha][\frac{1}{u}] = R[\alpha, \frac{1}{t}] = K$.

Nach Lemma B, angewandt auf $R[\frac{1}{t}]$, gibt es $s \in R[\frac{1}{t}] - \{0\}$ so, dass $R[\frac{1}{t}][\frac{1}{s}]$

Körper ist. Mit $s = b_m \frac{1}{t^m} + \dots + b_0$, $b_j \in R$

$$= \frac{1}{t^m}(b_m + \dots + b_0 t^m) = \frac{1}{t^m} \cdot r, \quad r \in R$$

und $v = r \cdot t$ folgt $\frac{1}{t} = \frac{r}{v}$, $\frac{1}{s} = \frac{t^m}{r} = \frac{t^{m+1}}{v}$, es

folgt $R[\frac{1}{v}] \supseteq R[\frac{1}{t}][\frac{1}{s}] \supseteq R[\frac{1}{v}]$ Körper und

$R[\frac{1}{v}][\alpha] = K$ und $\alpha$ algebraisch über $R[\frac{1}{v}]$ □

<u>Lemma F</u> Sei $K$ Körper, $A \subseteq K$ Teilring, $\alpha_1, \dots, \alpha_n \in K$. Wenn $A[\alpha_1, \dots, \alpha_n] = K$ gilt, so gibt es $s \in A - \{0\}$ so, dass $A[\frac{1}{s}]$ Körper ist und $K$ endliche Erweiterung von $A[\frac{1}{s}]$.

<u>Beweis</u> Setze $R_1 = A[\alpha_1, \dots, \alpha_{n-1}]$, $\alpha = \alpha_n$, $n = 1$ und wende Lemma E an. Es folgt die Existenz von $v_1 \in R_1$ so, dass $K_1 = R_1[\frac{1}{v_1}]$ Körper ist und $\alpha_n$ algebraisch über $K_1$, $K$ endlich über $K_1$. Induktiv weiter mit $R_j = A[\alpha_1, \dots, \alpha_{n-j}] \subseteq K_{j+1}$ und Lemma E und erhalte endliche Körperketten

$$K \supseteq K_1 \supseteq K_2 \supseteq \dots \supseteq K_n$$

$$K_j = A[\alpha_1, \dots, \alpha_{n-j}][\frac{1}{v_j}]$$

$K_n = A[\frac{1}{v_n}]$ setze $s = v_n$. □

10. <u>Theorem</u> (<u>Hilberts Nullstellensatz</u>) Sei $K$ Körper, $F \subseteq K$ Teilkörper, $\alpha_1, \dots, \alpha_n \in K$ mit $F[\alpha_1, \dots, \alpha_n] = K$. Dann ist $K$ endliche Erweiterung von $F$.

<u>Beweis</u>: Wende Lemma F in §3.9 auf $A = F$ an. $\square$

11. <u>Theorem</u> Ist $K$ ein Körper, der als Ring endlich erzeugt ist, so ist $K$ endlich.

<u>Beweis</u>: Sei $\mathbb{Z}[T_1, \dots, T_n] \xrightarrow{\varphi} K$ surjektiver Ringhomomorphismus, vgl §3.3. Sei $A = \varphi(\mathbb{Z}) \subseteq K$. Es folgt $K = A[\alpha_1, \dots, \alpha_n]$ für Elemente $\alpha_j \in K$. Nach §3.9 Lemma F gibt es $s \in A - \{0\}$ so, dass $A[\frac{1}{s}]$ Körper ist. Es folgt $A \not\cong \mathbb{Z}$ (§3.9 Lemma G') also $A \cong \mathbb{Z}/p$ für ein $p \geq 2$. Da $A \subseteq K$ nullteilerfrei ist, ist $p$ eine Primzahl $\Rightarrow A$ Körper, $A[\frac{1}{s}] = A$.

Also ist $K$ endliche Erweiterung von $A \cong \mathbb{F}_p$. $\square$

## 12. Der klassische Nullstellensatz aus der algebraischen Geometrie.

**Theorem A** ("Schwacher Nullstellensatz"). Sei $F$ ein algebraisch abgeschlossener Körper, sei $R = F[T_1, \dots, T_n]$, sei $I \trianglelefteq R$ ein maximales echtes Ideal. Dann gibt es $\alpha_1, \dots, \alpha_n \in F$ mit $I = (T_1 - \alpha_1, \dots, T_n - \alpha_n)$.

Bew. Setze $K = R/_I$. Da $I$ maximal ist, ist $K$ ein Körper. Betrachte

$$\begin{tikzcd} F \arrow[r, hook] \arrow[dr, "\rho"'] & R \arrow[d, "\pi"] \\ & R/_I = K \end{tikzcd}$$

$\pi(f) = f + I$ Projektion. Damit können wir $F$ als Teilkörper von $K$ auffassen. Nach dem Nullstellensatz §3.10, angewandt auf $\pi(T_1) \dots, \pi(T_n)$, ist $K$ endliche Erweiterung von $F$. Da $F$ algebraisch abgeschlossen ist, folgt $K = F$. Also gibt es Elemente $\alpha_1, \dots, \alpha_n \in F$ mit $T_i - \alpha_i \in I$, d.h.
$J = (T_1 - \alpha_1, \dots, T_n - \alpha_n) \subseteq I$. Wegen $R/_J \cong F$ ist $J \trianglelefteq R$ maximal, also $J = I$. □

Anschauung: Ist $J \underset{\neq}{\triangleleft} R$ ein beliebiges Ideal, so wähle $I \supseteq J$ maximal. Dann existiert ein Punkt $(\alpha_1, \dots, \alpha_n) \in F^n$ so, dass für alle $f \in I \supseteq J$ gilt $f(\alpha_1, .., \alpha_n) = 0$, es gibt eine gemeinsame Nullstelle.

# 13. Noethers Normalisierungssatz

**Lemma 1** Seien $f_1, \dots, f_r \in \mathbb{Q}[T]$ mit $f_i \neq f_j$ für $i \neq j$. Dann gibt es $d \in \mathbb{N}$ mit $f_i(d) \neq f_j(d)$ für alle $i \neq j$.

**Bew.** Für $i \neq j$ ist $\{q \in \mathbb{Q} \mid f_i(q) = f_j(q)\}$ endlich. $\square$

**Lemma 2** Sei $K$ Körper, $R \subseteq K$ Teilring, sei $S = \{\alpha \in K \mid \alpha \text{ ganz über } R\}$. Dann ist $S$ Teilring und wenn $\beta \in K$ ganz über $S$ ist, so gilt schon $\beta \in S$.

**Bew.** (ÜA) $\square$

**Theorem** (Noethers Normalisierungssatz)

Sei $A$ ein Integritätsbereich, $F \subseteq A$ ein Teilkörper, seien $\alpha_1, \dots, \alpha_m \in A$ mit $F[\alpha_1, \dots, \alpha_m] = A$. Dann gibt es $\beta_1, \dots, \beta_n \in A$, für ein $n \leq m$, so dass der Einsetzungshomomorphismus

$$F[T_1, \dots, T_n] \to F[\beta_1, \dots, \beta_n], \quad T_i \mapsto \beta_i$$

injektiv ist, und $A$ ist ganz über

$$F[\beta_1, \dots, \beta_n].$$

**Bew.** Induktion nach $m$. Für $m = 0$ ist nichts zu zeigen.

$m=1$ ⇝ $A = F[\alpha_1]$. Betrachte $\Phi: F[T_1] \to F[\alpha_1]$, $T_1 \mapsto \alpha_1$. Falls $\Phi$ injektiv ist, sind wir fertig mit $\beta_1 = \alpha_1$. Wenn $p \in \ker(\Phi)$ normiert ist, so ist $\alpha_1$ ganz über $F$ ⇝ auch fertig.

Induktionsschritt. Sei jetzt $m \geq 2$. Falls

$\Phi: F[T_1,\dots,T_m] \to F[\alpha_1,\dots,\alpha_m]$, $T_i \mapsto \alpha_i$

injektiv ist, sind wir wieder fertig. Sonst gibt es

$0 \neq p \in \ker(\Phi)$

$$p = \sum a_{n_1\dots n_m} T_1^{n_1}\cdots T_m^{n_m} \neq 0$$

OE kommt $T_1$ als Variable vor in $p$!

Mit dem Lemma finden wir ein $d \in \mathbb{Z}$ so, dass die Summen $n_1 + dn_2 + d^2 n_3 + \dots + d^{m-1} n_m$ paarweise verschieden sind für alle $a_{n_1\dots n_m} \neq 0$.

Betrachte $q(T_1, S_2, \dots, S_m) \in F[T_1, S_2, \dots, S_m]$

$$q(T_1, S_2, \dots, S_m) = p(T_1, T_1^d + S_2, T_1^{d^2} + S_2, \dots, T_1^{d^{m-1}} + S_m)$$

$$= \sum a_{n_1\dots n_m} T_1^{n_1 + dn_2 + \dots + d^{m-1} n_m} + g_{n_1,\dots,n_m}(T_1, S_2, \dots, S_m)$$

$g_{n_1,\dots,n_m} \in F[S_2,\dots,S_m][T_1]$ hat Grad (in $T_1$) echt kleiner als $n_1 + dn_2 + \dots + d^{m-1} n_m$.

Wir können annehmen, dass $q$ als Polynom der Variable $T_1$ über $F[S_2, \dots, S_m]$ normiert ist. (!)

Setze $r_i = \alpha_i - \alpha_1^{d^{i-1}} \in A$ für $i \geq 2 \Rightarrow r_i + \alpha_1^{d^{i-1}} = \alpha_i$,

also $q(\alpha_1, r_2, \dots, r_m) = p(\alpha_1, r_2 + \alpha_1^{d}, \dots, r_m + r_1^{d^{m-1}}) =$

$$= p(\alpha_1, \dots, \alpha_m) = 0$$

Damit ist $\alpha_1$ ganz über $A_1 = F[r_2, \dots, r_m] \subseteq A$.

Nach Induktionsannahme gibt es $\beta_1, \dots, \beta_l$, $l \leq m-1$ mit $F[\beta_1, \dots, \beta_l] \cong F[T_1, \dots, T_l]$ und $A_1$ ist ganz über $F[\beta_1, \dots, \beta_l]$. Nach Lemma 2 ist $A$ ganz über $F[\beta_1, \dots, \beta_l]$ $\square$

Jetzt gehen wir zurück zu Matrizen.

14. <u>Erinnerung:</u> ein Ideal in einem nicht-kommutativen Ring $R$ ist eine Teilmenge $I \subseteq R$ mit

(1) $(I,+)$ ist Untergruppe von $(R,+)$

(2) Für alle $a \in R$, $h \in I$ gilt $ah \in I$ <u>und</u> $ha \in I$.

Man rechnet leicht nach: $R/I$ ist dann wieder ein Ring.

<u>Lemma</u> Ist $A$ ein kommutativer Ring, $R = A^{n\times n}$ und $I \trianglelefteq A$ ein Ideal, so ist $J = I^{n\times n} \subseteq R$ ein Ideal. Es gilt $R/J \cong (A/I)^{n\times n}$

<u>Beweis</u> Klar: $I^{n\times n}$ ist Untergruppe von $R^{n\times n}$, $h \in I^{n\times n}$, $a \in A^{n\times n} \Rightarrow ah, ha \in I^{n\times n}$ (Rechenregeln für Matrizen). Der Kern der Abbildung (von Gruppen)

$$A^{n\times n} \to (A/I)^{n\times n}$$

ist genau $I^{n\times n}$, also $A^{n\times n}/I^{n\times n} \cong (A/I)^{n\times n}$ $\square$

<u>Folgerung</u> Für $I \trianglelefteq A$ erhalten wir einen Homomorphismus

$$\begin{tikzcd} GL_n(A) \arrow[r, "\pi"] \arrow[d, equal] & GL_n(A/I) \arrow[d, equal] \\ (A^{n\times n})^* & ((A/I)^{n\times n})^* \end{tikzcd}$$

Wir definieren die <u>Kongruenzuntergruppe</u>

$$\Gamma(I) = \ker(\pi)$$

Es gilt also: $g \in \Gamma(I) \Leftrightarrow$ es gibt $h \in I^{n \times n}$ mit $g = \mathbb{1}_n + h$ und $\det(\mathbb{1}_n + h) \in A^*$.

15. <u>Theorem</u> (Malcev) Ist $A$ endlich erzeugter Integritätsbereich, so ist $GL_n(A)$ residuell endlich.
Insbesondere ist jede endlich erzeugte Matrizengruppe (über einem Körper $F$) residuell endlich.

<u>Beweis</u> Wir wählen ein maximales Ideal $I \trianglelefteq A$.

(1) <u>Beh</u> $A/_I$ ist endlich

Denn: $A/_I$ ist Körper (weil $I$ maximal) und als Ring endlich erzeugt. Nach § 3.11 ist $A/_I$ endlich. □

(2) <u>Beh</u> Für jedes $m \geq 1$ ist $I^m/_{I^{m+1}}$ endlich

<u>Beweis</u> Da $A$ noethersch ist (§ 3.7) ist $I = (x_1, \ldots, x_n)$. Damit ist $I^m/_{I^{m+1}}$ ein endlich erzeugter $A$-Modul. Für alle $x \in I^m$, $j \in I \subseteq A$ gilt $jx \in I^{m+1} \Rightarrow I^m/_{I^{m+1}}$ ist endlich erzeugter $A/_I$-Modul, also endlich-dimensionaler Vektorraum über $A/_I$ □

(3) Beh Für alle $k, l \geq 1$ ist

$$I^k / I^{k+l} \quad \text{und} \quad A/I^k \quad \text{endlich.}$$

Induktion nach $l$, $l = 1$ ist (2), damit

$$I^k / I^{k+l+1} \to \underbrace{I^k / I^{k+l}}_{\text{endlich}} \quad \text{hat Kern} \quad \underbrace{I^{k+l} / I^{k+l+1}}_{\text{endlich}}$$

$$\Rightarrow \quad I^k / I^{k+l+1} \text{ endlich.}$$

$A/I$ ist endlich, Induktion nach $k$:

$$A/I^{k+1} \to A/I^k \quad \text{hat Kern} \quad \underbrace{I^k / I^{k+1}}_{\text{endlich}}$$

(4) Beh Es gilt $\bigcap_{l \geq 1} \Gamma(I^l) = \{1_n\}$

Denn: $\bigcap_{l \geq 1} (I^l)^{n \times n} = \{0\}$ nach

Krulls Durchschnittssatz § 3.8.

(5) Beh $\Gamma(I^l) \trianglelefteq GL_n(A)$ hat endlich

Index.

Denn $GL_n(A/I^l)$ ist endlich, da

$A/I^l$ endlicher Ring ist. $\square$

16. Lemma Sei $A$ endlich erzeugt Integritätsbereich, sei $I \trianglelefteq A$ maximales Ideal mit $\operatorname{char}(A/I) = p > 0$. Dann gilt für alle

$$g \in \Gamma(I^k), \text{ dass } g^{p^\ell} \in \Gamma(I^{k+\ell})$$

Bew.: Schreibe $g = 1\!\!1_n + h$, $h \in (I^k)^{n \times n}$.

Es folgt $g^p = (1\!\!1_n + h)^p = 1\!\!1_n + \underbrace{p\,h + \sum_{j=2}^{p} \binom{p}{j} h^j}_{\in (I^{k+1})^{n\times n}}$

denn $p \in I$. Also $g^p \in \Gamma(I^{k+1})$ □

17. Korollar (Satz von Platonov in Charakteristik $p$)

Sei $A$ endlich erzeugt Integritätsbereich der Charakteristik $p > 0$. Sei $I \trianglelefteq A$ maximales Ideal. Dann ist $\Gamma(I)$ residuell eine $p$-Gruppe.

Bew.: Für alle $k \geq 1$ ist $\Gamma(I)/\Gamma(I^k)$ eine $p$-Gruppe, und $\bigcap_{k\geq 1} \Gamma(I^k) = \{1\}$ □

Anders formuliert: ist $A$ endlich erzeugter Integritätsbereich der Charakteristik $p > 0$, so ist $GL_n(A)$ virtuell residuell $p$-Gruppe.

18. <u>Satz</u> Sei $A$ ein endlich erzeugter Integritätsbereich mit $\mathrm{char}(A) = 0$. Dann gibt es nur endlich viele Primzahlen $p$ mit $\frac{1}{p} \in A$.

<u>Beweis</u> Sei $K$ Quotientenkörper von $A = \mathbb{Z}[\alpha_1, \dots, \alpha_m]$.
Betrachte $\tilde{A} = \mathbb{Q}[\alpha_1, \dots, \alpha_m] \supseteq A$. Nach Noethers Normalisierungssatz § 3.13 gibt es $\beta_1, \dots, \beta_n \in \tilde{A}$ so, dass $\tilde{A}$ ganz ist über $\mathbb{Q}[\beta_1, \dots, \beta_n]$ und
$\mathbb{Q}[T_1, \dots, T_n] \to \mathbb{Q}[\beta_1, \dots \beta_n]$ ist Isomorphismus.
$T_i \mapsto \beta_i$

Es gibt $b_i \in \mathbb{Z}, b_i \neq 0$ so, dass $\beta_i b_i \in A$, OE also $\beta_i \in A$ (und die $\beta_i$ bleiben algebraisch unabhängig).

Jedes $\alpha_i$ ist ganz über $\mathbb{Q}[\beta_1, \dots, \beta_n]$. Damit finden wir eine Zahl $l \neq 0$ in $\mathbb{Z}$ so, dass $\alpha_1, \dots, \alpha_m$ ganz sind über $\mathbb{Z}[\frac{1}{l}][\beta_1, \dots, \beta_n]$.
Folglich ist $A[\frac{1}{l}]$ ganz über $\mathbb{Z}[\frac{1}{l}][\beta_1, \dots, \beta_n]$.
Angenommen, $p$ ist Primzahl, $\frac{1}{p} \in A \subseteq A[\frac{1}{l}]$.
Es folgt $\left(\frac{1}{p}\right)^k + a_1 \left(\frac{1}{p}\right)^{k-1} + \dots + a_k = 0$, $a_j \in \mathbb{Z}[\frac{1}{l}][\beta_1, \dots, \beta_n]$

$$\Rightarrow \frac{1}{p} + a_1 p + \dots + a_k p^k = 0 \Rightarrow \frac{1}{p} \in \mathbb{Z}[\tfrac{1}{l}][\beta_1, \dots, \beta_n]$$

$\cong \mathbb{Z}[\frac{1}{l}][T_1, \dots, T_m] \Rightarrow \frac{1}{p} \in \mathbb{Z}[\frac{1}{l}]$, etwa

$$\frac{1}{p} = z_0 \frac{1}{l^s} + z_1 \frac{1}{l^{s-1}} + \dots + z_s, \quad z_i \in \mathbb{Z}$$

$$\ell^s = p\cdot z_0 + \dots + \ell^s \cdot z_s\, p \Rightarrow p \mid \ell^s \Rightarrow p \mid \ell \qquad \square$$

19. <u>Theorem</u> <u>(Satz von Platonov in Charakteristik 0)</u>
Sei $A$ ein endlich erzeugter Integritätsbereich der Charakteristik 0. Dann ist $GL_n(A)$ virtuell residuell $p$-Gruppe für fast alle Primzahlen $p \in \mathbb{P}$.

<u>Beweis</u> Sei $\frac{1}{p} \notin A$. Dann ist $pA \neq A$. Wähle maximales Ideal $I \trianglelefteq A$ mit $pA \subseteq I$. Es folgt $\mathrm{char}(A/I) = p$, wende jetzt die Schritte (1)–(5) aus dem Beweis von § 3.15 an $\Rightarrow$ $\Gamma(I)$ residuell $p$-Gruppe mit endlichem Index in $GL_n(A)$. $\square$

20. <u>Theorem</u> (Satz von Selberg) Sei $A$ ein endlich erzeugter Integritätsbereich mit $\mathrm{char}(A) = 0$. Dann ist $GL_n(A)$ virtuell torsionsfrei, d.h. $GL_n(A)$ hat Untergruppe von endlichem Index, die keine Elemente $\neq 1\!\!1_n$ endlicher Ordnung enthält.

Für den Beweis benötigen wir folgendes Lemma:

<u>Lemma</u> Ist $H$ residuell ein $p$-Gruppe, so ist für alle Torsionselemente $h \in H$, dass $o(h)$ eine $p$-Potenz ist.

<u>Beweis</u> Angenommen, $q \neq p$ ist Primzahl und $q \mid o(h)$, $o(h) = q \cdot r \Rightarrow o(h^r) = q$. Wähle $N \trianglelefteq H$ mit endlichem Index, $h^r \notin N$. Dann ist $H/_N$ $p$-Gruppe $\Rightarrow p \mid o(h^r N)$ ↯ □

<u>Beweis von Selbergs Theorem:</u> Nach § 3.19 gibt es Primzahlen $p \neq q$ und Untergruppen $H, K \leq GL_n(A)$ mit endlichem Index so, dass $H$ residuell $p$-Gruppe und $K$ residuell $q$-Gruppe ist. Dann ist $H \cap K$ nach dem Lemma torsionsfrei, und $[GL_n(A) : H \cap K] < \infty$. □

21. Wir fassen zusammen. Sei $F$ Körper, sei $\Gamma \leq GL_n(F)$ endlich erzeugte Gruppe. Dann gilt Folgendes.

(1) Ist $\mathrm{char}(F) = p > 0$, so ist $\Gamma$ virtuell residuell $p$-Gruppe.

(2) Ist $\mathrm{char}(F) = 0$, so ist $\Gamma$ virtuell residuell $p$-Gruppe für fast alle Primzahlen $p$.

(3) Ist $\mathrm{char}(F)=0$, so ist $\Gamma$ virtuell torsionsfrei.

22. Das Beispiel $A=\mathbb{Z}$  $\mathbb{Z}$ ist endlich erzeugter Hauptidealbereich (also noethersch). Die Ideale in $\mathbb{Z}$ sind alle von der Form $I=(k)=k\mathbb{Z}$, für $k\in\mathbb{N}$. Es gilt

$$(k)\cap(\ell)=(m) \qquad m=\mathrm{kgV}(k,\ell)$$

$$(k)\cdot(\ell)=(k\ell)$$

$$(k)^n=(k^n)$$

Krulls Durchschnittsatz §3.8 besagt

$$\bigcap_{n\geq 1}(k)^n=\bigcap_{n\geq 1}(k^n)=(0)$$

Die maximalen Ideale in $\mathbb{Z}$ sind $(p)$, mit $p\in\mathbb{P}$. Für jedes Ideal $I\neq(0)$ ist $\mathbb{Z}/I$ endlich, dazu brauchen wir §3.11 nicht.

Wir setzen $\Gamma_n(k)=\ker(GL_n(\mathbb{Z})\to GL_n(\mathbb{Z}/k))$

Wegen $(k)^{n\times n}\cap(\ell)^{n\times n}=(m)^{n\times n}$  $m=\mathrm{kgV}(k,\ell)$

Folgt $\Gamma_n(k)\cap\Gamma_n(\ell)=\Gamma_n(\ell)$

Mit dem Lemma aus §3.20 folgt sofort: ist $p,q\in\mathbb{P}$, $p\neq q$, so ist

$\Gamma_n(p\cdot q)$ torsionsfrei.

Andererseits ist keine Primzahl in $\mathbb{Z}$ invertierbar $\Rightarrow$ $GL_n(\mathbb{Z})$ ist virtuell residuell $p$-Gruppe für alle Primzahlen $p \in \mathbb{Z}$.

<u>Lemma</u> Sei $p \in \mathbb{P}$. Für $p \geq 3$ ist $\Gamma_n(p)$ torsionsfrei. Ist $g \in \Gamma_n(2)$ mit $o(g) < \infty$, so ist $o(g) = 2$. Weiter ist $\Gamma_n(4)$ torsionsfrei.

<u>Beweis</u> Sei $p \in \mathbb{P}$, sei $g \in \Gamma_n(p)$ mit $o(g) = q \in \mathbb{P}$. Mit dem Lemma aus § 37.20 folgt $p = q$, denn $\Gamma_n(p)$ ist residuell $p$-Gruppe. Schreibe $g = \mathbb{1}_n + h$, $h \in (p)^{n\times n}$.

Wegen $g^p = \mathbb{1}$ folgt

$$\mathbb{1}_n = \sum_{j=0}^{p} \binom{p}{j} h^j = \mathbb{1}_n + ph + \binom{p}{2} h^2 + \sum_{j=3}^{p} \binom{p}{j} h^j$$

Sei $p^s$ die größte $p$-Potenz, die alle Einträge von $h$ teilt, dann ist $p^{s+1}$ die größte $p$-Potenz, die alle Einträge von $ph = -\binom{p}{2} h^2 - \sum_{j=3}^{p} \binom{p}{j} h^j$ teilt.

Für $p \geq 3$ folgt, dass $p^{2s+1}$ alle Einträge rechts teilt $\Rightarrow$ $s+1 \geq 2s+1 \Rightarrow 0 \geq s$ $\lightning$

also gibt es in $\Gamma(p)$ keine Elemente der Ordnung $q$, für $q \in \mathbb{P}$ beliebig $\Rightarrow \Gamma(p)$ torsionsfrei.

Für $p = 2$ erhalten wir $2h = -h^2$ und damit $s = 1$. Es folgt $h \notin (4)^{n \times n}$ $\Rightarrow g \notin \Gamma_n(4)$, damit ist $\Gamma_n(4)$ auch torsionsfrei. Für alle $g \in \Gamma_n(2)$ gilt $g^2 \in \Gamma_n(4)$ (wegen $(\mathbb{1}+h)^2 = \mathbb{1} + 2h + h^2$), damit haben alle Elemente endlicher Ordnung in $\Gamma_n(2)$ Ordnung 1 oder 2.

<u>Korollar</u> Für alle $k \geq 3$ ist $\Gamma_n(k)$ torsionsfrei.

Denn: $k = 2^t$ mit $t \geq 2 \Rightarrow \Gamma_n(k) \subseteq \Gamma_n(4)$, sonst

$k = p \cdot r$, $p$ ungerade Primzahl $\Rightarrow \Gamma_n(k) \subseteq \Gamma_n(p)$ □

23. <u>Satz</u> Für alle $g \in GL_2(\mathbb{Z})$ gilt

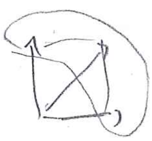
$o(g) \in \{1, 2, 3, 4, 6, \infty\}$

<u>Denn</u>: Sei $g \in GL_n(\mathbb{Z})$ mit endlicher Ordnung.

1. Fall $g \in \Gamma_2(2) \Rightarrow o(g) = \{1, 2\}$

2. Fall $g \notin \Gamma_2(2) \Rightarrow g$ hat nicht triviales Bild unter $GL_2(\mathbb{Z}) \xrightarrow{\pi} GL_2(\mathbb{Z}/2)$

Es gilt $\# GL_2(\mathbb{Z}/2) = 3 \cdot 2 = 6$, $GL_2(\mathbb{Z}/2) \cong \mathrm{Sym}(3)$



$\Rightarrow o(\pi(g)) \in \{1, 2, 3\}$

$\# (\langle g \rangle \cap \Gamma_2(2)) \in \{1, 2\}$

$\Rightarrow$ $o(g) \in \{1,2,3,4,6\}$ (denn $g^r \in \Gamma_2(2) \Rightarrow g^{2r} = 1$).

Es gibt tatsächlich Elemente dieser Ordnung:

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in SL_2\mathbb{Z} \qquad o(a) = 4$$

$$b = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in SL_2\mathbb{Z} \qquad o(b) = 6$$

□

__Bem__ Ist $G \leq GL_2\mathbb{R}$ endliche Untergruppe, so ist $G$ konjugiert zu einer Untergruppe von $O(2)$ (wähle ein $G$-invariantes Skalarprodukt auf $\mathbb{R}^2$).
Die endlichen Untergruppen von $SO(2) \leq O(2)$ sind zyklische Gruppen $\mathbb{Z}/m$ (Drehungen um Winkel $\frac{2\pi}{m}$), damit sind die Untergruppen von $O(2)$ Diedergruppen der Ordnung $2m$ oder zyklische Gruppen der Ordnung $m$, $m \geq 1$ beliebig.
Die Gruppe $GL_2\mathbb{Z}$ ist die Gruppe aller Matrizen, die $\mathbb{Z} \oplus \mathbb{Z} \leq \mathbb{R} \oplus \mathbb{R}$ invariant lässt. Die endlichen Untergruppen von $GL_2\mathbb{Z}$ nennt man kristallographische Punktgruppen in der Ebene – hier ist nur $m = 1,2,3,4,6$ möglich!

__Bem__ Für $n \geq 2$ enthält $SL_n(\mathbb{Z})$ ein Element der Ordnung 6 $\rightsquigarrow \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, also ist $SL_n(\mathbb{Z})$ für __kein__ $p \in \mathbb{P}$ residuell $p$-Gruppe. (!)

24 Erinn. Ein kommutativer Integritätsbereich $A$ heißt <u>euklidisch</u>, wenn es eine Gradfunktion $\delta: A \to \mathbb{N}$ gibt, mit: (1) für alle $a, b \in A$, $b \neq 0$ gibt es $s, r \in R$ mit $a = sb + r$, $\delta(r) < \delta(b)$ (Teilen mit Rest)

(2) OE ($\delta(r) = \delta(-r)$) alle $a, b \in R$

<u>Bsp</u>
- $\mathbb{Z}$ mit $\delta(z) = |z|$
- $F$ Körper, $\delta(x) = \begin{cases} 1 & \text{wenn } x \neq 0 \\ 0 & \text{wenn } x = 0 \end{cases}$

Euklidische Ringe sind Hauptidealringe.

<u>Def</u> Ein kommutativer Ring $A$ heißt <u>lokaler Ring</u>, wenn $A - A^*$ ein Ideal ist.

<u>Bsp</u>
- $F$ Körper
- $p \in \mathbb{P}$, $s \geq 1 \Rightarrow \mathbb{Z}/p^s$ ist lokaler Ring, denn: $(p)$ ist Ideal in $\mathbb{Z}/p^s$
  $x \in \mathbb{Z} - p\mathbb{Z} \Rightarrow ggT(x, p) = 1 \Rightarrow$ es gibt $y, q \in \mathbb{Z}$ mit $xy + pq = 1 \Rightarrow$ $x + p^s\mathbb{Z}$ Einheit in $\mathbb{Z}/p^s$

Erinn: $m \in \mathbb{Z}$, $m \geq 2$ mit Primfaktorzerlegung

$$m = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k} \qquad p_1 < p_2 < \ldots < p_k \text{ Primzahl}, \; l_i \geq 1$$

$$\Rightarrow \mathbb{Z}/m \cong \mathbb{Z}/p_1^{l_1} \times \ldots \times \mathbb{Z}/p_k^{l_k}$$ Produkt von lokalen Ringen.

Es folgt

$$(\mathbb{Z}/m)^{n\times n} \cong (\mathbb{Z}/p_1^{e_1})^{n\times n} \times \dots \times (\mathbb{Z}/p_k^{e_k})^{n\times n}$$

$$GL_n(\mathbb{Z}/m) \cong GL_n(\mathbb{Z}/p_1^{e_1}) \times \dots \times GL_n(\mathbb{Z}/p_k^{e_k})$$

25. <u>Definition</u> Für $i \neq j$ und $a \in A$ sei $T_{ij}(a) \in A^{n\times n}$ die Matrix

$$\begin{array}{cl} \begin{pmatrix} 1 & & a \\ & \ddots & \\ 0 & & 1 \end{pmatrix} & - i \\ \quad\quad\;\; j & \end{array}$$

Es gilt: $T_{ij}(a)\, T_{ij}(b) = T_{ij}(a+b)$

Solche Matrizen heißen <u>Elementarmatrizen</u>.

Wir definieren $E_n(A) = \langle \{ T_{ij}(a) \mid i \neq j,\ a \in A \} \rangle$

Beachte: für $A = \mathbb{Z}$ wird diese Gruppe also erzeugt von den $n^2 - n$ Matrizen $\{ T_{ij}(1) \mid i \neq j \}$

$\Rightarrow$ $E_n(\mathbb{Z})$ ist endlich erzeugt. Genauso $E_n(\mathbb{Z}/m)$.

Sei $D_n = \left\{ \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in A^{n\times n} \;\middle|\; a \in A^* \right\} \cong A^*$

<u>Theorem</u> Ist $A$ ein lokaler oder endlicher Ring, so gilt $GL_n(A) = D_n \cdot E_n(A)$ und $E_n(A) = SL_n(A)$

<u>Beweis</u> $E_n(A) \subseteq SL_n(A)$, denn $\det(T_{ij}(a)) = 1$.

Weiter normalisiert $D_n$ die Menge der $T_{ij}(a)$:

$$\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} T_{ij}(s) \begin{pmatrix} a_1^{-1} & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \begin{cases} T_{ij}(a^{-1}s) & j = 1 \\ T_{ij}(s) & i,j \neq 1 \\ T_{ij}(as) & i = 1 \end{cases}$$

Weiter gilt $E_n(A) \cap D_n = \{1\!\!1\}$, denn

$\det\begin{pmatrix} a & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix} = a$. Also ist $E_n(A) D_n$ ein

semidirektes Produkt und eine Untergruppe von $GL_n(A)$.

<u>Beh</u> $GL_n(A) = D_n \cdot E_n(A)$ mit Induktion nach $n$.

<u>$n=1$</u> $GL_1(A) = A^* = D_1$ (✓)

<u>$n \geq 2$</u> <u>Vorüberlegung</u>: es gilt $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

$= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ⇝ wir können mit Elementen aus $E_n(A)$

Zeilen und Spalten (bis auf Vorzeichen) vertauschen sowie

zu Zeilen und Spalten Vielfache anderer Zeilen und

Spalten addieren.

Zuerst der Fall, wo $A$ euklidisch ist.

Sei jetzt $g \in GL_n(A)$. Betrachte die Menge

$X = E_n(A) g E_n(A) \subseteq GL_n(A)$. Wähle $\tilde{g} \in X$

so, dass $\tilde{g}$ einen Eintrag $\tilde{g}_{ij} \neq 0$ mit $\delta(\tilde{g}_{ij})$

minimal hat. OE $i=j=n$, $\tilde{g}_{ij} = s$

$$\tilde{g} = \begin{pmatrix} \boxed{\phantom{xx}} & \vdots \\ & t \\ & \vdots \\ \cdots & s \end{pmatrix}$$

$t = as + r$ $\quad \delta(r) < \delta(s)$

$r = t - as$ kommt als

Eintrag einer Matrix in $X$

$\forall r \Rightarrow r = 0$

$\Rightarrow$ wir finden $\tilde{\tilde{g}} = \begin{pmatrix} \boxed{a} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ 0 \cdots 0 & s \end{pmatrix} \in X$

$a \in GL_{n-1}(A)$

Nach Induktionsannahme gilt $a \in E_{n-1}(A)\cdot D_{n-1}$.

Weiter $\begin{pmatrix} 1 & & \\ & \ddots & 0 \\ 0 & & 1_s \end{pmatrix} \in E_n(A)\cdot D_n$, also $\tilde{g} \in E_n(A)\cdot D_n$

$g = a\tilde{g}b$, $a,b \in E_n(A) \Rightarrow g \in E_n(A)\cdot D_n$ $\square$

Wenn $A$ lokaler Ring ist, so hat $g \in GL_n(A)$ mindestens einen Eintrag $s = g_{ij} \in A^*$, denn sonst $\det(g) \in A - A^*$, weil $A - A^*$ Ideal ist. Es folgt wie oben

$$\begin{pmatrix} \square & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ 0 \;\cdots\; 0 & s \end{pmatrix} \in X \Rightarrow \text{genauso weiter}$$ $\square$

<u>Korollar</u> Ist $p \in \mathbb{P}$, so wird $SL_n(\mathbb{Z}/p^s)$ von den Matrizen $\tau_{ij}(1)$, $i \neq j$ erzeugt. Genauso $SL_n(\mathbb{Z})$.

<u>Korollar</u> Ist $m \in \mathbb{Z}$, $m \geq 2$, so wird $SL_n(\mathbb{Z}/m)$ von den Matrizen $\tau_{ij}(1)$, $i \neq j$ erzeugt. Insbesondere ist $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/m)$ surjektiv.

<u>Beweis</u> Schreibe $m = p_1^{l_1} \cdots p_s^{l_s}$, $l_j \geq 1$, $p_j \in \mathbb{P}$, $p_1 < p_2 < \dots < p_s$ Primfaktorzerlegung.

$\mathbb{Z}/m \cong \mathbb{Z}/p_1^{l_1} \oplus \dots \oplus \mathbb{Z}/p_s^{l_s}$ als Ring,

denn betrachte $\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{l_1} \oplus \dots \oplus \mathbb{Z}/p_s^{l_s}$

$$x \longmapsto (x_1, \dots, x_s)$$
$$x_i = x + p_i^{l_i}\mathbb{Z}$$

Der Kern ist genau $\mathbb{Z}/m$ und $\pi$ ist surjektiv:

$1 = u\, p_1^{l_1} + v\, p_2^{l_2} \cdots p_s^{l_1} \Rightarrow (1, 0, \dots 0)$ im Bild,

genauso die restlichen $s-1$ Erzeuger der zyklischen Gruppen

$\mathbb{Z}/p_i^{l_i}$. Nun folgt $(\mathbb{Z}/m)^{n\times n} \cong (\mathbb{Z}/p_1^{l_1})^{n\times n} \times \dots \times (\mathbb{Z}/p_s^{l_s})^{n\times n}$

$$\Rightarrow GL_n(\mathbb{Z}/m) \cong GL_n(\mathbb{Z}/p_1^{l_1}) \times \dots \times GL_n(\mathbb{Z}/p_s^{l_s})$$

$$\Rightarrow SL_n(\mathbb{Z}/m) \cong SL_n(\mathbb{Z}/p_1^{l_1}) \times \dots \times SL_n(\mathbb{Z}/p_s^{l_s})$$

$u, v$ wie oben gewählt $\Rightarrow$

$$\tau_{ij}(1) \xmapsto{\pi} (\underset{\uparrow}{\tau_{ij}(1)}, \tau_{ij}(0), \dots, \tau_{ij}(0))$$

Erzeuger für 1. Gruppe. $\square$

Achtung: $GL_n(\mathbb{Z}) = \{ g \in \mathbb{Z}^{n\times n} \mid \det(g) = \pm 1 \}$,

daher ist $GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/m)$ im Allgemeinen nicht surjektiv.

Wir definieren $S\Gamma_n(l) = \Gamma_n(l) \cap SL_n(\mathbb{Z})$

<u>Bem</u> Für allgemeine Ringe ist $E_n(A) \subsetneq SL_n(A)$, das führt auf Fragen in der algebraischen K-Theorie von Ringen.

27. Definition Wir definieren die Gruppe $E_n(m) \trianglelefteq SL_n(\mathbb{Z})$ als normalen Abschluss der Elemente $\{\tau_{ij}(m) \mid i \neq j\}$ in $SL_n(\mathbb{Z})$

$$E_n(m) = \langle\langle \{\tau_{ij}(m) \mid i \neq j\} \rangle\rangle_{SL_n(\mathbb{Z})}$$ ($\tau_{ij}(m) \in \Gamma_n(m)$ ist klar!)

Theorem (Mennicke) Für $n \geq 3$ gilt $S\Gamma_n(m) = E_n(m)$

Damit erhalten wir folgendes wichtiges Ergebnis

Theorem (Bass-Milnor-Serre (Mennicke)) Sei $n \geq 3$ und $N \trianglelefteq SL_n\mathbb{Z}$ mit endlichem Index. Dann gibt es $m \geq 2$ mit $S\Gamma(m) \subseteq N$.

Beweis Da $N$ endlichen Index hat, gibt es ein $m_{ij} \geq 2$ mit $\tau_{ij}(m) \in N$ (denn sonst hätten wir $\mathbb{Z} \cong \langle \tau_{ij}(1) \rangle \cap N = \{1\}$ ↯) Damit folgt $\tau_{ij}(m) \in N$ für $m = \prod_{k<l} m_{k,l}$. $\square$

Mit dem Theorem kann man im Prinzip alle endlichen Untergruppen in $SL_n(\mathbb{Z})$ mit endlichem Index beschreiben: sie entsprechen den endlichen Untergruppen von $SL_n(\mathbb{Z}/m)$. Denn:

$H \subseteq SL_n(\mathbb{Z})$ mit endlichem Index $\Rightarrow$ wähle $m$ minimal mit $S\Gamma_n(m) \subseteq H$

$\Rightarrow \quad \pi : SL_n(\mathbb{Z}) \twoheadrightarrow SL_n(\mathbb{Z}/m)$

$\pi(H)$ Untergpp in $SL_n(\mathbb{Z}/m)$ mit

$H = \pi^{-1}\pi(H)$, weil $\ker(\pi) \subseteq H$.

Wir kennen jetzt Hennickes Theorem - das braucht einige Sätze

28. Konvention: via $a \mapsto \begin{pmatrix} \boxed{a} & 0 \\ 0 & 1 \end{pmatrix}$ fassen wir $\mathbb{Z}^{n\times n}$ als Teilmenge von $\mathbb{Z}^{(n+1)\times(n+1)}$ auf, entsprechend $E_n(\mathbb{Z}) \hookrightarrow E_{n+1}(\mathbb{Z})$ usw.

<u>Lemma A</u> Sei $n \geq 3$, seien $a_1, \ldots, a_n \in \mathbb{Z}$ mit $(a_1) + (a_2) + \ldots + (a_n) = \mathbb{Z}$. Dann gibt es $c_2, \ldots, c_n \in \mathbb{Z}$ mit $(a_2 + c_2 a_1) + \ldots + (a_n + c_n a_1) = \mathbb{Z}$

<u>Beweis</u> Wenn ein $a_i = 0$ ist, dann ist das klar, OE $a_i \neq 0$ für alle $i$.
Es gilt $ggT(a_1, \ldots, a_n) = 1$. Sei

$b = ggT(a_3, \ldots, a_n)$ mit Primfaktoren $p_1 < \ldots < p_k$.

Die $p_j$ können $a_1$ und $a_2$ nicht gleichzeitig teilen $\Rightarrow$

$\Rightarrow a_2 + \lambda_j a_1 \not\equiv 0 \pmod{p_j}$ für $\lambda_j \in \{0,1\}$.

Es existiert $c \in \mathbb{Z}$ mit $c \equiv \lambda_j \pmod{p_j}$ für alle $j$

((Chinesischer Restsatz, vgl §3.24)

$\Rightarrow a_2 + c a_1 \not\equiv 0 \pmod{p_j}$

$\Rightarrow ggT(a_2 + c a_1, b) = 1$

$\Rightarrow (a_2 + c a_1) + (a_3) + \ldots + (a_n) = \mathbb{Z}$ $\square$

**Lemma B** $S\Gamma_n(l)$ wird von $S\Gamma_2(l) \cup E_n(l)$ erzeugt, für alle $n \geq 2$ und $l \geq 2$.

**Beweis** Induktion nach $n$, $n = 2$ klar. Es genügt dann zu zeigen, dass $S\Gamma_{n-1}(l) \cup E_n(l)$ ein EZS für $S\Gamma_n(l)$ bilden. Betrachte $g \in S\Gamma_n(l)$,

$$g = \begin{pmatrix} & * & \\ a_1 & & a_n \end{pmatrix} \qquad \begin{array}{ll} a_1, \dots, a_{n-1} & \equiv 0 \pmod{l} \\ a_n & \equiv 1 \pmod{l} \end{array}$$

Sei $d = ggT(a_1, \dots, a_n) \Rightarrow d \mid \det(g) = 1$.

Kein Primteiler $p$ von $l$ teilt $a_n$, also $ggT(l a_1, a_2, \dots, a_n) = 1$. Mit Lemma A finden wir $c_i \in \mathbb{Z}$ mit

$$ggT(\underbrace{a_2 + c_2 l a_1}_{= a_2'}, \dots, \underbrace{a_n + c_n l a_1}_{= a_n'}) = 1$$

$$\Rightarrow g \equiv \begin{pmatrix} & * & \\ a_1 & a_2' \dots & a_n' \end{pmatrix} \mod E_n(l)$$

Es gibt $z_i \in \mathbb{Z}$ mit $a_2' z_2 + \dots + a_n' z_n = 1$

$$\Rightarrow a_2' l \cdot z_2 + \dots + a_n' l \cdot z_n = l$$

$$\Rightarrow g \equiv \begin{pmatrix} & * & \\ l & a_2' & a_n' \end{pmatrix} = \tilde{g} \qquad \text{denn } l \mid a_1$$

Weiter $a_n' \equiv a_n \equiv 1 \pmod{l} \Rightarrow a_n' = 1 + k \cdot l$.

Es gilt also

$$\tilde{g}\,\tau_{n,1}(-k) = \begin{pmatrix} & * & \\ l\,a_1' & a_{n-1}' & 1 \end{pmatrix}$$

$$\Rightarrow \tilde{g}\,\tau_{n,1}(-h)\,h = \begin{pmatrix} & * & \\ 0 & \cdots\; 0 & 1 \end{pmatrix} \qquad h \in E_n(l)$$

$$\Rightarrow \tilde{g}\,\underbrace{\tau_{n,1}(-h)\,h\,\tau_{n,1}(h)}_{\in E_n(l)} = \begin{pmatrix} & * & \\ 0 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow g \equiv \begin{pmatrix} * & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ 0 \;\cdots\; 0 & 1 \end{pmatrix} \mod E_n(l) \to \text{fertig mit Induktion.} \quad \square$$

#

29. Wir definieren $Q_n(l) = S\Gamma_n(l) / E_n(l)$

Unser Ziel ist: $Q_n(l) = 1$ für $n \geq 3$.

Aus §3.28 folgt jedenfalls, dass $Q_n(l)$ vom Bild von $S\Gamma_2(l)$ erzeugt wird.

**Lemma A** Sei $a, b \in \mathbb{Z}$, $\operatorname{ggT}(a,b) = 1$, $a \equiv 1 \pmod{\ell}$, $b \equiv 0 \pmod{\ell}$

Dann gibt es $c, d \in \mathbb{Z}$ mit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S\Gamma_2(\ell)$

Bew. $ax + by = 1 \Rightarrow x \equiv 1 \pmod{\ell}$. Setze

$$\left.\begin{array}{l} c = (a-1)y \\ d = by + x \end{array}\right\} \quad ad - bc = aby + ax - by(a-1)$$
$$= ax + by = 1$$

$d \equiv 1 \mod \ell$

$c \equiv 0 \mod \ell$ $\square$

**Lemma B** Ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a & b \\ \tilde{c} & \tilde{d} \end{pmatrix} \in \Gamma_2(\ell)$

so gilt $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ \tilde{c} & \tilde{d} \end{pmatrix} \mod E_u(\ell)$

Bew. $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ \tilde{c} & \tilde{d} \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ \underbrace{c\tilde{d} - d\tilde{c}}_{\in \ell\mathbb{Z}} & 1 \end{pmatrix}$ $\square$

**Definition** Das Mennicke-Symbol

$\begin{bmatrix} b \\ a \end{bmatrix}_\ell$ ist das Bild von $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_2(\ell)$

in $Q_u(\ell)$

Also wird $Q_u(\ell)$ von den Mennicke-Symbolen erzeugt.

**Satz** $Q_n(\ell)$ ist endlich erzeugt und abelsch, wenn $n \geq 3$.
Die Gruppe $SL_n(\mathbb{Z})$ wirkt durch Konjugation trivial auf $Q_n(\ell)$.

**Beweis** $SL_n(\mathbb{Z})$ ist endlich erzeugt nach §3.25 und $S\Gamma_n(\ell)$ hat endlichen Index, ist also nach §1.8 ebenfalls endlich erzeugt, damit auch $Q_n(\ell) = S\Gamma_n(\ell)/E_n(\ell)$.

Sei $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S\Gamma_2(\ell)$. Für $i,j \geq 3$ gilt $\tau_{ij}(t)g = g\tau_{ij}(t)$.

Weiter gilt $[\tau_{ij}(s), \tau_{jk}(t)] = \tau_{ik}(s \cdot t)$ für $i,j,k$ paarweise verschieden. Da $n \geq 3$ ist, wird $SL_n\mathbb{Z}$ von den Kommutatoren $[\tau_{ij}(1), \tau_{jk}(1)] = \tau_{ik}(1)$ erzeugt. Modulo $E_n(\ell)$ vertauscht diese Matrix mit $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$:

$$\underbrace{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{\tau_{13}(1)} \underbrace{\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{g} \underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{\tau_{13}(-1)} \underbrace{\begin{pmatrix} d & -b & 0 \\ -c & a & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{g^{-1}} =$$

$$\begin{pmatrix} 1 & 0 & 1-a \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \in E_n(\ell) \quad \text{denn } \ell \mid c$$

$$a = k\ell + 1 \Rightarrow \ell \mid 1-a$$

Andere Rechnung ähnlich. $\square$

## 30. Eigenschaft der Mennicke-Symbole

Für jedes $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = 1$, $a \equiv 1 \pmod{l}$, $b \equiv 0 \pmod{l}$

ist das Mennicke-Symbol $\begin{bmatrix} b \\ a \end{bmatrix}_l$ definiert als Bild

der Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S\Gamma_2(l)$ in $Q_n(l)$, vgl § 3.29.

<u>Lemma A</u> $\quad \begin{bmatrix} b \\ a \end{bmatrix}_l = \begin{bmatrix} b+lta \\ a \end{bmatrix}_l = \begin{bmatrix} b \\ a+tb \end{bmatrix}_l$, $\begin{bmatrix} 0 \\ 1 \end{bmatrix}_l = 1$,

$t \in \mathbb{Z}$ beliebig $\quad \begin{bmatrix} bb' \\ a \end{bmatrix}_l = \begin{bmatrix} b \\ a \end{bmatrix}_l \begin{bmatrix} b' \\ a \end{bmatrix}_l$ wenn alle drei Symbole existieren

<u>Beweis</u> $\quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & tl \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+tla \\ * & * \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} a+bt & b \\ * & * \end{pmatrix}$$

$\begin{pmatrix} 1 & \\ -t & 1 \end{pmatrix}$ wirkt trivial auf $Q_n(l)$!

$$\begin{pmatrix} a & b' & 0 \\ c' & d' & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} d' & 0 & -c' \\ 0 & 1 & 0 \\ -b' & 0 & a \end{pmatrix} \mod E_n(l)$$

Multiplikation mit $\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$ ergibt

$$\begin{pmatrix} ad' & b & -ac' \\ * & * & * \\ -b' & 0 & a \end{pmatrix} \equiv \begin{pmatrix} a & bb' & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix} \mod E_n(l) \qquad \square$$

**Lemma B** Wenn $b \equiv \pm 1 \pmod a$, so gilt

$$\begin{bmatrix} b \\ a \end{bmatrix}_l = 1.$$

**Denn**
$$\begin{bmatrix} b \\ a \end{bmatrix}_l \underset{l \mid b}{=} \begin{bmatrix} b-ab \\ a \end{bmatrix}_l = \begin{bmatrix} b(1-a) \\ a \end{bmatrix}_l \underset{b=ka\pm 1}{=} \begin{bmatrix} (ka\pm 1)(1-a) \\ a \end{bmatrix}$$

$$= \begin{bmatrix} \pm(1-a) + ka(1-a) \\ a \end{bmatrix}_l \underset{1-a \equiv 0 \,(\mathrm{mod}\, l)}{=} \begin{bmatrix} \pm(1-a) \\ a \end{bmatrix}_l = \begin{bmatrix} \mp(a-1) \\ 1+(a-1) \end{bmatrix}_l$$

$$= \begin{bmatrix} \mp(a-1) \\ 1 \end{bmatrix}_l \underset{l \mid a-1}{=} \begin{bmatrix} 0 \\ 1 \end{bmatrix}_l \qquad \square$$

Erinnerung: die Eulersche $\varphi$-Funktion ist $\varphi(m) = \#(\mathbb{Z}/m)^*$.

**Lemma C**
$$\begin{bmatrix} b \\ a \end{bmatrix}_l^{\varphi(a)} = 1$$

**Denn**: $ggT(a,b) = 1 \Rightarrow b$ Einheit in $\mathbb{Z}/a$

$\Rightarrow b^{\varphi(a)} \equiv 1 \pmod a$. Nach Lemma B folgt

$$\begin{bmatrix} b^{\varphi(a)} \\ a \end{bmatrix}_l = 1 = \begin{bmatrix} b \\ a \end{bmatrix}_l^{\varphi(a)} \qquad \square$$

Da $Q_n(l)$ endlich erzeugt abelsch ist, folgt schon:
$Q_n(l)$ ist <u>endlich</u>.

Dirichlets Primzahlsatz (vgl. Apostol, Analytic Number Theory) besagt: ist $ggT(a,b) = 1$, so gilt: $(a + b\mathbb{Z}) \cap \mathbb{P}$ ist unendlich.

Lemma D $\quad Q_n(\ell)$ ist 2-Gruppe.

Denn: wähle Primzahl $p \in a + b\mathbb{Z} \Rightarrow$ $a \equiv p \pmod b$. Es folgt $a = kb + p$, also

$$\left[\begin{matrix} b \\ a \end{matrix}\right]_e = \left[\begin{matrix} b \\ p \end{matrix}\right]_e \text{ und } \left[\begin{matrix} b \\ p \end{matrix}\right]_e^{p-1} = 1 \text{ nach Lemma C.}$$

Seien $q_1 < \ldots < q_s$ die ungeraden Primfaktoren von $p-1$.

Es gilt $p \nmid b$ (weil $p \equiv a \not\equiv 0 \pmod b$)

$p \nmid q_j$ (weil $p \equiv 1 \bmod q_j$)

Wähle Primzahlen $u \in -p + b q_1 \cdots q_s \mathbb{Z}$

$u \neq v \qquad v \in -1 + b q_1 \cdots q_s \mathbb{Z}$

$\Rightarrow uv \equiv p \pmod b$, $uv = p + k \cdot b$

$$\Rightarrow \left[\begin{matrix} b \\ p \end{matrix}\right]_e = \left[\begin{matrix} b \\ uv \end{matrix}\right]_e$$

Weiter $\varphi(uv) = (u-1)(v-1) \Rightarrow \left[\begin{matrix} b \\ p \end{matrix}\right]_e^{(u-1)(v-1)} = 1$

$(u-1)(v-1) \equiv (p+1) \cdot 2 \pmod{q_j}$. Da $q_j$ ungerade und $q_j \mid p-1 \Rightarrow q_j \nmid 2$ und

$q_j \nmid p+1 \Rightarrow q_j \nmid (p+1) \cdot 2$

Also ist $q_j$ kein Teiler der Ordnung von $\begin{bmatrix} b \\ a \end{bmatrix}_e$. Damit ist die Ordnung eine 2er-Potenz □

**Lemma E** Wenn $a \equiv 3 \pmod 4$, dann $\begin{bmatrix} b \\ a \end{bmatrix}_e = 1$

**Denn** $\mathrm{ggT}(a,b) = 1 = \mathrm{ggT}(a,4b)$. Wähle Primzahl $p \in a + 4b\mathbb{Z}$ mit $p \equiv 3 \pmod 4$

$\Rightarrow b^{\frac{p-1}{2}} = \pm 1 \mod (p)$ und $\frac{p-1}{2}$ ungerade.

$$\begin{bmatrix} b \\ a \end{bmatrix}_e = \begin{bmatrix} b \\ p \end{bmatrix}_e, \quad \begin{bmatrix} b \\ p \end{bmatrix}_e^{\frac{p-1}{2}} = \begin{bmatrix} \pm 1 \\ p \end{bmatrix}_e = 1 \text{ (Lemma B)}$$

Da die Ordnung von $\begin{bmatrix} b \\ a \end{bmatrix}_e$ nach Lemma D gerade ist und $\frac{p-1}{2}$ ungerade, folgt $\begin{bmatrix} b \\ a \end{bmatrix}_e = 1$ □

**Lemma F** Wenn $b \not\equiv 0 \pmod 4$, dann $\begin{bmatrix} b \\ a \end{bmatrix}_e = 1$.

**Denn** Wenn $a \equiv 3 \pmod 4$ fertig mit Lemma E.

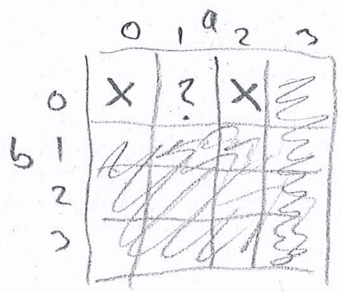
$b \equiv 1,3 \pmod 4$ $\quad a' = a + kb \equiv 3 \pmod 4$

für geeignetes $k$ $\Rightarrow \begin{bmatrix} b \\ a \end{bmatrix}_e = \begin{bmatrix} b \\ a' \end{bmatrix}_e = 1$ (Lemma E)

$b \equiv 2 \pmod 4$ $\Rightarrow a$ ungerade, $a \equiv 1 \pmod 4$

$\Rightarrow a' = a + b \equiv 3 \pmod 4$ $\quad \begin{bmatrix} b \\ a \end{bmatrix}_e = \begin{bmatrix} b \\ a' \end{bmatrix}_e = 1$ (Lemma E) □

Bleibt als letzter zu betrachten Fall $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$




**Lemma G** Wenn $a \equiv 1 \pmod 4$ $b \equiv 0 \pmod 4$, so

$$\begin{bmatrix} b \\ a \end{bmatrix}_e = 1.$$

Denn: Wähle $p \in -a + b\mathbb{Z} \Rightarrow \begin{bmatrix} b \\ a \end{bmatrix}_e = \begin{bmatrix} b \\ -p \end{bmatrix}_e$

$p \equiv 3 \pmod 4 \Rightarrow b^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ $\frac{p-1}{2}$ ungerad

$$\begin{bmatrix} b \\ a \end{bmatrix}_e = \begin{bmatrix} b \\ -p \end{bmatrix}_e, \quad \begin{bmatrix} \pm 1 \\ -p \end{bmatrix}_e = 1 \quad \text{wie eben}$$

$\uparrow$ Lemma B

$$\Rightarrow \begin{bmatrix} b \\ a \end{bmatrix}_e = 1 \qquad \square$$

Damit ist Rennichs Theorem bewiesen.

31. Bemerkung zu $SL_2\mathbb{Z}$.

In Gruppentheorie I hatten wir in §2.15 gezeigt, dass $PSL_2\mathbb{Z} \cong \mathbb{Z}/2 * \mathbb{Z}/3$ mit Erzeugern $\bar{a}, \bar{b}$, $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $ab = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$

$o(a) = 4$ $o(b) = 6$

Mit etwas Arbeit folgt $SL_2\mathbb{Z} \cong \mathbb{Z}/4 \underset{\mathbb{Z}/2}{*} \mathbb{Z}/6$.

Damit wirkt diese Gruppe auf einem Baum $T$ ohne Inversion, mit endlichen Stabilisatoren. Ist $H \leq SL_2\mathbb{Z}$ torsionsfrei, so wirkt also $H$ frei auf $T$. Nach Gruppentheorie I, §6.18 ist $H$ dann frei.

Freie Gruppen haben viele Untergruppen von endlichem Index. Die meisten dieser Untergruppen in $SL_2\mathbb{Z}$ enthalten keine der Kongruenzgruppen $\Gamma_2(\ell)$. Für $n = 2$ gilt Mennickes Theorem nicht.

32. Ausblick: zwei wichtige Sätze über lineare Gruppen, die wir nicht beweisen.

__Theorem__ (J. Tits – Die Tits-Alternative)

Sei $F$ Körper, $\Gamma \leq GL_n(F)$ endlich erzeugte Untergruppe. Dann gibt es entweder einen Monomorphismus $F_2 \to \Gamma$ ("$\Gamma$ enthält freie Untergruppe") oder $\Gamma$ ist virtuell auflösbar.

Beweis benutzt algebraische Geometrie / alg. Gruppen.

__Theorem__ (G. Margulis – Der Normalteilersatz)

Sei $n \geq 3$, sei $N \trianglelefteq SL_n(\mathbb{Z})$ unendlich.

Dann gilt $[SL_n(\mathbb{Z}) : N] < \infty$

Beweis benutzt harmonische Analysis auf Liegruppen.
Der Satz gilt allgemein für "irreduzible Gitter von höherem Rang."

Für $n = 2$ ist das falsch! $\Gamma(4) \leq SL_2\mathbb{Z}$ torsionsfrei $\Rightarrow$ frei $\Rightarrow$ $D\Gamma(4)$ hat unendlich Index in $\Gamma(4)$ $\Rightarrow$ $D\Gamma(4)$ hat unendlich Index in $SL_2\mathbb{Z}$ und ist normal.