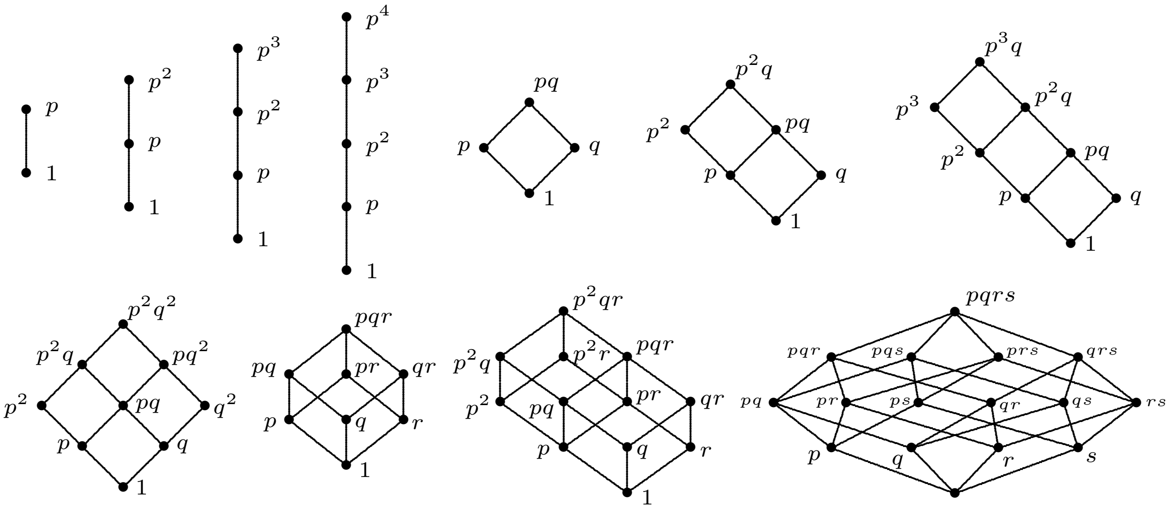
Nachtrag: Die Untergruppen der zyklischen Gruppen C_n. Sei $G = C_n$, sei g ein erzeugendes Element, es gilt also: die Elemente $1, g, g^2, \ldots, g^{n-1}$ sind paarweise verschieden und $g^n = 1$. *Zu jedem Teiler m von n gibt es genau eine Untergruppe von C_n der Ordnung m, diese Untergruppe ist wieder zyklisch, und man erhält auf diese Weise alle Untergruppen.* Mit Hilfe von g erhält man die Untergruppen auf folgende Weise: *Ist m ein Teiler von n, etwa $mm' = n$, so wird die Untergruppe der Ordnung m von $g^{m'}$ erzeugt.* Und insbesondere gilt: *Ist p eine Primzahl, so hat C_p nur die Untergruppen $C_1 = \{1\}$ und C_p.*

Zum Beweis dieser Aussagen zeigt man: (1) Ist $n = mm'$, so hat $h = g^{m'}$ die Ordnung m. (Offensichtlich ist $h^m = 1$. Wäre $h^d = 1$ für ein d mit $1 \leq d < m$, so wäre $g^{m'd} = h^m = 1$, Widerspruch.) Damit sieht man, daß es zu jedem Teiler von n eine Untergruppe dieser Ordnung gibt. (2) Dies sind die einzigen zyklischen Untergruppen von C_n; denn ist $1 \leq a < n$, und ist a' der ggT von a und n, so ist $\langle g^a \rangle = \langle g^{a'} \rangle$. (Da a' ein Teiler von a ist, ist $\langle g^a \rangle \subseteq \langle g^{a'} \rangle$. Für die umgekehrte Inklusion ist zu zeigen, daß $g^{a'}$ eine Potenz von g^a ist. Es gilt aber: der ggT a' läßt sich nach Bézout als ganzzahlige Linearkombination von a und n schreiben, etwa $a' = ua + vn$ mit $u, v \in \mathbb{Z}$. Es ist $g^{a'} = g^{ua+vn} = g^{ua} g^{vn} = (g^a)^u$.) (3) Jede von zwei Elemente erzeugte Untergruppe ist zyklisch: denn wird die Untergruppe U von g^a und g^b erzeugt, und ist c der ggT von a und b, so wird U von g^c erzeugt (wieder verwende Bézout). Mit Induktion folgt nun: Jede Untergruppe ist zyklisch.

Der Untergruppen-Verband von C_n entspricht gerade dem Verband der Teiler von n. Hier die möglichen Verbände, wenn n das Produkt von höchstens vier Primzahlen ist (dabei seien p, q, r, s paarweise verschiedene Primzahlen):



2. Normalteiler und Homomorphismen.

Linksnebenklassen. Ist U eine Untergruppe der Gruppe G und $g \in G$, so nennt man gU die *Linksnebenklasse* von U, die g enthält. *Zwei Linksnebenklassen gU und hU mit nicht-leerem Schnitt sind gleich.* Ist nämlich $gu_1 = hu_2$ mit Elementen $u_1, u_2 \in U$, so ist $h^{-1}g = u_2 u_1^{-1} \in U$. Setzen wir $u = u_2 u_1^{-1}$, so gilt $g = hu$, also $gU = huU = hU$ (wir sehen also: *Genau dann gilt $gU = hU$, wenn $h^{-1}g$ zu U gehört*).

Ist G eine endliche Gruppe, U eine Untergruppe, so bezeichnet man mit $[G : U]$ die Anzahl der Linksnebenklassen von U in G und nennt dies den *Index* von U in G. Ist gU eine Linksnebenklasse, so liefert die Abbildung $u \mapsto gu$ für $u \in U$ eine Bijektion zwischen der Menge U und der Menge gU; alle Linksnebenklassen haben also die gleiche Anzahl von Elementen. Es gilt demnach

$$|G| = |U| \cdot [G : U],$$

insbesondere sehen wir: *Die Ordnung einer Untergruppe U ist ein Teiler der Gruppenordnung* (**Satz von Lagrange**), und auch: *Der Index einer Untergruppe ist ein Teiler der Gruppenordnung.*

Die Ordnung einer Untergruppe U der Gruppe G ist ein Teiler von $|G|$. Im Fall einer endlichen zyklischen Gruppe gilt, wie wir wissen, eine schärfere Aussage: die Zuordnung $U \mapsto |U|$ liefert eine Bijektion zwischen der Menge der Untergruppen von C_n und der Menge der Teiler von n. Im allgemeinen ist die Zuordnung $U \mapsto |U|$ weder injektiv noch surjektiv. Typisches Beispiel ist die Gruppe $G = A_4$ der Ordnung 12. Sie hat **keine** Untergruppe der Ordnung 6, aber vier Untergruppen der Ordnung 3 und drei Untergruppen der Ordnung 2.

Entsprechend heißt Ug die *Rechtsnebenklasse* von U, die g enthält; genau dann gilt $Ug = Uh$ für zwei Elemente $g, h \in G$, wenn gh^{-1} zu U gehört. Unter $gU \mapsto Ug^{-1}$ entsprechen sich die Linksnebenklassen und die Rechtsnebenklassen bijektiv; deshalb ist $[G : U]$ auch die Anzahl der Rechtsnebenklassen von U in G.

Sei G eine Gruppe und U eine Untergruppe. *Die folgenden Eigenschaften sind äquivalent:*

(a) *U ist ein Normalteiler (also $gUg^{-1} = U$ für alle g).*
(b) *$gU = Ug$ für alle g.*
(c) *Linksnebenklassen sind Rechtsnebenklassen.*
(d) *Die Menge der Linksnebenklassen bildet eine Gruppe bezüglich der Multiplikation $gU \cdot hU = ghU$.*

Da die Linksnebenklassen und die Rechtsnebenklassen eines Normalteilers übereinstimmen, nennt man sie einfach die *Nebenklassen.* Man nennt die in (d) gegebene Gruppe der Nebenklassen von G die *Faktorgruppe* von G modulo U und notiert sie in der Form G/U. Die Faktorgruppe modulo einer Untergruppe U ist also genau dann definiert, wenn U ein Normalteiler ist, und dann ist $|G/U| = [G : U]$. Ist U Normalteiler von G, so schreibt man oft einfach $U \trianglelefteq G$.

Untergruppen einer Gruppe hat man früher auch “Teiler” der Gruppe genannt, spezielle solche Untergruppen waren dann die “normalen” Teiler, oder kurz die “Normalteiler”. Es sei daran erinnert, daß zumindest für eine endliche zyklische Gruppe G die Untergruppen von G gerade den Teilern von $|G|$ entsprechen.

Beweis der Äquivalenz von (a), (b), (c) und (d): Offensichtlich folgt (c) aus (b), und natürlich sind die Bedingungen (a) und (b) äquivalent.

(c) $\implies$ (b): Sei $gU = Uh$. Es ist $g = uh$ für ein $u \in U$, also ist $Ug = Uuh = Uh = Ug$.

(b) $\implies$ (d): Seien $g, g_1, g_2 \in G$. Es ist $g_1U \cdot g_2U = g_1 \cdot g_2 \cdot U \cdot U = (g_1g_2)U$ (dabei haben wir $Ug_2 = g_2U$ verwendet). Die elementweise Multiplikation zweier

Linksnebenklassen liefert also eine Linksnebenklasse. Die Menge U, aufgefaßt als Linksnebenklasse $U = 1{\cdot}U$, hat die Eigenschaften eines Einselements, denn $(gU){\cdot}U = gU = U \cdot (gU)$. Wegen $gU \cdot g^{-1}U = U$ können wir $(gU)^{-1} = g^{-1}U$ setzen.

(d) $\implies$ (b): Es ist $U \cdot U = U$, also ist die Nebenklasse U das Einselement. Betrachte: $Ug \subseteq U \cdot gU = gU$. Entsprechend sehen wir $Ug^{-1} \subseteq g^{-1}U$. Die letzte Inklusion liefert aber bei Multiplikation mit g von links und von rechts $gU \subseteq Ug$. Insgesamt sehen wir $Ug = gU$.

Offensichtlich gilt: *Eine Untergruppe U einer Gruppe G vom Index* 2 *ist ein Normalteiler* (denn es gibt als Linksnebenklassen die beiden Mengen U und $G\backslash U$, und dies sind auch die beiden Rechtsnebenklassen) und es ist $G/U \simeq C_2$. Insbesondere ist die alternierende Gruppe A_n für $n \geq 2$ eine Untergruppe der S_n vom Index 2, also ein Normalteiler.

Ist N ein Normalteiler der Gruppe G, so ist die Zuordnung $G \to G/N$, mit $g \mapsto gN$ ein Gruppen-Homomorphismus mit Kern N, man nennt ihn den *kanonischen* Homomorphismus $G \to G/N$. Umgekehrt gilt:

Erster Isomorphie-Satz. *Sei ϕ: $G \to H$ ein Gruppen-Homomorphismus. Der Kern* $\operatorname{Ker}\phi$ *von ϕ ist ein Normalteiler, und es gilt*

$$G/\operatorname{Ker}\phi \simeq \operatorname{Im}\phi.$$

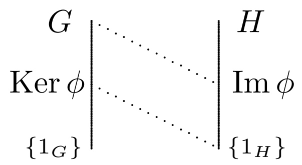
Beweis: Sei $g \in N = \operatorname{Ker}\phi$, sei $h \in G$. Es ist

$$\phi(hgh^{-1}) = \phi(h)\phi(g)\phi(h)^{-1} = \phi(h)\phi(h)^{-1} = 1,$$

dies zeigt, daß N ein Normalteiler ist. Sind $g, h \in G$ und gilt $gN = hN$, so ist $h^{-1}g \in N$, also ist $\phi(h^{-1}g) = 1$, und demnach $\phi(g) = \phi(h)$. Und umgekehrt gilt: Ist $\phi(g) = \phi(h)$, so ist $h^{-1}g \in N$, also $gN = hN$. Wir sehen also: unter der Abbildung ϕ sind die Urbilder der einzelnen Bildpunkte gerade die Nebenklassen von N.

Wir definieren eine Abbildung $\overline{\phi}$: $G/N \to H$ durch $\overline{\phi}(gN) = \phi(g)$. Wie wir gesehen haben, ist diese Abbildung wohldefiniert und injektiv. Es ist einfach zu verifizieren, daß dies ein Gruppen-Homomorphismus ist. Also liefert $\overline{\phi}$ einen Isomorphismus von G/N auf $\operatorname{Im}\phi$.

Zur Veranschaulichung diene folgende Skizze:



Wir haben oben gesehen: Ist N ein Normalteiler, so ist N der Kern vom kanonischen Homomorphismus $G \to G/N$. Umgekehrt ist der Kern jedes Gruppen-Homomorphismus ein Normalteiler: *Die Normalteiler sind also gerade die Kerne von Homomorphismen.*

Typische Beispiele:

(a) Betrachte den Homomorphismus

$$\text{sign}\colon\ S_n \to C_2,$$

der jeder Permutation ihr Signum zuordnet; er ist surjektiv und sein Kern ist die A_n, also ist $S_n/A_n \simeq C_2$.

(b) Entsprechend ist für jeden Körper k der Gruppen-Homomorphismus

$$\det\colon\ \mathrm{GL}_n(k) \to k^*$$

surjektiv und der Kern ist $\mathrm{SL}_n(k)$. Also ist $\mathrm{GL}_n(k)/SL_n(k) \simeq k^*$.

(c) Sei G eine Gruppe, sei $g \in G$. Wir erhalten einen Gruppen-Homomorphismus ϕ: $(\mathbb{Z}, +) \to G$ durch $\phi(z) = g^z$ für $z \in \mathbb{Z}$. Das Bild dieser Abbildung, also die Menge der Elemente g^z mit $z \in \mathbb{Z}$, ist die von g erzeugte Untergruppe $\langle g \rangle$. Es gibt zwei Möglichkeiten:

Fall 1: Diese Abbildung ϕ ist injektiv. Dann hat g unendliche Ordnung, und die von g erzeugte Untergruppe ist zu $(\mathbb{Z}, +)$ isomorph.

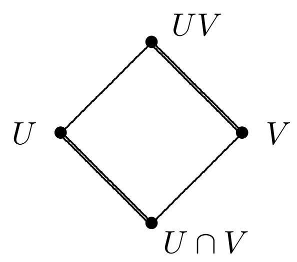
Fall 2: Die Abbildung ϕ ist nicht injektiv. Dann gibt es $n \geq 1$ mit $g^n = 1$. Wählt man n minimal, so hat g gerade die Ordnung n und die von g erzeugte Untergruppe ist zu C_n isomorph.

Zusatz: Hat g endliche Ordnung, so läßt sich g^{-1} als Potenz von g mit Exponenten in $\mathbb{N}_1$ schreiben. (Denn ist $g^n = 1$, so ist $g^{-1} = g^{n-1}$).

Zweiter Isomorphiesatz. *Seien U, V Untergruppen von G, sei $uV = Vu$ für alle $u \in U$. Dann ist $UV = \{uv \mid u \in U, v \in V\}$ eine Untergruppe von G; es ist V ein Normalteiler von UV und*

$$UV/V \simeq U/(U \cap V).$$

Ist V eine Untergruppe und X eine Teilmenge einer Gruppe G, und gilt $xV = Vx$ für alle $x \in X$, so sagt man: X *normalisiert* V. Im zweiten Isomorphiesatz wird also vorausgesetzt, daß V von U normalisiert wird.



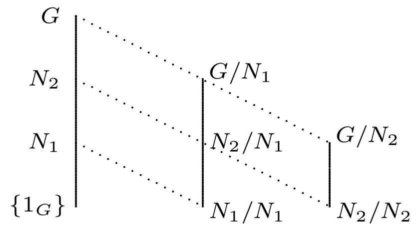
Beweis des zweiten Isomorphiesatzes: Es ist einfach zu sehen, daß die Menge UV unter Multiplikation und unter Inversenbildung abgeschlossen, also eine Untergruppe ist und offensichtlich ist V ein Normalteiler von UV. Definiere ϕ: $U \to UV/V$ durch $\phi(u) = uV$. Man verifiziert unmittelbar, daß ϕ ein Gruppen-Homomorphismus und surjektiv ist. Der Kern besteht aus denjenigen $u \in U$, für die $uV = V$ gilt, dies sind aber gerade die Elemente $u \in U$, die auch zu V gehören. Also ist der Kern von ϕ

gerade $U \cap V$. Nach dem ersten Isomorphie-Satz ist $U \cap V$ ein Normalteiler von U und ϕ induziert einen Isomorphismus $U/(U \cap V) \to UV/V$.

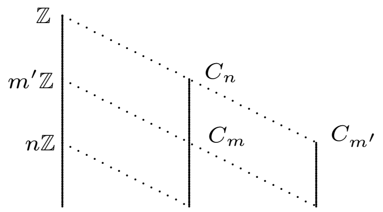
Dritter Isomorphiesatz. *Seien N_1, N_2 Normalteiler der Gruppe G mit $N_1 \subseteq N_2$. Dann ist N_2/N_1 ein Normalteiler in G/N_1 und es gilt*

$$G/N_2 \simeq (G/N_1)/(N_2/N_1).$$

Beweis: Definiere eine Abbildung ϕ: $G/N_1 \to G/N_2$ durch $\phi(gN_1) = gN_2$. Man zeigt: Diese Zuordnung ist wohldefiniert und liefert einen (surjektiven) Gruppen-Homomorphismus. Offensichtlich ist der Kern gerade N_2/N_1. Der erste Isomorphiesatz liefert die Behauptung.

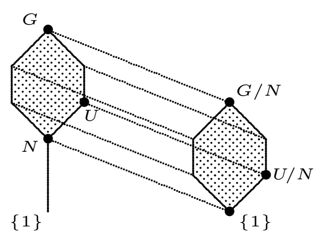


Noch einmal ein Beispiel zu den zyklischen Gruppen: Seien $m, m' \in \mathbb{N}_1$, sei $n = mm'$. Sei C_n die zyklische Gruppe der Ordnung n, sei g ein erzeugendes Element. Sei $h = g^{m'}$. Wir wissen: die von h erzeugte Untergruppe U ist isomorph zu C_m. In $\mathbb{Z}$ haben wir die Untergruppen (natürlich Normalteiler!) $n\mathbb{Z} \subseteq m'\mathbb{Z} \subseteq \mathbb{Z}$.



Es folgt: $C_n/C_m \simeq C_{m'}$.

Bijektionssatz. *Sei N ein Normalteiler der Gruppe G, sei π: $G \to G/N$ die kanonische Projektion. Ist U eine Untergruppe von G, so ist $\pi(U)$ eine Untergruppe von G/N. Diese Zuordnung $U \mapsto \pi(U)$ liefert eine Bijektion zwischen den Untergruppen von G, die N enthalten, und den Untergruppen von G/N. Unter dieser Bijektion entsprechen sich die Normalteiler von G, die N enthalten, und die Normalteiler von G/N.*



Beweis: Verifikation.

(Allgemeiner gilt: Ist ϕ: $G \to H$ ein Gruppen-Homomorphismus, so gibt es die folgende Zuordnungen: Sei U eine Untergruppe von G, sei V eine Untergruppe von H. Dann gilt:

$$\phi^{-1}\phi(U) = UN \qquad \text{und} \qquad \phi\phi^{-1}(V) = V \cap B.$$

Diese Zuordnung liefert eine Bijektion zwischen den Untergruppen von G, die den Kern von ϕ enthalten, und den Untergruppen des Bildes von ϕ.)

Eine Kette

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

wobei G_{i-1} Normalteiler von G_i ist, nennt man eine *Normalreihe* der Gruppe G, die Zahl n ist die *Länge* dieser Normalreihe, die Gruppen G_i/G_{i-1} nennt man die *Faktoren* dieser Reihe. Sind die Faktoren G_i/G_{i-1} einer Normalreihe einfache Gruppen, so nennt man diese Normalreihe eine *Kompositionsreihe,* und die Faktoren *Kompositionsfaktoren.*

Satz von Jordan-Hölder. *Besitzt eine Gruppe eine Kompositionsreihe, so läßt sich jede Normalreihe zu einer Kompositonsreihe verfeinern. Sind zwei Kompositionsreihen einer Gruppe G gegeben:*

$$\begin{aligned}\{1\} &= G_0 \subset G_1 \subset \cdots \subset G_n = G,\\ \{1\} &= G'_0 \subset G'_1 \subset \cdots \subset G'_m = G,\end{aligned}$$

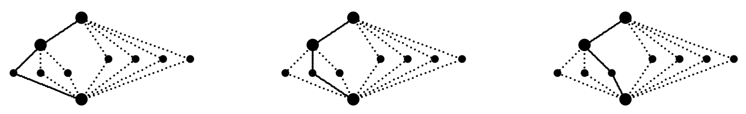
so ist $n = m$ und es gibt eine Permutation π von $\{1, \dots, n\}$ mit

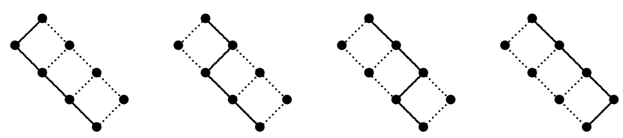
$$G_i/G_{i-1} \simeq G'_{\pi(i)}/G'_{\pi(i)-1}.$$

(Man sagt: Je zwei Kompositionsreihen sind äquivalent; die Kompositionsfaktoren sind bis auf Reihenfolge und Isomorphie eindeutig bestimmt.)

Beweis: siehe zum Beispiel Meyberg, p.89-91.

Hier die drei Kompositionsreihen der A_4 und die vier Kompositionsreihen einer zyklischen Gruppe der Form C_{p^3q} mit paarweise verschiedenen Primzahlen p, q:





Das Beispiel der A_4 zeigt auch, daß eine Gruppe nicht-verfeinerbare Ketten von **Untergruppen** besitzen kann, die verschiedene Längen haben.

Zusatz: Einfachheit der Gruppen $\mathrm{PSL}_n(k)$**.**

Erinnerung: Sei k ein Körper. Die Untergruppe $\mathrm{SL}_n(k)$ von $\mathrm{GL}_n(k)$ ist die Menge aller $(n \times n)$-Matrizen mit Koeffizienten in k und Determinante 1.

Satz. *Sei k ein Körper. Ist N ein Normalteiler von $G = \mathrm{SL}_n(k)$, so gilt:*
(a) *Enthält N nicht nur Skalarmatrizen, so ist G/N abelsch.*
(b) *G besitzt nicht-triviale abelsche Faktorgruppen nur für $n = 2$ und $|k| \le 3$.*

Folgerung. *Ist $n > 2$ oder $|k| > 3$, und bezeichnen wir mit Z die Untergruppe der Skalarmatrizen in $\mathrm{SL}_n(k)$, so ist die Gruppe $\mathrm{PSL}_n(k) = \mathrm{SL}_n(k)/Z$ einfach.*

Zusatz: Die Untergruppe Z (das "Zentrum" von G) besteht offensichtlich aus den Skalarmatrizen λI_n mit $\lambda^n = 1$ (mit I_n bezeichnen wir hier die $(n \times n)$-Einheitsmatrix. Es gibt höchstens n Elemente λ mit $\lambda^n = 1$ (nämlich die möglichen Nullstellen des Polynoms $T^n - 1$ in k, man nennt diese Nullstellen die n-ten Einheitswurzeln in k).

Es gibt zwei Ausnahme-Fälle, über die (c) keine Aussage macht: nämlich $n = 2$ und $|k| = 2$ oder $|k| = 3$. Man kann ziemlich einfach zeigen: Ist $|k| = 2$, so ist $\mathrm{PSL}_2(k)$ isomorph zur symmetrischen Gruppe S_3. Ist $|k| = 4$, so ist $\mathrm{PSL}_2(k)$ isomorph zur alternierenden Gruppe A_4.

Beweis des Satzes. Die Matrizen der Form $Q_{ij}(\mu) = I_n + \mu E_{ij}$ mit $\mu \in k$ und $i \ne j$ bezeichnen wir hier als "Elementarmatrizen" (dabei ist E_{ij} die Matrix mit Koeffizient 1 an der Stelle (i, j) und Nullen sonst). Die üblichen Methoden der Linearen Algebra zeigen:

(1) *Die Gruppe $\mathrm{SL}_n(k)$ wird von den Elementarmatrizen erzeugt.*

Beim Beweis verwendet man, daß man Matrizen der Form $\left[\begin{smallmatrix} c & 0 \\ 0 & c^{-1} \end{smallmatrix}\right]$ als Produkt von Elementarmatrizen schreiben kann: Es ist

$$Q_{12}(c)Q_{21}(-c^{-1})Q_{12}(c) = \begin{bmatrix} 0 & c \\ -c^{-1} & 0 \end{bmatrix},$$

die entsprechende Matrix für $c = -1$ bezeichnen wir mit P_{12} (allgemeiner sei $P_{ij} = Q_{ij}(-1)Q_{ji}(1)Q_{ij}(-1)$, bis auf ein Vorzeichen ist dies eine Permutationsmatrix); die folgende Multiplikation liefert die gewünschte Matrix:

$$\begin{bmatrix} 0 & c \\ -c^{-1} & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} c & 0 \\ 0 & c^{-1} \end{bmatrix}.$$

Ist nun eine beliebige Matrix in $\mathrm{SL}_n(k)$ gegeben, so bringt man sie zuerst durch Multiplikation mit Elementarmatrizen auf Diagonalform (dabei verwendet man statt der üblichen Permutationsmatrizen die Matrizen der Form P_{ij}).

(2) *Jede Elementarmatrix ist in $\mathrm{SL}_n(k)$ zu einer Elementarmatrix der Form $Q_{1j}(\mu)$ konjugiert.*

Beweis: Es ist

$$P_{ij}Q_{ij}(t)P_{ij}^{-1} = Q_{ji}(-t),$$

also ist jede Elementarmatrix zu einer mit $i < j$ konjugiert. Sei nun $i < j$. Dann bilden wir

$$P_{1i}Q_{ij}(t)P_{1i}^{-1} = Q_{1j}(-t).$$

Wir bezeichnen mit $e_1, \ldots, e_n$ die kanonische Basis von $V = k^n$. Sei U die Menge aller $u \in \mathrm{SL}_n(k)$, die e_1 als Eigenvektor besitzen; dies ist eine Untergruppe von $\mathrm{SL}_n(k)$, und zwar besteht sie gerade aus den Matrizen der Form

$$\left[\begin{array}{c:c} a & b \\ \hdashline 0 & C \end{array}\right]$$

in der $\mathrm{SL}_n(k)$ (dabei ist a ein Skalar, also C eine $((n-1) \times (n-1))$-Matrix). Sei A die Untergruppe von U aller derartigen Matrizen mit $a = 1$ und $C = I_{n-1}$. Ganz mühelos lassen sich die folgenden beiden Aussagen (3) und (4) verifizieren:

(3) *Es ist A eine abelsche Gruppe.*

(4) *Es ist A ein Normalteiler von U.*

Sei nun N ein Normalteiler von $G = \mathrm{SL}_n(k)$, der nicht nur Skalarmatrizen enthält. Sei $f \in N$ keine Skalarmatrix. Dann gibt es einen Vektor $0 \neq x \in V$, der kein Eigenvektor von f ist, also sind die beiden Vektoren $x, f(x)$ linear unabhängig.

(5) *Ist $0 \neq y \in V$, so gibt es $h \in N$ mit $h(e_1) \in k^*y$.* Dies ist klar, falls $y \in k^*e_1$, denn dann wählen wir $h = 1$. Seien also e_1, y linear unabhängig. Da die beiden Vektoren $x, f(x)$ und auch die beiden Vektoren e_1, y jeweils linear unabhängig sind, gibt es $g \in \mathrm{SL}_n(k)$ mit $g(x) = e_1, g(f(x)) = cy$ für ein $c \in k^*$. Setze $h = gfg^{-1}$. Da N ein Normalteiler von $\mathrm{SL}_n(k)$ ist, liegt mit f auch $h = gfg^{-1}$ in N. Und es ist $h(e_1) = gfg^{-1}(e_1) = gf(x) = cy$.

(6) *Es ist $G = NU$.* Sei $g \in G = \mathrm{SL}_n(k)$. Zu $y = g(e_1)$ gibt es nach (5) ein $h \in N$ mit $h(e_1) \in k^*y$, etwa $h(e_1) = cy$ mit $c \in k^*$. Also ist $h^{-1}g(e_1) = h^{-1}y = c^{-1}e_1$, demnach gehört $u = h^{-1}g$ zu U, also $g = hu$ zu NU.

(7) *NA ist ein Normalteiler von G.* Beweis: Zu zeigen ist $gNA = NAg$ für jedes $g \in G$. Wegen (6) reicht es, dies für $g \in N$ und für $g \in U$ zu zeigen. Ist $g \in N$, so ist $gN = N = Ng$, und es ist auch $AN = NA$, also $gNA = NA = AN = ANg = NAg$. Ist $g \in U$, so ist $gNA = NgA = NAg$, hier verwenden wir (4).

(8) *Also sehen wir: $G = NA$.* Dies folgt aus (7), (2) und (1).

Der zweite Isomorphiesatz zeigt: $G/N = NA/N \simeq A/(N \cap A)$, also G/N ist isomorph zu einer Faktorgruppe von A. Nach (3) ist A abelsch, also ist auch G/N abelsch. Damit ist (a) bewiesen.

Wir zeigen nun (b). Sei also $n > 2$ oder $|k| > 3$. *Unter dieser Voraussetzung ist jede Elementarmatrix ein Kommutator.* Für $n \geq 3$ betrachte man paarweise verschiedene Indizes i, j, k, und erhält

$$Q_{ij}(-c)Q_{jk}(-1)Q_{ij}(c)Q_{jk}(1) = Q_{ik}(c),$$

also ist $Q_{ik}(c)$ ein Kommutator. Für $n = 2$ betrachten wir die Diagonalmatrix $D(\mu) = \left[\begin{smallmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{smallmatrix}\right]$ und sehen:

$$D(\mu)Q_{12}(\lambda)D(\mu^{-1})Q_{12}(-\lambda) = Q_{12}((\mu^2 - 1)\lambda),$$

Ist nun $|k| > 3$, so können wir für μ ein beliebiges Element in $k \setminus \{0, 1, -1\}$ wählen: es ist dann $\mu \neq 0$, also ist $D(\mu)$ definiert und wegen $\mu \notin \{1, -1\}$ ist $\mu^2 \neq 1$. Um ein beliebiges Element $Q_{12}(c)$ als Kommutator zu schreiben, nehme man nun einfach $\lambda = (\mu^2 - 1)^{-1}c$.

Da G von Kommutatoren erzeugt wird, besitzt G keine nicht-triviale abelsche Faktorgruppe, also ist $G/N = 1$, und demnach $G = N$.