<u>Bsp</u> Sei $p \geq 3$ prim. Sei $n \geq 2$.

Es ist $GL_n(\mathbb{F}_p)$ <u>nicht einfach</u>,

da wir den Gruppenmorphismus

$$GL_n(\mathbb{F}_p) \xrightarrow{\det} U(\mathbb{F}_p) = \mathbb{F}_p^\times$$

haben, mit Kern $\underbrace{SL_n(\mathbb{F}_p)}_{:= \operatorname{Kern}(\det)} \trianglelefteq GL_n(\mathbb{F}_p)$.

Nach Homomorphiesatz ist

$$GL_n(\mathbb{F}_p)/SL_n(\mathbb{F}_p) \simeq \mathbb{F}_p^\times .$$

Insbesondere ist der Index

$$[GL_n(\mathbb{F}_p) : SL_n(\mathbb{F}_p)] = p-1 .$$

Also ist die Ordnung

$$|SL_n(\mathbb{F}_p)| = \frac{1}{p-1} |GL_n(\mathbb{F}_p)|$$

$$= \frac{1}{p-1} \cdot (p^n - p^0)(p^n - p^1) \cdots (p^n - p^{n-1})$$

Somit

$$1 \overset{n \geq 2}{<} |SL_n(\mathbb{F}_p)| \overset{p-1 \geq 2}{<} |GL_n(\mathbb{F}_p)|$$

Folglich:

$$1 < SL_n(\mathbb{F}_p) \triangleleft GL_n(\mathbb{F}_p)$$

<u>Bsp</u> Es hat A_5 keine Untergruppe von Ordnung 20.

<u>Annahme</u>, doch. Sei $\mathcal{U} \leq A_5$ mit $|\mathcal{U}| = 20$ gegeben. Dann operiert A_5 transitiv auf $\underbrace{A_5/\mathcal{U}}_{\text{dreielementige Menge}}$, und dies gibt einen Gruppenmorphismus

$$\varphi : A_5 \longrightarrow S_{A_5/\mathcal{U}} \simeq S_3$$

Es ist $\mathrm{Kern}(\varphi) \neq A_5$,

da φ nicht jedes Element

nach id schickt, da

A_5/U eine transitive

A_5 - Menge ist.

Nun ist aber A_5 eine

<u>einfache</u> Gruppe.

Da $\mathrm{Kern}(\varphi) \trianglelefteq A_5$, folgt

$$\mathrm{Kern}(\varphi) = 1.$$

Also ist φ injektiv.

Aber $|A_5| = 60$ und $|S_{A_5/U}|$

$= |S_3| = 6$. <u>Widerspruch</u>.

<u>Bsp</u> Es gibt keine einfache Gruppe von Ordnung 48.

<u>Annahme</u>, G ist eine einfache Gruppe mit $|G| = 48$.

Dann ist $|Syl_2(G)|$ ein Teiler von $\frac{48}{16} = 3$.

Da $|Syl_2(G)|$ nur dann gleich 1 ist, wenn G eine normale Untergruppe von Ordnung 16 enthält, was wegen G einfach aber nicht so ist, folgt $|Syl_2(G)| = 3$.

Es ist $\mathrm{Syl}_2(G)$ gemäß Satz 141.(2) eine transitive G-Menge. Also haben wir einen Gruppenmorphismus

$$\varphi : G \longrightarrow S_{\mathrm{Syl}_2(G)} \simeq S_3 .$$

Es ist $\mathrm{Kern}(\varphi) \trianglelefteq G$.

Es ist $\mathrm{Kern}(\varphi) \neq G$, da G transitiv und also nichttrivial auf $\mathrm{Syl}_2(G)$ operiert.

Wegen G einfach folgt $\mathrm{Kern}(\varphi) = 1$. Somit ist

φ injektiv. Aber

$|G| = 48$ und $|S_{Syl_2(G)}| = |S_3| = 6$,

Widerspruch.

Bsp für den Grad einer

Körpererweiterung:

Sei K ein Körper.

Wir wollen $[K(X) : K(X^2)] \overset{!}{=} 2$

nachweisen.

Dazu sollten wir eine

$K(X^2)$-lineare Basis von $K(X)$

angeben, die zwei Elemente ...

... enthält.

Wir behaupten, daß $(1, X)$ eine solche Basis ist.

- Lineare Unabhängigkeit:

Sei $\underbrace{\frac{f_0(X^2)}{g_0(X^2)}}_{\in K(X^2)} \cdot 1 + \underbrace{\frac{f_1(X^2)}{g_1(X^2)}}_{\in K(X^2)} \cdot X = 0.$

Zu zeigen ist: $\frac{f_0(X^2)}{g_0(X^2)} \stackrel{!}{=} 0$, $\frac{f_1(X^2)}{g_1(X^2)} \stackrel{!}{=} 0$.

Zu zeigen ist: $f_0(X^2) \stackrel{!}{=} 0$, $f_1(X^2) \stackrel{!}{=} 0$

Wir haben folgende Gleichung in $K[X]$:

$$f_0(X^2) \cdot g_1(X^2) \cdot 1 + f_1(X^2) \cdot g_0(X^2) \cdot X = 0$$

Da $f_0(X^2) \cdot g_1(X^2)$ eine

K-Linearkombination der Monome

$$X^0, X^2, X^4, \ldots$$

ist, und da $f_1(X^2) \cdot g_0(X^2) \cdot X$

eine K-Linearkombination

der Monome

$$X^1, X^3, X^5, \ldots$$

ist, folgt

$$f_0(X^2) \cdot g_1(X^2) = 0$$

und

$$f_1(X^2) \cdot g_0(X^2) \cdot X = 0 .$$

Da ferner $g_1(X^2) \neq 0$

und $g_0(X^2) \cdot X \neq 0$ sind,

folgt $f_0(X^2) = 0$ und $f_1(X^2) = 0$.

- Erzeugendensystem.

Sei $\dfrac{u(X)}{v(X)} \in K(X)$,

wobei $u(X) \in K[X]$, $v(X) \in K[X]^*$.

Gesucht sind $\dfrac{f_0(X^2)}{g_0(X^2)}$, $\dfrac{f_1(X^2)}{g_1(X^2)} \in K(X^2)$

mit $\dfrac{u(X)}{v(X)} \overset{!}{=} \dfrac{f_0(X^2)}{g_0(X^2)} \cdot 1 + \dfrac{f_1(X^2)}{g_1(X^2)} \cdot X$.

Wir merken an, daß

für $v(X) = \sum\limits_{i \geq 0} a_i X^i$

sich mit ...

$$\tilde{v}(X) := \sum_{i \geq 0} a_i (-1)^i X^i$$

ergibt:

$$v(X) \cdot \tilde{v}(X)$$

$$= \left(\sum_{i \geq 0} a_i X^i \right) \left(\sum_{j \geq 0} a_j (-1)^j X^j \right)$$

$$= \sum_{k \geq 0} \Big(\underbrace{\sum_{i \in [0,k]} a_i \cdot (-1)^{k-i} a_{k-i}}_{= 0 \text{ falls } k \equiv_2 1} \Big) X^k$$

$$= \sum_{\substack{k \geq 0 \\ k \equiv_2 0}} \left(\sum_{i \in [0,k]} a_i \cdot (-1)^{k-i} a_{k-i} \right) X^k$$

$$\in K[X^2]^\times.$$

Also ist

$$\frac{u(X)}{v(X)} = \frac{u(X)\,\tilde{v}(X)}{v(X)\,\tilde{v}(X)} .$$

Spalten wir noch auf:

$$u(X)\,\tilde{v}(X) =: f_0(X^2) + f_1(X^2)\cdot X ,$$

wobei $f_0(X), f_1(X) \in K[X]$.

Schreiben wir

$$v(X)\,\tilde{v}(X) =: g_0(X^2) =: g_1(X^2) ,$$

wobei $g_0(X) = g_1(X) \in K[X]$.

Damit wird:

$$\frac{u(X)}{v(X)} = \frac{u(X)\,\tilde{v}(X)}{v(X)\,\tilde{v}(X)} = \frac{f_0(X)}{g_0(X)}\cdot 1 + \frac{f_1(X^2)}{g_1(X^2)}\cdot X ,$$

wie gesucht.