Einfachheit von $\mathrm{PSL}_n(k)$ (bis auf $n=2$, $k \in \{\mathbf{F}_2, \mathbf{F}_3\}$)

Wir folgen E. Artins *Geometric Algebra,* mit dem Unterschied, daß wir uns auf den Fall eines kommutativen Körpers beschränken und daß wir die Verwendung von Matrizen nicht zu vermeiden versuchen.

Sei $n \geq 2$. Sei k ein (kommutativer) Körper. Schreibe

$$\begin{array}{rcrcl} \mathrm{GL} & := & \mathrm{GL}_n(K) & = & \{A \in K^{n\times n} \;:\; \det A \neq 0\} \\ \mathrm{SL} & := & \mathrm{SL}_n(K) & = & \{A \in K^{n\times n} \;:\; \det A = 1\} \;=\; \mathrm{Kern}(\mathrm{GL} \xrightarrow{\det} k^*) \\ \mathrm{PSL} & := & \mathrm{PSL}_n(K) & = & \mathrm{SL}_n(K)/\mathrm{Z}(\mathrm{SL}_n(K))\;. \end{array}$$

Seien $i,\, j \in [1,n]$ mit $i \neq j$, und sei $\lambda \in k$. Schreibe $E_{i,j}(\lambda) \in \mathrm{SL}$ für die Matrix, deren Hauptdiagonaleinträge gleich 1 sind, deren Eintrag an Position (i,j) gleich λ ist, und deren sonstige Einträge gleich 0 sind.

Bemerkung. Es ist das Zentrum $\mathrm{Z}(\mathrm{SL})$ von SL gleich $\{\lambda E \,:\, \lambda \in k,\ \lambda^n = 1\}$. Ferner ist $\mathrm{Z}(\mathrm{GL}) = \{\lambda E \,:\, \lambda \in k^*\}$. Beides folgt bereits durch einen Vergleich von $E_{i,j}(1)A$ mit $AE_{i,j}(1)$ für $i,j \in [1,n]$, $i \neq j$. Insbesondere ist $\mathrm{Z}(\mathrm{SL}) = \mathrm{Z}(\mathrm{GL}) \cap \mathrm{SL}$.

Bemerkung. Ist $|k| = q$, so hat das Polynom $X^n - 1 \in k[X]$ genau $d := \mathrm{ggT}(n, q-1)$ Nullstellen in k. Denn $k^* \simeq C_{q-1} = \langle \alpha \rangle$, und $(\alpha^j)^n = 1$ gilt für $j \in \mathbf{Z}$ genau dann, wenn $q-1 \mid jn$, i.e. wenn $(q-1)d^{-1} \mid j$. Dies ist für $j \in [0, (q-1)-1]$ gerade $d$mal der Fall.

Insbesondere ist $|\mathrm{Z}(\mathrm{SL})| = d$, und folglich

$$|\,\mathrm{PSL}\,| \;=\; d^{-1}(q-1)^{-1} \prod_{i\in[0,n-1]} (q^n - q^i) \;=\; d^{-1} q^{n(n-1)/2} \prod_{i \in [2,n]} (q^i - 1)\;.$$

Beispiel. Sei $n = 2$ und $k = \mathbf{F}_2$. Es enthält $\mathrm{PSL}_2(\mathbf{F}_2) = \mathrm{SL}_2(\mathbf{F}_2) = \mathrm{GL}_2(\mathbf{F}_2)$ gerade 6 Elemente, ist also nicht einfach, da eine normale 3-Sylowgruppe enthalten ist.

Beispiel. Sei $n = 2$ und $k = \mathbf{F}_3$. Es enthält $\mathrm{PSL}_2(\mathbf{F}_3)$ gerade 12 Elemente, enthält also entweder gerade eine 3-Sylowgruppe, oder aber vier 3-Sylowgruppen, und dann nur eine 2-Sylowgruppe. In beiden Fällen folgt, daß die Gruppe nicht einfach ist.

Definition. Eine Matrix $T \in \mathrm{GL}$ heißt *Scherung,* falls sie GL-konjugiert ist zu $E_{2,1}(1)$.

Beispiel. Sei $a \in k^n \setminus \{0\}$, sei $f \in (k^n)^* \setminus \{0\}$, und sei $f(a) = 0$. Sei A die beschreibende Matrix von $k^n \longrightarrow k^n$, $x \longmapsto x + f(x)a$ bezüglich der Standardbasis. Dann ist A eine Scherung. Denn sei $x_1 \in k^n \setminus \mathrm{Kern}\, f$, sei $x_2 = f(x_1)a$, und sei $(x_2, x_3 \ldots, x_n)$ eine Ergänzung zu einer Basis von $\mathrm{Kern}\, f$. Bezüglich der Basis $(x_1, x_2, x_3 \ldots, x_n)$ von k^n wird unser Endomorphismus nun beschrieben von $E_{2,1}(1)$.

Insbesondere ist für $\lambda \in k^*$ und $i,\, j \in [1,n]$ mit $i \neq j$ unter Verwendung der Projektion f auf die j-te Koordinate, und von $a = \lambda e_i$ die Matrix $E_{i,j}(\lambda)$ als Scherung erkannt.

Ferner ist unter Verwendung der Projektion f auf die erste Koordinate, und einem nichtverschwindenden Vektor a mit erstem Eintrag 0 auch eine Matrix der Form $\left(\begin{smallmatrix} 1 & 0 \\ * & E_{n-1} \end{smallmatrix}\right)$ ungleich E_n als Scherung erkannt.

Lemma 1 *Jede Scherung ist* SL*-konjugiert zu* $E_{2,1}(\lambda)$ *für ein* $\lambda \in k^*$.

Beweis. Sei T Scherung, und sei $S \in \mathrm{GL}$ mit $S^{-1}TS = E_{2,1}(1)$. Sei $\lambda := (\det S)^{-1}$. Dann ist $\tilde{S} := S \left(\begin{smallmatrix} \lambda & 0 \\ 0 & E_{n-1} \end{smallmatrix}\right) \in \mathrm{SL}$ und

$$\tilde{S}^{-1} T \tilde{S} \;=\; \left(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & E_{n-1} \end{smallmatrix}\right) E_{2,1}(1) \left(\begin{smallmatrix} \lambda & 0 \\ 0 & E_{n-1} \end{smallmatrix}\right) = E_{2,1}(\lambda)\;.$$

□

Lemma 2 *Ist $n \geq 3$, so ist jede Scherung ist* SL*-konjugiert zu $E_{2,1}(1)$.*

Beweis. Sei T eine Scherung. Mit Lemma 1 dürfen wir $T = E_{2,1}(\lambda)$ mit $\lambda \in k^*$ annehmen. Wir konjugieren in $\mathrm{SL}_3(k)$ vermöge

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ \lambda & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

und setzen dies durch E_{n-3} fort auf SL. ▫

Lemma 3 *Die Scherungen in* GL *erzeugen* SL*.*

Beweis. Dies folgt mit $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = E_{1,2}(-1)E_{2,1}(1)E_{1,2}(-1)$, mit $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{smallmatrix}\right) = E_{1,2}(\lambda)E_{2,1}(-\lambda^{-1})E_{1,2}(\lambda) \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ für $\lambda \in k^*$ und mit dem Gaußschen Algorithmus, da $E_{i,j}(\lambda)$ stets eine Scherung ist. ▫

Lemma 4 *Es ist $[\mathrm{GL}, \mathrm{GL}] =: \mathrm{GL}' = \mathrm{SL}$, außer möglicherweise, wenn $n = 2$ und $k = \mathbf{F}_2$.*

Beweis. Wir behaupten, daß jede Scherung T in GL' liegt, woraus mit Lemma 3 dann $\mathrm{SL} \leq \mathrm{GL}'$ folgt. Wegen $\mathrm{GL}' \trianglelefteq \mathrm{GL}$ dürfen wir $T = E_{2,1}(1)$ annehmen.

Ist $\mathrm{char}\, k \neq 2$, so ist $T^2 = E_{2,1}(2)$ ebenfalls eine Scherung. Die Restklassen von T^2 und von T in der abelschen Gruppe $\mathrm{GL} / \mathrm{GL}'$ sind also gleich. Kürzen zeigt, daß die Restklasse von T verschwindet, i.e. daß $T \in \mathrm{GL}'$.

Ist $n \geq 3$, so sind auch $T' = E_{3,1}(1)$ und TT' Scherungen. Es liegen T' und TT' in derselben Restklasse modulo GL', so daß Kürzen zeigt, daß $T \in \mathrm{GL}'$. Dies zeigt die Behauptung.

Da wegen des Morphismus $\mathrm{GL} \xrightarrow{\det} k^*$ sicher $\mathrm{GL}' \leq \mathrm{SL}$ liegt, folgt das Lemma. ▫

Lemma 5 *Sei $G \leq \mathrm{GL}$ invariant unter* SL*-Konjugation und enthalte es eine Scherung. Es ist $\mathrm{SL} \leq G$, außer möglicherweise wenn $n = 2$, $\mathrm{char}\, k = 2$ und $k^2 \subsetneq k$.*

Beweis. Ist $n \geq 3$, so liegt nach Lemma 2 mit einer Scherung zugleich jede Scherung in G, und wir sind fertig mit Lemma 3.

Sei $n = 2$. Wir dürfen mit Lemma 1 annehmen, daß $E_{2,1}(\lambda) \in G$ für ein $\lambda \in k^*$. Seien $\alpha, \beta, \gamma \in k$ mit $\alpha\gamma = 1$. Dann ist auch $\left(\begin{smallmatrix} \gamma & 0 \\ \beta & \alpha \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} \gamma & 0 \\ \beta & \alpha \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ \lambda\alpha^2 & 1 \end{smallmatrix}\right) \in G$. Wir sind also fertig mit Lemma 1 und Lemma 3, falls sich jedes Element $x \in k$ als $\mathbf{Z}$-Linearkombination von Quadraten in k schreiben läßt.

Ist $\mathrm{char}\, k \neq 2$, so folgt dies mit $x = (\frac{x+1}{2})^2 - (\frac{x-1}{2})^2$.

Ist $\mathrm{char}\, k = 2$ und $k^2 = k$, so ist dies klar. ▫

Lemma 6 *Sei $n = 2$, und sei $G \leq \mathrm{GL}$ invariant unter* SL*-Konjugation. Falls G ein Element der Form $\left(\begin{smallmatrix} \gamma & 0 \\ \beta & \alpha \end{smallmatrix}\right)$ mit $\alpha, \beta, \gamma \in k$ und $\alpha \neq \gamma$ enthält, so ist $\mathrm{SL} \leq G$.*

Beweis. Für jedes $\lambda \in k^*$ ist

$$\begin{pmatrix} \gamma & 0 \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} \gamma & 0 \\ \beta & \alpha \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (\alpha\gamma^{-1}-1)\lambda & 1 \end{pmatrix} \in G\,.$$

Mit Lemma 1 liegen alle Scherungen in G, und wir sind fertig mit Lemma 3. ▫

Lemma 7 *Sei $l \in [0, n]$, und seien $\left(\begin{smallmatrix} A & B \\ 0 & E_l \end{smallmatrix}\right), \left(\begin{smallmatrix} C & 0 \\ 0 & E_l \end{smallmatrix}\right) \in \mathrm{GL}$. Dann ist*

$$\begin{pmatrix} A & B \\ 0 & E_l \end{pmatrix} \begin{pmatrix} C & 0 \\ 0 & E_l \end{pmatrix} \begin{pmatrix} A & B \\ 0 & E_l \end{pmatrix}^{-1} \begin{pmatrix} C & 0 \\ 0 & E_l \end{pmatrix}^{-1} = \begin{pmatrix} ACA^{-1}C^{-1} & (E_{n-l}-ACA^{-1})B \\ 0 & E_l \end{pmatrix}\,.$$

Satz 8 *Sei $G \leq \mathrm{GL}$ invariant unter SL-Konjugation, und sei $G \not\leq \mathrm{Z}(\mathrm{GL})$. Es ist $\mathrm{SL} \leq G$, außer möglicherweise wenn $n = 2$ und $k \in \{\mathbf{F}_2, \mathbf{F}_3\}$.*

Beweis. Sei $S \in G \setminus \mathrm{Z}(G)$. Wir bemerken zunächst, daß es ein $x \in k^n$ mit $Sx \notin \langle x \rangle$ gibt. Denn andernfalls gäbe es für alle $x \in k^n$ ein $\lambda_x \in k$ mit $Sx = \lambda_x x$, und es wäre für $x, y \in k^n$ mit (x, y) linear unabhängig wegen $S(x+y) \overset{1.}{=} \lambda_{x+y}(x+y) \overset{2.}{=} \lambda_x x + \lambda_y y$ auch $\lambda_x = \lambda_y$, was, angewandt auf die Standardbasis, $S \in \mathrm{Z}(\mathrm{GL})$ nach sich zöge.

Fall $n = 2$. Sei $x \in k^n$ mit (Sx, x) linear unabhängig gewählt. Sei $U \in \mathrm{GL}$ die Matrix mit Spaltentupel (Sx, x). Wegen $\mathrm{SL} \trianglelefteq \mathrm{GL}$ genügt es zu zeigen, daß $\mathrm{SL} \leq U^{-1}GU$. Da außerdem wegen $\mathrm{SL} \trianglelefteq \mathrm{GL}$ mit G auch $U^{-1}GU$ invariant unter SL-Konjugation ist, dürfen wir G durch $U^{-1}GU$ und S durch $U^{-1}SU$ ersetzen und erhalten $S = \left(\begin{smallmatrix} \gamma & 1 \\ \beta & 0 \end{smallmatrix}\right) \in G$, für gewisse $\gamma,\ \beta \in k$, wobei $\beta \neq 0$.

Für $\xi \in k^*$ erhalten wir

$$R_\xi := \left(\begin{smallmatrix} 0 & -\xi \\ \xi^{-1} & \gamma\xi \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} \gamma & 1 \\ \beta & 0 \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} 0 & -\xi \\ \xi^{-1} & \gamma\xi \end{smallmatrix}\right) \left(\begin{smallmatrix} \gamma & 1 \\ \beta & 0 \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} -\beta\xi^2 & 0 \\ -\gamma(\xi^{-2}\beta^{-1}+1) & -\beta^{-1}\xi^{-2} \end{smallmatrix}\right) \;\in\; G\ .$$

Um Lemma 6 anwenden zu können, sollte $\xi^4 \neq \beta^{-2}$ sein. Falls $|k^*| > 4$, ist dies sicher erreichbar. Falls $|k^*| = 3$, so ist wegen $k^* \simeq C_3$ bereits $\xi^4 = \xi$, und damit $\xi \in k^* \setminus \{\beta^{-2}\}$ wählbar.

Bleibt der Fall $|k^*| = 4$, i.e. $k = \mathbf{F}_5$ zu betrachten. Ist $\beta \notin \{-1, +1\}$, so ist $\beta^{-2} \neq 1$, und $\xi^4 = \beta^{-2}$ sogar unlösbar mit $\xi \in k^*$, da $k^* \simeq C_4$. Bleibt der Fall $\beta \in \{-1, +1\}$ zu betrachten. Wähle $\xi \in k^*$ so, daß $\xi^2 = \beta = \beta^{-1}$, z.B. $1^2 = 1$, $2^2 = -1$.

Ist $\gamma \neq 0$, so wird $R_\xi^2 = \left(\begin{smallmatrix} 1 & 0 \\ 4\gamma^2 & 1 \end{smallmatrix}\right)$, und wir sind fertig mit Lemma 5.

Ist $\gamma = 0$, so ist mit $V := \left(\begin{smallmatrix} 1 & 1 \\ -\xi & \xi \end{smallmatrix}\right)$

$$V^{-1} \left(\begin{smallmatrix} 0 & 1 \\ \beta & 0 \end{smallmatrix}\right) V \;=\; \left(\begin{smallmatrix} -\xi & 0 \\ 0 & \xi \end{smallmatrix}\right) \;\in\; V^{-1}GV\ .$$

Mit Lemma 6 und der Tatsache, daß auch $V^{-1}GV$ invariant unter SL-Konjugation ist, folgt $\mathrm{SL} \leq V^{-1}GV$, und mit $\mathrm{SL} \trianglelefteq \mathrm{GL}$ vollends $\mathrm{SL} \leq G$.

Fall $n \geq 3$. Sei $x \in k^n$ mit (Sx, x) linear unabhängig gewählt, sei dieses Tupel zu einer Basis $(Sx, x, x_3, \ldots, x_n)$ ergänzt, und sei U die Matrix mit diesem Spaltentupel. Wegen $\mathrm{SL} \trianglelefteq \mathrm{GL}$ genügt es zu zeigen, daß $\mathrm{SL} \leq U^{-1}GU$. Somit dürfen wir G durch $U^{-1}GU$ ersetzen, S durch $U^{-1}SU$ und erhalten $S = (*, e_1, *, \ldots, *) \in G$. In anderen Worten, wir können $S = \left(\begin{smallmatrix} 1 & * \\ 0 & \tilde{S} \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & E_{n-2} \end{smallmatrix}\right)$ schreiben mit $\tilde{S} \in \mathrm{GL}_{n-1}(k)$. Wir erhalten

$$SE_{2,1}(1)S^{-1} \;=\; \left(\begin{smallmatrix} 1 & * \\ 0 & \tilde{S} \end{smallmatrix}\right) E_{1,2}(1) \left(\begin{smallmatrix} 1 & * \\ 0 & \tilde{S}^{-1} \end{smallmatrix}\right) \;=\; \left(\begin{smallmatrix} 1 & * \\ 0 & E_{n-1} \end{smallmatrix}\right)\ ,$$

und damit

$$M \;:=\; SE_{2,1}(1)S^{-1}E_{2,1}(-1) \;=\; \left(\begin{smallmatrix} \alpha & \beta & \gamma & * \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & E_{n-3} \end{smallmatrix}\right) \;\in\; G$$

für gewisse $\alpha,\ \beta,\ \gamma \in k$. Mit Lemma 7 wird also

$$ME_{1,3}(1)M^{-1}E_{1,3}(-1) \;=\; \left(\begin{smallmatrix} 1 & 0 & \alpha-1 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & E_{n-3} \end{smallmatrix}\right) \;\in\; G\ ,$$

da

$$\left(\begin{smallmatrix} \alpha & \beta & \gamma \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} \alpha & \beta & \gamma \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)^{-1} \;=\; \left(\begin{smallmatrix} 1 & 0 & \alpha \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{smallmatrix}\right)\ .$$

Somit enthält G eine Scherung, so daß Lemma 5 liefert, daß $\mathrm{SL} \leq G$. $\square$

Korollar 9 *Es ist* PSL *eine einfache Gruppe, außer wenn* $n = 2$ *und* $k \in \{\mathbf{F}_2, \mathbf{F}_3\}$.

Beweis. Ist $1 \lhd N \unlhd \mathrm{PSL}$, so ist das Urbild $\tilde{N}$ von N unter der Restklassenabbildung $\mathrm{SL} \longrightarrow \mathrm{PSL}$ eine Untergruppe von $\mathrm{SL} \leq \mathrm{GL}$, welche unter SL-Konjugation invariant ist, und welche $\mathrm{Z(SL)} = \mathrm{Z(GL)} \cap \mathrm{SL}$ echt enthält, welche also insbesondere nicht in Z(GL) enthalten ist. Mit Satz 8 ist außer in den Ausnahmefällen also $\mathrm{SL} \leq \tilde{N} \leq \mathrm{SL}$, und somit $\tilde{N} = \mathrm{SL}$.

Ferner sind, wie oben festgestellt, $\mathrm{PSL}_2(\mathbf{F}_2)$ und $\mathrm{PSL}_2(\mathbf{F}_3)$ in der Tat nicht einfach. $\square$