UNIVERSITÄT
DES
SAARLANDES

Bestimmung des minimalen Kongruenzlevels für arithmetische Untergruppen der $\mathrm{SL}(n, \mathbb{Z})$ und $\mathrm{Sp}(n, \mathbb{Z})$

Bachelorarbeit

vorgelegt von

Simon Döring

Betreuerin:
Prof. Dr. Weitze-Schmithüsen

Erstkorrektorin:
Prof. Dr. Weitze-Schmithüsen

Zweitkorrektor:
Prof. Dr. Brandhorst

15.10.2021

Selbstständigkeitserklärung

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Saarbrücken, _____ _____

E R K L Ä R U N G

Ich versichere hiermit, dass die gedruckte und die elektronische Version der Arbeit inhaltlich übereinstimmen.

Saarbrücken, _____ _____

(Datum) (Unterschrift)

Ich räume der Universität das Recht ein, die elektronische Version (evt. unter Übertragung in ein anderes gängiges Dateiformat) in Datennetzen zu vervielfältigen und öffentlich wiederzugeben.

Saarbrücken, _____ _____

(Datum) (Unterschrift)

Danksagung

Ich möchte mich zunächst bei meinen Eltern bedanken, da sie mir bei meinem Lebensweg immer treu zur Seite gestanden haben. Außerdem möchte ich mich bei Prof. Weitze-Schmithüsen für ihre herausragende Betreuung bedanken. Des Weiteren möchte ich mich bei A. Detinko, D. L. Flannery und A. Hulpke bedanken, da ohne ihr Paper diese Arbeit nicht möglich gewesen wäre.

Schlussendlich will ich mich noch bei Sabrina Hinrichs für ihr sehr aufmerksames Korrekturlesen und ihre typographischen Vorschläge bedanken.

Inhaltsverzeichnis

Kapitel I.

Einleitung

1. Motivation

In dieser Arbeit beschäftigen wir uns mit Untergruppen H der $\mathrm{SL}(n,\mathbb{Z})$ oder $\mathrm{Sp}(n,\mathbb{Z})$ von endlichem Index. Häufig möchten wir den Index berechnen oder wir möchten wissen, ob $g \in H$ für Elemente g aus $\mathrm{SL}(n,\mathbb{Z})$ bzw. $\mathrm{Sp}(n,\mathbb{Z})$ gilt. Es kann auch sein, dass wir das *orbit-stabilizer problem* lösen wollen. Hierbei wollen wir für Vektoren v, w wissen, ob es ein $h \in H$ gibt mit $v = hw$, oder wir möchten $\mathrm{Stab}_H(u) = \{g \in H : gu = u\}$ bestimmen. Diese und viele andere Fragen könnten wir sehr viel leichter beantworten, wenn wir Matrizen über $\mathbb{Z}/m\mathbb{Z}$ betrachten würden. Um hiermit aber die ursprünglichen Probleme für die Gruppe H zu lösen, benötigen wir, dass der Kern der Projektion $\varphi_m\colon \mathrm{SL}(n,\mathbb{Z}) \to \mathrm{SL}(n,\mathbb{Z}/m\mathbb{Z})$ in H liegt, das heißt, dass die Gruppe H eine Kongruenzgruppe von Level m ist. Nach einem Ergebnis von Bass-Milnor-Serre gibt es für $n > 2$ stets ein solches m. Diese Eigenschaft ist als *congruence subgroup property* bekannt. Aus Effizienzgründen wollen wir das *minimale Kongruenzlevel* M, d. h. das kleinstmögliche M mit dieser Eigenschaft, finden, denn durch die Betrachtung eines möglichst kleinen M können wir H in eine möglichst kleine endliche Gruppe projizieren. Im Paper [7] von Detinko-Flannery-Hulpke wurde ein Algorithmus entwickelt, welcher dies berechnet, sofern H einige zusätzliche Bedingungen erfüllt. Die Betrachtung des Algorithmus wird das erste Hauptresultat dieser Arbeit sein.

Während der Betrachtung des Algorithmus werden wir einen anderen Algorithmus *nebenbei* entdecken, welcher ebenfalls von Detinko-Flannery-Hulpke stammt. Dieser kann die Zariski-Dichheit von Untergruppen der $\mathrm{SL}(n,\mathbb{Z})$ oder $\mathrm{Sp}(n,\mathbb{Z})$ überprüfen. Zwar gibt es bereits Algorithmen (siehe Abschnitt III.7), welche dies überprüfen können, allerdings wird unser Algorithmus, unter Berücksichtigung der Laufzeit und der Genauigkeit, einige Vorteile haben. Außerdem

werden wir sehen, dass wir durch das Anwenden unserer Algorithmen auf Zariski-dichte Untergruppen das Level der minimalen arithmetischen Obergruppe bestimmen können.

2. Grundbegriffe und einführende Beispiele

Wir wollen zunächst die Grundbegriffe dieser Arbeit einführen.

Definition I.2.1:

(i) Mit $\mathcal{G}(n, \mathbb{Z})$ bezeichnen wir eine Gruppe von $n \times n$-Matrizen über $\mathbb{Z}$.

(ii) Die spezielle lineare Gruppe $\mathrm{SL}(n, \mathbb{Z})$ über $\mathbb{Z}$ besteht aus allen Matrizen über $\mathbb{Z}$, welche die Determinante 1 haben.

(iii) Die symplektische Gruppe ist definiert als

$$\mathrm{Sp}(2s, \mathbb{Z}) := \{x \in \mathrm{GL}(2s, \mathbb{Z}) \,:\, xJx^\top = J\} \text{ mit } J = \begin{pmatrix} 0_s & I_s \\ -I_s & 0_s \end{pmatrix}.$$

Sie ist eine Untergruppe der $\mathrm{SL}(2s, \mathbb{Z})$ (siehe [14, II.9.19]).

Die symplektische Gruppe ist ein Analogon für orthogonale Matrizen. Orthogonale Matrizen erhalten bekanntlich Skalarprodukte. Elemente der symplektischen Gruppe erhalten die symplektische Form einer alternierenden Bilinearform, welche durch die Grammatrix J gegeben ist.

Definition I.2.2: Wir bezeichnen eine Untergruppe H mit $H \leq \mathcal{G}(n, \mathbb{Z})$. Wir bezeichnen diese Untergruppe als *arithmetisch*, falls $[\mathcal{G}(n, \mathbb{Z}) : H] < \infty$ gilt.

Definition I.2.3: Wir wollen die folgende Notation einführen: $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

Arithmetisch kann an sich allgemeiner definiert werden, für unseren Kontext genügt jedoch Definition I.2.2. Wir können uns nun viele verschiedene Fragen über die Untergruppe H stellen, zum Beispiel, was der Index von $[\mathcal{G}(n, \mathbb{Z}) : H]$ ist oder ob ein Element in unserer Untergruppe liegt. Hierbei haben wir das Problem, dass Matrixgruppen über $\mathbb{Z}$ meistens unendlich viele Elemente haben. Dies macht z. B. das Überprüfen, ob $g \in H$ gilt, viel schwieriger, weshalb wir diese Gruppen auf endliche Gruppen projizieren wollen.

Definition I.2.4: Wir bezeichnen mit $\varphi_m : \mathcal{G}(n, \mathbb{Z}) \to \mathcal{G}(n, \mathbb{Z}_m)$ die elementweise Projektion nach $\mathbb{Z}_m$. Wir bezeichnen mit $\Gamma_{n,m}$ den Kern von φ_m. Es gilt $\Gamma_{n,1} = \mathcal{G}(n, \mathbb{Z})$.

Der Kern $\Gamma_{n,m}$ heißt *Kongruenzuntergruppe* zum Level m. Wir bezeichnen das kleinste m mit $\Gamma_{n,m} \leq H$ als M und nennen es *das Level von* H.

Es sei angemerkt, dass wir voraussetzen wollen, dass $\mathcal{G}(n,\mathbb{Z}) \leq \mathrm{GL}(n,\mathbb{Z})$ gilt und das Projizieren φ_m ein wohldefinierter Gruppenhomomorphismus ist. Wir können natürlich nicht jede Untergruppe auf ein beliebiges $\mathbb{Z}_m$ schicken und hoffen, dass sämtliche Eigenschaften der Untergruppe erhalten bleiben. Falls aber der Kern von φ_m in unserer Untergruppe H liegt, können wir viele Eigenschaften mit Hilfe der Projektion herausfinden.

Beispiel I.2.5: Sei $\Gamma_{n,m} \leq H \leq \mathcal{G}(n,\mathbb{Z})$ arithmetisch, dann gilt

$$[\mathcal{G}(n,\mathbb{Z}) : H] = [\mathcal{G}(n,\mathbb{Z})/\Gamma_{n,m} : H/\Gamma_{n,m}] = [\mathcal{G}(n,\mathbb{Z}_m) : \varphi_m(H)]$$

und $g \in H \Leftrightarrow \varphi_m(g) \in \varphi_m(H)$.

Beweis: Die erste Gleichung gilt, da ein Normalteiler das System von Nebenklassen respektiert (siehe [14, I.3.10 b)]). Die zweite Gleichung folgt direkt aus dem Homomorphiesatz. Bei der Äquivalenz ist die Hinrichtung offensichtlich. Die Rückrichtung zeigen wir per Kontraposition. Angenommen es gilt $g \notin H$, dann ist H eine echte Untergruppe von $\langle g, H\rangle$. Daher gilt $[\mathcal{G}(n,\mathbb{Z}) : H] > [\mathcal{G}(n,\mathbb{Z}) : \langle g, H\rangle]$. Aus der obigen Gleichung folgt nun $[\mathcal{G}(n,\mathbb{Z}_m) : \varphi_m(H)] > [\mathcal{G}(n,\mathbb{Z}_m) : \varphi_m(\langle g, H\rangle)]$, weshalb $\varphi_m(g)$ kein Element von $\varphi_m(H)$ sein kann. □

Beispiel I.2.6: Seien $H_1, H_2 \leq \mathcal{G}(n,\mathbb{Z})$ zwei Untergruppen vom Level M_1 beziehungsweise M_2. Sei $\ell = \mathrm{kgV}(M_1, M_2)$, dann ist $H_1 \cap H_2$ das Urbild von $\varphi_\ell : \Sigma(n,\mathbb{Z}) \to \Sigma(n,\mathbb{Z}_\ell)$ angewendet auf $\varphi_\ell(H_1) \cap \varphi_\ell(H_2)$.

Beweis: Nach Lemma II.1.4 (ii) gilt $\Gamma_{n,\ell} = \Gamma_{n,M_1} \cap \Gamma_{n,M_2}$ und daraus folgt $\Gamma_{n,\ell} \leq H_1 \cap H_2$. Es gilt außerdem

$$\varphi_\ell^{-1}(\varphi_\ell(H_1) \cap \varphi_\ell(H_2)) \supseteq \varphi_\ell^{-1}(\varphi_\ell(H_1 \cap H_2)) \supseteq H_1 \cap H_2.$$

Sei $x \in \varphi_\ell^{-1}(\varphi_\ell(H_1) \cap \varphi_\ell(H_2))$, dann gibt es $a \in H_1$ und $b \in H_2$, sodass $\varphi_\ell(x) = \varphi_\ell(a) = \varphi_\ell(b)$ ist. Es gilt daher $xa^{-1} \in \Gamma_{n,\ell} \leq H_1$; daraus folgt $x \in H_1$. Analog folgt $x \in H_2$. Es gilt also $\varphi_\ell^{-1}(\varphi_\ell(H_1) \cap \varphi_\ell(H_2)) \subseteq H_1 \cap H_2$. □

Bemerkung I.2.7: Weitere Beispiele sind in [8, Kapitel 3] zu finden. Hierbei findet man das *orbit-stabilizer problem* in [8, Kapitel 4].

Unser Ziel ist es, einen solchen Kern zu finden. Allerdings gibt es nicht für alle arithmetischen Untergruppen immer eine Kongruenzuntergruppe, weshalb wir im Folgenden ausschließlich Gruppen betrachten werden, welche die folgende Eigenschaft haben.

Definition I.2.8: Die Gruppe $\mathcal{G}(n,\mathbb{Z})$ hat die *congruence subgroup property*, falls für jede arithmetische Untergruppe H ein m exisiert mit $\Gamma_{n,m} \leq H$.

Ein wichtiges Resultat von Bass-Milnor-Serre sagt aus, dass die Gruppen $\mathrm{SL}(n,\mathbb{Z})$ und $\mathrm{Sp}(n,\mathbb{Z})$ für $n \geq 3$ diese Eigenschaft haben.

Beispiel I.2.9 (aus [1, Theorem 14.1]): Die Gruppen $\mathrm{SL}(n,\mathbb{Z})$ für $n \geq 3$ und $\mathrm{Sp}(2s,\mathbb{Z})$ für $s \geq 2$ haben die *congruence subgroup property*.

Wir wollen uns im Folgenden nur noch mit $\mathrm{SL}(n,\mathbb{Z})$ und $\mathrm{Sp}(n,\mathbb{Z})$ beschäftigen. Es sei kurz angemerkt, dass $\varphi_m\colon \mathrm{SL}(n,\mathbb{Z}) \to \mathrm{SL}(n,\mathbb{Z}_m)$ wohldefiniert ist. Es gilt nämlich $\det(A) \equiv \det(\varphi_m(A)) \mod m$. Daher werden Matrizen mit Determinante 1 auf Matrizen mit Determinante 1 geschickt.

Da $\varphi_m(AB) = \varphi_m(A)\,\varphi_m(B)$ gilt, folgt unmittelbar, dass φ_m für $\mathrm{Sp}(n,\mathbb{Z})$ wohldefiniert ist.

Definition I.2.10: Wir führen die folgende Notation ein:

$$\begin{aligned}
\Sigma(n,\mathbb{Z}) &:= \mathrm{SL}(n,\mathbb{Z}) \text{ oder } \mathrm{Sp}(n,\mathbb{Z}) \\
\mathrm{P}\Sigma(n,\mathbb{Z}) &:= \mathrm{PSL}(n,\mathbb{Z}) \text{ oder } \mathrm{PSp}(n,\mathbb{Z}) \\
\Sigma(n,p) &:= \mathrm{SL}(n,\mathbb{F}_p) \text{ oder } \mathrm{Sp}(n,\mathbb{F}_p) \\
\mathrm{P}\Sigma(n,p) &:= \mathrm{PSL}(n,\mathbb{F}_p) \text{ oder } \mathrm{PSp}(n,\mathbb{F}_p) \\
\pi(M) &:= \{\, p \,:\, p \text{ ist Primteiler von } M\} \\
\Pi(H) &:= \{\, p \,:\, p \text{ ist prim und } \varphi_p(H) \neq \Sigma(n,p)\}
\end{aligned}$$

Wir verwenden also $\Sigma(n,\mathbb{Z})$ immer dann, wenn wir sowohl $\mathrm{SL}(n,\mathbb{Z})$ als auch $\mathrm{Sp}(n,\mathbb{Z})$ betrachten wollen. Die PSL und PSp entsteht, indem man das Zentrum von SL bzw. Sp herausteilt, sprich $\mathrm{PSL}(n,\mathbb{Z}) := \mathrm{SL}(n,\mathbb{Z})/Z_{\mathrm{SL}(n,\mathbb{Z})}$. Wir werden meistens $\mathbb{F}_p$ mit $\mathbb{Z}_p$ identifizieren.

3. Aufbau der Arbeit

Sei $H \leq \Sigma(n, \mathbb{Z})$ arithmetisch. Unser Ziel wird es zunächst sein, das Level M von H zu bestimmen.

In Abschnitt III.1 werden wir den Algorithmus `LevelMaxPCS` betrachten. Dieser kann M aus der Menge der Primteiler $\pi(M)$ berechnen. Um wiederum die Primteiler zu finden, werden wir die Menge $\Pi(H)$ betrachten. Diese besteht aus den Primzahlen p, sodass das Bild von H unter φ_p nicht alles ist. Das Hauptresultat des Kapitels II ist, dass $\Pi(H) = \pi(M)$ fast immer gilt.

Wir werden bereits in Abschnitt II.1 zeigen, dass $\Pi(H) \subseteq \pi(M)$ immer gilt. Im Abschnitt II.4 werden wir dann sehen, dass die andere Inklusion fast immer gilt. Es wird sich herausstellen, dass 2 die einzige kritische Primzahl ist. Allerdings werden wir in Abschnitt II.5 einen Test entwickeln, um $2 \in \pi(M)$ zu überprüfen. Dadurch sind wir in der Lage, die Menge $\pi(M)$ mit Hilfe von $\Pi(H)$ zu bestimmen.

Der Vorteil der Menge $\Pi(H)$ ist, dass wir in Abschnitt III.3 den Algorithmus `PrimesOverestimation` entwickeln werden, welcher eine Obermenge $\Pi_1(H) \supseteq \Pi(H)$ bestimmen kann. Wir werden anschließend in Abschnitt III.5 diesen Algorithmus leicht modifizieren, um den Algorithmus `isDense` zu entwickeln. Dieser kann die Zariski-Dichtheit von H überprüfen; hierbei muss H nicht zwingend arithmetisch sein. Es sei aber angemerkt, dass man für beide Algorithmen eine Transvektion $t \in H$ (siehe Defintion III.3.2 (i)) benötigt. Außerdem muss n ungerade oder $\Sigma(n, \mathbb{Z}) = \mathrm{Sp}(n, \mathbb{Z})$ sein.

Anschließend werden wir in Abschnitt III.6 die Voraussetzung, dass H arithmetisch ist, fallen lassen und uns stattdessen mit Zariski-dichten Untergruppen beschäftigen. In diesem Fall kann man die Algorithmen `PrimesOverestimation` und `LevelMaxPCS` verwenden, um das Level der minimalen arithmetischen Obergruppe zu bestimmen.

Im Abschnitt III.7 werden wir dann eine Laufzeitschranke des Algorithmus `isDense` bestimmen und diese mit anderen Algorithmen vergleichen, welche ebenfalls die Zariski-Dichtheit überprüfen.

Schlussendlich werden wir in Kapitel IV das Level und den Index von einigen Beispielen berechnen. Hierbei werden wir uns u. a. mit hypergeometrischen Gruppen beschäftigen. Wir werden im Abschnitt IV.3 die Laufzeit der verschiedenen Dichtheitstests empirisch vergleichen.

Große Teile dieser Arbeit basieren auf einem Paper von Detinko-Flannery-Hulpke (siehe [7]).

Kapitel II.

Der Zusammenhang zwischen $\pi(M)$ und $\Pi(H)$

Ziel dieses Kapitels ist es, zu zeigen, wie wir die Menge $\pi(M)$ mit Hilfe der Menge $\Pi(H)$ bestimmen können. Dies wird wichtig sein, da wir die Menge $\pi(M)$ im Kapitel III benötigen werden, um M zu bestimmen.

1. Eigenschaften von Kernen der Projektionsfunktionen

Wir wollen zunächst einige Informationen über den Kern $\Gamma_{n,m}$ sammeln, welche im Verlauf dieser Arbeit nützlich sein werden. Hierfür wollen wir uns damit beschäftigen, wie man den Kern bestimmen kann. Wir betrachten die folgenden Untergruppen.

Definition II.1.1: Sei $t_{i,j}(m) = I_n + mE_{i,j}$. Wir definieren für $\mathrm{SL}(n,\mathbb{Z})$ die Untergruppe

$$\mathcal{E}_{n,m} := \langle t_{i,j}(m) \,:\, 1 \leq i \neq j \leq n \rangle \leq \Gamma_{n,m}$$

und für $\mathrm{Sp}(2s,\mathbb{Z})$ mit $n := 2s$ definieren wir

$$\begin{aligned}\mathcal{E}_{n,m} := \langle \{ & t_{i,j+s}(m)\, t_{j,i+s}(m),\ t_{i+s,j}(m)\, t_{j+s,i}(m), \\ & t_{i,i+s}(m),\ t_{i+s,i}(m) : 1 \leq i < j \leq s \} \rangle \leq \Gamma_{n,m}\end{aligned}$$

Im Fall $\mathrm{SL}(n,\mathbb{Z})$ ist die Form sehr simpel. Wir haben die Einheitsmatrix mit einem zusätzlichen m außerhalb der Hauptdiagonalen. Wenn wir nun φ_m auf eine solche Matrix anwenden, so verschwindet dieser Eintrag und wir erhalten die Einheitsmatrix.

$$t_{1,3+2}(m)\,t_{2,3+1}(m) = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & m & 0 \\ 0 & 1 & 0 & m & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$(t_{1,3+2}(m)\,t_{2,3+1}(m))^k = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & km & 0 \\ 0 & 1 & 0 & km & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) = t_{1,3+2}(km)\,t_{2,3+1}(km)$$

Abbildung II.1.: Einige Erzeuger von $\mathcal{E}_{6,m}$ als Beispiel.

Im Falle von $\mathrm{Sp}(n,\mathbb{Z})$ befinden sich entweder ein m auf der Hauptdiagonalen des *oberen* oder *unteren* Blocks oder zwei m, welche entlang dieser Hauptdiagonalen gespiegelt sind (siehe Abbildung II.1).

Der Grund, warum wir die Gruppen $\mathcal{E}_{n,m}$ betrachten, ist, dass der *normale Abschluss* von $\mathcal{E}_{n,m}$ der Kern $\Gamma_{n,m}$ ist.

Definition II.1.2: Sei G eine Gruppe mit Untergruppe H, dann bezeichnen wir mit H^G den *normalen Abschluss* von H in G, Dies ist die kleinste Untergruppe N in G mit der Eigenschaft $H \leq N \trianglelefteq G$. Es gilt also

$$H^G := \bigcap_{H \leq S \trianglelefteq G} S$$

Indem wir also den Kern $\Gamma_{n,m}$ mit Hilfe von $\mathcal{E}_{n,m}$ beschreiben, können wir einige hilfreiche Eigenschaften über $\Gamma_{n,m}$ beweisen.

Theorem II.1.3 (aus [17, Theorem], [1, Prop. 13.2 a)], [11, Theor. 4.3.9]): *Es gilt* $\mathcal{E}_{n,m}^{\Sigma(n,\mathbb{Z})} = \Gamma_{n,m}$. *Außerdem gilt* $\mathcal{E}_{n,1} = \Sigma(n,\mathbb{Z})$.

Lemma II.1.4 (aus [8, Lemma 1.16]):

(i) *Seien* $m_1, m_2 \in \mathbb{N}$ *und* $m = \mathrm{ggt}(m_1, m_2)$, *dann gilt*

$$\Gamma_{n,m_1}\Gamma_{n,m_2} = \Gamma_{n,m}.$$

(ii) *Seien* $m_1, m_2 \in \mathbb{N}$ *und* $\ell = \mathrm{kgV}(m_1, m_2)$*, dann gilt*

$$\Gamma_{n,m_1} \cap \Gamma_{n,m_2} = \Gamma_{n,\ell}.$$

Beweis: (i) Offensichtlich gilt $\Gamma_{n,m_1}\Gamma_{n,m_2} \subseteq \Gamma_{n,m}$, denn m_1 und m_2 sind Vielfache von m und daher gilt $m_1 \equiv m_2 \equiv 0 \mod m$. Deshalb sind Γ_{n,m_1} und Γ_{n,m_2} Untergruppen von $\Gamma_{n,m}$. Für die andere Richtung können wir Theorem II.1.3 verwenden. Wir müssen also $\mathcal{E}_{n,m}^{\Sigma(n,\mathbb{Z})} \leq \mathcal{E}_{n,m_1}^{\Sigma(n,\mathbb{Z})}\mathcal{E}_{n,m_2}^{\Sigma(n,\mathbb{Z})}$ zeigen. Da das Produkt von normalen Untergruppen wieder normal ist, müssen wir lediglich nachrechnen, dass wir jeden Erzeuger in $\mathcal{E}_{n,m}$ in $\mathcal{E}_{n,m_1}\mathcal{E}_{n,m_2}$ darstellen können. Wir machen dies exemplarisch für Elemente der Form $t_{i,j}(m)$, es sei aber angemerkt, dass der Beweis für sämtliche Erzeuger analog funktioniert. Nach dem Lemma von Bézout gibt es ganze Zahlen a und b mit $am_1 + bm_2 = m$. Es gilt

$$t_{i,j}(m_1)^a\, t_{i,j}(m_2)^b = t_{i,j}(am_1 + bm_2) = t_{i,j}(m).$$

Also gilt $t_{i,j}(m) \in \mathcal{E}_{n,m_1}\mathcal{E}_{n,m_2}$.

(ii) Offensichtlich gilt $\Gamma_{n,\ell} \leq \Gamma_{n,m_1} \cap \Gamma_{n,m_2}$. Sei andererseits $x \in \Gamma_{n,m_1} \cap \Gamma_{n,m_2}$. Da $\varphi_{m_1}(x) = I_n = \varphi_{m_2}(x)$ ist, gilt $x = I_n + m_1y_1 = I_n + m_2y_2$ mit $y_1, y_2 \in \mathbb{Z}^{n\times n}$. Es gilt also $x_{i,i} \equiv 1 \mod m_1$ und $x_{i,i} \equiv 1 \mod m_2$, weshalb nach dem chinesischen Restsatz $x_{i,i} \equiv 1 \mod \ell$ gilt. Außerdem gilt $x_{i,j} \equiv 0 \mod m_1$ und $x_{i,j} \equiv 0 \mod m_2$ für $i \neq j$, weshalb nach dem chinesischen Restsatz $x_{i,j} \equiv 0 \mod \ell$ gilt. □

Lemma II.1.5: *Für jedes arithmetische* $H \leq \Sigma(n, \mathbb{Z})$ *gibt es bzgl. Inklusion ein eindeutiges maximales* $\Gamma_{n,M} \leq H$*. Es gilt außerdem* $M \mid k$ *für alle* $\Gamma_{n,k} \leq H$*. Insbesondere gilt* $\Gamma_{n,k} \leq \Gamma_{n,M}$ *für alle* $k \mid M$*, was den Begriff* maximal *motiviert.*

Beweis: Nach Beispiel I.2.9 gibt es mindestens ein $\Gamma_{n,m} \leq H$. Wir bezeichnen mit M das kleinste m mit $\Gamma_{n,m} \leq H$. Sei nun $\Gamma_{n,k} \leq H$, dann gilt die Gleichheit $\Gamma_{n,\mathrm{ggt}(M,k)} = \Gamma_{n,k}\Gamma_{n,M} \leq H$. Aus der Minimalität von M folgt $\mathrm{ggt}(k, M) = M$, weshalb $M \mid k$ sein muss, und schließlich $\Gamma_{n,k} \leq \Gamma_{n,M}$. □

Wir können an dieser Stelle bereits $\Pi(H) \subseteq \pi(M)$ zeigen.

Theorem II.1.6 (aus [7, Lemma 2.1]): *Sei* $H \leq \Sigma(n, \mathbb{Z})$ *arithmetisch und es gelte* $\Gamma_{n,M} \leq H$*, dann gilt* $\Pi(H) \subseteq \pi(M)$*.*

Beweis: Sei p eine Primzahl und $p \notin \pi(M)$, dann gilt

$$\varphi_p(H) = \varphi_p(\Gamma_{n,p}H) = \varphi_p(\Gamma_{n,p}\Gamma_{n,M}H) = \varphi_p(\Gamma_{n,1}H) = \Sigma(n, p).$$

Also gilt $p \notin \Pi(H)$ nach Definition. □

Wir werden im Folgenden nicht nur von $\mathbb{Z}$ nach $\mathbb{Z}_m$ projizieren, sondern auch von $\mathbb{Z}_m$ nach $\mathbb{Z}_r$. Dies werden wir in Abschnitt II.2 benötigen.

Definition II.1.7: Sei $r \mid m$. Wir bezeichnen mit $\varphi_{m,r}\colon \Sigma(n,\mathbb{Z}_m) \to \Sigma(n,\mathbb{Z}_r)$ die kanonische Projektion, wobei wir auf $\Sigma(n,\mathbb{Z}_m)$ die Funktion elementweise ausführen. Wir bezeichnen den Kern als $K_{m,r}$.

Bemerkung II.1.8: Nach [8, Proposition 1.2] und [18, Theorem 1] sind alle $\varphi_m\colon \Sigma(n,\mathbb{Z}) \to \Sigma(n,\mathbb{Z}_m)$ surjektiv. Hieraus folgt, dass $\varphi_{m,r}$ ebenfalls surjektiv ist, denn es gilt $\varphi_{m,r}(\Sigma(n,\mathbb{Z}_m)) = \varphi_r(\Sigma(n,\mathbb{Z}))$.

Genauso wie bei φ_m können wir uns auch bei $\varphi_{m,r}$ fragen, wie der Kern aussieht. Hierbei wird der Spezialfall φ_{p^a,p^b} in Abschnitt II.2 besonders wichtig werden, weshalb wir die Struktur des Kerns genauer analysieren wollen.

Lemma II.1.9: *Sei p eine Primzahl, $a > b \geq 1$. Dann ist K_{p^a,p^b} eine p-Gruppe.*

Beweis: Sei $x \in K_{p^a,p^b}$, dann gilt $x = (I_n + p^b y)$, da $\varphi_{p^a,p^b}(x) = I_n$ gilt. Nach dem binomischen Lehrsatz gilt für alle c

$$x^{p^c} = (I_n + p^b y)^{p^c} = \sum_{k=0}^{p^c} \binom{p^c}{k} I_n (p^b)^k y^k = \sum_{k=0}^{a} \binom{p^c}{k} I_n (p^b)^k y^k,$$

wobei der letzte Schritt aus $(p^b)^k \equiv p^{bk} \equiv 0 \bmod p^a$ für alle $k \geq a$ folgt. Wenn wir also ein c finden, sodass $\binom{p^c}{k} \equiv 0 \bmod p^a$ für alle $1 \leq k \leq a$ gilt, dann folgt nach der obigen Rechnung $x^{p^c} = I_n$, weshalb K_{p^a,p^b} eine p-Gruppe ist.

Jedes $1 \leq k \leq a$ zerlegen wir in $k = p^{d_k} q_k$ mit $p \nmid q_k$. Sei $d = \max(d_1, \ldots, d_k)$, dann gilt

$$\binom{p^{a+d}}{k} = \frac{p^{a+d}}{k}\binom{p^{a+d}-1}{k-1} = \frac{p^{a+d-d_k}}{q_k}\binom{p^{a+d}-1}{k-1}.$$

Da aber $\binom{p^{a+d}}{k}$ eine natürliche Zahl ist, muss $\binom{p^{a+d}-1}{k-1}$ ein Vielfaches von q_k sein, weshalb $\binom{p^{a+d}}{k}$ ein Vielfaches von p^{a+d-d_k} ist. Da $d \geq d_k$ gilt, folgt

$$\binom{p^{a+d}}{k} \equiv 0 \mod p^a \text{ für alle } 1 \leq k \leq a.$$

□

Lemma II.1.10 (aus [7, Lemma 2.6]): *Sei $a > b \geq 1$ und $2b \geq a$.*

(i) *Der Kern K_{p^a,p^b} von $\varphi_{p^a,p^b} : \mathrm{SL}(n, \mathbb{Z}_{p^a}) \to \mathrm{SL}(n, \mathbb{Z}_{p^b})$ hat die Form*

$$K_{p^a,p^b} = \{I_n + p^b x \ : \ x \in \mathbb{Z}_{p^{a-b}}^{n\times n},\ \mathrm{tr}(x) \equiv 0 \mod p^{a-b}\}$$

und ist isomorph zu einer Untergruppe von $(\mathbb{Z}_{p^{a-b}}^{n\times n}, +)$.[1]

(ii) *Sei $n = 2s$. Der Kern K_{p^a,p^b} von $\varphi_{p^a,p^b}\colon \mathrm{Sp}(n, \mathbb{Z}_{p^a}) \to \mathrm{Sp}(n, \mathbb{Z}_{p^b})$ hat die Form*

$$K_{p^a,p^b} = \{I_n + p^b x \ : \ x = \begin{pmatrix} A & B \\ C & -A^\top \end{pmatrix} \text{ mit } A, B, C \in \mathbb{Z}_{p^{a-b}}^{s\times s}, \\ B = B^\top,\ C = C^\top\}$$

und ist isomorph zu einer Untergruppe von $(\mathbb{Z}_{p^{a-b}}^{n\times n}, +)$.

(iii) *Sei $c = (I_n + p^b x) \in K_{p^a,p^b}$, dann gilt $c^{-1} = I_n - p^b x$.*

Beweis: (i) Wir zeigen per Induktion, dass $\det(I_n + p^b x) \equiv 1 + p^b \mathrm{tr}(x) \mod p^a$ für $I_n, x \in \mathbb{Z}_{p^{a-b}}^{n\times n}$ gilt.

Induktionsanfang $n = 1$: Es gilt $\det(I_1 + p^b x) = 1 + p^b x_{1,1} = 1 + p^b \,\mathrm{tr}(x)$.

Induktionsvoraussetzung: Es gelte $\det(I_n + p^b x) = 1 + p^b \mathrm{tr}(x)$.

Induktionsschritt $n \to n+1$: Wir definieren $B := I_{n+1} + p^b x$ und machen eine Laplace-Entwicklung nach der ersten Zeile. Es gilt

$$\begin{aligned} \det(B) &= (1 + p^b x_{1,1}) \det(B_{1,1}) + \sum_{j=2}^{n+1} (-1)^{j+1} p^b x_{1,j} \det(B_{1,j}) \\ &= (1 + p^b x_{1,1}) \det(B_{1,1}) + 0 \\ &\overset{\text{I.V.}}{=} (1 + p^b x_{1,1})(1 + p^b \sum_{j=2}^{n+1} x_{j,j}) = 1 + p^b \,\mathrm{tr}(x). \end{aligned}$$

Hierbei gilt die zweite Gleichheit, da jede Streichungsmatrix $B_{i,j}$ für $i \neq j$ mindestens eine Zeile hat, wo alle Elemente die Form $p^b x_{s,t}$ haben. Wir können also p^b raus ziehen und erhalten zusammen mit den anderen p^b den Wert $p^b p^b \equiv p^{2b} \equiv 0 \mod p^a$, wobei wir ausnutzen, dass $2b \geq a$ gilt. Diesen Umstand haben wir auch bei der letzten Gleichung ausgenutzt.

[1] Rein formal gilt eigentlich $x \in \{0, 1, \ldots, p^{a-b} - 1\}^{n\times n}$ für $\{0, 1, \ldots, p^{a-b} - 1\} \subseteq Z_{p^a}$. Wir werden aber auf diesen Unterschied im Folgenden nicht weiter eingehen.

Wir bezeichnen mit $A_{p,a,b}$ die alternative Darstellung des Kerns. Wir wollen also $A_{p,a,b} = K_{p^a,p^b}$ zeigen. Es gilt offensichtlich $A_{p,a,b} \leq \mathrm{SL}(n, \mathbb{Z}_{p^a})$ und $A_{p,a,b} \leq K_{p^a,p^b}$, da alle Einträge außerhalb der Diagonalen ein Vielfaches von p^b sind.

Sei nun $B \in K_{p^a,p^b}$, dann erhalten wir $B = I_n + c$. Es muss nun $\varphi_{p^a,p^b}(c) = 0$ sein, da sonst B nicht im Kern liegen würde. Daraus folgt aber $c = p^b x$, da jeder Eintrag ein Vielfaches von p^b sein muss. Gleichzeitig können wir annehmen, dass $x_{i,j} < p^{a-b}$ gilt, da wir in $\mathbb{Z}_{p^a}$ sind. Aus $\det(1_n + p^b x) = 1 + p^b \operatorname{tr}(x)$ folgt, dass $\operatorname{tr}(x) \equiv 0 \mod p^{a-b}$ sein muss.

Für die Isomorphie betrachten wir die folgende Abbildung

$$\psi \colon K_{p^a,p^b} \to \mathbb{Z}_{p^{a-b}}^{n\times n};\ (I_n + p^b x) \mapsto x.$$

Wir müssen nachrechnen, dass aus der Matrixmultiplikation eine Addition wird. Es gilt

$$(I_n + p^b x)(I_n + p^b y) = I_n + p^b(x+y) + p^{2b}xy = I_n + p^b(x+y)$$

Also können wir aus der Multiplikation eine Addition machen.

(ii) Sei $Y \in K_{p^a,p^b}$ beliebig, dann gibt es aus den gleichen Gründen wie in (i) ein x mit $0 \leq x_{i,j} < p^{a-b}$ und $Y = (I_n + p^b x)$. Wir betrachten nun

$$x = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ mit } A, B, C, D \in \mathbb{Z}_{p^a}^{s\times s}$$

und folgern

$$\begin{aligned}
& & Y J Y^\top &= J \\
\Leftrightarrow & & J + p^b(xJ + Jx^\top) + p^{2b} x J x^\top &= J \\
\Leftrightarrow & & p^b\left(xJ + Jx^\top\right) &= 0 \\
\Leftrightarrow & & -p^b J x^\top J^{-1} &= p^b x \\
\Leftrightarrow & & p^b \begin{pmatrix} -D^\top & B^\top \\ C^\top & -A^\top \end{pmatrix} &= p^b \begin{pmatrix} A & B \\ C & D \end{pmatrix}.
\end{aligned}$$

Wir zeigen, dass aus $p^b B = p^b B^\top$ bereits $B = B^\top$ folgt. Hierfür zeigen wir, dass für $p^b s \equiv p^b t \mod p^a$ für $0 \leq s, t < p^{a-b}$ bereits $s \equiv t \mod p^{a-b}$ gilt. Es gilt

$$p^b x \equiv p^b y \mod p^a \ \Leftrightarrow\ p^b(x-y) \equiv 0 \mod p^a \ \Rightarrow\ (x-y) \equiv 0 \mod p^{a-b}.$$

Hieraus folgt $s = t$, da $0 \leq s,\, t < p^{a-b}$ gilt.

Es folgt nun $B = B^\top$. Analog geht man vor, um $C = C^\top$ zu zeigen. Nach der obigen Rechnung gilt $p^b D = -p^b A^\top$, woraus

$$Y = \left(I_n + p^b \begin{pmatrix} A & B \\ C & D \end{pmatrix}\right) = \left(I_n + p^b \begin{pmatrix} A & B \\ C & -A^\top \end{pmatrix}\right)$$

folgt. Wir sehen also, dass ein Element genau dann in K_{p^a,p^b} liegt, wenn es die beschriebene Form hat. Man bedenke außerdem, dass alle Element in der alternativen Darstellung des Kerns die Determinante 1 haben und daher invertierbar sind. Dies sieht man durch die Induktion in (i). Ebenso ist der Isomorphismus analog zur (i).

(iii) Folgt direkt aus dem Isomorphismus in (i) bzw. (ii). □

Wir wollen an dieser Stelle noch zwei kleine Hilfslemmata einführen.

Lemma II.1.11: *Seien A, B, C Untergruppen von G und C ein Normalteiler mit $AC = A$, dann gilt $(A \cap B)C = AC \cap BC = A \cap BC$.*

Beweis: Sei $x \in AC \cap BC$. Dann gilt $x = a = bc$ mit $a \in A$, $b \in B$ und $c \in C$, weshalb $b = ac^{-1} \in AC \cap B$ gilt, also $bc \in (A \cap B)C$. Sei umgekehrt $x \in (A \cap B)C$, dann gilt $x = dc$ mit $d \in A \cap B$. Es gilt $dc \in AC$ und $dc \in BC$.□

Lemma II.1.12: *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus und* $\mathrm{Kern}(\varphi) = N \leq L$, $K \leq G$ *zwei Untergruppen mit $\varphi(L) \subseteq \varphi(K)$, dann gilt $L \subseteq K$. Insbesondere gilt die Aussage, wenn wir L oder K durch eine Gruppe AN substituieren.*

Beweis: Nach dem vierten Isomorphiesatz (siehe [14, I.3.10 a)]) müssen wir lediglich $L/N \subseteq K/N$ zeigen. Wir verwenden den natürlichen Isomorphismus $\overline{\varphi}\colon G/N \to \varphi(G)$. Sei $\overline{x} \in L/N$, dann gibt es einen Repräsentanten $x \in L$ mit $\overline{\varphi}(\overline{x}) = \varphi(x) \in \varphi(K)$. Es gibt also ein $y \in K$ mit Nebenklasse $\overline{y} \in K/N$ und $\overline{\varphi}(\overline{x}) = \varphi(x) = \varphi(y) = \overline{\varphi}(\overline{y})$. Da $\overline{\varphi}$ ein Isomorphismus ist, folgt nun $\overline{x} = \overline{y} \in K/N$. □

2. Der Schritt von p^{a-1} nach p^a

Momentan haben wir noch ein Spannungsverhältnis. Prinzipiell arbeiten wir mit arithmetischen Untergruppen des Levels M, wollen aber die Primteiler $\pi(M)$ finden. Der große Unterschied zwischen M und $\pi(M)$ ist, dass in M Primzahlen *mehrfach* als Potenzen vorkommen können. Wir müssen also einen Weg finden, mit Potenzen umgehen zu können. Sei p im Folgenden stets eine Primzahl.

Definition II.2.1: Sei $H \leq G$ eine Untergruppe. Wir bezeichnen $U \trianglelefteq G$ als *Supplement* von H falls $G = HU$ gilt. Die Untergruppe U heißt *echt*, falls $U \neq G$ gilt.

Theorem II.2.2 (aus [7, Theorem 2.5]): *Seien a, $n \geq 2$ und $G = \mathrm{SL}(n, \mathbb{Z}_{p^a})$ oder $\mathrm{Sp}(2n, \mathbb{Z}_{p^a})$. Dann hat $K_{p^a,p^{a-1}}$ genau dann ein echtes Supplement in G, wenn G eine der folgenden Gruppen ist:*

$$\mathrm{SL}(2, \mathbb{Z}_4), \quad \mathrm{SL}(2, \mathbb{Z}_9), \quad \mathrm{SL}(3, \mathbb{Z}_4), \quad \mathrm{SL}(4, \mathbb{Z}_4). \tag{II.1}$$

Dieses Lemma wird später in Lemma II.4.1 wichtig sein, um eine Induktion über die Potenz p^a führen zu können. Bevor wir aber dieses Lemma beweisen können, müssen wir einige Hilfslemmata sammeln.

Lemma II.2.3: *Sei p prim, $n \geq 2$, $K = K_{p^3,p^2}$ und $L = K_{p^3,p^1}$, dann gilt $K = \langle L^p \rangle$ für $L^p := \{\ell^p : \ell \in L\}$.*

Beweis: Wir machen eine Fallunterscheidung:

Fall $\Sigma(n, \mathbb{Z}_{p^3}) = \mathrm{SL}(n, \mathbb{Z}_{p^3})$: Wir verwenden den Isomorphismus aus Lemma II.1.10 (i). Sei $T := \{x \in \mathbb{Z}_p^{n\times n} : \mathrm{tr}(x) \equiv 0 \mod p\}$. Da $K \cong T$ gilt, können wir das Problem auf T reduzieren. Offensichtlich ist

$$M := \{\pm E_{i,j} : 1 \leq i \neq j \leq n\} \cup \{\pm E_{i,i} \mp E_{i+1,i+1} : 1 \leq i < n\}$$

ein Erzeugendensystem von T. Wir beachten, dass die Gruppenverknüpfung die Addition ist. Um zu zeigen, dass $\langle L^p \rangle = K$ gilt, müssen wir zeigen, dass es für jedes $(I_n + p^2 x) \in K$ mit $x \in M$ ein $(I_n + py) \in L$ gibt mit

$$(I_n + py)^p = I_n + p^2 x.$$

Wir betrachten eine Fallunterscheidung.

Fall $p \geq 3$: Es gilt nun in $\mathrm{SL}(n, \mathbb{Z}_{p^b})$

$$(I_n + py)^p = I_n + ppy + \sum_{j=2}^{p} \binom{p}{j} p^j y^j = I_n + p^2 y + 0 = I_n + p^2 y$$

Wir müssen also lediglich zeigen, dass $(I_n + px) \in L$ für alle $x \in M$ gilt. Für $x_1 = \pm E_{i,j}$ mit $i \neq j$ gilt offensichtlich $\det(I_n + px) = 1$. Für $x_2 = E_{i,i} - E_{i+1,i+1}$ betrachten wir die Matrix $y_2 = E_{i,i} - E_{i+1,i+1} + E_{i,i+1} - E_{i+1,i}$. Es gilt nun

$$\det(I_n + py_2) = \det\left(\begin{pmatrix} 1+p & p \\ -p & 1-p \end{pmatrix}\right) = 1,$$

woraus $(I_n + py_2) \in L$ und $(I_n + py_2)^p = I_n + p^2y_2 \in K$ folgt. Das Problem ist, dass $I_n + p^2y_2$ zwei unerwünschte Werte auf den Nebendiagonalen hat. Da wir aber bereits alle $\pm E_{i,j}$ konstruiert haben und wir in K den Isomorphismus zur additiven Gruppe haben, können wir die Nebendiagonale eliminieren. Wir können also den Erzeuger $E_{i,i} - E_{i+1,i+1}$ konstruieren. Analog können wir $-E_{i,i} + E_{i+1,i+1}$ konstruieren. Also können wir alle Erzeuger bauen, weshalb die Aussage gilt.

Fall $p = 2$: Es gilt

$$(I_n + 2y)^2 = I_n + 2^2y + 2^2y^2 = I_n + 2^2(y + y^2).$$

Wir wollen x_1 und x_2 wie im letzten Fall konstruieren. Da $x_1^2 = y_2^2 = 0$ und daher $(I_n + 2x_1)^2 = I_n + 2^2x_1$ bzw. $(I_n + 2y_2)^2 = I_n + 2^2y_2$ gilt, können wir die Konstruktionen aus dem vorherigen Fall nehmen.

Fall $\Sigma(n, \mathbb{Z}_{p^3}) = \mathrm{Sp}(n, \mathbb{Z}_{p^3})$: Sei $n = 2s$. Wir verwenden den Isomorphismus aus Lemma II.1.10 (ii). Sei

$$T := \{x = \begin{pmatrix} A & B \\ C & -A^\top \end{pmatrix} : A, B, C \in \mathbb{Z}_p^{s\times s} \text{ und } B = B^\top,\, C = C^\top\},$$

dann gilt $K \cong T$, weshalb wir das Problem auf T reduzieren können. Offensichtlich ist

$$\begin{aligned} M :=& \{\pm E_{i,j} \mp E_{j+s,i+s} : 1 \le i, j \le s\} \\ &\cup \{\pm E_{i,j+s} \pm E_{j,i+s},\ \pm E_{i,i+s} : 1 \le i \ne j \le s\} \\ &\cup \{\pm E_{i+s,j} \pm E_{j+s,i},\ \pm E_{i+s,i} : 1 \le i \ne j \le s\} \end{aligned}$$

ein Erzeugendensystem von T. Um zu zeigen, dass $\langle L^p \rangle = K$ gilt, müssen wir zeigen, dass es für jedes $x \in M$ ein $(I_n + py) \in L$ existiert mit

$$(I_n + py)^p = I_n + p^2x.$$

Wir betrachten eine Fallunterscheidung.

Fall $p \ge 3$: Es gilt $(I_n + py)^p = I_n + p^2y$ nach dem $\mathrm{SL}(n, \mathbb{Z}_{p^a})$-Fall. Wir stellen uns zunächst die Frage, wann für $x \in T$ die Matrix $I_n + px$ in L liegt. Hierfür

muss die folgende Rechnung gültig sein

$$\begin{aligned}
& & (I_n + px)J(I_n + px)^\top &= J \\
\Leftrightarrow & & pxJ + pJx^\top + p^2xJx^\top &= 0 \\
\Leftrightarrow & p\begin{pmatrix} -B & A \\ A^\top & C \end{pmatrix} + p\begin{pmatrix} B^\top & -A \\ -A^\top & -C^\top \end{pmatrix} + p^2xJx^\top &= 0 \\
\Leftarrow & & xJx^\top &= 0 \\
\Leftrightarrow & & \begin{pmatrix} AB^\top - BA^\top & -A^2 - BC^\top \\ (A^\top)^2 + CB^\top & -CA + A^\top C^\top \end{pmatrix} &= 0. \qquad \text{(II.2)}
\end{aligned}$$

Wir betrachten zunächst den Erzeuger $x_1 = E_{i,j+s} + E_{j,i+s}$. Wenn wir x_1 als Blockmatrix darstellen, gilt

$$x_1 = \begin{pmatrix} A & B \\ C & -A^\top \end{pmatrix} = \begin{pmatrix} 0 & E_{i,j} + E_{j,i} \\ 0 & 0 \end{pmatrix}.$$

Nach der obigen Rechnung gilt $(I_n + px_1) \in L$ und da $(I_n + px_1)^p = (I_n + p^2x_1)$ ist, können wir diesen Erzeuger konstruieren. Für $x_2 = \pm E_{i,i+s},\ x_3 = \pm E_{i+s,j} \pm E_{j+s,i}$ und $x_4 = \pm E_{i+s,i}$ gehen wir analog vor.

Als nächstes wollen wir den Erzeuger $x_5 := E_{i,j} - E_{j+s,i+s}$ für $i \neq j$ betrachten. Hierfür betrachten wir die Matrix

$$x_5 = \begin{pmatrix} A & B \\ C & -A^\top \end{pmatrix} = \begin{pmatrix} E_{i,j} & 0 \\ 0 & -E_{j,i} \end{pmatrix}.$$

Auch hier gilt $(I_n + px_5) \in L$, wobei wir $E_{i,j}^2 = 0$ berücksichtigen. Es bleibt also $x_6 := E_{i,i} - E_{i+s,i+s}$ übrig. Hierfür definieren wir

$$y_6 := \begin{pmatrix} A & B \\ C & -A \end{pmatrix} = \begin{pmatrix} E_{i,i} & E_{i,i} \\ -E_{i,i} & -E_{i,i} \end{pmatrix}.$$

Es gilt nun $(I_n + py_6) \in L$ nach (II.2). Der Unterschied zwischen y_6 und dem gewünschten Erzeuger x_6 ist, dass y_6 im Block B und C Einträge hat. Da wir aber bereits alle Erzeuger für die Blöcke B und C konstruiert haben, können wir diese Einträge eliminieren. Daher können wir x_6 konstruieren.

Fall $p = 2$. Es gilt

$$(I_n + 2y)^2 = I_n + 2^2(y + y^2).$$

Wir wollen x_1 bis x_6 wie oben konstruieren. Da $x_1^2 = x_2^2 = \ldots = x_5^2 = 0 = y_6^2$ und daher $(I_n + 2x_i)^2 = I_n + 2^2x_i$ für $1 \leq i \leq 5$ bzw. $(I_n + 2y_6)^2 = I_n + 2^2y_6$ gilt, können wir die Konstruktionen aus dem vorherigen Fall nehmen. □

Korollar II.2.4: *Seien p prim, $n \geq 2$, $a \geq 3$, $K = K_{p^a,p^{a-1}}$ und $L = K_{p^a,p^{a-2}}$ Untergruppen der $\Sigma(n, \mathbb{Z}_{p^a})$, dann gilt $K = \langle L^p \rangle$.*

Beweis: **Fall** $a = 3$: Folgt direkt aus Lemma II.2.3.

Fall $a \geq 4$: Sei $(I_n + p^{a-1}x) \in K$. Da $2(a-2) \geq a$ folgt nach Lemma II.1.10 (i) und (ii), dass $(I_n + p^{a-2}x) \in L$ ist. Wir können nun den Isomorphismus und den Verweis auf die additive Matrixgruppe von Lemma II.1.10 verwenden und erhalten

$$(I_n + p^{a-2}x)^p = I_n + p^{a-2}px = I_n + p^{a-1}x,$$

wobei wir beim ersten Schritt ausgenutzt haben, dass aus der p-fachen Multiplikation eine p-fache Addition wird. Also gilt $K = L^p$. □

Lemma II.2.5 (aus [7, Lemma 2.7]): *Sei $n \geq 2$ und $a \geq 3$. Wir betrachten $G = \mathrm{SL}(n, \mathbb{Z}_{p^a})$ oder $G = \mathrm{Sp}(2n, \mathbb{Z}_{p^a})$. Dann liegt $K = K_{p^a,p^{a-1}}$ im Zentrum von $L = K_{p^a,p^{a-2}}$ und hat kein echtes Supplement in L.*

Beweis: Man kann einfach zeigen, dass $K = \{I_n + p^{a-1}x \in \Sigma(n, \mathbb{Z}_{p^a})\}$ und $L = \{I_n + p^{a-2}y \in \Sigma(n, \mathbb{Z}_{p^a})\}$ gilt. Da $2a - 3 \geq a$ gilt, folgt für alle $s \in K$ und $t \in L$:

$$\begin{aligned} st = (I_n + p^{a-1}x)(I_n + p^{a-2}y) &= I_n + p^{a-1}x + p^{a-2}y + p^{2a-3}xy \\ &= I_n + p^{a-1}x + p^{a-2}y = (I_n + p^{a-2}y)(I_n + p^{a-1}x) = ts. \end{aligned}$$

Also liegt K im Zentrum von L.

Nach Korollar II.2.4 gilt $K = L^p := \langle \{x^p \ : \ x \in L\} \rangle$. Angenommen U wäre ein Supplement von K, dann würde $L = KU$ gelten. Es gilt nun

$$K = L^p = K^p U^p = \langle \{s^p t^p \ : \ s \in K, t \in U\} \rangle,$$

wobei wir hier ausnutzen, dass K im Zentrum liegt. Da $K = K_{p^a,p^{a-1}}$ und $2(a-1) \geq a$ gilt, können wir den Isomorphismus aus Lemma II.1.10 verwenden. Wir sehen also, dass $s^p = (I_n + p^{a-1}x)^p = I_n + p^a x = I_n$ für $s \in K$ gilt, weshalb wir mit

$$= \langle \{I_n t^p\} \rangle \leq U$$

fortfahren können. Also ist K eine Untergruppe von U, weshalb $KU = U = L$ sein muss. Daher existiert kein echtes Supplement. □

Lemma II.2.6 (aus [7, Lemma 2.8]): *Seien $G = \mathrm{Sp}(4, \mathbb{Z}_{p^2})$ und $H = \mathrm{Sp}(2, \mathbb{Z}_{p^2})$ mit p ungerade. Falls es ein echtes Supplement von $C := K_{p^2,p}$ in G gibt, dann existiert ein echtes Supplement von $D := K_{p^2,p}$ in H.*

Beweis: Wir betrachten zunächst die Einbettung

$$\lambda\colon H \to G;\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Wir wollen die Wohldefiniertheit überprüfen. Wir wissen nach [14, II.9.12], dass $\mathrm{Sp}(2, \mathbb{Z}_{2^a}) = \mathrm{SL}(2, \mathbb{Z}_{2^a})$ gilt. Daher folgt für eine Matrix in H stets $ad - bc = 1$. Weil

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{\top} J \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -(ad-bc) & 0 \\ 0 & 0 & 0 & -1 \\ ad-bc & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

gilt, ist λ wohldefiniert. Wir stellen nun D wie in Lemma II.1.10 (ii) dar:

$$D = \left\{ \begin{pmatrix} 1+pa & pb \\ pc & 1-ap \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}. \tag{II.3}$$

Man sieht, dass $\lambda(D) \leq C$ gilt. Wir betrachten nun die Untergruppe N von C, deren Elemente die Form $I_4 + pr$ mit

$$r = \begin{pmatrix} 0 & v_1 & 0 & w_1 \\ -w_3 & v_2 & w_1 & w_2 \\ 0 & v_3 & 0 & w_3 \\ v_3 & v_4 & -v_1 & -v_2 \end{pmatrix},\ v_1, \ldots, v_4, w_1, w_2, w_3 \in \{0, 1, \ldots, p-1\} \tag{II.4}$$

haben. Wir definieren außerdem die Untergruppe $W := C\lambda(H)$. Es gilt, dass N ein Supplement von $\lambda(D)$ in C ist, was wir nun zeigen wollen. Indem wir C wie in Lemma II.1.10 (ii) darstellen, können wir die Funktion

$$\kappa'\colon C \to H; \begin{pmatrix} 1+pa_1 & pa_2 & pb_1 & pb_2 \\ pa_3 & 1+pa_4 & pb_2 & pb_4 \\ pc_1 & pc_2 & 1-pa_1 & -pa_2 \\ pc_2 & pc_4 & -pa_3 & 1-pa_4 \end{pmatrix} \mapsto \begin{pmatrix} 1+pa_1 & pb_1 \\ pc_1 & 1-pa_1 \end{pmatrix}$$

definieren. Da

$$\det\left(\begin{pmatrix} 1+pa_1 & pb_1 \\ pc_1 & 1-pa_1 \end{pmatrix} \right) \equiv 1 \mod p^2$$

gilt, ist die Funktion wohldefiniert. Wir beachten hierbei $\mathrm{Sp}(n, \mathbb{Z}_{2^a}) = \mathrm{SL}(n, \mathbb{Z}_{2^a})$. Mit Hilfe von (II.3) sieht man $\kappa'(\lambda(D)) = \kappa'(C)$. Es gilt $\mathrm{Kern}(\kappa') = N$, weshalb $\lambda(D)N = C$ nach Lemma II.1.12 folgt. Daher gilt

$$W = C\lambda(H) = N\lambda(D)\lambda(H) = N\lambda(H).$$

Des Weiteren gilt $hNh^{-1} = N$ für alle $h \in \lambda(H)$, denn es gilt für alle $n \in N$

$$\begin{aligned} hnh^{-1} &= \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \left(I_4 + p \begin{pmatrix} 0 & v_1 & 0 & w_1 \\ -w_3 & v_2 & w_1 & w_2 \\ 0 & v_3 & 0 & w_3 \\ v_3 & v_4 & -v_1 & -v_2 \end{pmatrix} \right) \begin{pmatrix} a & 0 & b & 0 \\ 0 & 1 & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & apv_1 + bpv_3 & 0 & apw_1 + bpw_3 \\ \frac{cpw_1 + dpw_3}{bc-ad} & 1 + pv_2 & \frac{-apw_1 - bpw_3}{bc-ad} & pw_2 \\ 0 & cpv_1 + dpv_3 & 1 & cpw_1 + dpw_3 \\ \frac{-cpv_1 - dpv_3}{bc-ad} & pv_4 & \frac{apv_1 + bpv_3}{bc-ad} & 1 - pv_2 \end{pmatrix} \\ &= I_4 + p \begin{pmatrix} 0 & av_1 + bv_3 & 0 & aw_1 + bw_3 \\ -(cw_1 + dw_3) & v_2 & aw_1 + bw_3 & w_2 \\ 0 & cv_1 + dv_3 & 0 & cw_1 + dw_3 \\ cv_1 + dv_3 & v_4 & -(av_1 + bv_3) & -v_2 \end{pmatrix}. \end{aligned}$$

Hieraus können wir folgern, dass N ein Normalteiler von W ist, denn es gilt für alle $a = nh \in W = N\lambda(H)$ mit $n \in N$ und $h \in \lambda(H)$:

$$aNa^{-1} = nhNh^{-1}n^{-1} = nNn^{-1} = N.$$

Daher ist N ein Normateiler in W. Außerdem gilt offensichtlich $N \cap \lambda(H) = \{I_4\}$. Hieraus folgt nach [14, I.3.12]

$$W/N = N\lambda(H)/N \cong \lambda(H)/(N \cap \lambda(H)) = \lambda(H)/\{I_4\} \cong \lambda(H).$$

Mit der Isomorphie definieren wir $\kappa'' \colon W/N \to \lambda(H)$. Sei $\pi_N \colon W \to W/N$ die natürliche Projektion. Des Weiteren ist λ offensichtlich injektiv, weshalb wir auf $\lambda(H)$ den Homomorphismus $\lambda^{-1}_{|\lambda(H)}$ betrachten können. Sei $\kappa \colon W \to H$ der Homomorphismus, welcher durch $\kappa := \lambda^{-1}_{|\lambda(H)} \circ \kappa'' \circ \pi_N$ definiert ist. Aus $\lambda(D)N = C$ folgt $\kappa(C) = D$. Offensichtlich ist N der Kern von κ. Wir nehmen nun an, dass S ein Supplement von C in G ist, weshalb $\kappa(S \cap W)$ ein Supplement von D in H sein muss. Es gilt nämlich

$$\kappa(S \cap W)D = \kappa(S \cap W)\,\kappa(C) \overset{\text{II.1.11}}{=} \kappa(G \cap W) = \kappa(W) = H\,.$$

Wir wollen nun zeigen, dass $\kappa(S \cap W)$ unser gesuchtes echtes Supplement von D in H ist. Angenommen $\kappa(S \cap W)$ wäre kein echtes Supplement, dann folgte $\kappa(S \cap W) = H$. Nun folgt aber $\kappa(S \cap C) = D$. Es gilt $\kappa(S \cap C) \subseteq D$, da $\kappa(C) \subseteq D$ gilt. Um $\kappa(S \cap C) \supseteq D$ zu zeigen, betrachten wir ein beliebiges $d \in D$. Es gibt ein $s \in S$ mit $\kappa(s) = d$ und $s = n\lambda(h)$ mit $n \in N$, $h \in H$, da

$$\kappa(S \cap N\lambda(H)) = \kappa(S \cap W) = H \supseteq D$$

gilt. Es folgt nun $\kappa(s) = \kappa(\lambda(h)) = h = d$. Also gilt $s = n\lambda(d)$. Da wir weiter oben gezeigt haben, dass N, $\lambda(D) \subseteq C$ gilt, folgt $s \in S \cap C$ und daher $d \in \kappa(S \cap C)$.

Wir wollen nun unter der Annahme $\kappa(S \cap C) = D$ zeigen, dass $C \leq S$ und daher $G = SC = S$ gilt, weshalb S kein Supplement wäre. Hieraus folgt die Aussage.

Wir wollen $S \cap C \trianglelefteq G$ zeigen. Zunächst folgt $S \cap C \trianglelefteq S$ nach [14, I.3.12]. Außerdem können wir C nach Lemma II.1.10 (ii) als abelsche Untergruppe ansehen, weshalb $S \cap C \trianglelefteq C$ gilt. Da $G = SC$ gilt, können wir jedes $g \in G$ in $s \in S$ und $c \in C$ zerlegen. Hieraus folgt

$$g^{-1}(S \cap C)g = s^{-1}c^{-1}(S \cap C)cs = s^{-1}(S \cap C)s = (S \cap C).$$

Wir verwenden Lemma II.1.10 (ii) und betrachten C als additive Untergruppe der $\mathbb{Z}_p^{4\times 4}$, wobei wir anstelle von $I_4 + px$ immer $x \in \mathbb{Z}_p^{4\times 4}$ betrachten wollen. Wann immer wir also von einem Element x in C oder $S \cap C$ sprechen, meinen wir eigentlich das Element $I_4 + px$ (vgl. Isomorphismus aus Lemma II.1.10). Wir werden auch die Rechenregel aus Lemma II.1.10 (iii) verwenden. Hierdurch können wir annehmen, dass für $a, b \in S \cap C$ auch $-a, a - b \in S \cap C$ folgt. Offensichtlich gilt für $a \in S \cap C$ auch $ka \in S \cap C$ für $k \in \mathbb{Z}_p$. Da p ungerade ist, gilt insbesondere $\frac{1}{2} \in \mathbb{Z}_p$.

Es gilt $\kappa(S \cap C) = D$, daher gibt es ein $a = r + E_{3,1} \in S \cap C$ mit einem r wie in Gleichung (II.4), weil $I_2 + E_{1,2} \in D$ gilt. Sei $b_1 = I_4 + E_{1,3} \in G$. Wir werden im Folgenden die Notation $x^y := y^{-1}xy$ verwenden. Es sei daran erinnert, dass für $x \in S \cap C$ und $y \in G$ stets $x^y \in S \cap C$ folgt, da $S \cap C$ ein Normalteiler in G ist. Wir betrachten

$$a_1 = a - a^{b_1} = E_{1,1} + E_{1,3} - E_{3,3} + v_3(E_{1,2} - E_{4,3}) + w_3(E_{2,3} + E_{1,4}).$$

Dann gilt $a_2 = \frac{1}{2}(a_1^{b_1} - a_1) = E_{1,3} \in S \cap C$.

Weil G die Permutationsmatrix t von $(1, 2)(3, 4)$ beinhaltet, folgt daher $E_{2,4} = E_{1,3}^t \in S \cap C$. Wir wollen nun noch weitere Elemente konstruieren. Sei

hierfür $d_1 = I_4 + E_{3,1}$, $d_2 = I_4 + E_{1,4} + E_{2,3}$ und $d_3 = I_4 + E_{3,2} + E_{4,1}$. Wir betrachten

$$c_1 := \tfrac{1}{2}(a_2^{d_1} - a_2^{d_1^{-1}}) = E_{1,1} - E_{3,3}, \qquad c_2 := c_1^t = E_{2,2} - E_{4,4},$$
$$c_3 := \tfrac{1}{2}(a_2^{d_3} - a_2^{d_3^{-1}}) = E_{1,2} - E_{4,3}, \qquad c_4 := c_3^t = E_{2,1} - E_{3,4},$$
$$c_5 := \tfrac{1}{2}(-a_2^{d_1} + a_2^{d_2^{-1}} + a_2^{d_1 d_2} - a_2^{d_1^{-1} d_2}) = E_{1,4} + E_{2,3},$$
$$c_6 := \tfrac{1}{2}(2a_2 - a_2^{d_1} - a_2^{d_1^{-1}}) = E_{3,1}, \qquad c_7 := c_6^t = E_{4,2},$$
$$c_8 := -a_2 + a_2^{d_1} + a_2^{d_3} - a_2^{d_1 d_3} = E_{3,2} + E_{4,1},$$

welche alle in $S \cap C$ liegen. Wir betrachten zusätzlich die bereits konstruierten Elemente $c_9 := E_{1,3}$ und $c_{10} := E_{2,4}$. Diese zehn Elemente sind alle bezüglich des $\mathbb{Z}_p$-Vektorraums $(\mathbb{Z}_p^{4\times 4}, +)$, linear unabhängig. Man erkennt anhand der Struktur von Lemma II.1.10 (ii), dass C die $\mathbb{Z}_p$-Dimension 10 hat, daher gilt $S \cap C = C$, woraus $C \leq S$ folgt, was wir zeigen wollten. □

Definition II.2.7: Die Frattinigruppe von G ist der Durchschnitt aller maximalen Untergruppen von G.

Lemma II.2.8 (aus [2], [24, Theorem 1], [25] und [7, Beweis Theorem 2.5]):

(i) *Sei $G = \mathrm{SL}(n, \mathbb{Z}_{p^2})$ mit $n \geq 2$ keine der Gruppen aus (II.1), dann liegt $K_{p^2,p}$ in der Frattinigruppe von G.*

(ii) *Sei $G = \mathrm{Sp}(2n, \mathbb{Z}_{p^2})$ für $n \geq 3$ und $G \neq \mathrm{Sp}(6, \mathbb{Z}_4)$, dann liegt $K_{p^2,p}$ in der Frattinigruppe von G.*

Wir haben jetzt alles beisammen, um Theorem II.2.2 zu beweisen.

Beweis (Theorem II.2.2): Wir machen ein Fallunterscheidung:

Fall $a \geq 3$: Angenommen es existiert ein echtes Supplement $L \leq G$ mit $K_{p^a,p^{a-1}} L = G$, dann ist $L' := L \cap K_{p^a,p^{a-2}}$ ein echtes Supplement von $K_{p^a,p^{a-1}}$ in $K_{p^a,p^{a-2}}$. Dies kann aber nach Lemma II.2.5 nicht sein. Um zu zeigen, dass L' ein echtes Supplement ist, müssen wir zunächst $L' K_{p^a,p^{a-1}} = K_{p^a,p^{a-2}}$ zeigen, was aber direkt aus Lemma II.1.11 folgt.

Es bleibt zu zeigen, dass L' eine echte Untergruppe ist. Angenommen dies wäre nicht der Fall, dann würde

$$K_{p^a,p^{a-1}} \subseteq K_{p^a,p^{a-2}} \subseteq L$$

gelten. Es gilt aber $K_{p^a,p^{a-1}} L = L = G$, weshalb L kein echtes Supplement ist.

Fall $a = 2$: Wir betrachten $G \neq \mathrm{Sp}(4, \mathbb{Z}_{p^2})$ und $G \neq \mathrm{Sp}(6, \mathbb{Z}_4)$ und erhalten mit Lemma II.2.8, dass $K_{p^2,p}$ in der Frattinigruppe von G liegt. Allerdings gilt, dass Untergruppen, welche in der Frattinigruppe liegen, kein echtes Supplement haben können (siehe [14, III.3.2 b)]).

Als nächstes wollen wir uns mit $G = \mathrm{Sp}(4, \mathbb{Z}_{p^2})$ beschäftigen. Nach Lemma II.2.6 können wir diesen Fall auf $\mathrm{Sp}(2, \mathbb{Z}_{p^2})$ zurückführen. Gibt es nämlich ein echtes Supplement in $\mathrm{Sp}(4, \mathbb{Z}_{p^2})$, dann muss es auch eines in $\mathrm{Sp}(2, \mathbb{Z}_{p^2})$ geben. Nun gilt aber $\mathrm{Sp}(2, \mathbb{Z}_{p^2}) = \mathrm{SL}(2, \mathbb{Z}_{p^2})$, weshalb wir diesen Fall bereits betrachtet haben.

Es fehlt noch $G = \mathrm{Sp}(6, \mathbb{Z}_4)$. Man kann mit `GAP` nachrechnen, dass $K_{4,2}$ in diese Gruppe kein echtes Supplement hat. Außerdem können wir mit `GAP` nachrechnen, dass die Gruppen (II.1) tatsächlich ein echtes Supplement haben. Damit ist die Aussage bewiesen. □

Aus Theorem II.2.2 folgt der Umstand, dass es zu Ausnahmen kommen kann, wenn $n \leq 4$ und $p = 2$ gilt. Der Fall $p = 2$ oder 3 und $n = 2$ kommt zwar auch in Theorem II.2.2 vor, wird aber keine große Rolle spielen, da wir nur Gruppen mit $n > 2$ betrachten werden. Dies motiviert die nächste Definition.

Definition II.2.9: Wir bezeichnen (n, p) als *unexceptional*, falls $p > 3$ oder $n > 4$ gilt.

3. Das Kombinieren verschiedener Potenzen

Wir haben uns sehr ausführlich mit Potenzen beschäftigt. Allerdings sind die Potenzen in M alle *gemischt*. Sprich, wir wollen versuchen, $p^a q$ mit q koprim zu p aufzuspalten. Eine wichtige Komponente des Beweises wird es sein, das Problem von $\Sigma(n, \mathbb{Z}_{p^a})$ auf $\mathrm{P}\Sigma(n, p)$ zu übertragen, welche fast immer einfach und perfekt ist. Hierfür wollen wir uns zunächst mit dem Zentrum von $\Sigma(n, p)$ beschäftigen.

Lemma II.3.1: *Sei n, $p \geq 3$, dann liegt jeder echte Normalteiler von $\Sigma(n, p)$ im Zentrum $Z := Z_{\Sigma(n,p)}$, außer es gilt $\Sigma(n, p) = \mathrm{Sp}(4, 2)$.*

Beweis: Sei $N \trianglelefteq \Sigma(n, p)$ ein Normateiler. Da $\mathrm{P}\Sigma(n, p)$ nach [14, II.6.13 und II.9.22] einfach ist und NZ/Z ein Normalteiler ist, folgt $NZ/Z = \{e\}$ oder $NZ/Z = \mathrm{P}\Sigma(n, p)$. Im ersten Fall gilt $NZ = Z$, weshalb $N \subseteq Z$ gilt. Im zweiten Fall gilt $NZ = \Sigma(n, p)$. Da nach [14, II.6.10 und II.9.20] die Gruppe $\Sigma(n, p)$ perfekt ist, gilt

$$\Sigma(n, p) = [NZ, NZ] = [N, N] \subseteq N \subseteq \Sigma(n, p),$$

weshalb N kein echter Normalteiler ist. □

Definition II.3.2: Sei G eine Gruppe. Das *auflösbare Radikal* von G ist die eindeutige Untergruppe, welche durch die Vereinigung aller normalen, auflösbaren Untergruppen entsteht. Es ist daher die größte normale, auflösbare Untergruppe in G und eindeutig.

Wir können das auflösbare Radikal mittels des Zentrums beschreiben.

Lemma II.3.3: *Sei $n \geq 3$, p eine Primzahl, $a \geq 1$ und $G = \Sigma(n, \mathbb{Z}_{p^a})$. Sei außerdem R das auflösbare Radikal von $\Sigma(n, p^a)$ und $Z := Z_{\Sigma(n,p)}$ das Zentrum von $\Sigma(n, p)$, dann ist $R = \varphi_{p^a,p}^{-1}(Z)$.*

Beweis: Zunächst wollen wir $R' := \varphi_{p^a,p}^{-1}(Z) \leq R$ zeigen. Es gilt, dass Z normal ist und daher auch R' als Urbild. Außerdem ist R' auflösbar. Wir betrachten die Einschränkung $\varphi_{p^a,p|R'}$. Nach dem Homomorphiesatz ist $R'/\operatorname{Kern}(\varphi_{p^a,p|R'}) \cong Z$. Da Z abelsch ist, folgt, dass $R'/\operatorname{Kern}(\varphi_{p^a,p|R'})$ auflösbar ist. Gleichzeitig ist $\operatorname{Kern}(\varphi_{p^a,p|R'})$ eine Untergruppe von $K_{p^a,p}$. Für $a \geq 2$ ist $K_{p^a,p}$ nach Lemma II.1.9 eine p-Gruppe und damit nach [13, Theorem 7.2 und Proposition 7.10] auflösbar, weshalb auch $\operatorname{Kern}(\varphi_{p^a,p|R'})$ auflösbar ist. Für den Fall $a = 1$ ist $\varphi_{p^a,p|R'}$ die Identität, weshalb der Kern trivial ist. Daher ist auch R' nach [5, 5.4/8] auflösbar, weshalb $R' \leq R$ gilt.

Wir wollen nun $R \leq R'$ zeigen, wobei wir $R' \leq R$ verwenden dürfen. Wir machen eine Fallunterscheidung.

Fall $G \neq \operatorname{Sp}(4, \mathbb{Z}_{2^a})$: Wir wissen, dass $Z \leq \varphi_{p^a,p}(R) \leq \Sigma(n, p)$ gilt. Da R normal ist, ist auch $\varphi_{p^a,p}(R)$ normal, da $\varphi_{p^a,p}$ surjektiv ist. Daher ist auch $\varphi_{p^a,p}(R)/Z$ ein Normalteiler von $\mathrm{P}\Sigma(n, p)$. Da aber $\mathrm{P}\Sigma(n, p)$ nach [14, II.6.13 und II.9.22] einfach ist, außer es gilt $\mathrm{P}\Sigma(n, p) = \operatorname{PSp}(4, 2)$, folgt $\varphi_{p^a,p}(R) = Z$ oder $\varphi_{p^a,p}(R) = \Sigma(n, p)$. Letzteres kann nicht sein, weil sonst $\varphi_{p^a,p}(R)/Z = \mathrm{P}\Sigma(n, p)$ auflösbar wäre, da R auflösbar ist und Auflösbarkeit durch surjektive Homomorphismen erhalten wird. Die Gruppe $\mathrm{P}\Sigma(n, p)$, ausgenommen $\operatorname{PSp}(4, 2)$, ist aber nach [14, II.6.10 und II.9.20] nicht auflösbar, also ist $\varphi_{p^a,p}(R) = Z$ und daher $R' \leq R$.

Fall $G = \operatorname{Sp}(4, \mathbb{Z}_{2^a})$: Wir betrachten zunächst die $\operatorname{Sp}(4, 2)$. Dies ist nach [14, S. II.9.21] isomorph zu $\operatorname{Sym}(6)$. Da die $\operatorname{Sym}(6)$ und ihr einziger echter nichttrivaler Normalteiler $\operatorname{Alt}(6)$ nicht auflösbar sind, ist das auflösbare Radikal $R = \{e\} = Z_{\operatorname{Sp}(4,2)}$.

Sei R das auflösbare Radikal von $\operatorname{Sp}(4, \mathbb{Z}_{2^a})$ und $R' = \varphi_{2^a,2}^{-1}(Z_{\operatorname{Sp}(4,2)}) = K_{2^a,2}$. Da der Homomorphismus $\varphi_{2^a,2}$ surjektiv ist, ist $\varphi_{2^a,2}(R)$ normal und auflösbar, weshalb $\varphi_{2^a,2}(R) \leq \{e\}$ gilt, da das auflösbare Radikal von $\operatorname{Sp}(4, 2)$ trivial ist. Hieraus folgt aber $R \leq K_{2^a,2} = R'$.

Wir werden nun sehen, dass wir $\Sigma(n, \mathbb{Z}_{p^a})$ mittels des auflösbaren Radikals nach $\mathrm{P}\Sigma(n, p)$ schicken können.

Lemma II.3.4: *Sei $n \geq 3$, p eine Primzahl, $a \geq 1$, $A = \Sigma(n, \mathbb{Z}_{p^a})$ und R das auflösbare Radikal von A. Dann gilt $A/R \cong \mathrm{P}\Sigma(n, p)$.*

Beweis: Nach Lemma II.3.3 gilt $R = \varphi_{p^a,p}^{-1}(Z_{\Sigma(n,p)})$. Es gilt offensichtlich $K_{p^a,p} \subseteq R$. Außerdem folgt nach dem Homomorphiesatz $A/K_{p^a,p} \cong \Sigma(n, p)$ und $R/K_{p^a,p} \cong Z_{\Sigma(n,p)}$, wobei wir beides als Bild desselben Isomorphismus $\overline{\varphi}_{p^a,p} \colon A/K_{p^a,p} \to \Sigma(n, p)$ ansehen können. Daher gilt

$$A/R \cong (A/K_{p^a,p})/(R/K_{p^a,p}) \cong \Sigma(n, p)/Z_{\Sigma(n,p)} = \mathrm{P}\Sigma(n, p),$$

wobei die erste Isomorphie durch [14, I.3.10 c)] begründet ist. □

Lemma II.3.5 (aus [7, Lemma 2.9]): *Sei $n \geq 3$, p eine Primzahl, $a \geq 1$. Sei außerdem $G = \Sigma(n, \mathbb{Z}_{p^a})$ und $G \neq \mathrm{Sp}(4, \mathbb{Z}_{2^a})$, dann liegt jede echte normale Untergruppe von G im auflösbaren Radikal R von G. Im Fall $G = \mathrm{Sp}(4, \mathbb{Z}_{2^a})$ gibt es genau einen nichttrivialen Normalteiler $N \not\subseteq R$. Hierbei gilt $R \subseteq N$ und $[G : N] = 2$ gilt.*

Beweis: Nach Lemma II.3.3 wissen wir, dass $R = \varphi_{p^a,p}^{-1}(Z_{\Sigma(n,p)})$ für das auflösbare Radikal R gilt. Nach Lemma II.3.4 folgt

$$G/R = \Sigma(n, \mathbb{Z}_{p^a})/\varphi_{p^a,p}^{-1}(Z) \cong \Sigma(n, p)/Z = \mathrm{P}\Sigma(n, p),$$

weshalb G/R einfach nach [14, II.6.13 und II.9.22] ist, sofern $G \neq \mathrm{Sp}(4, \mathbb{Z}_{2^a})$ gilt. Wir wollen per Induktion über a zeigen, dass für alle Normalteiler $N \not\subseteq R$ bereits $N = G$ gilt.

Induktionsanfang $a = 1$: Folgt aus Lemma II.3.1, da $R = Z_{\Sigma(n,p)}$ ist.

Induktionsvoraussetzung: Für alle Normalteiler $N \not\subseteq R$ in $G = \Sigma(n, \mathbb{Z}_{p^a})$ gelte $N = G$.

Induktionsschritt $a \to a+1$: Wir wissen, dass $R = \varphi_{p^{a+1},p}^{-1}(Z_{\Sigma(n,p)})$ gilt. Daher gilt $K_{p^{a+1},p} \subseteq R$. Es gilt nun, dass $\varphi_{p^{a+1},p^a}(N)$ ein Normalteiler ist und daher nach Induktionsvoraussetung im auflösbaren Radikal $\varphi_{p^a,p}^{-1}(Z_{\Sigma(n,\mathbb{Z})})$ liegt oder $\varphi_{p^{a+1},p^a}(N) = \Sigma(n, \mathbb{Z}_{p^a})$ gilt. Im ersten Fall gilt

$$N \subseteq \varphi_{p^{a+1},p^a}^{-1}(\varphi_{p^{a+1},p^a}(N)) \subseteq \varphi_{p^{a+1},p^a}^{-1}(\varphi_{p^a,p}^{-1}(Z_{\Sigma(n,\mathbb{Z})})) = R.$$

Für den zweiten Fall machen wir eine Fallunterscheidung:

Fall $a + 1 = 2 = p$, $n \in \{3, 4\}$ und wir sind in $\mathrm{SL}(n, \mathbb{Z}_4)$: Man rechnet mit Hilfe von `GAP` nach, dass es keinen echten Normalteiler $N \not\subseteq R$ in $\mathrm{SL}(3, \mathbb{Z}_4)$ oder $\mathrm{SL}(4, \mathbb{Z}_4)$ gibt.

Fall sonst: Es gilt $\varphi_{p^{a+1},p^a}(N) = \Sigma(n, \mathbb{Z}_{p^a})$, woraus $NK_{p^{a+1},p^a} = \Sigma(n, \mathbb{Z}_{p^{a+1}})$ folgt. Es kann aber nach Theorem II.2.2 kein echtes Supplement von K_{p^{a+1},p^a} geben, weshalb $N = \Sigma(n, \mathbb{Z}_{p^{a+1}})$ sein muss.

Wir betrachten nun die Gruppe $G = \mathrm{Sp}(4, 2)$. Sei N ein Normalteiler. Weil $\mathrm{Sp}(4, 2) \cong \mathrm{Sym}(6)$ nach [14, II.9.21] gilt, folgt $R = \{I_4\}$, weshalb immer $R \subseteq N$ gilt. Da der einzige nichttriviale Normalteiler von Sym(6) die Alt(6) ist, gilt die Aussage.

Die allgemeine Version mit $G = \mathrm{Sp}(4, 2^a)$ gilt nach [7, Lemma 2.9] □

Bemerkung II.3.6: Seien $2 \geq r$, m teilerfremd, dann gilt

$$\Sigma(n, \mathbb{Z}_{mr}) \cong \Sigma(n, \mathbb{Z}_m) \times \Sigma(n, \mathbb{Z}_r).$$

Beweis: Wir betrachten den Homomorphismus $\Psi(x) = (\varphi_{mr,m}(x), \varphi_{mr,r}(x))$. Die Injektivität folgt direkt aus dem chinesischen Restsatz. Es gilt

$$\begin{aligned}
\Psi(\varphi_{mr}(\Gamma_{n,r})) &= \varphi_{mr,m}(\varphi_{mr}(\Gamma_{n,r})) \times \{e\} \\
&= \varphi_{mr,m}(\varphi_{mr}(\Gamma_{n,r})\, \varphi_{mr}(\Gamma_{n,m})) \times \{e\} \\
&\overset{\text{II.1.4 (i)}}{=} \varphi_{mr,m}(\varphi_{mr}(\Sigma(n, \mathbb{Z}))) \times \{e\} = \Sigma(n, \mathbb{Z}_m) \times \{e\},
\end{aligned}$$

wobei wir verwendet haben, dass $\varphi_{mr,m}$ und $\varphi_{mr,r}$, nach Bemerkung II.1.8 surjektiv sind. Analog können wir $\Psi(\varphi_{mr}(\Gamma_{n,m})) = \{e\} \times \Sigma(n, \mathbb{Z}_r)$ zeigen. Hieraus folgt direkt, dass Ψ surjektiv sein muss. □

Das folgende Korollar wird im Beweis von Lemma II.5.3 wichtig werden.

Korollar II.3.7: *Sei m ungerade mit Primfaktorzerlegung $m = p_1^{a_1} \cdots p_t^{a_t}$ und $H \trianglelefteq \Sigma(n, \mathbb{Z}_m)$ ein Normalteiler mit $\varphi_{m,p_k^{a_k}}(H) \neq \Sigma(n, \mathbb{Z}_{p_k^{a_k}})$ für alle $1 \leq k \leq t$, dann ist H auflösbar.*

Beweis: Nach Bemerkung II.3.6 folgt

$$\Sigma(n, \mathbb{Z}_m) \cong \Sigma(n, \mathbb{Z}_{p_1^{a_1}}) \times \ldots \times \Sigma(n, \mathbb{Z}_{p_t^{a_t}}),$$

weshalb wir H als Untergruppe von $A_1 \times \ldots \times A_t$ mit $A_k := \varphi_{m,p_k^{a_k}}(H)$ auffassen können. Nach Voraussetzung sind alle A_k echte normale Untergruppen von $\Sigma(n, p_k^{a_k})$, weshalb A_k nach Lemma II.3.5 auflösbar ist. Also ist $A_1 \times \ldots \times A_t$ auflösbar und daher auch H als Untergruppe einer auflösbaren Gruppe. □

Definition II.3.8: Sei G eine Gruppe. Eine *Section* von G ist der Quotient einer Untergruppe von G, sprich eine Gruppe der Form H/N, wobei H eine Untergruppe und N ein Normalteiler von H ist.

Da der Beweis der folgenden Aussage einiges Wissen über klassische Gruppen voraussetzen würde, welches nicht Teil dieser Arbeit ist, werden wir den Beweis überspringen.

Lemma II.3.9 (aus [7, Lemma 2.11]): *Sei $n \geq 3$ und p, q zwei unterschiedliche Primzahlen. Wenn $P = \mathrm{P}\Sigma(n, \mathbb{Z}_q)$ eine Section von $\Sigma(n, p)$ ist, dann gilt $P = \mathrm{PSL}(3, 2)$ oder $\mathrm{PSp}(4, 2)$. Insbesondere kann P keine Section von $\Sigma(n, p)$ sein, wenn (n, q)* unexceptional *ist.*

Lemma II.3.10: (i) *Sei G eine Gruppe, N ein Normalteiler und R das auflösbare Radikal von G mit $N \leq R$, dann ist R/N das auflösbare Radikal von G/N.*

(ii) *Seien G, H zwei Gruppen, R das auflösbare Radikal von G und $\psi\colon G \to H$ ein Isomorphismus, dann ist $\psi(R)$ das auflösbare Radikal von H.*

Beweis: (i) Sei R' das auflösbare Radikal von G/N. Da $N \leq R$ ist, ist N auflösbar und daher auch R/N. Da R normal ist, ist R/N normal. Es gilt daher $R/N \leq R'$. Nach [14, I.3.10 a)] gibt es eine Gruppe $N \leq U \leq G$ mit $U/N = R'$. Da R' und N auflösbar und normal sind, muss auch U auflösbar und normal sein (siehe [5, 5.4/8]). Man bedenke hierbei, dass man U als Urbild von U/N bezüglich der natürlichen Projektion $\pi_N\colon G \to G/N$ ansehen kann. Daher gilt $U \leq R$, weshalb $R' = U/N \leq R/N$ gilt.

(ii) Gilt da ein Isomorphismus Strukturen erhält. □

Wir wollen nun das Hauptresultat dieses Abschnitts beweisen, mit dessen Hilfe wir in Abschnitt II.4 $p^a q$ aufspalten können. Mittels dieser Aussage können wir nämlich die *gesamte* Gruppe $\Sigma(n, \mathbb{Z}_{p^a})$ in $\Sigma(n, \mathbb{Z}_{p^a q})$ wiederfinden. Gemeint ist, dass wir nach Bemerkung II.3.6 die Gruppe $\Sigma(n, \mathbb{Z}_{p^a q})$ als $\Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_q)$ auffassen können. Wenn wir hiervon eine Untergruppe U betrachten, dann gilt unter bestimmten Voraussetzungen $\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n, \mathbb{Z}_q)}\} \leq U$. Wir können also $\Sigma(n, \mathbb{Z}_{p^a})$ als eine Teilmenge von U, bis auf Isomorphie, auffassen.

Lemma II.3.11 (aus [7, Lemma 2.12]): *Sei $n \geq 3$, $a \geq 1$, $q \geq 2$. Sei außerdem p eine Primzahl, welche koprim zu q ist und (n, p) ist* unexceptional. *Wir nehmen an, dass $U \leq \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_q) \cong \Sigma(n, \mathbb{Z}_{p^a q})$ und $\pi_1(U) = \Sigma(n, \mathbb{Z}_{p^a})$ gilt, wobei π_1 auf die erste Komponente projiziert. Dann gilt $\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n, \mathbb{Z}_q)}\} \leq U$.*

Beweis: Sei $A := \pi_1(U) = \Sigma(n, \mathbb{Z}_{p^a})$ und $B := \pi_2(U)$. Wir betrachten im Folgenden nur noch π_1 und π_2 eingeschränkt auf U. Wir betrachten zunächst

den Fall, dass $q = r^b$ für r prim gilt. Es reicht aus zu zeigen, dass $\{e\} \times B \leq U$ gilt, denn hieraus würde $U = A \times B$ folgen. Ist nämlich $(a, b) \in A \times B$, dann gibt es nach Voraussetzung ein $x \in B$ mit $(a, x) \in U$ und es gilt $(e, x^{-1}b) \in U$. Daraus folgt $(a, b) \in U$. Gilt $U = A \times B$, dann folgt insbesondere $A \times \{e\} \leq U$, was wir zeigen wollen.

Angenommen es gilt nicht $\{e\} \times B \leq U$, dann haben A, B zwei nichttriviale Quotienten A/N und B/M, welche isomorph sind. Um diese zu konstruieren, betrachten wir $\mathrm{Kern}(\pi_1) := \{e\} \times M$ und $\mathrm{Kern}(\pi_2) := N \times \{e\}$. Es gilt, dass $M \trianglelefteq B$ und $N \trianglelefteq A$, was man daran sehen, dass der Kern von π_i ein Normalteiler ist und dieser durch eine surjektive Projektion erhalten wird. Wir können also die Gruppenhomomorphismen $\pi_M \colon B \to B/M$ und $\pi_N \colon A \to A/N$ betrachten. Es gilt nun

$$B/M \xleftarrow{\pi_M} B \xleftarrow{\pi_2} U \xrightarrow{\pi_1} A \xrightarrow{\pi_N} A/N.$$

Offensichtlich sind die Abbildungen $\pi_M \circ \pi_2$ und $\pi_N \circ \pi_1$ surjektiv. Außerdem gilt $\mathrm{Kern}(\pi_M \circ \pi_2) = N \times M = \mathrm{Kern}(\pi_N \circ \pi_1)$. Dass $\mathrm{Kern}(\pi_M \circ \pi_2) \supseteq N \times M$ gilt, ist offensichtlich. Sei andererseits $(a, m) \in \mathrm{Kern}(\pi_m \circ \pi_2)$, dann gilt $a \in A$ und $m \in M$. Es gibt nun ein $(e, m^{-1}) \in \mathrm{Kern}(\pi_1) \leq U$, weshalb $(a, e) \in \mathrm{Kern}(\pi_2)$ gilt. Hieraus folgt nun, dass $a \in N$ gilt, womit die andere Inklusion gezeigt ist. Analog geht man für $N \times M = \mathrm{Kern}(\pi_N \circ \pi_1)$ vor. Nach dem Homomorphiesatz gilt

$$B/M \cong U/(N \times M) \cong A/N.$$

Außerdem ist M eine echte Untergruppe von B, da sonst $\{e\} \times B \leq U$ gelten würde.

Sei R das auflösbare Radikal von A. Nach Lemma II.3.5 gilt $N \leq R$, da (n, p) *unexceptional* ist, weshalb $(A/N)/(R/N) \cong A/R \cong \mathrm{P}\Sigma(n, p)$ nach Lemma II.3.4 folgt. Die letzte Isomorphie ist durch Lemma II.3.4 gerechtfertigt.

Wir wollen nun zeigen, dass A/R bis auf Isomorphie eine Section von $\Sigma(n, r)$ ist. Dies wäre nach Lemma II.3.9 ein Widerspruch, da (n, p) *unexceptional* ist.

Wir wollen zunächst einen Normalteiler Q finden, sodass $A/R \cong B/Q$ gilt. Nach dem obigen Teil gibt es einen Isomorphismus $\psi \colon A/N \to B/M$. Gleichzeitig hat der Homomorphismus $\varphi \colon A/N \to A/R;\ aN \mapsto aR$ nach [14, I.3.10 c)] den Kern R/N. Wir definieren $Q := \psi(R/N)$. Es gilt nun, dass $\varphi \circ \psi^{-1}$ surjektiv ist und $\mathrm{Kern}(\varphi \circ \psi^{-1}) = \psi(R/N)$, weshalb Q ein Normalteiler ist und $A/R \cong (B/M)/Q$ gilt. Wir haben oben gesehen, dass $N \leq R$ gilt, weshalb wir Lemma II.3.10 (i) auf R/N anwenden können. Daher ist R/N das auflösbare Radikal von A/N. Indem wir nun Lemma II.3.10 (ii) auf R/N anwenden, erhalten wir, dass Q das auflösbare Radikal von B/M ist. Sei R' das auflösbare Radikal von B. Wir machen eine Fallunterscheidung

Fall $M \leq R'$: Nach Lemma II.3.10 (i) folgt nun $Q = R'/M$. Hieraus folgt

$$A/R \cong (B/M)/Q \cong (B/M)/(R'/M) \cong (B/R').$$

Es gilt außerdem

$$(\Sigma(n, r^b)/R') \cong \mathrm{P}\Sigma(n, r) = \Sigma(n, r)/Z_{\Sigma(n,r)},$$

wobei die Isomorphie durch Lemma II.3.4 gerechtfertigt ist. Also ist A/R isomorph zu einer Untergruppe von $\Sigma(n, r)/Z_{\Sigma(n,r)}$. Nach [14, I.3.10 a)] gibt es daher eine Untergruppe $C \leq \Sigma(n, r)$ mit $A/R \cong C/Z_{\Sigma(n,r)}$. Also ist A/R eine Section von $\Sigma(n, r)$.

Fall $M \not\leq R'$: Da M ein echter Normalteiler ist, folgt nach Lemma II.3.5, dass $\Sigma(n, r^b) = \mathrm{Sp}(4, 2^b)$ und $[\Sigma(n, r^b) : M] = 2$ sein muss. Daher hat B/M maximal zwei Elemente. Da wir oben $A/R \cong (B/M)/Q$ gezeigt haben, folgt nun, dass auch $A/R \cong \mathrm{P}\Sigma(n, p)$ maximal zwei Elemente hat. Nach [14, II.6.2 und II.9.12] hat die Gruppe $\mathrm{P}\Sigma(n, p)$ aber mehr als zwei Elemente, weshalb dieser Fall nicht eintreten kann.

Wir haben also den Fall $q = r^b$ gezeigt. Wir wollen nun die Aussage für ein beliebiges q per struktureller Induktion der Primfaktorisierung $q = q_1^{a_1} \cdots q_k^{a_k}$ zeigen.

Induktionsanfang $q = q_1^{a_1}$: Siehe oben.

Induktionsvoraussetzung: Für $U \leq \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_q)$ mit $q = q_1^{a_1} \cdots q_k^{a_k}$ gilt $\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n,\mathbb{Z}_q)}\} \leq U$.

Induktionsschritt $q = q_1^{a_1} \cdots q_k^{a_k} \cdot q_{k+1}^{a_{k+1}}$: Wir definieren $s := q_1^{a_1} \cdots q_k^{a_k}$. Sei $U \leq \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_q)$ mit $\pi_1(U) = \Sigma(n, \mathbb{Z}_{p^a})$ und $D := \Sigma(n, \mathbb{Z}_{q_{k+1}^{a_{k+1}}})$. Dann ist U nach Lemma II.3.6 isomorph zu einer Untergruppe U' von $\Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_s) \times D$. Wir bezeichnen mit

$$\pi_{1,3} \colon \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_s) \times D \to \Sigma(n, \mathbb{Z}_{p^a}) \times D;\ (a, b, c) \mapsto (a, c)$$

die Projektion auf die Koordinaten 1 und 3. Offensichtlich gilt $\pi_1(\pi_{1,3}(U)) = \Sigma(n, \mathbb{Z}_{p^a})$, weshalb $\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_D\} \leq \pi_{1,3}(U)$ nach der obigen Rechnung gilt. Es gibt also für jedes $a \in \Sigma(n, \mathbb{Z}_{p^a})$ ein $b \in \Sigma(n, \mathbb{Z}_s)$ mit $(a, b, e) \in U'$.

Wir betrachten die Gruppe $V := U' \cap \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_s) \times \{e_D\}$. Sei $a \in \Sigma(n, \mathbb{Z}_{p^a})$, dann gibt es nach dem letzten Paragraphen ein $b \in \Sigma(n, \mathbb{Z}_s)$ mit $(a, b, e) \in U'$. Also gilt $\pi_1(V) = \Sigma(n, \mathbb{Z}_{p^a})$. Wir definieren analog zu $\pi_{1,3}$ die Funktion

$$\pi_{1,2} \colon \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_s) \times D \to \Sigma(n, \mathbb{Z}_{p^a}) \times \Sigma(n, \mathbb{Z}_s);\ (a, b, c) \mapsto (a, b).$$

Da $\pi_1(V) = \pi_1(\pi_{1,2}(V))$ gilt, folgt nach Induktionsvoraussetzung

$$\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n,\mathbb{Z}_s)}\} \leq \pi_{1,2}(V).$$

Dadurch, dass alle Element in V die Form (a, b, e_D) haben, erhalten wir nun

$$\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n,\mathbb{Z}_s)}\} \times \{e_D\} \leq V \leq U'.$$

Nach der Isomorphie aus Lemma II.3.6 folgt $\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n,\mathbb{Z}_q)}\} \leq U$. □

4. Der Zusammenhang von $\pi(M)$ und $\Pi(H)$ im *unexceptional* Fall

Wir wollen nun die Ergebnisse der letzten beiden Abschnitte zusammentragen, um zu zeigen, dass $\pi(M) = \Pi(H)$ im *unexceptional* Fall gilt.

Lemma II.4.1 (aus [7, Lemma 2.13]): *Sei $n > 2$ und $H \leq \Sigma(n, \mathbb{Z})$ arithmetisch von Level $M > 1$. Ist (p, n)* unexceptional *und $p \notin \Pi(H)$, folgt $p \notin \pi(M)$.*

Beweis: Die Beweisidee ist, dass wir M als $M = p^a q$ darstellen. Nun verwenden wir Theorem II.2.2, um zu zeigen, dass $\varphi_{p^a}(H) = \Sigma(n, \mathbb{Z}_{p^a})$ gilt. Anschließend verwenden wir Lemma II.3.11, um p^a von q zu trennen. Wir zeigen zunächst per Induktion, dass für alle k bereits $\varphi_{p^k}(H) = \Sigma(n, \mathbb{Z}_{p^k})$ gilt.

Induktionsanfang $k = 1$: Gilt nach Voraussetzung.

Induktionsvoraussetzung: Es gelte $\varphi_{p^{k-1}}(H) = \Sigma(n, \mathbb{Z}_{p^{k-1}})$.

Induktionsschritt $k - 1 \to k$: Wir wollen zeigen, dass $\varphi_{p^k}(H)$ ein Supplement von $K_{p^k,p^{k-1}}$ ist. Daraus folgt sofort, dass $\varphi_{p^k}(H)$ bereits alles ist, da es nach Theorem II.2.2 kein echtes Supplement geben kann. Wir müssen also $\varphi_{p^k}(H)K_{p^k,p^{k-1}} = \Sigma(n, \mathbb{Z}_{p^k})$ zeigen. Nach dem Homomorphiesatz gilt

$$\Sigma(n, \mathbb{Z}_{p^k})/K_{p^k,p^{k-1}} \cong \Sigma(n, \mathbb{Z}_{p^{k-1}}) \overset{\text{I.V.}}{=} \varphi_{p^{k-1}}(H) = \varphi_{p^k,p^{k-1}}(\varphi_{p^k}(H)).$$

Nach Lemma II.1.12 folgt nun $\varphi_{p^k}(H)K_{p^k,p^{k-1}} = \Sigma(n, \mathbb{Z}_{p^k})$. Also ist die Induktion gezeigt. Insbesondere gilt $\varphi_{p^a}(H) = \Sigma(n, \mathbb{Z}_{p^a})$. Wir fahren nun mit einer Fallunterscheidung fort, um zu zeigen, dass $p \notin \pi(M)$ gilt.

Fall $M = p^a$: Da $\Gamma_{n,p^a} \leq H$, $\Sigma(n, \mathbb{Z})$ und $\varphi_{p^a}(H) = \Sigma(n, \mathbb{Z}_{p^a}) = \varphi_{p^a}(\Sigma(n, \mathbb{Z}))$ gilt, folgt $H = \Sigma(n, \mathbb{Z})$ nach Lemma II.1.12. Dies kann nicht sein, da nach Voraussetzung $M > 1$ gilt.

Fall $M = p^a q$ mit $p \nmid q$ und $q \geq 1$: Sei $\psi\colon \Sigma(n, p^a q) \to \Sigma(n, p^a) \times \Sigma(n, q)$ die Isomorphie aus Lemma II.3.6. Sei $U := \varphi_{p^a q}(H)$ und $U' := \psi(U) \leq \varphi_{p^a}(U) \times$

$\varphi_q(U)$. Wegen der Konstruktion der Isomorphie und der obigen Induktion folgt $\pi_1(U') = \varphi_{p^a q, p^a}(U) = \varphi_{p^a}(H) = \Sigma(n, \mathbb{Z}_{p^a})$, weshalb wir Lemma II.3.11 auf U' anwenden können. Wir erhalten daher $\Sigma(n, \mathbb{Z}_{p^a}) \times \{e\} \leq U'$. Es gilt außerdem

$$\psi(\Gamma_{n,q}) = \Sigma(n, p^a) \times \{e\} \leq U' = \psi(U),$$

woraus $\Gamma_{n,q} \leq H$ folgt. Daher muss $a = 0$ wegen der Minimalität von M sein. □

Theorem II.4.2: *Sei $H \leq \Sigma(n, \mathbb{Z})$ arithmetisch, p eine Primzahl und (n, p)* unexceptional*, dann gilt $p \in \pi(M) \Leftrightarrow p \in \Pi(H)$.*

Beweis: Nach Lemma II.1.6 gilt die Rückrichtung immer, auch wenn (n, p) *exceptional* ist. Die Hinrichtung wurde in Lemma II.4.1 bewiesen. □

5. Ein Test für die Primzahl 2

Wir sehen, dass immer $\Pi(H) \subseteq \pi(M)$, gilt und $\pi(M) \subseteq \Pi(H)$ dann gilt, falls es keine Primzahl p in $\pi(M)$ gibt, sodass (n, p) *exceptional* ist. Nach Definition von *unexceptional* ist aber die einzige kritische Primzahl die 2, weshalb wir im Folgenden einen Test entwickeln wollen, welcher $2 \in \pi(M)$ testet. Hierfür benötigen wir aber zunächst eine Hilfsfunktion.

Definition II.5.1: Sei $H \leq \Sigma(n, \mathbb{Z})$ und $n > 2$. Wir definieren die Funktion

$$\delta_H(m) := [\Sigma(n, \mathbb{Z}) : \Gamma_{n,m} H] = [\Sigma(n, \mathbb{Z}_m) : \varphi_m(H)].$$

Die Idee hinter dieser δ-Funktion ist, dass wir nur dann Probleme durch das Projizieren nach $\mathbb{Z}_m$ bekommen, wenn der Kern $\Gamma_{n,m}$ nicht in unserer Gruppe liegt. Also fügen wir den Kern zur Gruppe hinzu. Daher müssen wir den Index nur über eine endliche Gruppe bestimmen. Wir wollen zunächst einige Eigenschaften der δ-Funktion sammeln.

Lemma II.5.2 (aus [7, Lemma 2.16]):

(a) *Wenn $m \mid m'$ gilt, dann folgt $\delta_H(m) \mid \delta_H(m')$.*

(b) *Sei H von Level M. Es gilt also $\delta_H(M) = [\Sigma(n, \mathbb{Z}) : H]$, dann folgt für alle $m \in \mathbb{N}$:*

  (i) *$\delta_H(m) \mid \delta_H(M)$.*

  (ii) *$\delta_H(m) = \delta_H(M)$ genau dann, wenn $M \mid m$ gilt.*

Beweis: (a) Aus $m \mid m'$ folgt $\Gamma_{n,m'} \leq \Gamma_{n,m}$. Daher gilt $\Gamma_{n,m'}H \leq \Gamma_{n,m}H$, weshalb $[\Sigma(n,\mathbb{Z}) : \Gamma_{n,m}H]$ ein Teiler von $[\Sigma(n,\mathbb{Z}) : \Gamma_{n,m'}H]$ ist.

(b) (i) Es gilt $\Gamma_{n,M}H = H \leq \Gamma_{n,m}H$ für alle m, weshalb $[\Sigma(n,\mathbb{Z}) : \Gamma_{n,m}H]$ ein Teiler von $[\Sigma(n,\mathbb{Z}) : \Gamma_{n,M}H]$ ist.

(ii) Angenommen es gilt $\delta_H(m) = \delta_H(M)$, dann muss $H = \Gamma_{n,m}H$ gültig sein. Aus der Minimalität von M und Lemma II.1.5 folgt nun $M \mid m$.

□

Theorem II.5.3 (aus [7, Lemma 2.17]): *Sei $n > 2$ und $H \leq \Sigma(n,\mathbb{Z})$ arithmetisch von Level $M > 1$. Sei q das Produkt aller ungeraden Primzahlen in $\Pi(H)$. Dann gilt $2 \in \pi(M)$ genau dann, wenn $\delta_H(q) < \delta_H(4q)$ gilt.*

Beweis: Wir beweisen die Rüchrichtung der Äquivalenz per Kontraposition. Sei also $2 \notin \pi(M)$. Wir wissen, dass $\Pi(H)$ eine Teilmenge von $\pi(M)$ ist (siehe Theorem II.1.6), daher muss q bereits M teilen. Es gilt daher $\operatorname{ggt}(4q, M) = q$, weshalb $\Gamma_{n,4q}\Gamma_{n,M} = \Gamma_{n,q}$ nach Lemma II.1.4 gilt. Es folgt nun

$$\begin{aligned}\delta_H(q) &= [\Sigma(n,\mathbb{Z}) : \Gamma_{n,q}H] = [\Sigma(n,\mathbb{Z}) : \Gamma_{n,4q}\Gamma_{n,M}H] \\ &= [\Sigma(n,\mathbb{Z}) : \Gamma_{n,4q}H] = \delta_H(4q).\end{aligned}$$

Für die Hinrichtung nehmen wir an, dass $M = 2^\ell s$ gerade ist, wobei s ungerade ist. Wir betrachten zunächst den Fall, dass $2 \leq \ell$ gilt.

Angenommen es gilt $\delta_H(2q) = \delta_H(4q)$, dann folgt $\delta_H(2s) = \delta_H(2^\ell s)$ nach Lemma III.1.1 (ii). Da $M = 2^\ell s$ gilt, folgt nun $2s = M$ nach Lemma II.5.2 (b) (ii). Da dies nicht sein kann, muss $\delta_H(q) \leq \delta_H(2q) < \delta_H(4q)$ sein.

Wir betrachten also den Fall $M = 2s$. Wir wählen das kleinste Vielfache r von q, welches s teilt, sodass $\delta_H(r) < \delta_H(2r)$ gilt. Sei $m = 2r$, $A = \varphi_2(H), B = \varphi_r(H)$, $L = \varphi_m(\Gamma_{n,2} \cap H)$ und $N = \varphi_m(\Gamma_{n,r} \cap H)$.

Wir betrachten zunächst den Fall, dass $A \neq \Sigma(n,2)$ gilt. Hieraus folgt $\varphi_4(H) \neq \Sigma(n,\mathbb{Z}_4)$. Es gilt nun, dass $\delta_H(q) < \delta_H(4q)$ ist. Wären die Werte gleich, so würde $[\Gamma_n : \Gamma_{n,q}H] = [\Gamma_n : \Gamma_{n,4q}H]$ folgen. Da $\Gamma_{n,4q} \leq \Gamma_{n,q}$ gilt, folgt nun $\Gamma_{n,q}H = \Gamma_{n,4q}H$. Es gilt nun $\varphi_4(\Gamma_{n,4q}H) = \varphi_4(H) \neq \Sigma(n,\mathbb{Z}_4)$ nach Voraussetzung, andererseits gilt

$$\begin{aligned}\varphi_4(\Gamma_{n,4q}H) &= \varphi_4(\Gamma_{n,q}H) = \varphi_4(\Gamma_{n,4})\,\varphi_4(\Gamma_{n,q}H) \\ &= \varphi_4(\Gamma_{n,4}\Gamma_{n,q}H) = \varphi_4(\Gamma_{n,1}H) = \Sigma(n,\mathbb{Z}_4),\end{aligned}$$

was ein Widersprich ist.

Wir können nun den Fall $A = \Sigma(n,2) = \varphi_2(H)$ betrachten. Wir wollen $A/\varphi_{m,2}(N) \cong B/\varphi_{m,r}(L)$ zeigen. Wir definieren den Isomorphismus

$$\begin{aligned}\Psi\colon \varphi_2(H)/\varphi_2(\Gamma_{n,r}\cap H) &\to \varphi_r(H)/\varphi_r(\Gamma_{n,2}\cap H);\\ \varphi_2(x)\varphi_2(\Gamma_{n,r}\cap H) &\mapsto \varphi_r(x)\varphi_r(\Gamma_{n,2}\cap H).\end{aligned}$$

Wir überprüfen die Wohldefiniertheit dieser Funktion. Seien $x,\, y \in H$ mit $\varphi_2(x)\varphi_2(\Gamma_{n,r}\cap H) = \varphi_2(y)\varphi_2(\Gamma_{n,r}\cap H)$, dann gibt es ein $n \in \Gamma_{n,r}\cap H$ mit $\varphi_2(y)\varphi_2(n) = \varphi_2(x)$. Daraus folgt $x^{-1}yn \in \Gamma_{n,2}\cap H$. Es folgt nun

$$\begin{aligned}\varphi_r(x)\varphi_r(\Gamma_{n,r}\cap H) &= \varphi_r(x(\Gamma_{n,2}\cap H)) = \varphi_r(x(x^{-1}yn)(\Gamma_{n,2}\cap H))\\ &= \varphi_r(y)\varphi_r(n)\varphi_r(\Gamma_{n,2}\cap H) = \varphi_r(y)\varphi_r(\Gamma_{n,2}\cap H).\end{aligned}$$

Also ist die Funktion wohldefiniert. Da φ_2 und φ_r Homomorphismen sind, ist auch Ψ einer. Man kann die Umkehrfunktion Ψ^{-1} analog zu Ψ definieren, weshalb Ψ ein Isomorphismus ist.

Sei $K = \varphi_r(H\cap\Gamma_{n,q})$. Wir werden weiter unten $K\varphi_{m,r}(L) \neq B$ zeigen. Hieraus folgt, dass $\varphi_{2q}(H)$ eine echte Untergruppe von $\varphi_2(H)\times\varphi_q(H) = \Sigma(n,2)\times\varphi_q(H)$ ist. Hierfür betrachten wir den Isomorphismus Ψ^{-1}. Da $K\varphi_{m,r}(L) \neq B$ ist, ist $K\varphi_{m,r}(L)/\varphi_{m,r}(L)$ eine echte Untergruppe von $B/\varphi_{m,r}(L)$ und daher auch

$$\Psi^{-1}(K\varphi_{m,r}(L)/\varphi_{m,r}(L)) = (\varphi_2(H\cap\Gamma_{n,q})\varphi_2(H\cap\Gamma_{n,2}))\,/\,\varphi_{m,2}(N).$$

Hieraus folgt nun $\varphi_2(H\cap\Gamma_{n,q})\varphi_2(H\cap\Gamma_{n,2}) < A = \varphi_2(H)$. Wir nehmen an, dass $\varphi_{2q}(H) \cong \varphi_2(H)\times\varphi_q(H)$ gilt, dann müsste $\varphi_2(H)\times\{e_{\Sigma(n,\mathbb{Z}_q)}\}$ in $\varphi_{2q}(H)$ liegen. Offensichtlich ist dies das Bild von $\varphi_{2q}(\Gamma_{n,q}\cap H) \cong \varphi_2(\Gamma_{n,q}\cap H)\times\{e_{\Sigma(n,\mathbb{Z}_q)}\}$. Es gilt aber nach oben

$$\varphi_2(H) > \varphi_2(H\cap\Gamma_{n,q}),$$

weshalb $\varphi_{2q}(H)$ eine echte Untergruppe von $\varphi_2(H)\times\varphi_q(H)$ sein muss.

Es gilt also $|\varphi_{2q}(H)| < |\Sigma(n,2)||\varphi_q(H)|$, woraus

$$\delta_H(2q) = \frac{|\Sigma(n,2q)|}{|\varphi_{2q}(H)|} > \frac{|\Sigma(n,q)||\Sigma(n,2)|}{|\Sigma(n,2)||\varphi_q(H)|} = \frac{|\Sigma(n,q)|}{|\varphi_q(H)|} = \delta_H(q)$$

folgt. Es gilt daher $\varphi_H(q) < \varphi_H(2q) \leq \varphi_H(4q)$, was wir zeigen wollten.

Es bleibt also $K\varphi_{m,r}(L)B \neq B$ zu zeigen. Zunächst ist $\varphi_{m,2}(N)$ ein echter Normalteiler von A. Angenommen dies wäre nicht der Fall, dann könnten wir

$$\begin{aligned} &\Gamma_{n,r} \leq \Sigma(n,\mathbb{Z}) \overset{(1)}{=} (\Gamma_{n.r} \cap H)\Gamma_{n,2} \\ \overset{(2)}{\Rightarrow}\ &\Gamma_{n,r} \leq (\Gamma_{n,r} \cap H)(\Gamma_{n,2} \cap \Gamma_{n,r}) \\ \overset{(3)}{\Rightarrow}\ &\Gamma_{n,r} \leq (\Gamma_{n,r} \cap H)\Gamma_{n,m} \\ \overset{(4)}{\Rightarrow}\ &\delta_H(r) = \delta_H(m) \end{aligned}$$

folgern. Hierbei folgt (1), da wir annehmen, dass

$$\varphi_{m,2}(N) = \varphi_2(\Gamma_{n,r} \cap H) = A = \Sigma(n,\mathbb{Z}_2)$$

gilt und daher $\Sigma(n,\mathbb{Z})/\Gamma_{n,2} = (\Gamma_{n,r} \cap H)/\Gamma_{n,2}$, woraus $\Sigma(n,\mathbb{Z}) = (\Gamma_{n,r} \cap H)\Gamma_{n,2}$ nach Lemma II.1.12 folgt.

Die Implikation (2) gilt, da wir für alle $x \in \Gamma_{n,r}$ zwei Elemente $a \in (\Gamma_{n,r} \cap H)$ und $b \in \Gamma_{n,2}$ finden können mit $x = ab$. Es gilt nun

$$e_{\Sigma(n,\mathbb{Z}_r)} = \varphi_r(x) = \varphi_r(a)\varphi_r(b) = e_{\Sigma(n,\mathbb{Z}_r)}\varphi_r(b) = \varphi_r(b),$$

weshalb $b \in \Gamma_{n,2} \cap \Gamma_{n,r}$ sein muss.

Schritt (3) folgt direkt aus Lemma II.1.4 (ii). Die Implikation (4) folgt, da

$$\Gamma_{n,r}H \leq (\Gamma_{n,r} \cap H)\Gamma_{n,m}H = (\Gamma_{n,r} \cap H)H\Gamma_{n,m} = H\Gamma_{n,m} = \Gamma_{n,m}H$$

gilt.

Hieraus folgt $\delta_H(r) \geq \delta_H(m)$. Gleichzeitig gilt nun $\delta_H(r) \leq \delta_H(m)$, da $\Gamma_{n,m} \leq \Gamma_{n,r}$ ist. Insgesamt gilt also $\delta_H(r) = \delta_H(m)$, was ein Widerspruch zur Wahl von r ist. Wir können daher annehmen, dass $\varphi_{m,2}(N)$ ein echter Normalteiler ist. Hierbei folgt die Normalität in A aus

$$\varphi_{m,2}(N) = \varphi_2(\Gamma_{n,r} \cap H) = \varphi_2(\Gamma_{n,r}) \cap A = \varphi_2(\Gamma_{n,r}).$$

Da φ_2 surjektiv ist und $\Gamma_{n,r}$ normal ist, ist auch $\varphi_{m,2}(N)$ in A normal.

Wir können nun eine Fallunterscheidung machen, wobei wir zunächst annehmen, dass $A/\varphi_{m,2}(N)$ auflösbar ist. Dann darf $\varphi_{m,2}(N)$ nicht auflösbar sein, da sonst A auflösbar wäre, was aber nicht sein kann, weil $A = \Sigma(n,2) \cong \mathrm{P}\Sigma(n,2)$ (ausgenommen $A = \mathrm{Sp}(4,2)$) nach [14, II.6.13 und II.9.22] nicht auflösbar ist (man beachte, dass in diesem Fall das Zentrum von $\Sigma(n,2)$ trivial ist, was die Isomorphie begründet). Da aber $\varphi_{m,2}(N)$ normal ist, entsteht ein Widerspruch zu Lemma II.3.5. Die einzige Ausnahme ist der Fall $A = \mathrm{Sp}(4,2)$. Da aber $\varphi_{m,2}(N)$

ein echter Normalteiler ist, folgt nach Lemma II.3.5 nun $[A : \varphi_{m,2}(N)] = 2$. Angenommen es gilt $K\varphi_{m,r}(L) = B$, dann gilt wegen der obigen Isomorphie

$$\frac{|A|}{|\varphi_{m,2}(N)|} = \frac{|B|}{|\varphi_{m,r}(L)|} = 2 \Rightarrow |B| = 2\varphi_{m,r}(L) \Rightarrow |K| = 2.$$

Es gilt aber, dass die Ordnung von K ungerade ist. Dies gilt, da die Ordnung von $\varphi_r(\Gamma_{n,q})$ ungerade ist, woraus folgt, dass die Ordnung von K ungerade sein muss, da $K = \varphi_r(H \cap \Gamma_{n,q}) \leq \varphi_r(H) \cap \varphi_r(\Gamma_{n,q})$ nach Konstruktion eine Untergruppe von $\varphi_r(\Gamma_{n,q})$ ist. Sei $r = q_1^{a_1} \cdots q_t^{a_t}$ die Primzahlzerlegung von r. Nach Voraussetzung gilt $q = q_1 \cdots q_t$ und

$$\varphi_r(\Gamma_{n,q}) \leq \varphi_{q_1^{a_1}}(\Gamma_{n,q}) \times \ldots \times \varphi_{q_t^{a_t}}(\Gamma_{n,q}) \leq K_{q_1^{a_1},q_1} \times \ldots \times K_{q_t^{a_t},q_t},$$

wobei wir beim ersten $\leq$ die Isomorphie aus II.3.6 betrachten.

Nach Lemma II.1.9 und [13, Corollary 5.3] ist die Ordnung von $K_{q_c^{a_c},q_c}$ eine Potenz von q_c für $a_c \geq 2$ und somit ungerade. Für $a_c = 1$ ist die Ordnung 1. Also ist die Ordnung der Gruppe $K_{q_1^{a_1},q_1} \times \ldots \times K_{q_t^{a_t},q_t}$ ungerade, weshalb auch die Ordnung von $\varphi_r(\Gamma_{n,q})$ ungerade sein muss.

Wir betrachten nun den Fall, dass $A/\varphi_{m,2}(N)$ nicht auflösbar ist. Dann ist wegen der obigen Isomorphie auch $B/\varphi_{m,r}(L)$ nicht auflösbar und daher kann B nicht auflösbar sein. Wir wollen zeigen, dass K und $\varphi_{m,r}(L)$ auflösbar sind, woraus folgt, dass $K\varphi_{m,r}(L)$ auflösbar ist, weshalb $K\varphi_{m,r}(L) \neq B$ gilt.

Nach Voraussetzung gilt $q_k \in \Pi(H)$, weshalb

$$\varphi_{q_k^{a_k},q}(\varphi_{r,q_k^{a_k}}(\varphi_r(H))) = \varphi_q(H) \neq \Sigma(n, \mathbb{Z}_q)$$

ist. Hieraus folgt $\varphi_{r,q_k^{a_k}}(\varphi_r(H)) \neq \Sigma(n, \mathbb{Z}_{q_k^{a_k}})$ für alle $1 \leq k \leq t$ gilt. Da $\varphi_{m,r}(L), K \leq \varphi_r(H)$ gilt, folgt die Aussage nach Korollar II.3.7.

□

Theorem II.5.4 (aus [7, Theorem 2.18]): *Sei $n > 2$ und $H \leq \Sigma(n, \mathbb{Z})$ arithmetisch. Dann gilt*

$$\pi(M) = \tilde{\Pi}(H) := \begin{cases} \Pi(H) \cup \{2\}, & \textit{falls } n \leq 4 \textit{ und } \delta_H(4q) > \delta_H(q), \\ \Pi(H), & \textit{falls } n > 4. \end{cases}$$

Beweis: Folgt direkt aus Theorem II.4.2 und II.5.3. □

Kapitel III.

Algorithmen zur Berechnung von M und zur Überprüfung der Dichtheit

Im gesamten Kapitel gilt immer $n \geq 3$.

1. Die Berechnung von M mittels $\pi(M)$

Ziel dieses Abschnittes ist es, einen Algorithmus zu entwickeln, welcher aus den Primfaktoren $\pi(M)$ das Level M bestimmen kann. Hierbei ist die Grundidee des Algorithmus sehr simpel. Wir betrachten die Funktion δ_H (siehe Definition II.5.1) und erhöhen solange den Exponenten eines Primteilers, bis die Werte der Funktion δ_H stagnieren. Allerdings müssen wir hierbei beachten, dass beim Erhöhen eines Primfaktors auch alle anderen Primfaktoren mindestens mit der Potenz 1 berücksichtigt werden, damit der Algorithmus korrekt arbeiten kann. Dieser Umstand wird durch das nächste Lemma deutlich, welches zeigt, dass wir mit dem Berechnen aufhören können, wenn der Wert von δ_H zum ersten Mal stagniert.

Lemma III.1.1 (aus [7, Lemma 2.19]): (i) *Sei p eine Primzahl und koprim zu k. Wenn $\delta_H(kp^a) = \delta_H(kp^{a+1})$ gilt, dann folgt $\delta_H(kp^b) = \delta_H(kp^a)$ für alle $b \geq a \geq 1$.*

(ii) *Seien a, p und k die gleichen Werte wie in* (i)*, dann gilt $\delta_H(lp^b) = \delta_H(lp^a)$ für alle $b \geq a$. Hierbei ist l ein beliebiges Vielfaches von k mit $\pi(l) = \pi(k)$.*

Beweis: (i) Angenommen die Aussage wäre falsch, dann gäbe es ein minimales $b > a+1$ mit der Eigenschaft $\delta_H(kp^b) \neq \delta_H(kp^a)$ und $\delta_H(kp^{b-2}) = \delta_H(kp^{b-1}) = \delta_H(kp^a)$. Es gilt also $[\Sigma(n,\mathbb{Z}) : \Gamma_{n,kp^{b-2}}H] = [\Sigma(n,\mathbb{Z}) : \Gamma_{n,kp^{b-1}}H]$. Da $\Gamma_{n,kp^{b-1}}H \leq \Gamma_{n,kp^{b-2}}H$ gilt und der Index gleich ist, folgt

nun $\Gamma_{n,kp^{b-2}}H = \Gamma_{n,kp^{b-1}}H$. Hieraus folgt $\Gamma_{n,kp^{b-2}} \leq \Gamma_{n,kp^{b-1}}H$, was impliziert, dass $\Gamma_{n,kp^{b-2}} \cap H$ ein echtes Supplement von $\Gamma_{n,kp^{b-1}}$ in $\Gamma_{n,kp^{b-2}}$ ist. Es gilt nämlich

$$(\Gamma_{n,kp^{b-2}} \cap H)\Gamma_{n,kp^{b-1}} = \underbrace{\Gamma_{n,kp^{b-2}}\Gamma_{n,kp^{b-1}}}_{=\Gamma_{n,kp^{b-2}}} \cap \underbrace{\Gamma_{n,kp^{b-1}}H}_{\geq\Gamma_{n,kp^{b-2}}} = \Gamma_{n,kp^{b-2}}, \quad \text{(III.1)}$$

wobei die erste Gleichung nach Lemma II.1.11 gilt. Es ist ein echtes Supplement, da sonst $\Gamma_{n,kp^b} \subseteq \Gamma_{n,kp^{b-2}} \subseteq H$ gelten würde, woraus $\delta_H(kp^{b-2}) = \delta_H(kp^b)$ folgen würde.

Da k und p^c für alle $c \geq 1$ teilerfremd sind, können wir die Isomorphie $\Sigma(n, \mathbb{Z}_{kp^c}) \cong \Sigma(n, \mathbb{Z}_{p^c}) \times \Sigma(n, \mathbb{Z}_k)$ aus Lemma II.3.6 verwenden. Hieraus folgt nun

$$\Gamma_{n,kp^{b-2}}/\Gamma_{n,kp^b} \cong (\Gamma_{n,p^{b-2}} \times \Gamma_{n,k})/(\Gamma_{n,p^b} \times \Gamma_{n,k}) \cong \Gamma_{n,p^{b-2}}/\Gamma_{n,p^b}.$$

Nach dem selben Isomorphismus gilt $\Gamma_{n,kp^{b-1}}/\Gamma_{n,kp^b} \cong \Gamma_{n,p^{b-1}}/\Gamma_{n,p^b}$. Es gilt außerdem $\Gamma_{n,p^{b-1}}/\Gamma_{n,p^b} \cong K_{p^b,p^{b-1}}$, was man daran sehen kann, dass $\varphi_{p^b}(\Gamma_{n,p^{b-1}}) = K_{p^b,p^{b-1}}$ gilt, was direkt aus $\varphi_{p^{b-1}} = \varphi_{p^b,p^{b-1}} \circ \varphi_{p^b}$ folgt. Analog folgt $\Gamma_{n,p^{b-2}}/\Gamma_{n,p^b} \cong K_{p^b,p^{b-2}}$. Nach Gleichung (III.1) folgt

$$((\Gamma_{n,kp^{b-2}} \cap H)\Gamma_{n,kp^b})/\Gamma_{n,kp^b} \cdot \underbrace{\Gamma_{n,kp^{b-1}}/\Gamma_{n,kp^b}}_{\cong K_{p^b,p^{b-1}}} = \Gamma_{n,kp^{b-2}}/\Gamma_{n,kp^b} \cong K_{p^b,p^{b-2}}.$$

Dies würde aber bedeuten, dass $K_{p^b,p^{b-1}}$ ein echtes Supplement in $K_{p^b,p^{b-2}}$ hätte, was nach Lemma II.2.5 nicht möglich ist. Man bedenke hierbei, dass $(\Gamma_{n,kp^{b-2}} \cap H)\Gamma_{n,kp^b})/\Gamma_{n,kp^b}$ isomorph zu einem echten Supplement ist, da sonst $\Gamma_{n,kp^b}H = \Gamma_{n,kp^{b-2}}$ gälte, woraus $\delta_H(kp^{b-2}) = \delta_H(kp^b)$ folgte.

(ii) Angenommen es gäbe ein $b \geq a$ und ein Vielfaches ℓ von k mit $\pi(\ell) = \pi(\ell)$, sodass $\delta_H(\ell p^b) \neq \delta_H(\ell p^{b+1})$ gilt, dann folgte $\delta_H(kp^b) = \delta_H(kp^{b+1})$ nach (i). Wir definieren $\overline{H} = \Gamma_{n,kp^b} \cap \Gamma_{n,\ell p^{b+1}}H$. Es gilt nun

$$\Gamma_{n,kp^{b+1}}\overline{H} \overset{\text{II.1.11}}{=} \Gamma_{n,kp^b} \cap \Gamma_{n,kp^b}\Gamma_{n,k\ell^{b+1}}H \overset{\text{II.1.4 (i)}}{=} \Gamma_{n,kp^b} \cap \Gamma_{n,kp^b}H = \Gamma_{n,kp^b}. \quad \text{(III.2)}$$

Wir betrachten nun die Isomorphie

$$\Gamma_{n,kp^b}/\Gamma_{n,\ell p^{b+1}} \cong \Gamma_{n,\ell p^b}/\Gamma_{n,\ell p^{b+1}} \times \Gamma_{n,kp^{b+1}}/\Gamma_{n,\ell p^{b+1}}, \quad \text{(III.3)}$$

welche wir wie folgt begründen. Da $\Gamma_{n,kp^b} = \Gamma_{n,\ell p^b}\Gamma_{n,kp^{b+1}}$ (siehe Lemma II.1.4 (i)) gilt, können wir ein Element $x \in \Gamma_{n,kp^b}$ als $x = yz$ mit

$y \in \Gamma_{n,\ell p^b}$ und $z \in \Gamma_{n,kp^{b+1}}$ darstellen. Hieraus können wir nun einen Isomorphismus für (III.3) bauen, wobei man bedenkt, dass $\Gamma_{n,\ell p^{b+1}} = \Gamma_{n,\ell p^b} \cap \Gamma_{n,kp^{b+1}}$ nach Lemma II.1.4 (ii) gilt. Wir bemerken, dass $\overline{H}/\Gamma_{n,\ell p^{b+1}}$ eine echte Untergruppe ist, da sonst $\Gamma_{n,kp^b} = \overline{H}$ nach [14, I.3.10 a)] folgte. Hieraus würde aber $\Gamma_{n,\ell p^b} \subseteq \Gamma_{n,kp^b} \subseteq \Gamma_{n,\ell p^{b+1}} H$ folgen, weshalb dann $\delta_H(\ell p^b) = \delta_H(\ell p^{b+1})$ gälte. Es gilt also

$$\overline{H}/\Gamma_{n,\ell p^{b+1}} \leq A/\Gamma_{n,\ell p^{b+1}} \times B/\Gamma_{n,\ell p^{b+1}},$$

wobei wir hier mit $\leq$ die Isomorphie aus (III.3) meinen und $A/\Gamma_{n,\ell p^{b+1}}$ eine echte Untergruppe von $\Gamma_{n,\ell p^b}/\Gamma_{n,\ell p^{b+1}}$ ist. Ansonsten würde $\overline{H} \geq \Gamma_{n,\ell p^b}$ gelten, woraus $\Gamma_{n,\ell p^b} \subseteq \Gamma_{n,\ell p^{b+1}} H$ und daher $\delta_H(\ell p^b) = \delta_H(\ell p^{b+1})$ folgte.

Wir können also eine echte Untergruppe $K < \Gamma_{n,\ell p^b}$ finden mit

$$K/\Gamma_{n,\ell p^{b+1}} \cong A/\Gamma_{n,\ell p^{b+1}} \times \{e_{\Gamma_{n,kp^{b+1}}/\Gamma_{n,\ell p^{b+1}}}\}. \tag{III.4}$$

Nach Konstruktion gilt nun $K \cap \Gamma_{n,kp^{b+1}} = \Gamma_{n,\ell p^{b+1}}$, woraus

$$\Gamma_{n,kp^{b+1}} K/\Gamma_{n,\ell p^{b+1}} \cong A/\Gamma_{n,\ell p^{b+1}} \times \Gamma_{n,kp^{b+1}}/\Gamma_{n,\ell p^{b+1}} \cong \Gamma_{n,kp^{b+1}} \overline{H}/\Gamma_{n,\ell p^{b+1}} \tag{III.5}$$

folgt. Hierbei folgt die letzte Isomorphie aus

$$\Gamma_{n,kp^{b+1}}/\Gamma_{n,\ell p^{b+1}} \cong \{e_{\Gamma_{n,\ell p^b}/\Gamma_{n,\ell p^{b+1}}}\} \times \Gamma_{n,kp^{b+1}}/\Gamma_{n,\ell p^{b+1}}. \tag{III.6}$$

Mit Gleichung (III.2) und Isomorphien (III.5), (III.4), (III.6), (III.3) folgt

$$\begin{aligned}
\Gamma_{n,kp^b}/\Gamma_{n,\ell p^{b+1}} &= \Gamma_{n,kp^{b+1}} \overline{H}/\Gamma_{n,\ell p^{b+1}} \cong \Gamma_{n,kp^{b+1}} K/\Gamma_{n,\ell p^{b+1}} \\
&\cong A/\Gamma_{n,\ell p^{b+1}} \times \Gamma_{n,kp^{b+1}}/\Gamma_{n,\ell p^{b+1}} \\
&< \Gamma_{n,\ell p^b}/\Gamma_{n,\ell p^{b+1}} \times \Gamma_{n,kp^{b+1}}/\Gamma_{n,\ell p^{b+1}} \cong \Gamma_{n,kp^b}/\Gamma_{n,\ell p^{b+1}},
\end{aligned}$$

was ein Widerspruch ist.

□

Algorithm 1 (aus [7]): `LevelMaxPCS`(S, σ)

Input: endliche Menge S, die $H \leq \Sigma(n, \mathbb{Z})$ erzeugt, endliche Menge von Primzahlen σ

Output: N

1: **for** p in σ **do** ▷ Initialisiere Startwerte
2: $\mu_p := 1$ ▷ Potenz der Primzahl p
3: $z_p := \prod_{q \in \sigma, q \neq p} q$
4: **end for**
5: **while** $\exists\, p \in \sigma$ mit $\delta_H(p^{1+\mu_p} z_p) > \delta_H(p^{\mu_p} z_p)$ **do** ▷ Solange nicht stagniert
6: $\mu_p := \mu_p + 1$
7: **end while**
8: **return** $N := \prod_{p \in \sigma} p^{\mu_p}$

Theorem III.1.2 (aus [7, Theorem 2.22]): *Sei S endlich und $H = \langle S \rangle$, sodass H von Level M ist. Der Algorithmus* `LevelMaxPCS` *terminiert bei Eingabe S und $\pi(M)$ immer und gibt den Wert N zurück, welcher gleich M ist.*

Beweis: Wir wissen, dass δ_H durch $\delta_H(M)$ beschränkt ist, da $\delta_H(m) \mid \delta(M)$ für alle m nach Lemma II.5.2 (b) (i) gilt. Daher terminiert der Algorithmus immer.

Wir wollen nun $N \mid M$ zeigen. Sei p^a der p-Teil von M, $q \mid M$ koprim zu p und μ_p der p-Teil vom Output N (siehe Algorithmus). Wir wollen $\delta_H(p^{a+1}q) = \delta_H(p^a q)$ zeigen. Es gilt $\mathrm{ggt}(p^{a+1}q, M) = p^a q$, weshalb nun nach Lemma II.1.4

$$\begin{aligned}\delta_H(p^{a+1}q) &= [\Sigma(n,\mathbb{Z}) : \Gamma_{n,p^{a+1}q} H] = [\Sigma(n,\mathbb{Z}) : \Gamma_{n,p^{a+1}q}\Gamma_{n,M} H] \\ &= [\Sigma(n,\mathbb{Z}) : \Gamma_{n,p^a q} H] = \delta_H(p^a q)\end{aligned}$$

folgt. Also gilt $\mu_p \leq a$. Wenn wir diese Rechnung für alle Primzahlen $p \in \pi(M)$ durchführen, erhalten wir $N \mid M$.

Andererseits wollen wir $\delta_H(N) = \delta_H(M)$ zeigen. Gilt dies, dann folgt nach Lemma II.5.2 (b) (ii) bereits $M \mid N$. Um diese Gleichheit zu zeigen, stellen wir N und M bezüglich ihrer Primfaktorzerlegung da. Es gilt $N = p_1^{\mu_1} \cdots p_n^{\mu_n}$ und $M = p_1^{a_1} \cdots p_n^{a_n}$. Nach Konstruktion haben N und M die gleichen Primteiler. Da $N \mid M$ gilt, folgt bereits $\mu_j \leq a_j$ für alle $1 \leq j \leq n$. Wir definieren nun $q_1 := p_2^{\mu_2} \cdots p_n^{\mu_n}$. Da der Algorithmus terminiert hat, verändert sich $\delta_H(N)$ nicht, wenn wir ein weiteres p_1 hinzufügen. Es gilt also

$$\delta_H(N) = \delta_H(p_1^{\mu_1} q_1) = \delta_H(p_1^{1+\mu_1} q_1) \overset{\text{III.1.1 (i)}}{=} \delta_H(p_1^{a_1} q_1). \tag{III.7}$$

Wir definieren nun $q_2 := p_1^{a_1} p_3^{\mu_3} \cdots p_n^{\mu_n}$ und $q_2' := p_1^{\mu_1} p_3^{\mu_3} \cdots p_n^{\mu_n}$ und können ähnlich zur (III.7)

$$\delta_H(N) = \delta_H(p_2^{\mu_2} q_2') = \delta_H(p_2^{1+\mu_2} q_2') \overset{\text{III.1.1 (i)}}{=} \delta_H(p_2^{a_2} q_2')$$

folgern. Da $\pi(q_2) = \pi(q_2')$ und q_2 ein Vielfaches von q_2' ist, können wir nun die Gleichung (III.7) wie folgt fortsetzen:

$$= \delta_H(p_2^{\mu_2} q_2) \overset{\text{III.1.1 (ii)}}{=} \delta_H(p_2^{a_2} q_2).$$

Man kann so sukzessiv folgern, dass $\delta_H(N) = \delta_H(M)$ gilt. An dieser Stelle haben wir ausgenutzt, dass der Algorithmus in Zeile 5 mit allen Primzahlen in $\pi(M)$ rechnet. Ansonsten wären wir nicht in der Lage gewesen, q_i durch q_i' zu ersetzen. Daher ist es wichtig, dass wir immer $\delta_H(p^{\mu_p} z_p)$ berechnen, da wir sonst mit einem zu kleinen N enden könnten. Tatsächlich werden wir in Beispiel III.1.3 sehen, dass ein Algorithmus, welcher in Zeile 5 nicht mit z_p multipliziert, ein falsches Ergebnis liefert. Schlussendlich können wir nun $M \mid N$ und daher $N = M$ folgern. □

Beispiel III.1.3 (aus [7, Remark 2.1]): Wir betrachten die folgenden arithmetische Untergruppe $H \leq \mathrm{SL}(3,\mathbb{Z})$:

$$H = \left\langle \Gamma_{3,45}, \begin{pmatrix} 1 & 30 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -29 & 0 & -30 \\ 0 & 1 & 0 \\ 30 & 0 & 31 \end{pmatrix}, \begin{pmatrix} -29 & -45 & 15 \\ 30 & 1 & 30 \\ 30 & 0 & 31 \end{pmatrix}, \right.$$
$$\begin{pmatrix} 1 & 0 & 0 \\ 15 & -29 & -30 \\ 30 & 30 & 31 \end{pmatrix}, \begin{pmatrix} 16 & 15 & 0 \\ -255 & -239 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 16 & 15 & 30 \\ -255 & -239 & 15 \\ 0 & 0 & 1 \end{pmatrix},$$
$$\left. \begin{pmatrix} 1 & 0 & 30 \\ 0 & 1 & 30 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 10 & 0 & 9 \\ 36 & -137 & 66 \\ -99 & -453 & 22 \end{pmatrix} \right\rangle.$$

Es gilt $\delta_H(3) = \delta_H(9) = 5616, \delta_H(5) = \delta_H(25) = 124000, \delta_H(15) = 696384000$ und $\delta_H(45) = 2089152000$. Würden wir also in Zeile 5 nicht mit z_p multiplizieren, dann würden wir 15 als Ergebnis erhalten, obwohl das Level eigentlich 45 ist.

2. Basis der einhüllenden Algebra

In den nächsten zwei Abschnitten wollen wir einen Weg finden, die Menge $\Pi(H)$ zu berechnen. Für den Algorithmus wird die Basis der *einhüllenden Algebra* von $\langle t \rangle^H$ eine wichtige Rolle spielen. Diese wollen wir nun berechnen.

Definition III.2.1: Sei $H \subseteq \mathrm{GL}(n,\mathbb{F})$. Wir bezeichnen mit $\mathrm{span}_{\mathbb{F}}(H)$ die kleinste $\mathbb{F}$-Algebra in $\mathbb{F}^{n\times n}$, welche H beinhaltet. Wir nennen $\mathrm{span}_{\mathbb{F}}(H)$ die *einhüllende Algebra* von H.

Algorithm 2 (aus [9, Kapitel 3.1]): `BasisEnvAlgebra`(S)

Input: endliche Menge $S \subseteq \mathrm{GL}_n(n,\mathbb{F})$
Output: Basis B von $\mathrm{span}_{\mathbb{F}}(\langle S \rangle)$

1: $S' := S \cup S^{-1} \cup \{I_n\}$ ▷ $S^{-1} := \{S_i^{-1} : S_i \in S\}$
2: $B := \{I_n\}$
3: $e = 1$ ▷ Anzahl Element in B
4: **while** $\exists\, S_i \in S'$ und $B_j \in B : B_1, \ldots, B_e, B_j S_i$ linear unabhängig **do**
5: $\quad B := \{B_1, \ldots, B_e, B_j S_i\}$
6: $\quad e = e + 1$
7: **end while**
8: **return** B

Lemma III.2.2: *Der Algorithmus* `BasisEnvAlgebra` *gibt bei Eingabe einer endlichen Menge S die Basis der einhüllenden Algebra* $\mathrm{span}_{\mathbb{F}}(\langle S\rangle)$ *zurück, sofern diese endlichdimensional ist.*

Beweis: Sei $S' := S \cup S^{-1} \cup \{I_n\}$ mit $S^{-1} := \{S_i^{-1} : S_i \in S\}$. Da $\mathrm{span}_{\mathbb{F}}(\langle S\rangle)$ nach Voraussetzung endlichdimensinal ist, terminiert der Algorithmus immer und gibt eine linear unabhängige Menge $B := \{B_1, \ldots, B_n\}$ zurück. Nach Konstruktion gilt $\mathrm{span}_{\mathbb{F}}(B) \subseteq \mathrm{span}_{\mathbb{F}}(\langle S\rangle)$. Es bleibt also zu zeigen, dass die Basis B erzeugend ist. Nach Voraussetzung sind $B_1, \ldots, B_n, B_jS_i$ für alle $S_j \in S'$ und $B_j \in B$ linear abhängig, weshalb alle B_jS_i im Erzeugnis liegen. Sei

$$S^k := \bigcup_{S_i \in S'} S^{k-1}S_i \text{ mit } S^0 := \{I_n\} \text{ und } S^\infty := \bigcup_{k=0}^{\infty} S^k.$$

Offensichtlich ist $S^\infty = \langle S\rangle$, weshalb es ausreicht, $S^k \subseteq \mathrm{span}_{\mathbb{F}}(B)$ per Induktion zu zeigen.

Induktionsanfang $k = 0$: Nach Konstruktion gilt $\{I_n\} \subseteq \mathrm{span}_{\mathbb{F}}(B)$.

Induktionsvoraussetzung: Es gelte $S^k \subseteq \mathrm{span}_{\mathbb{F}}(B)$.

Induktionsschritt $k \to k+1$: Ein Elemente in S^{k+1} hat die Form CS_i mit $C \in S^k$ und $S_i \in S'$. Nach Induktionsvoraussetzung gilt $C = \sum_{j=1}^{n} \lambda_j B_j$ mit $\lambda_j \in \mathbb{F}$. Es gilt also

$$CS_i = \sum_{j=1}^{n} \lambda_j B_j S_i.$$

Da alle B_jS_i im Erzeugnis von B liegen, liegt auch CS_i im Erzeugnis, weshalb $B_1, \ldots, B_n$ eine Basis bildet. □

Algorithm 3 (aus [8]): `BasisAlgebraClosure`(K, S)

Input: endliche Mengen K und S in $\mathrm{GL}(n, \mathbb{F})$ mit $K \subseteq G$, wobei $G := \langle S\rangle$
Output: Basis der einhüllenden Algebra von $\langle K\rangle^G$

1: $S' := S \cup S^{-1} \cup \{I_n\}$
2: $B := K \cup K^{-1}$
3: **while** $\exists\, g \in S'$ und $A \in B : g^{-1}Ag \notin \mathrm{span}_{\mathbb{F}}(B)$ **do**
4: $\quad B := B \cup \{g^{-1}Ag\}$
5: **end while**
6: **return** `BasisEnvAlgebra`(B)

Lemma III.2.3: *Seien K und S endliche Mengen in* $\mathrm{GL}(n, \mathbb{F})$. *Wir definieren die Gruppe $G := \langle S\rangle$. Dann gibt der Algorithmus* `BasisAlgebraClosure` *bei*

Eingabe K und S eine Basis der einhüllenden Algebra von $\langle K\rangle^G$ zurück, sofern $\mathrm{span}_{\mathbb{F}}(\langle K\rangle^G)$ endlichdimensional ist. Hierbei ist $\langle K\rangle^G$ der normale Abschluss von $\langle K\rangle$ in G.

Beweis: Sei $K^{-1} := \{k^{-1} : k \in K\}$. Wir wollen zunächst die folgende Aussage beweisen.

Sei $K^G := \{g^{-1}kg : g \in G, k \in K \cup K^{-1}\}$, dann gilt $\langle K^G\rangle = \langle K\rangle^G$. Um $\langle K^G\rangle \supseteq \langle K\rangle^G$ zu zeigen, wollen wir nachrechnen, dass $\langle K^G\rangle$ ein Normalteiler in G ist. Hierfür reicht es aus, nachzurechnen, dass $g^{-1}(h^{-1}kh)g \in K^G$ für alle $g, h \in G$ und $k \in K \cup K^{-1}$ gilt, da wir nämlich jedes $x \in \langle K^G\rangle$ als ein endliches Produkt von Elementen der Form $h^{-1}kh$ darstellen können. Es gilt also $g^{-1}(h^{-1}kh)g = (hg)^{-1}k(hg) \in K^G$, weshalb $\langle K^G\rangle$ ein Normalteiler in G ist. Offensichtlich gilt $\langle K\rangle \leq \langle K^G\rangle$, weshalb $\langle K\rangle^G$ eine Teilmenge von $\langle K^G\rangle$ sein muss, da sie der Durchschnitt aller Normalteiler ist, welche $\langle K\rangle$ beinhalten.

Um $\langle K^G\rangle \subseteq \langle K\rangle^G$ zu zeigen, beachtet man, dass $\langle K\rangle^G$ ein Normalteiler ist, weshalb $g^{-1}kg \in \langle K\rangle^G$ für alle $g \in G$ und $k \in K$ gelten muss.

Wir müssen also zeigen, dass B eine Basis von $\mathrm{span}_{\mathbb{F}}(\langle K\rangle^G) = \mathrm{span}_{\mathbb{F}}(\langle K^G\rangle)$ ist. Nach Lemma III.2.2 müssen wir nur zeigen, dass das $B = \{B_1, \ldots, B_n\}$, welches vor dem Ausführen der Zeile 6 konstruiert wurde, ein Erzeugendensystem ist, sprich $\mathrm{span}_{\mathbb{F}}(\langle B\rangle) = \mathrm{span}_{\mathbb{F}}(\langle K^G\rangle)$.

Seien S', S^k und S^∞ wie im Beweis von Lemma III.2.2. Zunächst gilt nach Konstruktion $B \subseteq K^G$, weshalb $\mathrm{span}_{\mathbb{F}}(\langle B\rangle) \subseteq \mathrm{span}_{\mathbb{F}}(\langle K^G\rangle)$. Für die andere Teilmengenbeziehung zeigen wir $K^G \subseteq \mathrm{span}_{\mathbb{F}}(\langle B\rangle)$. Da $S^\infty = G$ gilt, reicht es aus, $\{g^{-1}kg : g \in S^k, k \in K \cup K^{-1}\} =: (K \cup K^{-1})^{S^k} \subseteq \mathrm{span}_{\mathbb{F}}(\langle B\rangle)$ per Induktion zu zeigen.

Induktionsanfang $k = 0$: Nach Zeile 2 gilt $K \cup K^{-1} \subseteq B$.

Induktionsvoraussetzung: Es gelte $(K \cup K^{-1})^{S^k} \subseteq \mathrm{span}_{\mathbb{F}}(\langle B\rangle)$.

Induktionsschritt $k \to k+1$: Sei $x \in (K \cup K^{-1})^{S^{k+1}}$, dann gilt $x = g^{-1}yg$ für $y \in (K \cup K^{-1})^{S^k}$ und $g \in S'$. Nach Induktionsvoraussetzung gilt nun $y = \sum_{i=1}^n \lambda_i B_i$ mit $\lambda_i \in \mathbb{F}$, weshalb wir

$$x = g^{-1}yg = \sum_{i=1}^{n} \lambda_i g^{-1} B_i g$$

folgern können. Da der Algorithmus terminiert hat, folgt nach Zeile 3, dass alle $g^{-1}B_ig$ in $\mathrm{span}_{\mathbb{F}}(\langle B\rangle)$ liegen, woraus die Aussage folgt. □

3. Die Berechnung von $\Pi(H)$

In diesem Abschnitt wollen wir einen Algorithmus entwickeln, um $\Pi(H)$ zu berechnen. Hierfür werden wir aber etwas Darstellungstheorie benötigen.

Definition III.3.1: Sei $\mathbb{K}$ eine Körpererweiterung von $\mathbb{F}$, V ein $\mathbb{F}$-Vektorraum und $G \leq \mathrm{GL}(V)$ eine Gruppe.

(i) Wir bezeichnen mit $G \otimes_{\mathbb{F}} 1_{\mathbb{K}}$ die Gruppe, deren Elemente die Form $g \otimes 1_{\mathbb{K}}$ für $g \in G$ haben. Es gilt $(g \otimes 1_{\mathbb{K}})(h \otimes 1_{\mathbb{K}}) = (gh \otimes 1_{\mathbb{K}})$ mit $g, h \in G$.

(ii) Sei $\sum_{j=1}^{k} v_j \otimes x_j$ ein Element in $V \otimes_{\mathbb{F}} \mathbb{K}$, dann gilt

$$\sum_{j=1}^{k} (g \otimes 1_{\mathbb{K}})(v_j \otimes x_j) = \sum_{j=1}^{k} (gv_j) \otimes (x_j).$$

Außerdem ist $g \otimes 1_{\mathbb{K}}$ ein Automorphismus des $\mathbb{K}$-Vektorraums $V \otimes_{\mathbb{F}} \mathbb{K}$.

Definition III.3.2: Sei $\mathbb{F}$ ein Körper, V ein $\mathbb{F}$-Vektorraum und $G \leq \mathrm{GL}(V)$.

(i) Ein Element $t \in \mathrm{GL}(n, \mathbb{F})$ heißt *Transvektion*, falls es unipotent ist und $I_n - t$ den Rang 1 hat.

(ii) Ein Untervektorraum U von V heißt *G-invariant*, falls $gU \subseteq U$ für alle $g \in G$ gilt. Da in G nur Isomorphismen sind, gilt sogar $gU = U$.

(iii) Die Gruppe G heißt *irreduzibel*, falls es keinen nichttrivialen Untervektorraum U gibt, welcher G-invariant ist.

(iv) Die Gruppe G heißt *absolut irreduzibel*, wenn $G \otimes_{\mathbb{F}} 1_{\mathbb{K}}$ irreduzibel bezüglich allen $\mathbb{K}$-Vektorräumen der Form $V \otimes_{\mathbb{F}} \mathbb{K}$ ist, wobei $\mathbb{K}$ eine algebraische Körpererweiterung von $\mathbb{F}$ ist.

(v) Wir können G als Teilmenge des $\mathbb{F}$-Vektorraums der Endomorphismen $\mathrm{End}(V)$ betrachten. Wir bezeichnen mit $\mathrm{span}_{\mathbb{F}}(G)$ den Spann der von G erzeugten $\mathbb{F}$-Algebra.

(vi) Wir bezeichnen mit $e_1, \ldots, e_n$ die Einheitsvektoren im $\mathbb{K}^n$.

Die nächste Aussage wird der Schlüssel sein, um später die Primzahlen zu bestimmen, für welche $\varphi_p(H) \neq \Sigma(n, p)$ gilt.

Theorem III.3.3 (aus [25, Theorem]): *Sei $n > 2$, p eine ungerade Primzahl und $H \leq \mathrm{GL}(n, p)$ besitze eine Transvektion t, sodass der normale Abschluss $\langle t \rangle^H$ irreduzibel ist. Dann enthält H die $\mathrm{SL}(n, p)$ oder eine Konjugation $g\,\mathrm{Sp}(n, p)g^{-1}$ der $\mathrm{Sp}(n, p)$ für ein $g \in \mathrm{GL}(n, p)$. Insbesondere gilt $\mathrm{SL}(n, p) \leq H$, wenn n ungerade ist.*[1]

[1] Im ursprünglichen Theorem aus dem Paper [25] wird G anstelle von $\langle t \rangle^H$ geschrieben.

Wir brauchen also, dass $\langle t \rangle^H$ irreduzibel ist, weshalb wir ein Kriterium kennenlernen wollen, um zu bestimmen, ob $\langle t \rangle^H$ absolut irreduzibel (und somit auch irreduzibel) ist.

Theorem III.3.4 (aus [3, Kapitel IV 2.10]): *Sei $G \leq \mathrm{GL}(n, \mathbb{F})$. Dann sind die folgenden Bedingungen äquivalent:*

(1) *G ist absolut irreduzibel.*

(2) $\dim_{\mathbb{F}}(\mathrm{span}_{\mathbb{F}}(G)) = n^2$.

Insbesondere gilt die Äquivalenz für $\mathbb{F} := \mathbb{Z}_p$ und $G := \varphi_p(\langle t \rangle^H) = \langle \varphi_p(t) \rangle^{\varphi_p(H)}$.

Wir wollen zunächst einige Lemmata sammeln, bevor wir diese Aussage beweisen können.

Lemma III.3.5 (aus [3, Kapitel IV 1.10]): *Sei H eine irreduzible Untergruppe von $\mathrm{GL}(n, \mathbb{F})$ und $\{0_{\mathbb{F}^{n\times n}}\} \neq W$ ein Untervektorraum von $\mathbb{F}^{n\times n}$ mit $HW = W$, dann gibt es einen Vektor $v \in \mathbb{F}^n$ mit $Wv = \mathbb{F}^n$.*

Beweis: Sei $0_{\mathbb{F}^{n\times n}} \neq w \in W$, dann gibt es mindestens eine Spalte i in w, welche keine Nullspalte ist, weshalb $we_i \neq 0_{\mathbb{F}^n}$ gilt. Daher gilt $We_i \neq \{0_{\mathbb{F}^n}\}$. Aus $H(We_i) = (HW)e_i \leq We_i$ folgern wir, dass (We_i) ein H-invarianter Untervektorraum ist, weshalb $We_i = \mathbb{F}^n$ aus der Irreduziblität von H folgt. □

Lemma III.3.6 (aus [3, Kapitel IV 2.7]): *Sei $\mathbb{F}$ algebraisch abgeschlossen und $H \leq \mathrm{GL}(n, \mathbb{F})$ irreduzibel. Weiterhin sei $u \in \mathbb{F}^{n\times n}$ mit*

$$\mathrm{tr}(uh) = 0 \quad \text{für alle } h \in H,$$

dann gilt $u = 0$.

Beweis: Offensichtlich ist $U = \{u \in \mathbb{F}^{n\times n} \ : \ \forall\, h \in H : \mathrm{tr}(uh) = 0\}$ ein Untervektorraum. Des Weiteren gilt $h_1 U = U$ für alle $h_1 \in H$, da für alle $u \in U$ und $h_2 \in H$

$$\mathrm{tr}(h_1 u h_2) = \mathrm{tr}(h_2 h_1 u) = 0$$

gilt. Es gilt also $HU \leq U$. Wir wollen $U = \{0\}$ zeigen. Angenommen dies wäre falsch, dann gäbe es nach Lemma III.3.5 einen Vektor $v \in \mathbb{F}^n$ mit $Uv = \mathbb{F}^n$. Seien $u_1, \ldots, u_n$ linear unabhängig in U, dann ist $u_1 v, \ldots, u_n v$ eine Basis von $\mathbb{F}^n$ und wir können ohne Einschränkung annehmen, dass $u_i v = e_i$ gilt.

Sei $w \in \mathbb{F}^n$, dann definieren wir die Matrix

$$A_w := \begin{pmatrix} u_1 w & | & \ldots & | & u_n w \end{pmatrix}.$$

Da $\mathbb{F}$ algebraisch abgeschlossen ist, existiert immer mindestens ein Eigenwert λ_w von A_w mit Eigenvektor $x_w = \sum_{i=1}^{n} \mu_i e_i$. Es folgt daher

$$\begin{aligned} 0_{\mathbb{F}^n} &= (A_w - \lambda_w I_n)x_w = (A_w - \lambda_w I_n)\sum_{i=1}^{n} \mu_i e_i \\ &= \sum_{i=1}^{n} \mu_i (A_w - \lambda_w I_n)e_i \overset{u_i v = e_i}{=} \sum_{i=1}^{n} \mu_i (u_i w - \lambda_w u_i v) = \sum_{i=1}^{n} \mu_i u_i (w - \lambda_w v), \end{aligned}$$

weshalb die Vektoren $u_1(w-\lambda_w v), \ldots, u_n(w-\lambda_w v)$ linear abhängig sind. Daher ist die Dimension des $\mathbb{F}^n$-Untervektorraums $U(w-\lambda_w v)$ kleiner als n. Da aber $HU(w-\lambda_w v) = (HU)(w-\lambda_w v) \leq U(w-\lambda_w v)$ gilt und daher $U(w-\lambda_w v)$ ein H-invarianter Untervektorraum ist, folgt

$$U(w-\lambda_w v) = \{0_{F^n}\} \ \forall\, w \in \mathbb{F}^n$$

aus der Irreduzibilität von H. Insbesondere gilt $u_i(e_j - \lambda_{e_j} v) = 0$ für alle $1 \leq i, j \leq n$. Also gilt

$$u_i e_j = \lambda_{e_j} u_i v = \lambda_{e_j} e_i \text{ für } 1 \leq i, j \leq n.$$

Es gilt daher

$$u_i = \left(\lambda_{e_1} e_i \ \mid \ \ldots \ \mid \ \lambda_{e_n} e_i\right). \tag{III.8}$$

Da nach Voraussetzung $u_i \in U$ und $I_n \in G$ gilt, folgt $0 = \mathrm{tr}(u_i I_n) = \mathrm{tr}(u_i) = \lambda_{e_i}$ für alle $1 \leq i \leq n$, weshalb $u_i = 0_{\mathbb{F}^{n\times n}}$ aus (III.8) folgt. Allerdings ist dies ein Widerspruch zur Wahl der u_i. □

Lemma III.3.7: *Sei $G \leq \mathrm{GL}(n, \mathbb{F})$ eine Gruppe und $\mathbb{K}$ eine Körpererweiterung von $\mathbb{F}$. Dann ist $\mathrm{span}_{\mathbb{F}}(G) \otimes_{\mathbb{F}} \mathbb{K}$ isomorph zu einer $\mathbb{K}$-Unteralgebra von $\mathbb{K}^{n\times n}$.*

Beweis: Da wir $\mathrm{span}_{\mathbb{F}}(G)$ als eine $\mathbb{F}$-Algebra auffassen können, gilt nach [14, V.11.1 a)], dass $\mathrm{span}_{\mathbb{F}}(G) \otimes_{\mathbb{F}} \mathbb{K}$ eine $\mathbb{K}$-Algebra ist. Aus Definition III.3.1 folgt $\mathrm{span}_{\mathbb{F}}(G) \otimes_{\mathbb{F}} \mathbb{K} \subseteq \mathrm{End}(\mathbb{F}^n \otimes_{\mathbb{F}} \mathbb{K})$. Nach [14, V.11.1 b)] gilt außerdem $\dim_{\mathbb{K}}(\mathbb{F}^n \otimes_{\mathbb{F}} \mathbb{K}) = n$, weshalb $\mathbb{F}^n \otimes_{\mathbb{F}} \mathbb{K} \cong \mathbb{K}^n$ aus Dimensionsgründen folgt. Daher gilt $\mathrm{End}(\mathbb{F}^n \otimes_{\mathbb{F}} \mathbb{K}) \cong \mathrm{End}(\mathbb{K}^n) \cong \mathbb{K}^{n\times n}$. □

Beweis (von Theorem III.3.4): Sei $\overline{\mathbb{F}}$ der algebraische Abschluss von $\mathbb{F}$. Sei zunächst G absolut irreduzibel. Wir nehmen ohne Einschränkung an, dass $\mathbb{F}$ bereits algebraisch abgeschlossen ist. Ansonsten betrachten wir die irreduzibel Gruppe $G \otimes_{\mathbb{F}} 1_{\overline{\mathbb{F}}}$ mit dem Spann $\mathrm{span}_{\mathbb{F}}(G) \otimes_{\mathbb{F}} \overline{\mathbb{F}}$. Nach Lemma III.3.7 können wir

$\text{span}_{\mathbb{F}}(G) \otimes_{\mathbb{F}} \overline{\mathbb{F}}$ in $\overline{\mathbb{F}}^{n\times n}$ einbetten. Ebenso können wir nach Definition III.3.1 die Gruppe G in $G \otimes_{\mathbb{F}} 1_{\overline{\mathbb{F}}}$ einbetten, weshalb wir im folgenden Beweis Lemma III.3.6 verwenden können. Wenn wir gezeigt haben, dass $\dim_{\overline{\mathbb{F}}}(\text{span}_{\mathbb{F}}(G) \otimes_{\mathbb{F}} \overline{\mathbb{F}}) = n^2$ gilt, dann folgt die Aussage mit Hilfe der Gleichung $\dim_{\overline{\mathbb{F}}}(\text{span}_{\mathbb{F}}(G) \otimes_{\mathbb{F}} \overline{\mathbb{F}}) = \dim_{\mathbb{F}}(\text{span}_{\mathbb{F}}(G))$ (siehe [14, V.11.1 b)]).

Sei also $\mathbb{F}$ algebraisch abgeschlossen und $m = \dim(\text{span}_{\mathbb{F}}(G))$. Wir definieren nun die Bilinearform $\beta(g_1, g_2) := \text{tr}(g_1 g_2)$ auf $\mathbb{F}^{n\times n}$.

Es gilt, dass β nicht ausgeartet ist. Sei A hierfür eine beliebige Matrix mit $A \neq 0_{\mathbb{F}^{n\times n}}$, dann gibt es einen Wert $A_{i,j} \neq 0$. Wir betrachten die Matrix $D_j P_{i,j}$. Hierbei ist die Matrix $D_j := \text{diag}(0, \ldots, 1, \ldots, 0)$ die Diagonalmatrix mit einer 1 in der j-ten Spalte. Die Matrix $P_{i,j}$ ist die Permutationsmatrix, welche die i-te mit der j-ten Spalte vertauscht. Es gilt nun $\beta(A, D_j P_{i,j}) = A_{i,j}$, weshalb β nicht links-ausgeartet ist. Analog beweist man, dass β nicht rechts-ausgeartet ist.

Daher hat das orthogonale Komplement $U := \text{span}_{\mathbb{F}}(G)^{\perp}$, bezüglich dieser Bilinearform, die Dimension $n^2 - m$. Sei außerdem $a \in U$ beliebig, dann gilt $\beta(a, g) = \text{tr}(ag) = 0$ für alle $g \in G$, da wir das orthogonale Komplement betrachten. Hieraus folgt $a = 0_{\mathbb{F}^{n\times n}}$ nach Lemma III.3.6. Also ist das orthogonale Komplement trivial, weshalb $n^2 - m = 0$ gilt und daher $m = n^2$ ist.

Für die Gegenrichtung verwenden wir die Kontraposition der Aussage. Wir nehmen also an, dass G nicht absolut irreduzibel ist. Daher finden wir eine Körpererweiterung $\mathbb{K}$ und einen Untervektorraum U, welcher bezüglich allen Matrizen aus G invariant ist. Hierbei verwenden wir die Einbettung aus Lemma III.3.7. Durch einen Basiswechsel können wir dafür sorgen, dass alle Matrizen aus $g \in G$ die Form

$$g = \begin{pmatrix} * & * \\ 0^{k\times k} & * \end{pmatrix}$$

haben, wobei $k = n - \dim(U)$ für alle Matrizen g immer gleich ist. Also ist die Dimension von $\text{span}_{\mathbb{F}}(G) \otimes \mathbb{K}$ immer kleiner als n^2 und daher gilt $\dim_{\mathbb{K}}(\text{span}_{\mathbb{F}}(G) \otimes \mathbb{K}) = \dim_{\mathbb{F}}(\text{span}_{\mathbb{F}}(G)) < n^2$. □

Lemma III.3.8: *Sei t eine Transvektion in $\text{GL}(n, \mathbb{Q})$ mit ganzzahligen Einträgen und p eine Primzahl mit $p \nmid t_{i,j}$ für $i \neq j$, dann ist $\varphi_p(t)$ eine Transvektion in $\text{GL}(n, \mathbb{Z}_p)$.*

Beweis: Da $\varphi_p(t - I_n)^k = \varphi_p((t - I_n)^k)$ gilt, bleibt $\varphi_p(t)$ unipotent. Dadurch, dass $p \nmid t_{i,j}$ gilt, kann $\varphi_p(t - I_n)$ nicht die Nullmatrix sein, weshalb der Rang mindestens 1 ist. Andererseits kann der Rang durch das Projizieren nur kleiner werden, weshalb $\text{rang}(\varphi_p(t - I_n)) = 1$ gilt. □

Lemma III.3.9: *Seien $v_1, \ldots, v_n \in \mathbb{Z}^n$, sodass $v_1, \ldots, v_n$ eine Basis von $\mathbb{Q}^n$ bilden. Sei außerdem p eine Primzahl, welche nicht die Determinante von*

$$A := \begin{pmatrix} v_1 & | & \ldots & | & v_n \end{pmatrix}$$

teilt, dann sind $\varphi_p(v_1), \ldots, \varphi_p(v_n)$ eine Basis über $\mathbb{Z}_p^n$.

Beweis: Sei

$$A_p := \begin{pmatrix} \varphi_p(v_1) & | & \ldots & | & \varphi_p(v_n) \end{pmatrix},$$

dann gilt $\det(A) \equiv \det(A_p) \mod p$, was man anhand der Leibniz-Formel sehen kann. Daher ist $\det(A_p)$ nach Voraussetzung in $\mathbb{Z}_p$ ungleich 0, also bildet $\varphi_p(v_1), \ldots, \varphi_p(v_n)$ eine Basis über $\mathbb{Z}_p^n$. □

Lemma III.3.10: *Sei $t \in H \leq \Sigma(n, \mathbb{Z})$, dann gilt $\varphi_p(\langle t \rangle^H) = \varphi_p(\langle t \rangle)^{\varphi_p(H)}$.*

Beweis: Wir betrachten im Folgenden die Funktion $\varphi_{p|H} \colon H \to \varphi_p(H)$. Es gilt $\varphi_p(\langle t \rangle^H) \supseteq \varphi_p(\langle t \rangle)^{\varphi_p(H)}$, da $\varphi_{p|H}$ surjektiv ist und daher $\varphi_p(\langle t \rangle^H) = \varphi_{p|H}(\langle t \rangle^H)$ ein Normalteiler von $\varphi_p(H)$ ist, welcher offensichtlich $\varphi_p(\langle t \rangle)$ beinhaltet.

Für die andere Teilmengenbeziehung nutzen wir aus, dass $\varphi_{p|H}^{-1}(\varphi_p(\langle t \rangle)^{\varphi_p(H)})$ wieder ein Normalteiler in H ist, welcher $\langle t \rangle$ beinhaltet. Hieraus folgt nun $\langle t \rangle^H \subseteq \varphi_{p|H}^{-1}(\varphi_p(\langle t \rangle)^{\varphi_p(H)})$. Es folgt daher

$$\varphi_p(\langle t \rangle^H) \subseteq \varphi_{p|H}(\varphi_{p|H}^{-1}(\varphi_p(\langle t \rangle)^{\varphi_p(H)})) = \varphi_p(\langle t \rangle)^{\varphi_p(H)}.$$ □

Algorithm 4 (aus [7]): `PrimesOverestimation`(S, t)

Input: endliche Menge S, $H := \langle S \rangle \leq \Sigma(n, \mathbb{Z})$, Transvektion $t \in H$, $N := \langle t \rangle^H$
Output: $\Pi_1(H)$

1: $B :=$ `BasisAlgebraClosure(t, S)` ▷ Basis $B_1, ..., B_k$ von $\text{span}_{\mathbb{Q}}(N)$
2: **if** $\#B \neq n^2$ **then** ▷ Brich ab, falls Basis zu klein
3: **return** $\emptyset$
4: **end if**
5: $A := [\text{tr}(B_i B_j)]_{i,j}$
6: $d := \det(A)$
7: $\Pi_1 := \pi(d)$ ▷ Betrachte alle Primzahlen, sodass Basis lin. abhängig
8: **for** $\forall\, 1 \leq i \neq j \leq n$ **do**
9: $\Pi_1 := \Pi_1 \cup \pi(t_{i,j})$ ▷ p wo Gefahr, dass $\varphi_p(t)$ keine Transvektion
10: **end for**
11: **return** Π_1

Wir haben nun alles beisammen, um einen Algorithmus anzugeben, welcher $\Pi(H)$ berechnen kann. Genauer wollen wir eigentlich eine endliche Obermenge $\Pi_1(H) \supseteq \Pi(H)$ bestimmen. Man kann anschließend für diese Elemente nachrechnen, ob $\varphi_p(H) \neq \Sigma(n,p)$ gilt, um die Menge $\Pi(H)$ zu gewinnen.

Sei $N = \langle t \rangle^H$. Wir betrachten die Basis $B_1, \ldots, B_{n^2}$ von $\mathrm{span}_{\mathbb{Q}}(N)$, welche n^2 Elemente nach Theorem III.3.4 hat (Zeile 1). Anschließend wollen wir die Primzahlen p bestimmen, wo $\varphi_p(B_1), \ldots, \varphi_p(B_{n^2})$ linear abhängig sind, weil hier die Gefahr besteht, dass $\dim_{\mathbb{Z}_p}(\varphi_p(N)) < n^2$ gilt, weshalb $\varphi_p(N)$ nicht absolut irreduzbel ist (Zeile 5 - 7). Anschließend wollen wir noch die Primzahlen p sammeln, wo die Gefahr besteht, dass $\varphi_p(t)$ keine Transvektion ist (Zeile 8 - 10).

Diese Primzahlen bilden dann unsere Menge $\Pi_1(H)$. Für alle anderen Primzahlen können wir schließlich Theorem III.3.3 verwenden, um zu zeigen, dass $\varphi_p(H) = \Sigma(n,p)$ gilt. Es sei aber darauf hingewiesen, dass wir hierfür benötigen, dass n ungerade ist oder $\Sigma(n,\mathbb{Z}) = \mathrm{Sp}(n,\mathbb{Z})$ gilt.

Theorem III.3.11 (aus [7, Abschnitt 3.2]): *Sei $n \geq 3$ und $H \leq \Sigma(n,\mathbb{Z})$ mit $H = \langle S \rangle$, wobei S endlich ist. Sei außerdem n ungerade oder $\Sigma(n,\mathbb{Z}) = \mathrm{Sp}(n,\mathbb{Z})$. Wenn $t \in H = \langle S \rangle$ eine Transvektion ist, sodass $\langle t \rangle^H$ absolut irreduzibel ist, dann gibt der Algorithmus* `PrimesOverestimation` *eine endliche Menge $\Pi_1(H)$ zurück, sodass $\Pi(H) \subseteq \Pi_1(H)$ gilt.*

Beweis: Sei $N := \langle t \rangle^H$ und $B = \{B_1, \ldots, B_{n^2}\}$ die Basis von $\mathrm{span}_{\mathbb{Q}}(N)$, welche es nach Theorem III.3.4 immer gibt, da N absolut irreduzibel ist. Es sei noch angemerkt, dass alle Matrizen in B ganzzahlig sind, da der Algorithmus `BasisAlgebraClosure` auf Eingabe $S \subseteq \Sigma(n,\mathbb{Z})$ und $t \in \Sigma(n,\mathbb{Z})$ nur Elemente zurückgibt, welche man als Produkt von Matrizen aus S und t darstellen kann.

Der Beweis folgt aus der folgenden Implikationskette:

$$
\begin{aligned}
p \notin \Pi(H) \quad &\Longleftrightarrow \varphi_p(H) = \Sigma(n,p) \\
&\overset{(3)}{\Longleftarrow} \varphi_p(\langle t \rangle^H) \text{ ist irreduzibel und } \varphi_p(t) \text{ ist eine Transvektion} \\
&\overset{(2)}{\Longleftarrow} \varphi_p(t) \text{ ist eine Transvektion und } \varphi_p(B_1), \ldots, \varphi_p(B_{n^2}) \\
&\qquad \text{sind linear unabhängig.} \\
&\overset{(1)}{\Longleftarrow} p \notin \Pi_1(H).
\end{aligned}
$$

(1) Sei $p \notin \Pi_1(H)$, dann ist $\varphi_p(t)$ nach Lemma III.3.8 eine Transvektion. Da $\beta(\varphi_p(B_i), \varphi_p(B_j)) = \mathrm{tr}(\varphi_p(B_i)\varphi_p(B_j))$ eine nicht entartete Bilinearform ist, folgt die lineare Unabhängigkeit von $\varphi_p(B_1), \ldots, \varphi_p(B_{n^2})$ aus dem Umstand, dass die Determinante der Matrix $\varphi_p(A)$ ungleich 0 ist (vgl. Lemma III.3.9), falls $p \notin \Pi_1(H)$ gilt (siehe Zeile 7 von Algorithmus 4).

(2) Da $\varphi_p(B_1), \ldots, \varphi_p(B_{n^2})$ linear unabhängig sind, gilt $\operatorname{span}_{\mathbb{Z}_p}(\varphi_p(\langle t\rangle^H)) = \mathbb{Z}_p^{n\times n}$. Mit Theorem III.3.4 folgt nun, dass $\varphi_p(\langle t\rangle^H)$ absolut irreduzibel ist.

(3) Wir betrachten eine Fallunterscheidung. Sei zunächst $H \leq \Sigma(n,\mathbb{Z}) = \mathrm{SL}(n,\mathbb{Z})$ für n ungerade. Nach Theorem III.3.3 enthält $\varphi_p(H)$ die Gruppe $\mathrm{SL}(n,p)$, woraus $\varphi_p(H) = \mathrm{SL}(n,p)$ folgt.

Sei n gerade und $H \leq \Sigma(n,\mathbb{Z}) = \mathrm{Sp}(n,\mathbb{Z})$. Nach Theorem III.3.3 enthält $\varphi_p(H)$ die Gruppe $\mathrm{SL}(n,p)$ oder eine Konjugation von $\mathrm{Sp}(n,p)$. Gilt $\mathrm{SL}(n,p) \leq \varphi_p(H)$, dann folgt $\varphi_p(H) = \mathrm{Sp}(n,p)$, da $\mathrm{Sp}(n,p) \leq \mathrm{SL}(n,p)$ ist. Gibt es ein $g \in \mathrm{GL}(n,p)$, mit $g\,\mathrm{Sp}(n,p)g^{-1} \leq \varphi_p(H) \leq \mathrm{Sp}(n,p)$, so folgt $\mathrm{Sp}(n,p) = \varphi_p(H)$, da $g\,\mathrm{Sp}(n,p)g^{-1} = \mathrm{Sp}(n,p)$ gilt. Dies folgt aus dem Umstand, dass beide Mengen isomorph sind und nach der obigen Überlegung $g\,\mathrm{Sp}(n,p)g^{-1} \leq \mathrm{Sp}(n,p)$ gilt. Hieraus folgt die Gleichheit, da wir endliche Mengen betrachten und diese wegen der Isomorphie gleichmächtig sind. □

Bemerkung III.3.12: Sei H arithmetisch und $t \in H$ eine Transvektion. Nach Korollar III.5.3 ist H dicht, weshalb $\langle t\rangle^H$ nach Theorem III.5.9 absolut irreduzibel ist. Also muss man bei arithmetischen Untergruppen nicht überprüfen ob, $\langle t\rangle^H$ absolut irreduzibel ist, sondern benötigt *nur* eine Transvektion.

Algorithm 5 (aus [7]): `PrimesForDense`(S,t)

Input: endliche Menge S, $H := \langle S\rangle \leq \Sigma(n,\mathbb{Z})$, Transvektion $t \in H$
Output: $\tilde{\Pi}(H)$

$\Pi_1 :=$ `PrimesOverestimation(S, t)`
$\tilde{\Pi} := \{\}$
$q := 1$ ▷ q aus Theorem II.5.3
for p in Π_1 **do**
  if $\varphi_p(H) \neq \Sigma(n,\mathbb{Z}_p)$ **then** ▷ Prüfe $p \in \Pi(H)$
    $\tilde{\Pi} := \tilde{\Pi} \cup \{p\}$
    if $p \neq 2$ **then** $q := q \cdot p$ **end if**
  end if
end for
if $n \leq 4$ and $\delta_H(q) < \delta_H(4q)$ **then** $\tilde{\Pi} := \tilde{\Pi} \cup \{2\}$ **end if**
return $\tilde{\Pi}$

Korollar III.3.13: *Sei $n \geq 3$ und $H \leq \Sigma(n, \mathbb{Z})$ arithmetisch mit $H := \langle S \rangle$, wobei S endlich ist. Sei außerdem n ungerade oder $\Sigma(n, \mathbb{Z}) = \mathrm{Sp}(n, \mathbb{Z})$. Wenn $t \in H$ eine Transvektion ist, dann gibt der Algorithmus* `PrimesForDense` *die Menge $\tilde{\Pi}(H)$ zurück.*

Beweis: Folgt direkt aus den Theoremen III.3.11, II.5.3 und II.5.4. □

4. (Absolut) primitive Gruppen

Wir wollen die Ergebnisse des letzten Abschnittes verwenden, um in den nächsten zwei Abschnitten einen Dichtheitstest bezüglich der Zariski-Topologie für eine Untergruppe $H \leq \Sigma(n, \mathbb{Z})$ zu entwickeln.

Dieser Abschnitt soll hierfür einige Grundlagen bieten, indem wir den Begriff der (absolut) primitiven Gruppen einführen. Ziel wird es sein, zu zeigen, dass $\Sigma(n, p)$ für $n \geq 3$ und $p \geq 3$ absolut primitiv ist.

Definition III.4.1:

(i) Wir bezeichnen eine Gruppe $H \leq \Sigma(n, \mathbb{F})$ als *imprimitiv*, falls es eine nichttrivale ($k \geq 2$) Zerlegung $\mathbb{F}^n = V_1 \oplus \ldots \oplus V_k$ gibt, sodass H auf dieser Zerlegung permutativ operiert, sprich für alle $A \in H$ und $1 \leq i, j \leq k$ gilt $AV_i = V_j$.

(ii) Eine Gruppe heißt *primitiv*, falls sie nicht *imprimitiv* ist.

(iii) Wir bezeichnen H als *absolut primitiv*, falls für alle algebraischen Körpererweiterungen $\mathbb{K}$ von $\mathbb{F}$ die Gruppe $H \otimes_{\mathbb{F}} 1_{\mathbb{K}}$ bezogen auf den $\mathbb{K}$-Vektorraum $\mathbb{F}^n \otimes_{\mathbb{F}} \mathbb{K}$ primitiv ist.

Definition III.4.2: Sei $\mathbb{F}$ ein Körper. Eine Gruppe $G \leq \mathrm{GL}(n, \mathbb{F})$ ist eine *T-Gruppe*, falls sie von Transvektionen erzeugt wird.

Bemerkung III.4.3: Seien n, $p \geq 3$, wobei p eine Primzahl ist. Nach [14, II.6.7 und II.9.18] ist $\Sigma(n, p)$ eine T-Gruppe.

Theorem III.4.4 (aus [25, 1.9]): *Sei V ein Vektorraum über einem Körper $\mathbb{F}$ mit $\mathrm{char}(\mathbb{F}) \neq 2$. Sei außerdem $G \leq \mathrm{GL}(V)$ eine irreduzible T-Untergruppe, dann ist G primitiv.*

Lemma III.4.5: *Seien n, $p \geq 3$, wobei p eine Primzahl ist, dann ist $\Sigma(n, p)$ absolut irreduzibel.*

Beweis: Wir verwenden Theorem III.3.4 und zeigen $\dim(\mathrm{span}_{\mathbb{Z}_p}(\Sigma(n,p))) = n^2$. Hierfür zeigen wir, dass $E_{i,j} \in \mathrm{span}_{\mathbb{Z}_p}(\Sigma(n,\mathbb{Z}_p))$ für alle $1 \leq i,j \leq n$ gilt.

Sei zunächst $\Sigma(n,p) = \mathrm{Sp}(n,p)$ mit $n = 2s$. Wir wollen uns zunächst der Frage widmen, wann eine Matrix X in $\mathrm{Sp}(n,p)$ liegt. Sei hierfür

$$X = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}(n,\mathbb{Z}_p) \text{ mit } A,\, B,\, C,\, D \in \mathbb{Z}_p^{s\times s}.$$

Es gilt nun

$$XJX^\top = \begin{pmatrix} -BA^\top + AB^\top & -BC^\top + AD^\top \\ -DA^\top + CB^\top & -DC^\top + CD^\top \end{pmatrix} = \begin{pmatrix} 0 & I_s \\ -I_s & 0 \end{pmatrix}.$$

Wir können dies ausnutzen, um zu zeigen, dass die Matrizen

$$X_1 := \begin{pmatrix} I_s & A \\ 0 & I_s \end{pmatrix};\ X_2 := \begin{pmatrix} I_s & 0 \\ A & I_s \end{pmatrix};\ X_3 := \begin{pmatrix} I_s + E_{i,j} & E_{i,i} \\ E_{i,j} + E_{j,i} & I_s \end{pmatrix};$$
$$X_4 := \begin{pmatrix} E_{i,i} & I_s \\ -I_s & 0 \end{pmatrix} \text{ mit } A = A^\top \in \mathbb{Z}_p^{s\times s} \text{ und } 1 \leq i \neq j \leq s$$

allesamt in $\mathrm{Sp}(n,p)$ liegen. Hierbei ist X_3 invertierbar, da $\det(X_3) = 1$ gilt. Wir betrachten hierfür die Additionsmatrix

$$A = \begin{pmatrix} I_s & -E_{i,s+i} \\ 0 & I_s \end{pmatrix},$$

welche die Determinante 1 hat. Es gilt nun, dass AX_3 eine untere Dreiecksmatrix ist, welche auf der Diagonalen nur Einsen hat. Sei

$$Y_1 := \begin{pmatrix} E_{i,j} & 0 \\ 0 & 0 \end{pmatrix} \text{ mit } 1 \leq i,\, j \leq s.$$

Falls $i \neq j$ gilt, dann folgt $X_3 - \frac{1}{2}X_1 - \frac{1}{2}X_2 = Y_1$. Für den Fall, dass $i = j$ gilt, folgt $X_4 - \frac{1}{2}X_1 - \frac{1}{2}X_2 = Y_1$. Also liegt Y_1 in $\mathrm{span}_{\mathbb{Z}_p}(\Sigma(n,\mathbb{Z}_p))$. Da $J \in \mathrm{Sp}(n,\mathbb{Z}_p)$ gilt, folgt

$$Y_2 := JY_1 = \begin{pmatrix} 0 & 0 \\ -E_{i,j} & 0 \end{pmatrix} \text{ mit } 1 \leq i,\, j \leq s.$$

Analog kann man

$$Y_3 := \begin{pmatrix} 0 & E_{i,j} \\ 0 & 0 \end{pmatrix};\ Y_4 := \begin{pmatrix} 0 & 0 \\ 0 & E_{i,j} \end{pmatrix} \text{ mit } 1 \leq i,\, j \leq s$$

konstruieren. Also liegen alle $E_{i,j}$ in $\mathrm{span}_{\mathbb{Z}_p}(\mathrm{Sp}(n,\mathbb{Z}_p))$.

Sei nun $\Sigma(n,p) = \mathrm{SL}(n,p)$. Offensichtlich gilt I_n, $(I_n + E_{i,j}) \in \mathrm{SL}(n,p)$ für $1 \leq i \neq j \leq n$, weshalb $E_{i,j} \in \mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$ gilt. Im Folgenden wollen wir zeigen, dass $E_{i,i} \in \mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$ für $1 \leq i \leq n$ liegt. Es gilt außerdem, dass die Matrix

$$X_1 := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

eine Permutationsmatrix ist. Daher gilt $\det(X_1) = \pm 1$. Indem wir, falls notwendig, eine Zeile der Matrix mit -1 multiplizieren, erhalten wir die Matrix $X_1' \in \mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$. Es sei angemerkt, dass die Hauptdiagonale von X_1' nur aus der 0 besteht. Da $n \geq 3$ gilt, können wir die Matrix

$$Y := \begin{pmatrix} 1 & 0 \\ 0 & X_1' \end{pmatrix}$$

konstruieren, welche in $\mathrm{SL}(n,p)$ liegt. Zusammen mit den anderen Matrizen, welche wir bis jetzt konstruiert haben, können wir $E_{1,1}$ konstruieren. Des Weiteren ist die Matrix

$$X_2 = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

in $\mathrm{SL}(n,p)$. Da $p \geq 3$ gilt, können wir folgern, dass

$$\frac{1}{2}(I_n - X_2) = Y_2 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

in $\mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$ liegt. Da wir bereits $E_{1,1}$ konstruiert haben, gilt, dass $E_{2,2}$ in $\mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$ liegt. Analog kann man

$$X_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & 0 & \dots & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

konstruieren, weshalb $E_{3,3} \in \mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$ gilt. Indem wir dies fortführen, erhalten wir $E_{i,i} \in \mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$. Also liegen alle $E_{i,j}$ in $\mathrm{span}_{\mathbb{Z}_p}(\mathrm{SL}(n,p))$.□

Theorem III.4.6: *Seien n, $p \geq 3$, wobei p eine Primzahl ist, dann ist $\Sigma(n,p)$ absolut primitiv.*

Beweis: Sei $\mathbb{K}$ eine Körpererweiterung von $\mathbb{Z}_p$, dann ist $\Sigma(n,p) \otimes_{\mathbb{Z}_p} 1_{\mathbb{K}}$ irreduzibel nach Lemma III.4.5. Da die Gruppe $\Sigma(n,p) \otimes_{\mathbb{Z}_p} 1_{\mathbb{K}}$ isomorph zur Gruppe $\Sigma(n,p)$ ist, ist $\Sigma(n,p) \otimes_{\mathbb{Z}_p} 1_{\mathbb{K}}$ eine T-Gruppe nach Bemerkung III.4.3.[2] Also folgt die Aussage aus Theorem III.4.4. □

5. Dichtheitstest für Untergruppen der $\Sigma(n,\mathbb{Z})$

Ziel dieses Abschnittes ist es, einen Dichtheitstest zu entwickeln. Hierfür werden wir eine Transvektion $t \in H$ benötigen. Wir werden sehen, dass die Dichtheit von H äquivalent zur absoluten Irreduzibiltät von $\langle t \rangle^H$ ist. Wir haben im Abschnitt III.3 gesehen, dass dies äquivalent zu $\mathrm{span}_{\mathbb{Q}}(\langle t \rangle^H) = n^2$ ist. Da wir mit dem Algorithmus `BasisAlgebraClosure` eine Basis von $\langle t \rangle^H$ berechnen können, können wir anschließend überprüfen, ob diese n^2 Elemente hat.

Bevor wir dies machen können, müssen wir ein fundamentales Resultat für die Zariski-Dichtheit betrachten, welches von Matthews–Vaserstein–Weisfeiler stammt.

Theorem III.5.1 ([16, Hauptresultat (Kapitel 0)] oder [20, Theorem 2.1]): *Die Gruppe $H \leq \Sigma(n,\mathbb{Z})$ ist dicht, wenn $\varphi_p(H) = \Sigma(n,p)$ für* fast alle *Primzahlen p gilt, wobei* fast alle *hier meint, dass es nur endlich viele Ausnahmen gibt.*

[2] Man bedenke, dass man ähnlich wie in Lemma III.3.7 die Gruppe $\Sigma(n,p) \otimes_{\mathbb{Z}_p} 1_{\mathbb{K}} \cong \Sigma(n,p)$ in $\mathbb{K}^{n\times n}$ einbetten kann. Offensichtlich bleibt eine Transvektion in $\mathbb{Z}_p^{n\times n}$ eine Transvektion in $\mathbb{K}^{n\times n}$.

Ein weiteres wichtiges Resultat von T. Weigel ist das folgende Theorem.

Theorem III.5.2 (aus [20, Theorem 2.4]): *Es gilt, dass $H \leq \Sigma(n, \mathbb{Z})$ genau dann dicht ist, wenn es eine Primzahl $p > 3$ mit $\varphi_p(H) = \Sigma(n, p)$ gibt.*

Korollar III.5.3: *Jede arithmetische Untergruppe $H \leq \Sigma(n, \mathbb{Z})$ ist Zariski-dicht.*

Beweis: Sei $H \leq \Sigma(n, \mathbb{Z})$ arithmetisch, dann gibt es ein M mit $\Gamma_{n,M} \leq H$. Sei $p > 3$ eine Primzahl, welche zu M koprim ist, dann gilt $\Gamma_{n,p}H \geq \Gamma_{n,p}\Gamma_{n,M} = \Gamma_{n,1} = \Sigma(n, \mathbb{Z})$, wobei wir Lemma II.1.4 (i) verwendet haben. Es folgt daher $\varphi_p(H) = \varphi_p(\Gamma_{n,p}H) = \Sigma(n, p)$, womit die Dichtheit nach Theorem III.5.2 folgt. □

Definition III.5.4: Sei V ein Vektorraum und $G \leq \mathrm{GL}(V)$.

(i) Wir können V als ein G-Modul auffassen, indem wir als Multiplikation $gv := g(v)$ mit $g \in G$ und $v \in V$ verwenden.

(ii) Sei U ein Untervektorraum von V. Wir können U als G-Untermodul auffassen, falls $gu \in U$ für alle $g \in G$ und $u \in U$ gilt.

(iii) Wir bezeichnen V als einen irreduziblen G-Modul, falls G irreduzibel bezüglich V ist (siehe Definition III.3.2).

(iv) Wir bezeichnen V als *vollständig reduziblen* G-Modul, falls es eine Zerlegung $V := V_1 \oplus \ldots \oplus V_k$ in irreduzible G-Untermoduln V_i gibt.

(v) Seien V_1 und V_2 zwei G-Moduln. Ein G-Modul-Homomorphismus ψ von V_1 nach V_2 ist ein Vektorraumhomomorphismus von V_1 nach V_2, sodass $\psi(gv) = g\psi(v)$ für alle $g \in G$ und $v \in V$ gilt.
Falls ψ ein Vektorraumisomorphismus mit dieser Eigenschaft ist, bezeichnen wir ψ als G-Modul-Isomorphismus.

(vi) Wir schreiben $V_1 \overset{G}{\sim} V_2$, falls es einen G-Modul-Isomorphismus zwischen V_1 und V_2 gibt.

Lemma III.5.5 (aus [14, V.3.2]): *Sei V ein endlichdimensonaler Vektorraum und $G \leq \mathrm{GL}(V)$. Sei außerdem $\mathfrak{W}$ eine Menge von irreduziblen G-Untermoduln von V, für welche*

$$V = \sum_{W \in \mathfrak{W}} W$$

gilt, dann ist V vollständig reduzibel.

Beweis: Wir wollen zeigen, dass wir für jeden irreduziblen G-Untermodul W einen G-Untermodul U finden können, sodass $V = W \oplus U$ gilt. Anschließend folgt die Aussage induktiv, wobei wir bedenken, dass die Dimension von V endlich ist und sich U als Summe irreduzibler G-Untermoduln schreiben lässt. Es gilt nämlich

$$U = \sum_{W \in \mathfrak{W}} (W \cap U).$$

Man bedenke, dass wegen der Irreduzibiltät von W stets $W \cap U = \{0\}$ oder $W \cap U = W$ gilt.

Sei zunächst T ein möglichst großer G-Untermodul, sodass $W \cap T = \{0\}$ gilt. Angenommen $W \oplus T$ ist ein echter Untermodul von V, dann gibt es ein irreduzibles $V_i \in \mathfrak{W}$ mit $V_i \not\subseteq W \oplus T$. Hieraus folgt $V_i \cap (W \oplus T) = \{0\}$, da V_i irreduzibel ist. Wir wollen nun $W \cap (T + V_i) = \{0\}$ zeigen.

Angenommen es ist

$$w = t + v \in W \cap (T + V_i) \quad \text{mit } w \in W,\, t \in T \text{ und } v \in V_i,$$

dann ist $v = w - t \in V_i \cap (W \oplus T) = \{0\}$. Also gilt $w = t$, da aber $W \cap T = \{0\}$ gilt, folgt $W \cap (T + V_i) = \{0\}$. Wir können also T entgegen unserer ursprünglichen Annahme größer wählen, weshalb $V = W \oplus T$ sein muss. □

Das folgende Theorem ist auch als *Clifford's Theorem* bekannt.

Theorem III.5.6 (aus [14, V.17.3 a), b) und d)]): *Sei V ein endlichdimensonaler Vektorraum, $G \leq \mathrm{GL}(V)$ und $N \trianglelefteq G$. Sei außerdem V ein irreduzibler G-Modul.*

(i) *Da V ein G-Modul ist, können wir ihn auch als N-Modul betrachten. Sei $W \neq \{0\}$ ein irreduzibler N-Untermodul von V, dann gilt*

$$V = \sum_{g \in G} gW.$$

Außerdem sind alle gW irreduzible N-Moduln, daher ist V nach Lemma III.5.5 ein vollständig reduzibler N-Modul.

(ii) *Sei*

$$\mathfrak{W} := \{W : W \leq V \text{ und ein irreduzibler } N\text{-Modul}\}$$

und $W_i \overset{N}{\sim} W_j$ die Äquivalenzrelation aus Definition III.5.4 (vi).

Sei $W_1, \ldots, W_n$ ein Vertretersystem von $\mathfrak{W}/\overset{N}{\sim}$, dann definieren wir die homogenen Koordinaten V_i *als*

$$V_i := \sum_{\substack{W \in \mathfrak{W} \\ W \overset{N}{\sim} W_i}} W \quad \text{für } 1 \leq i \leq n.$$

Es gilt nun

(a) $V_i = V_i^{(1)} \oplus \ldots \oplus V_i^{(a_i)}$ *mit* $V_i^{(j)} \in \mathfrak{W}$ *und* $V_i^{(j)} \overset{N}{\sim} W_i$.
(b) $V = \bigoplus_{i=1}^{n} V_i$.

(iii) *Seien die* $V_1, \ldots, V_n$ *wie oben definiert, dann permutiert jedes* $g \in G$ *die* $V_1, \ldots, V_n$.

Beweis: (i) Sei $V' = \sum_{g \in G} gW$, dann ist V' offensichtlich nicht leer. Außerdem ist V' ein G-invarianter Vektorraum, weshalb $V' = V$ sein muss, da V irreduzibel ist.

Sei $gw \in gW$, dann folgt für $n \in N$, dass $w' := g^{-1}ngw \in W$ gilt, da W ein N-Modul ist. Hieraus folgt

$$ngw = g \underbrace{g^{-1}ng}_{\in N} w = gw' \in gW.$$

Also ist gW wieder ein N-Modul. Es gilt zu zeigen, dass gW irreduzibel ist. Sei gU ein nichttrivialer Untervektorraum von gW, dann gibt es wegen der Irreduzibilität von W ein $n \in N$ mit $nU \not\subseteq U$. Da N ein Normalteiler ist, gilt $n' = gng^{-1} \in N$. Es gilt daher $n'gU = gnU \not\subseteq gU$.

(ii) Zuerst wollen wir Teil (a) der Aussage zeigen. Sei also V_i eine homogene Komponente, dann wollen wir zeigen, dass sich V_i als eine direkte Summe $V_i = V_i^{(1)} \oplus \ldots \oplus V_i^{(a_i)}$ schreiben lässt, wobei $V_i^{(j)} \in \mathfrak{W}$ und $V_i^{(j)} \overset{N}{\sim} W_i$ gilt.

Sei $V_i' := V_i^{(1)} \oplus \ldots \oplus V_i^{(a_i)}$ ein möglichst großer N-Untermodul von V_i, sodass $V_i^{(j)} \in \mathfrak{W}$ und $V_i^{(j)} \overset{N}{\sim} W_i$ gilt. Ist V_i' ein echter Untermodul von V_i, dann gibt es einen nichttrivialen Untermodul $W_i' \in \mathfrak{W}$ mit $W_i' \overset{N}{\sim} W_i$, sodass $W_i' \not\subseteq V_i'$ gilt. Da W_i' irreduzibel ist, gilt $V_i' \cap W_i' = \{0\}$, weshalb $V_i' \subseteq V_i' \oplus W_i'$ gilt. Das ist aber ein Widerspruch zur Wahl von V_i'. Es gilt daher $V_i = V_i'$.

Als nächstes wollen wir Teil (b) der Aussage zeigen. Hierfür zeigen wir zunächst, dass $V_i \cap V_j = \{0\}$ gilt. Seien also V_i und V_j zwei homogene Komponenten, dann gilt wegen der Irreduzibilität der einzelnen Komponenten $V_i^{(s)} \cap V_j^{(t)} = \{0\}$ oder $V_i^{(s)} = V_j^{(t)}$ für alle $1 \leq s \leq a_i$ und $1 \leq t \leq a_t$. Letzterer Fall kann aber nicht eintreten, weil sonst $V_i^{(s)} \overset{N}{\sim} V_j^{(t)}$ gelten würde, was nach Konstruktion nicht sein kann. Deshalb gilt $V_i \cap V_j = \{0\}$. Des Weiteren gilt nach der (i), dass wir V als Summe von irreduziblen N-Moduln auffassen können. Diese befinden sich alle in $\mathfrak{W}$. Hieraus folgt

$$V = \sum_{W \in \mathfrak{W}} W = \bigoplus_{i=1}^{n} V_i.$$

(iii) Nach (ii) (a) können wir $V_i = W_1' \oplus \ldots \oplus W_k'$ mit $W_a' \in \mathfrak{W}$ und $W_a \overset{N}{\sim} W_i$ für $1 \leq a \leq k$ annehmen. Es gilt also $gV_i = gW_1' \oplus \ldots \oplus gW_k'$. Nach (i) ist jedes gW_j' ein irreduzibler N-Modul. Wir wollen nun zeigen, dass $gW_s' \overset{N}{\sim} gW_t'$ gilt.

Nach (ii) gibt es einen N-Modul-Isomorphismus ψ zwischen W_s' und W_t'. Wir definieren die Funktion

$$\psi' \colon gW_s' \to gW_t';\quad ga \mapsto g\psi(a)$$

Diese Funktion ist wohldefiniert, da $g \in \mathrm{GL}(V)$ gilt. Außerdem kann man leicht überprüfen, dass ψ' ein Isomorphismus ist. Des Weiteren gilt für $n \in N$, $a \in W_s'$, $ga \in gW_s'$ und $a' = g^{-1}nga \in W_s'$:

$$\begin{aligned}\psi'(nga) &= \psi'(g\underbrace{g^{-1}ng}_{\in N}a) = \psi'(ga') = g\psi(a') \\ &= g\psi(g^{-1}nga) = gg^{-1}ng\psi(a) = n\psi'(ga).\end{aligned}$$

Also gilt $gW_s' \overset{N}{\sim} gW_t'$. Daher muss es ein $1 \leq p \leq n$ geben, sodass $gW_1' \overset{N}{\sim} \ldots \overset{N}{\sim} gW_k' \overset{N}{\sim} W_p$ gilt, wobei W_p einer der Repräsentanten aus (ii) ist. Daher gilt nach Konstruktion $gV_i \subseteq V_p$ mit $1 \leq p \leq n$.

Analog können wir zeigen, dass $V_i \subseteq g^{-1}V_p \subseteq V_q$ gelten muss. Da die $V_1, \ldots, V_n$ eine direkte Summe bilden, muss $V_i = g^{-1}V_p = V_q$ sein, weshalb $gV_i = V_p$ gilt.

Da $g \in \mathrm{GL}(V)$ gilt, folgt aus $gV_i = gV_j$ bereits $i = j$. Also permutiert jedes $g \in G$ die homogenen Komponenten.

□

Lemma III.5.7 (aus [7, Lemma 3.4]): *Sei H eine irreduzible Untergruppe von $\mathrm{GL}(n, \mathbb{F})$ und $t \in H$ eine Transvektion, sodass $\langle t \rangle^H$ reduzibel ist, dann ist H imprimitiv.*

Beweis: Wir definieren zunächst $N := \langle t \rangle^H$. Nach Theorem III.5.6 (ii) (b) gilt $\mathbb{F}^n := V_1 \oplus \ldots \oplus V_s$ wobei die V_i homogene Komponenten bzgl. der Aktion von N, sind. Nach Theorem III.5.6 (ii) (a) können wir jedes V_i als direkte Summe von irreduziblen N-Untermoduln $W_i^{(j)}$ auffassen. Indem wir V_i durch $W_i^{(1)} \oplus \cdots \oplus W_i^{(a_i)}$ substituieren, erhalten wir $\mathbb{F}^n = W_1 \oplus \ldots \oplus W_k$, wobei wir beim letzten Schritt die Notation vereinfacht haben, indem wir anstelle von $W_i^{(j)}$ einfach W_q schreiben.

Es gilt $k \geq 2$, da sonst N irreduzibel wäre. Da alle W_j irreduzible N-Moduln sind, können wir t als Blockdiagonalmatrix darstellen:

$$t = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k \end{pmatrix},$$

wobei A_i die Darstellungsmatrix von $t_{|W_i}$ ist. Wäre $k = n$, dann wäre t diagonalisierbar. Allerdings ist t eine Transvektion, weshalb die Jordannormalform von t die folgende Form hat:

$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Also gilt $k < n$. Man überlegt sich leicht, dass t sogar genau dann eine Tranvektion ist, wenn die JNF von t die obige Form hat. Wenn wir die JNF genauer betrachten, so fällt uns auf, dass es genau ein Jordankästchen der Größe 2 gibt. Indem wir uns die JNF der einzelnen A_i anschauen, fällt uns auf, dass es genau ein A_j gibt, welches eine Transvektion ist. Ansonsten gilt $t_{|W_i} = \mathrm{id}$ für $i \neq j$. Daher gilt $W_j \overset{N}{\not\cong} W_i$. Gäbe es nämlich einen N-Modul-Isomorphismus $\psi\colon W_i \to W_j$, dann gälte

$$\psi(x) \overset{t_{|W_i}=\mathrm{id}}{=} \psi(tx) = t\psi(x),$$

was ein Widerspruch dazu ist, dass $t_{|W_j}$ eine Transvektion ist.

Also gilt $W_j \overset{N}{\not\cong} W_i$, weshalb es mindestens zwei homogene Komponenten geben muss. Nach Theorem III.5.6 (iii) permutiert G diese, weshalb G imprimitiv sein muss.

□

Korollar III.5.8 (aus [7, Korollar 3.5 und 3.4]): *Sei $H \leq \Sigma(n, \mathbb{Z})$ und $t \in H$ eine Transvektion, sodass $\langle t \rangle^H$ nicht absolut irreduzibel ist, dann ist H nicht dicht.*

Beweis: Wir betrachten zunächst den Fall, dass H nicht absolut irreduzibel ist. Nach Theorem III.3.4 gilt $\mathrm{span}_{\mathbb{Q}}(H) = k < n^2$. Sei also $b_1, \dots, b_k$ eine

Basis, sodass alle Einträge der Vektoren in $\mathbb{Z}$ liegen. Sei p eine Primzahl. Offensichtlich ist $\varphi_p(b_1), \ldots, \varphi_p(b_k)$ ein Erzeugendensystem von $\mathrm{span}_{\mathbb{Z}_p}(\varphi_p(H))$, weshalb $\dim(\mathrm{span}_{\mathbb{Z}_p}(\varphi_p(H))) \leq k < n^2$ gilt. Also ist $\varphi_p(H)$ nicht absolut irreduzibel. Da aber $\Sigma(n,p)$ nach Korollar III.4.5 absolut irreduzibel ist, folgt $\varphi_p(H) \neq \Sigma(n,p)$, weshalb H nach Theorem III.5.1 nicht dicht sein kann.

Sei also H absolut irreduzibel, dann folgt wie im Beweis von III.3.11, dass $\varphi_p(H)$ absolut irreduzibel für fast alle Primzahlen p ist. Da $\langle t \rangle^H$ nicht absolut irreduzibel ist, folgt mit der Argumentation des obigen Abschnittes, dass auch $\varphi_p(\langle t \rangle^H) = \varphi_p(\langle t \rangle)^{\varphi_p(H)}$ nicht absolut irreduzibel ist, wobei wir Lemma III.3.10 ausgenutzt habe. Da $\varphi_p(t)$ nach Lemma III.3.8 für fast alle Primzahlen eine Transvektion ist, können wir für fast alle Primzahlen p Lemma III.5.7 verwenden. Es existiert nämlich eine Körpererweiterung $\mathbb{K}$ von $\mathbb{Z}_p$, sodass $\varphi_p(\langle t \rangle)^{\varphi_p(H)} \otimes_{\mathbb{Z}_p} 1_{\mathbb{K}}$ nicht reduzibel ist. Aus der absoluten Irreduziblität von $\varphi_p(H)$ können wir annehmen, dass $\varphi_p(H) \otimes_{\mathbb{Z}_p} 1_{\mathbb{K}}$ irreduzibel ist, weshalb $\varphi_p(H) \otimes_{\mathbb{Z}_p} 1_{\mathbb{K}}$ imprimitiv ist. Da aber $\Sigma(n,p)$ nach Lemma III.4.6 für $p > 2$ absolut primitiv ist, muss $\varphi_p(H) \neq \Sigma(n,p)$ für fast alle Primzahlen gültig sein, weshalb H nach Theorem III.5.1 nicht dicht ist. □

Theorem III.5.9 (aus [7, Proposition 3.7]): *Sei n ungerade oder $\Sigma(n,\mathbb{Z}) = \mathrm{Sp}(n,\mathbb{Z})$. Sei außerdem $H \leq \Sigma(n,\mathbb{Z})$ und $t \in H$ eine Transvektion, dann ist H dicht genau dann, wenn $\langle t \rangle^H$ absolut irreduzibel ist.*

Beweis: Die Hinrichtung ist die Kontraposition von Korollar III.5.8. Für die Gegenrichtung verwenden wir Theorem III.3.11. Wir bekommen eine endliche Menge $\Pi_1(H)$, sodass $p \notin \Pi_1(H)$ für alle Primzahlen p mit $\varphi_p(H) = \Sigma(n,p)$ gilt. Es gibt also eine Primzahl $p > 3$ mit $\varphi_p(H) = \Sigma(n,p)$, weshalb H nach Theorem III.5.2 eine dichte Untergruppe ist. □

Wir haben alles zusammen, um einen Algorithmus `isDense` anzugeben, welcher mittels einer Transvektion t die Dichtheit von H überprüfen kann, sofern n ungerade ist oder $\Sigma(n,\mathbb{Z}) = \mathrm{Sp}(n,\mathbb{Z})$ gilt. Hierfür reicht es nach Theorem III.5.9 aus, zu überprüfen, ob $\langle t \rangle^H$ absolut irreduzibel ist. Die absolute Irreduzibilität können wir nach Theorem III.3.4 überprüfen, indem wir mit Hilfe des Algorithmus 3 `BasisAlgebraClosure` die Basis von $\langle t \rangle^H$ berechnen und überprüfen, ob diese n^2 Elemente hat.

Korollar III.5.10: *Sei n ungerade oder $\Sigma(n,\mathbb{Z}) = \mathrm{Sp}(n,\mathbb{Z})$. Sei außerdem S eine endliche Menge, $H := \langle S \rangle \leq \Sigma(n,\mathbb{Z})$ eine Gruppe und $t \in H$ eine Transvektion. Der Algorithmus* `isDense` *gibt* `True` *aus, falls H dicht ist, und* `False`*, falls H nicht dicht ist.*

Beweis: Folgt direkt aus Theorem III.3.4 und Theorem III.5.9. □

Algorithm 6 (aus [7]): `isDense`(S, t)

Input: endliche Menge S, $H := \langle S \rangle \leq \Sigma(n, \mathbb{Z})$, Transvektion $t \in H$, $N := \langle t \rangle^H$
Output: `True`, falls H Zariski-dicht in $\Sigma(n, \mathbb{Z})$, sonst `False`.

1: $B :=$ `BasisAlgebraClosure(t, S)` ▷ Basis $B_1, ..., B_k$ von $\text{span}_{\mathbb{Q}}(N)$
2: **if** $\#B \neq n^2$ **then**
3: **return** `False`
4: **end if**
5: **return** `True`

6. Berechnung der minimalen arithmetischen Obergruppe

Wir wollen die Ergebnisse aus dem letzten Abschnitt verallgemeinern und uns anschauen, welche Ergebnisse wir für Untergruppen erhalten, welche lediglich Zariski-dicht und nicht notwendigerweise arithmetisch sind.

Definition III.6.1: Sei $n > 2$ und $H = \langle S \rangle \leq \Sigma(n, \mathbb{Z})$. Wir definieren die *minimale arithmetische Obergruppe* als den Durchschnitt aller arithmetischen Obergruppen, welche H beinhalten.

Nach der obigen Definition muss C nicht arithmetisch sein. Wenn aber C arithmetisch ist, so können wir das Level von H mittels des Levels von C definieren.

Definition III.6.2: Sei H Zariski-dicht und C die minimale arithmetische Obergruppe von H. Falls C arithmetisch ist, definieren wir das Level von H als das Level von C.

Lemma III.6.3 (aus [7, Lemma 3.11]): *Sei C die minimale arithmetische Obergruppe von H und C zusätzlich arithmetisch von Level ℓ, dann gilt $\pi(\ell) = \tilde{\Pi}(H)$ wie in* Theorem II.5.4.

Beweis: Sei $m \in \mathbb{N}$ beliebig. Wir wollen zunächst $\Gamma_{n,m}H = \Gamma_{n,m}C$ zeigen. Es gilt $\Gamma_{n,m}H \subseteq \Gamma_{n,m}C$, da $H \subseteq C$ nach Konstruktion ist. Es folgt außerdem $C \subseteq \Gamma_{n,m}H$, da $\Gamma_{n,m}H$ eine arithmetische Obergruppe von H ist. Hieraus folgt nun $\Gamma_{n,m}H = \Gamma_{n,m}C$.

Hieraus können wir $\varphi_m(H) = \varphi_m(\Gamma_{n,m}H) = \varphi_m(\Gamma_{n,m}C) = \varphi_m(C)$ folgern, woraus $\Pi(C) = \Pi(H)$ folgt. Es gilt außerdem

$$\delta_H(m) = [\Sigma(n, \mathbb{Z}) : \Gamma_{n,m}H] = [\Sigma(n, \mathbb{Z}) : \Gamma_{n,m}C] = \delta_C(m).$$

Daher können wir den Test (Lemma II.5.3) für die Primzahl 2 analog durchführen, woraus $\pi(\ell) = \tilde{\Pi}(C) = \tilde{\Pi}(H)$ nach Theorem II.5.4 folgt. □

Theorem III.6.4 (aus [7, Theorem 3.12]): *Sei $S \subseteq \Sigma(n, \mathbb{Z})$ endlich, $H = \langle S \rangle$ dicht und C die minimale arithmetische Obergruppe von H. Es gilt außerdem, dass es keine Primzahl $p \notin \tilde{\Pi}(H)$ gibt, sodass (n, p) nicht* unexceptional *ist, oder die Gruppe C ist arithmetisch.*

Falls der Algorithmus `LevelMaxPCS` *bei Eingabe S und $\tilde{\Pi}(H)$ mit Ausgabe N terminiert, so ist die minimale arithmetische Obergruppe C von H arithmetisch und von Level N.*

Beweis: Wir zeigen zunächst, dass aus dem Umstand, dass keine Primzahl $p \notin \tilde{\Pi}(H)$ existiert, sodass (n, p) nicht *unexceptional* ist, und dem Terminieren des Algorithmus bereits folgt, dass C arithmetisch ist. Wir definieren hierfür $C' = \Gamma_{n,N}H$. Es reicht aus zu zeigen, dass $\Gamma_{n,N}H \subseteq \Gamma_{n,M}H$ für alle $N \leq M$ gilt. Wenn wir dies gezeigt haben, können wir

$$C := \bigcap_{\substack{H \leq B \\ B \text{ ist arith.}}} B = \bigcap_{m \in \mathbb{N}} \Gamma_{n,m}H = \bigcap_{m=1}^{N} \Gamma_{n,m}H$$

folgern. Die zweite Gleichheit gilt, da nach Beispiel I.2.9 für jedes B ein $m \in \mathbb{N}$ existiert mit $\Gamma_{n,m} \leq B$. Daher gilt $\Gamma_{n,m}H \leq B$. Außerdem ist $\Gamma_{n,m}H$ arithmetisch. Da wir C als Durchschnitt endlich vieler Gruppen mit endlichem Index darstellen können, hat C selber einen endlichen Index und ist arithmetisch.

Wir betrachten zunächst den Fall $M = p^a M'$ mit $p \notin \tilde{\Pi}(H)$ und $p \nmid M'$. Wir wollen $\Gamma_{n,M}H = \Gamma_{n,M'}H$ zeigen. Es gilt nach Voraussetzung, dass (n, p) *unexceptional* ist. Da $p \notin \tilde{\Pi}(H)$ gilt, folgt $\varphi_p(H) = \Sigma(n, \mathbb{Z}_p)$. Indem wir die Induktion aus dem Beweis von Lemma II.4.1 verwenden, erhalten wir $\varphi_{p^a}(H) = \Sigma(n, \mathbb{Z}_{p^a})$. Es gilt $\Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n,\mathbb{Z}_{M'})}\} \leq \varphi_{p^a M'}(H)$ nach Lemma II.3.11, wobei wir bei der Teilmengenbeziehung eigentlich die Isomorphie aus Lemma II.3.6 betrachten. Daher gilt $\varphi_{p^a M'}(H) = \varphi_{p^a M'}(\Gamma_{n,M'}H)$, wobei man $\Gamma_{n,M'} \cong \Sigma(n, \mathbb{Z}_{p^a}) \times \{e_{\Sigma(n,\mathbb{Z}_{M'})}\}$ bedenkt. Hieraus folgt nun

$$\Gamma_{n,p^a M'}H = \Gamma_{n,p^a M'}\Gamma_{n,M'}H = \Gamma_{n,M'}H.$$

Daher können wir im Folgenden annehmen, dass $\pi(M) \subseteq \pi(N)$ gilt. Wir können sogar ohne Beschränkung der Allgemeinheit annehmen, dass $N \mid M$ gilt. Ansonsten betrachten wir ein M' mit $M \mid M'$ und $N \mid M'$. Es gilt daher $\Gamma_{n,M'}H \subseteq \Gamma_{n,M}H$. Indem wir nun zeigen, dass $\Gamma_{n,M'}H = \Gamma_{n,N}H$ gilt, können wir $\Gamma_{n,N}H \subseteq \Gamma_{n,M}H$ folgern.

Sei also M mit $N \mid M$. Da sowohl in Lemma III.1.1 (i) und (ii) als auch in Lemma II.5.2 (a) und (b) nicht vorausgesetzt wird, dass H arithmetisch ist, und der Algorithmus terminiert hat, können wir wie im Beweis von Theorem III.1.2 folgern, dass $\delta_H(N) = \delta_H(M)$ gilt. Man geht hierfür wie im Beweis induktiv vor und verwendet hierbei die Gleichung (III.7). Aus $\delta_H(N) = \delta_H(M)$ folgt $\Gamma_{n,N}H = \Gamma_{n,M}(H)$, da $\Gamma_{n,N}H \supseteq \Gamma_{n,M}(H)$ gilt und der Index gleich ist.

Wir können also für den Rest des Beweises annehmen, dass C arithmetisch ist. Nach Lemma III.6.3 gilt $\pi(\ell) = \pi(N)$. Da der Algorithmus terminiert, folgt mit dem Beweis von Lemma III.1.2 und Lemma III.6.3

$$\delta_C(\ell) \overset{\text{III.6.3}}{=} \delta_H(\ell) \overset{\text{III.1.2}}{=} \delta_H(N) \overset{\text{III.6.3}}{=} \delta_C(N),$$

woraus $\ell \mid N$ nach Lemma II.5.2 (b) (ii) folgt. Da $\delta_H(m) = \delta_C(m)$ gilt, können wir analog wie im Beweis von Theorem III.1.2 zeigen, dass $N \mid \ell$ gilt, da die Funktion δ_C genau dann stagniert, wenn δ_H stagniert. Daher gilt die Aussage.□

Bemerkung III.6.5: Da H Zariski-dicht ist, gibt es nach [7, Abschnitt 3.3] endlich viele arithmetische Obergruppen $D_1, \ldots, D_k$, welche H beinhalten. Also ist die minimale arithmetische Obergruppe $C = \cap_{i=1}^{k} D_i$. Da alle D_i arithmetisch sind, gilt $\Gamma_{n,m_i} \leq D_i$. Nach Lemma II.1.4 (ii) gilt $\Gamma_{n,m} \leq C$ mit $m = \mathrm{kgV}(m_1, \ldots, m_k)$. Also ist C ebenfalls arithmetisch und hat das Level M. Daher terminiert der Algorithmus `LevelMaxPCS` immer, da $\delta_H(m) = \delta_C(m)$ durch $\delta_C(M)$ beschränkt wird. Insbesondere benötigen wir die Voraussetzung $p \notin \tilde{\Pi}(H)$ in Theorem III.6.4 nicht.

Bemerkung III.6.6: Haben wir eine dichte Gruppe $H \leq \Sigma(n, \mathbb{Z})$ und eine Transvektion t, so können wir nach Bemerkung III.6.5 und Theorem III.6.4 das Level der arithmetischen Obergruppe von H bestimmen. Allerdings haben wir das Problem, dass wir anhand der Ausgabe von `LevelMaxPCS` nicht darauf schließen können, ob H arithmetisch ist.

7. Laufzeitanalyse der Dichtheitstests

Wir wollen die Laufzeit von Algorithmus 6 `isDense` mit der Laufzeit der Algorithmen `IsDenseIR1` und `IsDenseIR2` vergleichen. Beide Algorithmen benötigen im Gegensatz zu `isDense` keine Transvektion und funktionieren im Fall $\mathrm{SL}(n, \mathbb{Z})$ auch für ein gerades n.

Der Algorithmus `IsDenseIR1` aus [19, Algorithmus 1] implementiert ein Monte-Carlo-Verfahren, um die Dichtheit zu überprüfen. Der Vorteil hieran ist, dass der Algorithmus normalerweise sehr schnell ist. Der Nachteil ist, dass

die Ausgabe `False` auch bedeuten kann, dass die Monte-Carlo-Suche erfolglos war. Sprich der Algorithmus kann `False` zurückgeben, selbst wenn die Gruppe dicht ist. Man kann aber die Wahrscheinlichkeit, dass ein fehlerhalftes Ergebnis auftritt, verringern, wobei hierdurch die Laufzeit schlechter wird. Die Laufzeit im Fall $\mathrm{SL}(n,\mathbb{Z})$ ist $O(n^4\log(n))$. Im Fall $\mathrm{Sp}(n,\mathbb{Z})$ ist sie $O(n^8\log(n))$.

Der Algorithmus `IsDenseIR2` aus [19, Fact 9.1] ist deterministisch und gibt daher immer das korrekte Ergebnis zurück. Allerdings ist er dafür deutlich langsamer und hat eine Laufzeit von $O(n^{14}\log(\|\mathcal{G}\|))$. Hierbei ist $\|\mathcal{G}\|$ das Maximum der Frobeniusnorm aller Generatoren der Gruppe, deren Dichtheit untersucht wird.

Wir wollen nun die Laufzeit von `isDense` berechnen.

Lemma III.7.1: *Die Laufzeit des Algorithmus* 2 `BasisEnvAlgebra` *auf Eingabe* $S \subseteq \Sigma(n,\mathbb{Z})$ *liegt in* $O(|S|n^{2\omega+4})$. *Hierbei gilt* $\omega < 2.3728639$.

Beweis: Die Konstante ω ist definiert als die kleinste Zahl, sodass es einen Algorithmus für die Multiplikation von $n \times n$-Matrizen gibt, dessen Laufzeit in $O(n^\omega)$ liegt. Dieser Wert ist unbekannt. Nach [10] gilt $\omega < 2.3728639$. Außerdem können wir nach [15] in $O(m(n^2)^{\omega-1}) \subseteq O(n^{2\omega})$ bestimmen, ob m Vektoren in einem Vektorraum der Größe n^2 linear unabhängig sind.

Angenommen wir sind im k-ten Durchlauf der Schleife in Zeile 4, dann gibt es $(2|S|+1)k$ Kombinationen, um B_jS_i zu bestimmen. Außerdem müssen wir immer überprüfen, ob die $k+1$ Vektoren linear unabhängig sind. Zusätzlich müssen wir noch eine Matrixmultiplikation durchführen. Da die Schleife maximal (n^2-1)-mal ausgeführt wird, erhalten wir eine Laufzeit von

$$\sum_{k=1}^{n^2-1}(2|S|+1)k(n^{2\omega}+n^\omega) \leq (2|S|+1)2n^{2\omega}\sum_{k=1}^{n^2}k \in O(|S|n^{2\omega+4}). \qquad \square$$

Lemma III.7.2: *Die Laufzeit vom Algorithmus* 3 `BasisAlgebraClosure` *auf Eingabe* $S, K \subseteq \Sigma(n,\mathbb{Z})$ *liegt in* $O(|K||S|n^{2\omega+2} + (|S|+|K|)n^{2\omega+4} + n^{2\omega+6})$.

Beweis: Angenommen wir sind im k-ten Durchlauf der Schleife in Zeile 3, dann gibt es $(2|S|+1)(2|K|+k)$ Kombinationen, um $g^{-1}Ag$ zu wählen. Wir müssen daher zwei Matrixmultiplikationen durchführen. Um zu überprüfen, ob $g^{-1}Ag$ im Spann liegt, prüfen wir, ob $B_1,\ldots,B_k$, $g^{-1}Ag$ linear unabhängig sind. Hierbei gilt $B := \{B_1,\ldots,B_k\}$. Wir verwenden die Laufzeiten aus dem Beweis von Lemma III.7.1. Wir müssen die Schleife maximal n^2-mal ausführen

und erhalten

$$\begin{aligned}
&\sum_{k=1}^{n^2}(2|S|+1)(2|K|+k)(2n^\omega + n^{2\omega}) \\
\leq\ & (2|S|+1)3n^{2\omega}\sum_{k=1}^{n^2}(2|K|+k) \\
\leq\ & (2|S|+1)3n^{2\omega}(2|K|n^2) + (2|S|+1)3n^{2\omega}(n^2)^2 \\
\in\ & O(|K||S|n^{2\omega+2} + |S|n^{2\omega+4})
\end{aligned}$$

als Laufzeit für die Schleife. Anschließend führen wir noch `BasisEnvAlgebra` aus. Da $|B| \leq 2|K| + n^2$ gilt, erhalten wir

$$O((2|K| + n^2)n^{2\omega+4}) = O(|K|n^{2\omega+4} + n^{2\omega+6}),$$

nach Lemma III.7.1. Wenn wir alles zusammenaddieren, erhalten wir die gewünschte Laufzeit. □

Theorem III.7.3: *Die Laufzeit des Algorithmus* 6 `isDense` *auf* t *und* $S \subseteq \Sigma(n, \mathbb{Z})$ *liegt in* $O(|S|n^{2\omega+4} + n^{2\omega+6})$.

Beweis: Wenn wir in Zeile 1 den Algorithmus `BasisAlgebraClosure` ausführen, gilt $K = \{t\}$. Also gilt $|K| = 1$. Daher erhalten wir eine Laufzeit von

$$O(|K||S|n^{2\omega+2} + (|S| + |K|)n^{2\omega+4} + n^{2\omega+6}) = O(|S|n^{2\omega+4} + n^{2\omega+6}). \qquad \square$$

Bemerkung III.7.4: Indem wir annehmen, dass die Menge S in Theorem III.7.3 *klein* ist, erhalten wir eine Laufzeit von $O(n^{2\omega+6}) \subseteq O(n^{11})$. Diese liegt also zwischen den Laufzeiten von `IsDenseIR1` und `IsDenseIR2`.

Kapitel IV.

Anwendungsbeispiele

Alle Algorithmen aus diesem Kapitel wurden von Detinko-Flannery-Hulpke implementiert und können auf dem GitHub von A. Hulpke gefunden werden.[1] Wir werden hierbei die Version 1.12 verwenden (Stand 17.09.21).

1. Die spezielle lineare Gruppe

Zuerst wollen wir uns mit Beispielen aus der speziellen linearen Gruppe beschäftigen. Hierbei fangen wir mit Beispiel IV.1.1 an, bei welchem wir eine Gruppe konstruieren, welche zwar dicht ist, aber nicht arithmetisch. Solche Gruppen werden als *dünn* (*thin*) bezeichnet. Anschließend werden wir in Beispiel IV.1.3 sehen, dass $\mathcal{E}_{3,3}$ aus Definition II.1.1 nicht normal ist.

Beispiel IV.1.1 (aus [12, Theorem 1.1 und Theorem 3.3]): Wir betrachten die Matrix

$$\Delta(x) := \begin{pmatrix} 0 & x^2+1 & x \\ x & 0 & x+1 \\ -x+1 & x^2 & 0 \end{pmatrix}$$

und definieren für $1 \leq i \leq 3$ die Matrix

$$T_i := \prod_{\substack{j=1 \\ i \neq j}}^{3} (I_3 + \Delta_{i,j}(x) E_{i,j}).$$

Nach [12] sind alle T_i in $\mathrm{SL}(3,\mathbb{Z})$ und Transvektionen. Wenn wir $x = 11$ wählen, erhalten wir die Gruppe

$$H = \left\langle \begin{pmatrix} 1 & 122 & 11 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 11 & 1 & 12 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -10 & 121 & 1 \end{pmatrix} \right\rangle.$$

[1] `https://github.com/hulpke/arithmetic`

Diese Gruppe ist nach [12, Theorem 1.2 und Theorem 3.3] eine freie Gruppe von Rang 3, für welche $\varphi_p(H) = \mathrm{SL}(3,p)$ für alle Primzahlen p gilt. Tatsächlich ist die Gruppe nach `isDense` und `PrimesForDense` dicht und $\Pi(H) := \{\}$. Hierbei kann man als Transvektion einer der drei Erzeuger von H nehmen. Daher hat die Gruppe das Level 1. Allerdings gilt $H \neq \mathrm{SL}(n,\mathbb{Z})$, da H nicht arithmetisch ist.

Sei $n := 3$. Angenommen H wäre arithmetisch, dann würde $\Gamma_{n,k} \leq H$ für $k \in \mathbb{N}$ gelten. Sei U die Untergruppe aller oberen Dreiecksmatrizen, deren Hauptdiagonale nur aus Einsen bestehen. Offensichtlich gilt $U \subseteq \mathrm{SL}(n,\mathbb{Z})$. Außerdem ist U auflösbar, denn es gilt

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}^{-1} = \begin{pmatrix}1&0&-cx+az\\0&1&0\\0&0&1\end{pmatrix},$$

$$\begin{pmatrix}1&0&a\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&b\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&a\\0&1&0\\0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&0&b\\0&1&0\\0&0&1\end{pmatrix}^{-1} = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}.$$

Also ist $H \cap U \supseteq \Gamma_{n,k} \cap U$ auflösbar. Da H nach [12, Theorem 1.2] frei ist, ist auch $\Gamma_{n,k} \cap U$ frei, daher muss $\Gamma_{n,k} \cap U$ wegen der Auflösbarkeit zyklisch sein und damit abelsch. Allerdings ist $\Gamma_{n,k} \cap U$ für $n \geq 3$ offensichtlich nicht abelsch. Daher folgt aus $\Gamma_{n,k} \leq H$ ein Widerspruch, weshalb H nicht arithmetisch ist.

Bemerkung IV.1.2: Nach [12, Theorem 3.3] kann man Beispiel IV.1.1 für alle $x \geq 11$ durchführen. In [12, Theorem 3.3] wird ebenfalls eine Konstruktion angegeben, mit welcher man für jedes $n \geq 3$ eine Gruppe $H \leq \mathrm{SL}(n,\mathbb{Z})$ konstruieren kann, sodass H nicht arithmetisch ist und $\Pi(H) = \{\}$ gilt. Die Beweisidee, warum H arithmetisch ist, ist in diesem Fall dieselbe Beweisidee wie in Beispiel IV.1.1. Insbesondere berechnet der Algorithmus `LevelMaxPCS` das Level der arithmetischen Obergruppe von H, welche die $\mathrm{SL}(n,\mathbb{Z})$ ist.

Beispiel IV.1.3: Die Gruppe $\mathcal{E}_{3,3}$ aus Definition II.1.1 ist bezüglich der $\mathrm{SL}(3,\mathbb{Z})$ kein Normalteiler und damit gilt $\mathcal{E}_{3,3} \lneqq \Gamma_{3,3}$. Außerdem ist $\mathcal{E}_{3,3}$ dicht und arithmetisch.

Beweis: Nach Konstruktion der Gruppe liegt die Transvektion

$$t := \begin{pmatrix}1&0&3\\0&1&0\\0&0&1\end{pmatrix}$$

in $\mathcal{E}_{3,3}$, daher können wir die Algorithmen `isDense`, `PrimesForDense` und `LevelMaxPCS` verwenden. Wir erhalten, dass $\mathcal{E}_{3,3}$ dicht ist. Außerdem ist das Level der arithmetischen Obergruppe 9. Daher kann $\mathcal{E}_{3,3}$ kein Normalteiler sein, denn sonst würde $\mathcal{E}_{3,3} = \mathcal{E}_{3,3}^{\mathrm{SL}(3,\mathbb{Z})} = \Gamma_{3,3}$ nach Theorem II.1.3 folgen, aber das Level von $\Gamma_{3,3}$ ist 3.

Da das Level von $\mathcal{E}_{3,3}$ gleich 9 ist, folgt, dass $\mathcal{E}_{3,3}\Gamma_{3,9}$ die arithmetische Obergruppe von $\mathcal{E}_{3,3}$ ist. Nach [8, Proposition 1.12] gilt $\Gamma_{3,9} \leq \mathcal{E}_{3,3}$, weshalb $\mathcal{E}_{3,3}$ arithmetisch ist. Da offensichtlich $t \notin \Gamma_{3,9}$ ist, folgt $\Gamma_{3,9} \lneqq \mathcal{E}_{3,3} \lneqq \Gamma_{3,3}$.

Bemerkung IV.1.4: Sei $n \in \{3, 5, 7, 9\}$ und $m \in \{2, 3, \ldots, 20\}$, dann kann man wie in Beispiel IV.1.3 das Level von $\mathcal{E}_{n,m}$ berechnen. Dies ist immer m^2, weshalb man Beispiel IV.1.3 analog durchführen kann.

Bemerkung IV.1.5: Nach [8, Proposition 1.12] ist $\mathcal{E}_{n,m}$ im SL-Fall für alle $n \geq 3$ immer arithmetisch. Hat also H das Level M, dann ist H genau dann arithmetisch, wenn $\mathcal{E}_{n,M} \leq H$ gilt.

2. Die symplektische Gruppe

In diesem Abschnitt werden wir uns mit der symplektischen Gruppe beschäftigen. Wir werden zuerst sehen, dass man durch einen Basiswechsel das Level einer Gruppe verändern kann. Anschließend werden wir uns mit der Berechnung des Levels und Index von *hypergeometric groups* beschäftigen.

Bemerkung IV.2.1: Wir haben die Gruppe $\mathrm{Sp}(n, \mathbb{Z})$ als die Menge der invertierbaren Matrizen A definiert, sodass $AJA^\top = J$ gilt. Nach II.1.3 ist $\mathcal{E}_{n,1}$ ein Erzeuger von $\mathrm{Sp}(n, \mathbb{Z})$. Aus dem Aufbau der Erzeuger folgt aber direkt $A^\top \in \mathrm{Sp}(n, \mathbb{Z})$, falls $A \in \mathrm{Sp}(n, \mathbb{Z})$ gilt.

Insbesondere hätten wir für unsere Definition der symplektischen Gruppe auch die Gleichung $A^\top JA = J$ verwenden können.

Beispiel IV.2.2: Sei $n \geq 3$. Wir betrachten die $\mathcal{E}_{n,m}$ und die Matrix

$$B_\alpha := \begin{pmatrix} 1 & 0 & \frac{1}{\alpha} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

wobei wir $B_0 := I_4$ definieren. Wir betrachten im Folgenden die Gruppe $B_\alpha^{-1}\mathcal{E}_{n,m}B_\alpha$. Falls $B_\alpha^{-1}\mathcal{E}_{n,m}B_\alpha \subseteq \mathrm{Sp}(n, \mathbb{Z})$ gilt, können wir das Level und den Index der arithmetischen Obergruppe berechnen.

n	m	α	Level	Level	Index
4	576	0	331776	$2^{12}3^4$	$2^{85}3^{24}5^2$
4	576	1	331776	$2^{12}3^4$	$2^{85}3^{24}5^2$
4	576	2	663552	$2^{13}3^4$	$2^{85}3^{24}5^2$
4	576	3	995328	$2^{12}3^5$	$2^{85}3^{24}5^2$
4	576	4	1327104	$2^{14}3^4$	$2^{85}3^{24}5^2$
4	576	6	1990656	$2^{13}3^5$	$2^{85}3^{24}5^2$
4	576	8	2654208	$2^{15}3^4$	$2^{85}3^{24}5^2$
4	576	12	3981312	$2^{14}3^5$	$2^{85}3^{24}5^2$
4	576	24	7962624	$2^{15}3^5$	$2^{85}3^{24}5^2$

Tabelle IV.1.: Beispiele dafür, wie Konjugation ($B_\alpha^{-1}\mathcal{E}_{n,m}B_\alpha$) das Level verändert. Es sei angemerkt, dass $m = 576 = 24^2$ gilt. Hierbei ist 24 eine *highly composite number*, sprich eine Zahl mit möglichst vielen Teilern. Die Teiler von 24 stimmen mit α überein.

Anhand der Tabelle IV.1 sieht man, dass man durch Konjugation das Level, welches ursprünglich 331776 war, vergrößern kann. Die Primteiler werden allerdings nicht verändert. Genauso bleibt der Index unverändert. Es sei angemerkt, dass man analog auch Beispiele für die $\mathrm{SL}(n,\mathbb{Z})$ konstruieren kann, für die der Index durch Konjugation größer wird.

Bemerkung IV.2.3: Wir wollen uns nun einigen Ergebnissen aus dem Paper [22] widmen. Was folgt, ist eine Zusammenfassung von *1. Introduction*. In diesem Paper geht es um *hypergeometric groups*. Hierfür betrachten wir die Riemann-Fläche $S := \mathbb{P}^1 \setminus \{0, 1, \infty\}$ und den Ableitungsoperator $\theta = z\frac{d}{dz}$ auf dieser Fläche. Sei $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ und $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{C}^n$, dann wird durch

$$D = (\theta + \beta_1 - 1)\cdots(\theta + \beta_n - 1) - z(\theta + a_1)\cdots(\theta + a_n)$$

ein Ableitungsoperator auf S definiert. Wir betrachten nun die Fundamentalgruppe π von S zum Basispunkt $\frac{1}{2}$. Diese wird frei von $h_\infty,\ h_0,\ h_1$ erzeugt, mit der Einschränkung, dass $h_0h_1h_\infty = 1$ gilt. Hierbei ist h_i eine Schleife um den Punkt i.

Seien nun $f = \prod_{j=1}^n (X - a_j) = X^n + A_{n-1}X^{n-1} + \cdots + A_1X + A_0$ und $g = \prod_{j=1}^n (X - b_j) = X^n + B_{n-1}X^{n-1} + \cdots + B_1X + B_0$ mit $a_j = e^{2\pi i\alpha_j}$ und $b_j = e^{2\pi i\beta_j}$, dann betrachten wir die Matrizen

$$A := \begin{pmatrix} 0 & \dots & 0 & -A_0 \\ 1 & \dots & 0 & -A_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & -A_{n-1} \end{pmatrix}, \quad B := \begin{pmatrix} 0 & \dots & 0 & -B_0 \\ 1 & \dots & 0 & -B_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & -B_{n-1} \end{pmatrix}.$$

Nach den Ergebnissen von [4, Theorem 3.5 und Proposition 3.2] existiert eine Basis des Vektorraums der Lösungsmenge der Differentialgleichung $Du = 0$ auf der Kurve S, sodass man die Monodromiewirkung der Fundamentalgruppe π wie folgt beschreiben kann: h_∞ wirkt über B^{-1}, h_0 wirkt über A und h_1 über $C = A^{-1}B$. Außerdem ist C nach [22, Seite 4] eine Transvektion. Wir definieren $\Gamma := \langle A, B \rangle$.

Wir betrachten nun den Fall, dass f, $g \in \mathbb{Z}[X]$ keine gemeinsame Nullstelle haben und ein *primitives Paar* sind. Letzteres bedeutet, dass es keine Polynome f_1, $g_1 \in \mathbb{Z}[X]$ und ein $k \geq 2$ gibt, sodass $f(X) = f_1(X^k)$ und $g(X) = g_1(X^k)$ gilt. Nach [4, Theorem 4.3] und [22, Seite 3] gibt es nun eine nicht entartete symplektische Form Ω, sodass

$$\Gamma \subseteq \mathrm{Sp}_\Omega := \{A \in \mathrm{GL}(n, \mathbb{Z}) : A^\top \Omega A = \Omega\}$$

gilt.

Im Paper [22] wird insbesondere der Fall $n = 4$ und $A_0 = B_0 = 1$ betrachtet. Falls das Gleichungssystem

$$\begin{pmatrix} A_3 & 1 \\ B_3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 - A_2 \\ 1 - B_2 \end{pmatrix} \tag{IV.1}$$

eine Lösung hat, dann ist die symplektische Form (bis auf ein Vielfaches) durch

$$\Omega := \begin{pmatrix} 0 & 1 & x & y \\ -1 & 0 & 1 & x \\ -x & -1 & 0 & 1 \\ -y & -x & -1 & 0 \end{pmatrix}$$

bestimmt. Das Problem ist aber, dass Ω nicht mit unserer Definition von J (Definition I.2.1) übereinstimmt. Wir müssen also eine Basiswechselmatrix D finden, sodass $D^\top \Omega D = J$ gilt. Glücklicherweise kann man diese meistens direkt angeben:

$$D := \begin{pmatrix} 1 & 1 & 0 & \frac{-x}{-x^2-y-1} \\ 0 & -x & 1 & \frac{y}{-x^2-y-1} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \frac{-1}{-x^2-y-1} \end{pmatrix}.$$

Falls die Gleichung (IV.1) keine Lösung hat, ist $A_3 = B_3$. Wir erhalten die symplektische Form (bis auf ein Vielfaches) durch

$$\Omega := \begin{pmatrix} 0 & 0 & 1 & -A_3 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ A_3 & -1 & 0 & 0 \end{pmatrix}.$$

Die Basiswechselmatrix ist

$$D := \begin{pmatrix} 1 & 0 & 0 & 0 \\ A_3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Für $X := D^{-1}AD$ und $Y := D^{-1}BD$ folgt nun $X^\top JX = J$ und $Y^\top JY = J$. Das Problem ist, dass es durch den Basiswechsel sein kann, dass X, Y nicht mehr in $\mathbb{Z}^{4\times 4}$ liegen. Liegen die Matrizen aber in $\mathbb{Z}^{4\times 4}$, dann folgt $\langle X, Y\rangle \subseteq \mathrm{Sp}(4, \mathbb{Z})$ nach Bemerkung IV.2.1.

Beispiel IV.2.4: Nach [22, Table 5.1] sind alle f, $g \in \mathbb{Z}[X]$ der Tabelle IV.2 primitive Paare mit unterschiedlichen Nullstellen. Sie implizieren also eine Gruppe $\langle A, B\rangle \subseteq \mathrm{Sp}_\Omega$. Wir können Ω wie in Bemerkung IV.2.3 berechnen. Genauso berechnen wir die Basiswechselmatrix D. Wir berechnen dies für jeden Eintrag der Tabelle 5.1. Falls $D^{-1}AD$ und $D^{-1}BD$ in $\mathbb{Z}^{4\times 4}$ liegen, können wir die Algorithmen aus dieser Arbeit verwenden (als Transvektion können wir immer $C = A^{-1}B$ nehmen). Hierdurch erhalten wir die Tabelle IV.2, wobei wir die Nummerierung von [22, Table 5.1] beibehalten.

Es sei angemerkt, dass nach [22, Theorem 1.1] alle Gruppen der Tabelle IV.2 arithmetisch sind, allerdings wird in [22, Table 5.1] weder das Level noch der Index berechnet.

Beispiel IV.2.5: Wir wollen nun analog zum Beispiel IV.2.4 die Quelle [22, Table 5.3] analysieren. Hierbei analysieren wir wieder Gruppen, welche durch $f(X)$ und $g(X)$ beschrieben werden (vgl. Bemerkung IV.2.3). Bei den Beispielen aus [22, Table 5.3] handelt es sich um sich 14 Gruppen, welche mit *Calabi-Yau threefolds* in Verbindung stehen. Wir versuchen, wie in Beispiel IV.2.4, den Index und das Level zu berechnen, da diese in [22, Table 5.3] nicht aufgelistet sind. Hierbei wird ein Eintrag in [22, Table 5.3] übersprungen, sofern der Basiswechsel mit der Matrix D (siehe Bemerkung IV.2.3) misslingt. Als Ergebnis erhalten wir die Tabelle IV.3, deren Nummerierung mit [22, Table 5.3] übereinstimmt. Da für alle 14 Gruppen aus Table 5.3 immer $f(X) = (X-1)^4$ gilt, werden wir in Tabelle IV.3 nur $g(X)$ auflisten.

No.	$f(X)$	$g(X)$	Level	Index
13	$X^4 - X^3 - X + 1$	$X^4 - X^3 + 2X^2 - X + 1$	4	960
15	$X^4 - X^3 - X + 1$	$X^4 - X^3 + X^2 - X + 1$	2	6
18	$X^4 + 2X^3 + 3X^2 + 2X + 1$	$X^4 + 2X^3 + 2X^2 + 2X + 1$	2	10
19	$X^4 + 2X^3 + 3X^2 + 2X + 1$	$X^4 + X^3 + X^2 + X + 1$	1	1
22	$X^4 + 2X^3 + 3X^2 + 2X + 1$	$X^4 - X^2 + 1$	4	960
24	$X^4 - 2X^3 + 2X^2 - 2X + 1$	$X^4 - 2X^3 + 3X^2 - 2X + 1$	2	10
26	$X^4 - 2X^3 + 2X^2 - 2X + 1$	$X^4 + 1$	4	5760
27	$X^4 - 2X^3 + 2X^2 - 2X + 1$	$X^4 - X^3 + X^2 - X + 1$	2	6
29	$X^4 + 2X^2 + 1$	$X^4 + X^3 + X^2 + X + 1$	2	6
32	$X^4 + 2X^2 + 1$	$X^4 - X^3 + X^2 - X + 1$	2	6
33	$X^4 + 2X^3 + 2X^2 + 2X + 1$	$X^4 + X^3 + X^2 + X + 1$	2	6
35	$X^4 + 2X^3 + 2X^2 + 2X + 1$	$X^4 + 1$	4	5760
37	$X^4 + X^3 + 2X^2 + X + 1$	$X^4 + X^3 + X^2 + X + 1$	2	6
38	$X^4 + X^3 + 2X^2 + X + 1$	$X^4 + X^3 + X + 1$	4	960
42	$X^4 + X^3 + X^2 + X + 1$	$X^4 + X^3 + X + 1$	2	6
43	$X^4 + X^3 + X^2 + X + 1$	$X^4 + X^2 + 1$	1	1
45	$X^4 + X^3 + X^2 + X + 1$	$X^4 + 1$	2	6
46	$X^4 + X^3 + X^2 + X + 1$	$X^4 - X^3 + X^2 - X + 1$	4	4608
47	$X^4 + X^3 + X^2 + X + 1$	$X^4 - X^2 + 1$	1	1
50	$X^4 - 2X^3 + 3X^2 - 2X + 1$	$X^4 - X^3 + X^2 - X + 1$	1	1
51	$X^4 - 2X^3 + 3X^2 - 2X + 1$	$X^4 - X^2 + 1$	4	960
55	$X^4 + X^2 + 1$	$X^4 - X^3 + X^2 - X + 1$	1	1
57	$X^4 - X^3 + 2X^2 - X + 1$	$X^4 - X^3 + X^2 - X + 1$	2	6
59	$X^4 + 1$	$X^4 - X^3 + X^2 - X + 1$	2	6
60	$X^4 - X^3 + X^2 - X + 1$	$X^4 - X^2 + 1$	1	1

Tabelle IV.2.: Level und Index von Gruppen aus [22, Table 5.1]

No.	$g(X)$	Level	Index	Level*
5	$X^4 + 2X^2 + 1$	2^4	$2^{20}3^25$	2^6
8	$X^4 + X^3 + X^2 + X + 1$	2^15^2	$2^83^35^813$	2^15^3

Tabelle IV.3.: Level und Index von Gruppe aus [22, Table 5.3] und [7, Table 3]

Mit der Spalte Level* ist das Level in [7, Table 3] gemeint, wobei No. auch die Zeilennummer in dieser Tabelle ist. In diesem Paper wird ebenfalls das Level und der Index berechnet. Allerdings unterscheidet sich der Basiswechsel von unserer Methode aus Bemerkung IV.2.3, weshalb zwar der Index gleich ist, sich aber das Level unterscheidet. Der andere Basiswechsel wird in [7, Abschnitt 4.2] erklärt.

Es sei angemerkt, dass wir in Beispiel IV.2.2 bereits gesehen haben, dass sich das Level durch einen Basiswechsel verändern kann.

Die Gruppe Nummer 5 aus Tabelle IV.3 ist nach [21, Abschnitt 2.4] arithmetisch. Nach [6, Theorem 1] ist Nummer 8 nicht arithmetisch. Daher ist sie dünn.

3. Empirischer Laufzeitvergleich der Dichtheitstests

Wir wollen nun einen empirischen Laufzeitvergleich der Algorithmen `isDense`, `IsDenseIR1` und `IsDenseIR2` durchführen (siehe Abschnitt III.7 für eine Beschreibung der Algorithmen).

Der Algorithmus 6 `isDense` hat hierbei den Namen `IsDenseDFH`. Alle Berechnungen wurden auf einem `Intel© Core i5-7300HQ CPU @ 2.50GHz` Prozessor ausgeführt. Alle Zeitangaben sind in Sekunden. Sollte ein Programm bei dem Ausführen eines Beispieles weniger als 10 Sekunden benötigen, so wird die Berechnung 20-mal wiederholt und die Laufzeit gemittelt, um einen genaueren Wert zu erhalten. Falls in einer Tabelle ein $-$ steht, bedeutet es, dass die Suche nach 30 Minuten abgebrochen wurde. Wir wollen nun alle drei Algorithmen unter unterschiedlichen Bedingungen testen.

Beispiel IV.3.1: Als erstes betrachten wir die Gruppe

$$U_n := \langle \{ I_n + E_{i,j} : 1 \leq i < j \leq n \} \rangle$$

der oberen Dreiecksmatrizen, wo die Hauptdiagonale nur aus Einsen besteht. Es gilt offensichtlich $U_n \leq \mathrm{SL}(n, \mathbb{Z})$. Allerdings ist die Gruppe nicht dicht, da für alle Primzahlen die Gruppe $\varphi_p(U_n)$ nur aus Dreiecksmatrizen besteht, weshalb $\varphi_p(U_n) \neq \mathrm{SL}(n, p)$ gilt. Wir erhalten die Laufzeiten aus Tabelle IV.4.

Beispiel IV.3.2: Sei $n := 2s$. Als nächstes betrachten wir die Gruppe

$$V_n := \langle \{ I_n + E_{i,j+s} + E_{j,i+s}\,,\ \ I_n + E_{i,i+s} : 1 \leq i \neq j \leq n \} \rangle,$$

welche eine Untergruppe der $\mathrm{Sp}(n, \mathbb{Z})$ ist. Da diese ebenfalls nur aus oberen Dreiecksmatrizen besteht, kann man analog zu Beispiel IV.3.1 zeigen, dass V_n nicht dicht in $\mathrm{Sp}(n, \mathbb{Z})$ ist. Wir erhalten die Laufzeiten der Tabelle IV.5.

n	IsDenseDFH	IsDenseIR1	IsDenseIR2
3	0.031	0.002	0.010
5	0.012	0.002	15.129
7	0.023	0.003	–
9	0.040	0.003	–
11	0.066	0.004	–
13	0.109	0.005	–
27	1.253	0.036	–
29	1.599	0.043	–
31	1.926	0.053	–
33	2.819	0.073	–
35	3.653	0.092	–
37	4.512	0.111	–
39	5.825	0.203	–
41	7.638	0.179	–
43	8.459	0.280	–
45	13.354	0.275	–

Tabelle IV.4.: Laufzeiten für Beispiel IV.3.1

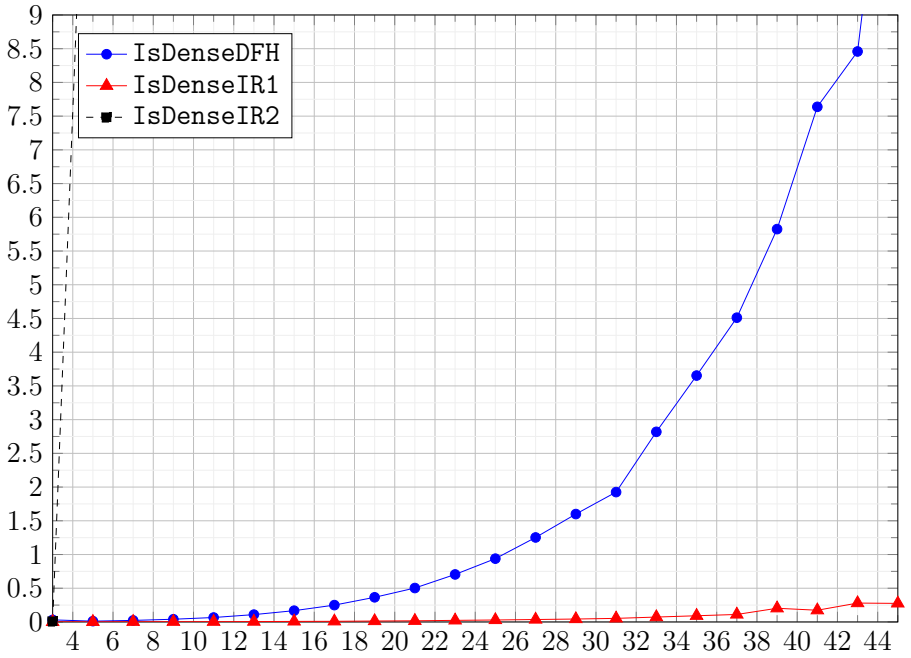

Abbildung IV.1.: Graph der Laufzeiten der Tabelle IV.4

n	`IsDenseDFH`	`IsDenseIR1`	`IsDenseIR2`
4	0.082	0.005	0.010
6	0.0083	0.007	0.462
8	0.013	0.008	11.838
10	0.019	0.009	209.427
12	0.035	0.013	–
14	0.043	0.013	–
16	0.060	0.015	–
18	0.124	0.018	–
20	0.119	0.055	–
40	1.659	0.090	–
42	1.953	0.103	–
44	2.303	0.120	–
70	14.819	0.610	–
72	14.025	0.579	–
74	15.257	0.639	–
100	48.207	2.197	–
102	50.294	2.31	–
104	54.187	2.521	–
140	193.438	9.417	–
142	180.640	10.009	–
170	384.608	23.030	–
172	449.599	24.413	–

Tabelle IV.5.: Laufzeiten für Beispiel IV.3.2

n	`IsDenseDFH`	`IsDenseIR1`	`IsDenseIR2`
3	0.053	0.009	0.193
5	0.168	0.074	772.832
7	1.554	0.895	–
9	23.672	6.609	–
11	30.902	33.762	–
13	–	163.140	–
15	–	427.279	–
17	–	1218.690	–
19	–	3512.838	–

Tabelle IV.6.: Laufzeiten für Beispiel IV.3.3

n	`IsDenseDFH`	`IsDenseIR1`	`IsDenseIR2`
4	0.369	0.048	0.960
6	0.405	0.298	135.516
8	5.768	1.447	–
10	14.999	6.317	–
12	190.693	26.007	–
14	255.136	92.319	–
16	–	502.655	–
18	–	753.269	–
20	–	1395.069	–

Tabelle IV.7.: Laufzeiten für Beispiel IV.3.4

Beispiel IV.3.3: Sei $n \geq 3$ und $\mathcal{E}_{n,1} \leq \mathrm{SL}(n, \mathbb{Z})$. Nach Theorem II.1.3 ist diese Gruppe arithmetisch und erzeugt die $\mathrm{SL}(n, \mathbb{Z})$. Wir erhalten die Laufzeiten der Tabelle IV.6.

Beispiel IV.3.4: Sei $n \geq 4$ und $\mathcal{E}_{n,1} \leq \mathrm{Sp}(n, \mathbb{Z})$. Nach Theorem II.1.3 ist diese Gruppe arithmetisch und erzeugt die $\mathrm{Sp}(n, \mathbb{Z})$. Wir erhalten die Laufzeiten der Tabelle IV.7.

Kapitel V.

Fazit

1. Beurteilung des Verfahrens

Wir haben in dieser Arbeit eine Methode kennengelernt, wie man das Level von arithmetischen Obergruppen bestimmen kann. Mit diesem Level kann man viele andere Probleme auf endliche Gruppe zurückführen, mit welchen man algorithmisch viel besser arbeiten kann. Dahingehend kann das Verfahren sehr praktisch sein, allerdings müssen wir drei Aspekte berücksichtigen.

Erstens funktioniert das Verfahren nur für eine Gruppe $H \leq \Sigma(n, \mathbb{Z})$, wenn n ungerade ist oder wenn $H \leq \mathrm{Sp}(n, \mathbb{Z})$ gilt.

Zweitens benötigen wir für Algorithmus 5 `PrimesForDense` immer eine Transvektion. Nach [23, Proposition 5.3] gibt es aber dichte Gruppen, welche keine unipotenten Elemente haben. Daher können diese Gruppen auch keine Transvektionen besitzen. Wenn aber H arithmetisch ist, dann gilt für ein M stets $\mathcal{E}_{n,M} \leq \Gamma_{n,M} \leq H$. Einige der Erzeuger von $\mathcal{E}_{n,M}$ sind nach Definition II.1.1 Transvektionen, weshalb es in arithmetischen Gruppe immer Transvektionen gibt. Allerdings muss man diese erst einmal finden, was in der Praxis schwierig sein kann, da Transvektionen selten sein können. Je nach Problem kann es aber sein, dass wir nach Konstruktion bereits eine Transvektion haben (siehe z. B. Bemerkung IV.2.3).

Das dritte Problem ist der Umstand, dass wir nach der erfolgreichen Berechnung des Levels nicht wissen, ob H arithmetisch ist. Wenn wir also anschließend das Level M verwenden, um ein Problem auf eine endliche Gruppe $\varphi_M(H)$ zurückzuführen, so kann es sein, dass wir letztlich nur Aussagen über die minimale arithmetische Obergruppe von H zeigen, was zu Problemen führen kann.

2. Vergleich der Dichtheitstests

Wir sehen anhand der Analyse im Abschnitt III.7 und Abschnitt IV.3 ein deutliches Ergebnis. Der mit Abstand schnellste Algorithmus ist `IsDenseIR1`, dann folgt der Algorithmus `IsDenseDFH`. Der langsamste Algorithmus ist `IsDenseIR2`. Hieraus lässt sich die folgende Empfehlung ableiten.

Wenn man die Dichtheit einer Gruppe H untersuchen will, so sollte man zunächst immer `IsDenseIR1` ausführen. Gibt dieser `True` zurück, so ist die Gruppe dicht. Bei der Ausgabe `False` kann es sein, dass die Suche erfolglos war.[1]

Falls n ungerade ist oder $H = \mathrm{Sp}(n, \mathbb{Z})$ gilt und man eine Transvektion t hat, kann man den Algorithmus `IsDenseDFH` ausführen, um die Dichtheit von H zu ermitteln.

Ist man aber in der Situation, dass man den Algorithmus `IsDenseDFH` nicht verwenden kann, so muss man auf `IsDenseIR2` zurückgreifen, welcher eine hohe Laufzeit hat. Daher kann es sein, dass man nie das Ergebnis erfahren wird.

[1] In der Implementierung von A. Hulpke kann man die Wahrscheinlichkeit einer falschen Ausgabe verringern, indem man den Wert `radius` erhöht.

Literatur

[1] H. Bass, J. Milnor und J. P. Serre. „Solution of the congruence subgroup problem for $\mathrm{SL}_n\,(n \geq 3)$ and $\mathrm{Sp}_{2n}\,(n \geq 2)$“. In: *Inst. Hautes Études Sci. Publ. Math.* 33 (1967), S. 59–137. ISSN: 0073-8301. URL: http://www.numdam.org/item?id=PMIHES_1967__33__59_0.

[2] B. Beisiegel. „Die Automorphismengruppen homozyklischer p-Gruppen“. In: *Arch. Math. (Basel)* 29.4 (1977), S. 363–366. ISSN: 0003-889X. DOI: 10.1007/BF01220419. URL: https://doi.org/10.1007/BF01220419.

[3] M. Chiara Tamburini Bellani. *The classical groups and their geometries*. Università del Salento - Coordinamento SIBA, 2016. ISBN: 978-88-8305-120-3.

[4] F. Beukers und G. Heckman. „Monodromy for the hypergeometric function ${}_nF_{n-1}$“. In: *Inventiones mathematicae* 95 (1989), S. 325–354. URL: https://doi.org/10.1007/BF01393900.

[5] S. Bosch. *Algebra*. 8. Aufl. Berlin: Springer Spektrum, 2013. DOI: 10.1007/978-3-642-39567-3.

[6] Christopher Brav und Hugh Thomas. „Thin monodromy in Sp(4)“. In: *Compositio Mathematica* 150.3 (2014), S. 333–343. ISSN: 1570-5846. DOI: 10.1112/s0010437x13007550. URL: http://dx.doi.org/10.1112/S0010437X13007550.

[7] A. Detinko, D. Flannery und A. Hulpke. „Zariski density and computing in arithmetic groups“. In: *Math. Comput.* 87 (2018), S. 967–986.

[8] A. S. Detinko, D. L. Flannery und A. Hulpke. „Algorithms for arithmetic groups with the congruence subgroup property“. In: *J. Algebra* 421 (2015), S. 234–259. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2014.08.027. URL: https://doi.org/10.1016/j.jalgebra.2014.08.027.

[9] A.S. Detinko und D.L. Flannery. „On deciding finiteness of matrix groups“. In: *J. Symbolic Comput* 44 (2009), S. 1037–1043.

[10] F. L. Gall. *Powers of Tensors and Fast Matrix Multiplication*. 2014. arXiv: 1401.7714 [cs.DS].

[11] Alexander J. Hahn und O. Timothy O'Meara. *The classical groups and K-theory*. Bd. 291. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. With a foreword by J. Dieudonné. Springer-Verlag, Berlin, 1989, S. xvi+576. ISBN: 3-540-17758-2. DOI: 10.1007/978-3-662-13152-7. URL: https://doi.org/10.1007/978-3-662-13152-7.

[12] S. P. Humphries. „Free Subgroups of SL(n, Z), n > 2, Generated by Transvections". eng. In: *Journal of Algebra* 116 (1988), S. 155–162.

[13] T. W. Hungerford. *Algebra*. 1. Aufl. New York: Springer-Verlag, 1974. ISBN: 978-1-4612-6103-2. DOI: 10.1007/978-1-4612-6101-8.

[14] B. Huppert. *Endliche Gruppen I*. Berlin: Springer-Verlag, 1967.

[15] O. H. Ibarra, S. Moran und R. Hui. „A generalization of the fast LUP matrix decomposition algorithm and applications". In: *Journal of Algorithms* 3.1 (1982), S. 45–56. ISSN: 0196-6774. DOI: https://doi.org/10.1016/0196-6774(82)90007-4. URL: https://www.sciencedirect.com/science/article/pii/0196677482900074.

[16] C. R. Matthews, L. N. Vaserstein und B. Weisfeiler. „Congruence properties of Zariski-dense subgroups. I". In: *Proc. London Math. Soc. (3)* 48.3 (1984), S. 514–532. ISSN: 0024-6115. DOI: 10.1112/plms/s3-48.3.514. URL: https://doi.org/10.1112/plms/s3-48.3.514.

[17] Jens L. Mennicke. „Finite Factor Groups of the Unimodular Group". In: *Annals of Mathematics* 81.1 (1965), S. 31–37. ISSN: 0003-486X. URL: http://www.jstor.org/stable/1970380.

[18] M. Newman und J. R. Smart. „Symplectic modulary groups". eng. In: *Acta Arithmetica* 9.1 (1964), S. 83–89. URL: http://eudml.org/doc/207465.

[19] I. Rivin. *Large Galois groups with applications to Zariski density*. 2015. arXiv: 1312.3009 [math.NT].

[20] I. Rivin. „Zariski density and genericity". In: *Int. Math. Res. Not. IMRN* 19 (2010), S. 3649–3657. ISSN: 1073-7928. DOI: 10.1093/imrn/rnq043. URL: https://doi.org/10.1093/imrn/rnq043.

[21] S. Singh. „Arithmeticity of Four Hypergeometric Monodromy Groups Associated to Calabi–Yau Threefolds: Table 1." In: *International Mathematics Research Notices* 2015.18 (2014), S. 8874–8889. ISSN: 1687-0247. DOI: 10.1093/imrn/rnu217. URL: http://dx.doi.org/10.1093/imrn/rnu217.

[22] S. Singh und T. N. Venkataramana. „Arithmeticity of certain symplectic hypergeometric groups“. In: *Duke Mathematical Journal* 163.3 (2014). ISSN: 0012-7094. DOI: 10.1215/00127094-2410655. URL: http://dx.doi.org/10.1215/00127094-2410655.

[23] T. N. Venkataramana. „Zariski dense subgroups of arithmetic groups“. In: *J. Algebra* 108.2 (1987), S. 325–339. ISSN: 0021-8693. DOI: 10.1016/0021-8693(87)90106-2. URL: https://doi.org/10.1016/0021-8693(87)90106-2.

[24] T. Weigel. „On a certain class of Frattini extensions of finite Chevalley groups“. In: *Groups of Lie type and their geometries (Como, 1993)*. Bd. 207. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1995, S. 281–288. DOI: 10.1017/CBO9780511565823.019. URL: https://doi.org/10.1017/CBO9780511565823.019.

[25] A. E. Zalesskiı und V. N. Serezkin. „Linear groups generated by transvections“. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 40.1 (1976), S. 26–49, 221. ISSN: 0373-2436.